December 2021

CAN Newsletter

Hardware + Software + Tools + Engineering

Automated sewer cleaning with CANopen

People counter enables social distancing

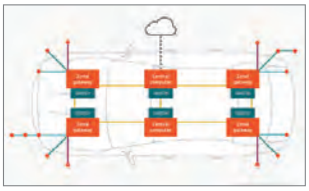
CAN data logger case studies

Applications

www.can-newsletter.org

Applications

CANopen



Lower layers

CAN in Automation (CiA) at SPS 2021

The SPS 2021 tradeshow takes place as in-person exhibition from November 23 to 25, 2021 in Nuremberg, Germany. With its concept, the SPS covers a spectrum of smart and digital automation – from sensors and actuators to automation system solutions. CAN in Automation (CiA) has a booth in hall 5, stand 410. The CiA team lead by Reiner Zitzmann assists you in case of any CAN-related questions or if you have some technical issues, development ideas, or marketing-oriented suggestions to be discussed. As usual, CiA shows some CANopen (FD) products from its members on its stand. Holger Zeltwanger, CiA Managing Director, will also be on the fairground to provide background information on the CAN standardization and upcoming CiA specifications.

sps
smart production solutions
(Source: Mesago Messe Frankfurt)

Imprint

Publisher
CAN in Automation GmbH
Kontumazgarten 3
DE-90429 Nuremberg

publications@can-cia.org
www.can-cia.org

Tel.: +49-911-928819-0
Fax: +49-911-928819-79

CEO
Reiner Zitzmann
AG Nürnberg 24338

Downloads September issue:
(retrieved November 07, 2021)
9149 full magazine

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

Layout
Nickel Plankermann

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

CANopen today, tomorrow, and beyond

The history of CANopen has not been written, yet. CANopen is still evolving. CAN in Automation (CiA) and its members are always maintaining and enhancing the set of CAN and CANopen specifications. Here's an update and a look into the future.

(Source: Adobe Stock)

About 25 years ago, CANopen had been developed for embedded machine control in modular machines. But CANopen is not limited to this application field. In the meantime, CANopen has propagated to many applications including medical devices, building automation, energy management, construction machines and off-highway vehicles as well as maritime electronics. CANopen is an attractive candidate for open and embedded networks, because it is scalable, flexible, robust, reliable, and available from different sources. Additionally, there exists the CAN in Automation independent users' and manufacturers' group, which provides support and advice, in case of any CAN-based challenges. To keep CANopen also in future an attractive networking technology, CiA members are ongoing to enhance CANopen, so that CANopen is able to meet the requirements of embedded networking today and tomorrow.

CiA is maintaining and extending the series of CANopen device and application profiles, to increase the plug-and-play capability of CANopen devices and to reduce the effort of system designers. In times of climate change and increasing costs for energy, applications are in the focus of CiA specification activities that need to do some energy management, in order to keep the energy consumption low. Applications such as service robots, AGVs (automated guided vehicles), and light electric vehicles buffer a limited amount of energy in a battery. By means of a sophisticated energy management, they attempt to provide the availability of the system, for a maximum duration. CiA assists system designers and maintainers of such applications by specifying harmonized application data. For example, the CANopen profiles for batteries and chargers (CiA 418 respectively CiA 419) are currently under systematic review. In many of the aforementioned applications, the end user respectively owner of the system has to modify the application (just by adding or changing some batteries, for example). But this end user has typically no or only limited knowledge about (CANopen) embedded networking.

Many tricky issues such as self-configuration, cybersecurity, reliability, or firmware updates have to be handled dynamically, by the embedded control systems themselves.

CiA assist also in this regard todays and tomorrows CANopen users. Dynamically changing systems are rather easy to handle, in case the network participants have the ability to check, who is available in a given system configuration. The CANopen heartbeat services as well as complex SDO connectivity allow this already in classic CANopen. A central host controller could monitor the system configuration, and could report on system changes, to all other devices. The new CANopen FD provides enough bandwidth as well as enhanced cross-communication capabilities, so that all the devices in the network could analyze by themselves, whether there has been a new device added to the system and whether they need to establish communication coherences to this new device. As a consequence, the central host controller would be unburdened from such tasks. In a dynamically modified system, the host controller would just use the updated, CAN FD based LSS FD (specified in CiA 1305), to assign the CANopen (FD) node-ID (and CANopen FD network-ID).

Recommendations and specifications on CANopen FD and the improved way of CANopen network management are discussed in the CiA interest group (IG) CANopen FD

▷

Figure 2: In order to detect devices consuming increasingly power over the time or under specific environment conditions (high or low temperature), CiA has standardized a CANopen profile for measuring the power consumption (Source: Adobe Stock)

and all of its sub-groups. The new established TF generic CAN bootloader develops a harmonized way of updating the firmware of CANopen devices. This group discusses lot of aspects of a firmware update via CAN, such as how a CANopen device can recognize a valid and trustable firmware, in which device state is a firmware update allowed, or has the current "user" even permission to initiate a firmware update, etc. Among others, these firmware updates are needed in order to meet cybersecurity requirements. These kinds of requirements are treated by the IG safety/security. This group analyses on the one hand potential threats to CAN-based systems. On the other hand, the group proposes security controls as appropriate counter measures. Furthermore, the interest group introduces a CANopen (FD) cybersecurity layer that allows grouping of CANopen devices. Devices belonging to the same group will support a harmonized procedure for communicating secrets and refreshing keys via CAN. To support CANopen users that operate in mission-critical applications, CiA has started the IG high availability. Derived from the well-proven approaches for maritime applications (CiA 307), the working group develops a generic approach, applicable in different application fields. Various redundancy concepts (bus-line-, device-, function-, or system-redundancy) are analyzed. A technical report shall summarize, which redundancy concept is applicable, to solve which availability issue in which kind of CANopen (FD) application.

The history of CANopen has not been written, yet. CANopen is going to be updated to make use of new generations of the CAN lower layers (CAN FD and CAN XL). Furthermore, CANopen is faced with additional challenges, in new as well as well-known application fields. Predictive maintenance, cybersecurity, high availability, energy saving, and energy management are just some of them. CiA and its members are maintaining and enhancing the set of CAN and CANopen specifications, to equip system designers and maintainers with all necessary CAN(open) "tools", to meet the requirements of embedded networking, today and tomorrow. This includes a formalized improvement process: All CiA documents are systematically reviewed, considering received comments and new feature requests. Of course, editorial improvements on understandability and terminology are introduced, as well. ◀

Further readings

CiA profiles dealing with energy management (CiA 302-9, CiA 320, CiA 418/419, CiA 437, CiA 454, CiA 458)

Author

Reiner Zitzmann
CAN in Automation
headquarters@can-cia.org
www.can-cia.org

Programmable power supplies and electronic loads

EA Elektro-Automatik (EA) offers CANopen-capable power supplies and electronic loads deployed e.g. while recycling of batteries and for fuel cell testing.

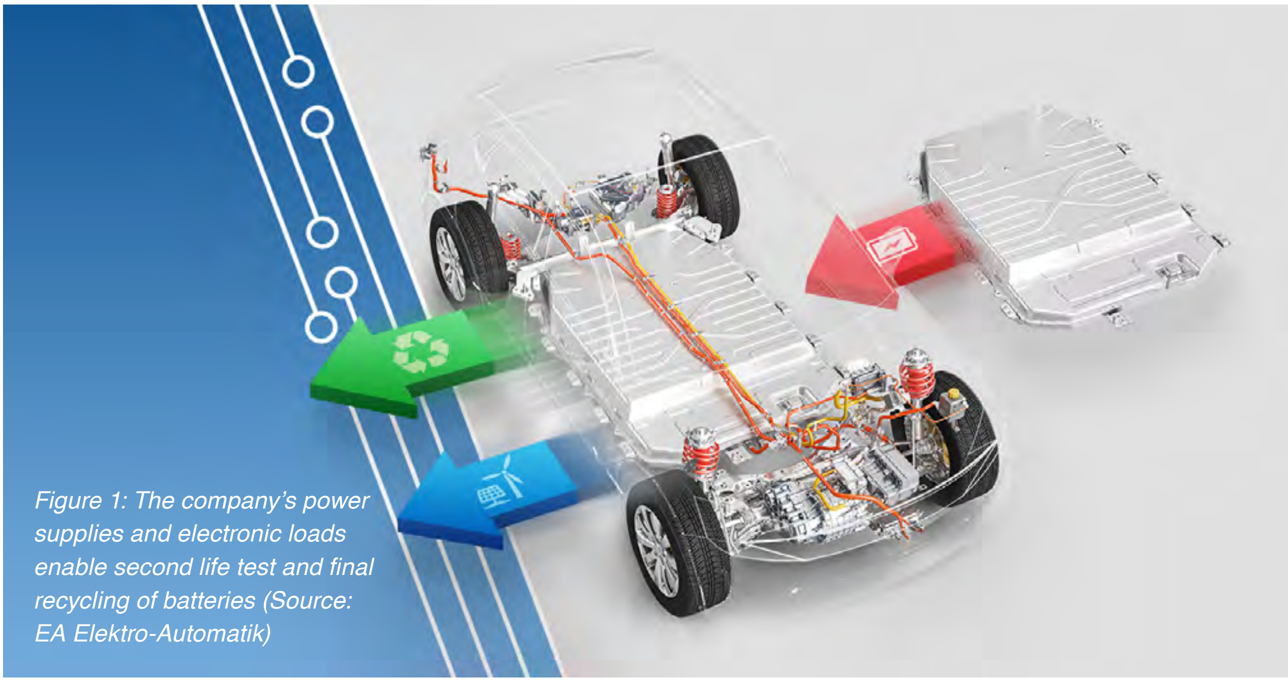


Figure 1: The company's power supplies and electronic loads enable second life test and final recycling of batteries (Source: EA Elektro-Automatik)

With increasing operating time, the lithium-ion batteries used in electric vehicles become less effective and need to be replaced. The old batteries then begin a second life or are finally recycled. EA has developed a range of products for initial battery production, recharging, second life test, and final recycling.

The batteries' second-life use

If the storage capacity of the lithium-ion battery systems is no longer sufficient for use in e-vehicles, residual capacities may well be available for second-life use. Potential applications of second-life batteries range from home storage, emergency power supplies, and energy storage for solar power or wind energy.

With the 30-kW EA-PSB 10000 bidirectional (charge/discharge) power supply, the batteries are tested for their remaining capacity by charging them to almost 100 % and then discharging them again. The DC power supply takes the energy from the connected battery during the discharge process and converts it into AC voltage with an efficiency of up to 96 %. This is then fed back into the local power grid. In a four-unit rack package, the power supplies offer a power density of up to 1,92 MW, thus, enabling for mass testing. Additional time savings are possible due to the device's capability to seamlessly switch between operation as source and sink. The true auto-ranging feature guarantees the maximum possible charge and complete discharge of the batteries through high load currents also at voltages below 2 V_{DC}.

▷

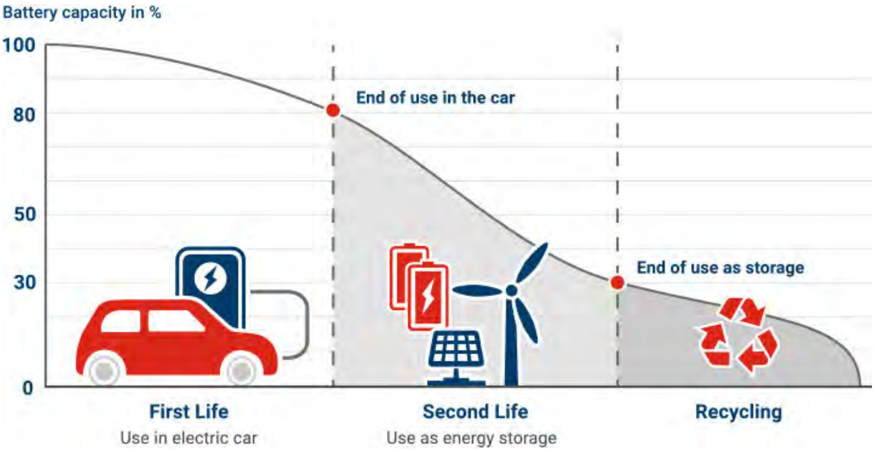


Figure 2: Battery lifecycle (Source: EA Elektro-Automatik)

Final battery recycling

After a certain operating time, batteries can only be finally recycled. For this purpose, they are disassembled into their individual parts, which can be further used. This process must be managed properly to ensure safety and prevent ignition. Lithium-ion batteries and lithium-ion polymer batteries must be completely discharged, which can be achieved with the 30-kW EA-ELR 10000 regenerative electronic load. The electronic load series can achieve up to 1,92 MW in rack systems. The residual battery charge can be extracted in a short time period and fed into the grid with an efficiency of up to 96 %. In this way, grid regeneration reduces operating costs, protects the environment, and lowers heat generation. In most cases, this makes external cooling systems unnecessary. Optionally, the EA-ELR 10000 is available in a sealed enclosure with a 90-% efficient water cooling.

Test and simulation of fuel cells

Use cases for fuel cells include power generation for commercial vehicles (e.g. forklifts, delivery vehicles, trucks and buses), backup power generation systems, and

Interfaces for automated test

The PSB 10000 supplies and the ELR 10000 loads have USB and Ethernet as standard interfaces and offer plug-and-play interface slots for CAN, CANopen, EIA-232, Modbus TCP, etc. The digital interface modules can be installed by the user and can be swapped out with a screwdriver. Via the galvanically-isolated CAN(open) interface, the instruments can be connected e.g. to industrial automation or automotive control systems.

EA's instruments are able to test fuel cells and to simulate fuel cell outputs at different voltages (Source: EA Elektro-Automatik)

The implementation of the CAN-based higher-layer protocol CANopen accords to the CiA 301 CANopen application layer and communication profile. The NMT (network management) server functionality is implemented. A respective CANopen EDS (electronic data sheet) file is shipped with the instruments. The devices support bit-rates up to 1 Mbit/s as well as the auto-baud function enabling to detect the bit-rate currently used in the CANopen network. The interface is accessible via a 9-pin Dsub connector. The interface's configuration is possible via a setup menu on the device.

other power sources. Fuel cell engineers have to conduct characterization (resistance), performance, and durability tests to adhere to required specifications. The performance is indicated via polarization (voltage and current) curves. A durability test is performed in operating conditions, where the stack is subjected to a continuous series of charge/discharge cycles. EA's regenerative loads enable to test fuel cell resistance, performance, and lifetime. The bidirectional laboratory power supplies are able to simulate the characteristics of different fuel cells.

With 30 kW of input power, the EA-ELR 10000 electronic loads connected in parallel can reach up to 1,92 MW for mass testing. Features include a built-in arbitrary waveform generator, function generator, and true auto-ranging function. Unlike other loads that need a separate AC instrument, the ELR load, with its built-in waveform generator, can perform the perturbation test to determine fuel cell resistance. The auto-ranging function enables to work with voltages of 0 V_{DC} to 60 V_{DC} up to 0 V_{DC} to 2 000 V_{DC}. Current outputs can reach up to 1 000 A. Due to the regenerative mode of operation, the energy can be fed back into the grid with an efficiency of up to 96 %. This saves power and eliminates the need for additional cooling systems.

The 30-kW EA-PSB 10000 power supply offers the same features and also provides an internal X-Y generator to simulate the fuel cell output at various voltages. The supply can add ripple and noise onto its output to determine how well a fuel-cell powered device can perform under different conditions.

Polarization and power-density curves of a fuel cell stack is a common indication for the cell performance. These curves are assessed under the optimal operating conditions (temperature, humidity, electrocatalysis, and ion-exchange membrane) of a fuel cell stack. The curve measurements can be obtained by programming a DC load in different current or resistance profiles. Load series ELR 9000 3U, ELR 9000 HP, and ELR 10000 4U enable such dynamic testing.

Figure 3: Via the CANopen interface the instruments can be connected e.g. to industrial automation applications (Source: EA Elektro-Automatik)

Market for fuel cells is growing

"In response to the demand for clean energy, the market for fuel cells is growing at a compound annual growth rate of 26,4 % and is projected to reach 848 million US $ by 2025. Uses for fuel cells include power generation for commercial vehicles such as buses and forklifts, backup power generation systems, and for other power sources. To ensure the design and manufacturing of quality fuel cells, EA Elektro-Automatik offers its EA PSB 10000 2-quadrant power supplies and EA ELR 10000 series electronic loads. Both the EA PSB power supplies and the EA ELR loads sink up to 30 kW and feed the energy back to the grid to enable testing of any size fuel cell stack," said Markus Schyboll, CEO of EA Elektro-Automatik.

HMI and software features

To interact with the supplies and the loads a 5-inch multicolor touchscreen display is available as a human machine interface (HMI). Via the display operators can control, setup, and program the device. Programmed and measured values can be shown in a chosen language. Using the EA Power Control software, the user can operate up to 20 devices remotely via a PC. Additional functions include sequencing and logging of data, a function generator, as well as automated remote maintenance with updates. Simulations of photovoltaic arrays is possible as well. ◀

Author

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

TX
RX
01000177
KVASER

The Janus attack

The Janus attack is a low-level CAN protocol attack where a single CAN frame contains two different payload contents.

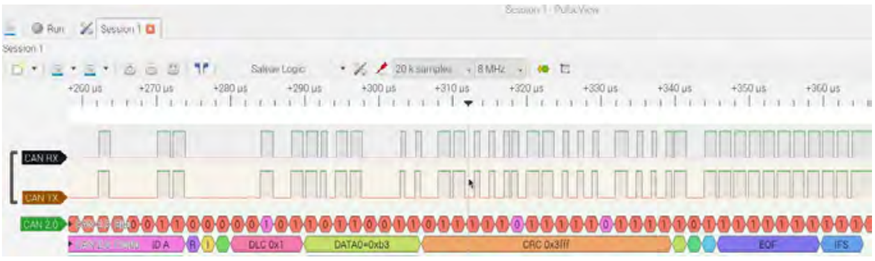


Figure 1: Logic analyzer trace of a Janus frame (Source: Canis Automotive Labs)

With the Janus Attack, a targeted device sees a different payload than other devices. This attack could be used to transmit a frame to evade an intrusion detection system (IDS), or it could put two different actuators into inconsistent states (e.g. moving a pair of motors in different directions). It breaks the atomic multicast feature of CAN (where every device sees the same frame) - an important property that lots of systems rely on (often implicitly).

The attack works by exploiting the CAN protocol synchronization rules and targets devices that have different sample points. The CAN specification defines the following rules:

a) Only one synchronization within one bit-time (between two sample points) shall be allowed. After an edge was detected, synchronizations shall be disabled until the next time the bus state, detected at the sample point, is recessive.

b) An edge shall cause synchronization only if the bus state detected at the previous sample point (previous read bus state) was recessive.

The attack can be mounted purely in software that takes control of the GPIO port connected to the CAN Tx pin of a CAN transceiver, so a hijacked device using a remote code execution vulnerability could be used to mount the attack.

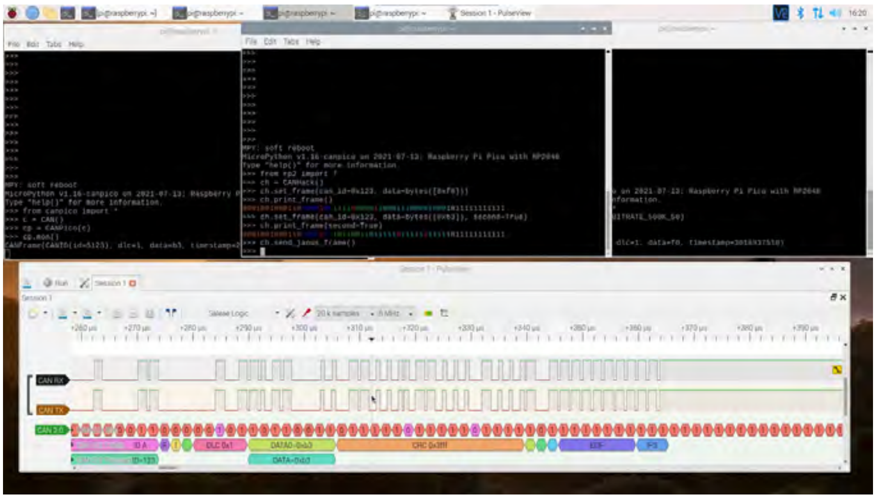
In a demonstration video of the attack, two CANPico boards (that contain the Microchip MCP2517/18FD CAN controller) are attacked by a CANHack board. The latter is a cut-down version of the CANPico that does not have a CAN controller, neatly proving that the attack can be mounted in pure software. The logic analyzer is running the Sigrok Pulseview CAN2 protocol decoder to show how the Janus signal is decoded into a CAN frame.

How does the attack work?

The attack forces CAN controllers to synchronize at the same time and then changes the CAN bus level after one controller has sampled the bus but before another. The bit sequences are set so that each device sees a valid frame, but the frames can have different payloads. The logic analyzer trace (Figure 1) shows how a Janus frame is made up of many more transitions than CAN bits but that form a valid CAN frame.

There are two restrictions on the bit sequences. First, the first and second CAN frame have to have the same length, so there must be the same number of stuff bits. The CANHack tool kit has a function to show the bit patterns of both halves of a Janus frame (Figure 2).

Second, if the Janus bit is ***10*** (i.e. the first sampled value in a CAN bit is a ***1*** but the second sampled value is a ***0***) then all controllers have to see the same subsequent bits (***00*** or ***11***) until they are brought back into sync (which happens after a ***11***).



```
MPY: soft reboot
MicroPython v1.16-canpico on 2021-07-13; Raspberry Pi Pico with RP2040
Type "help()" for more information.
>>> from canpico import *
>>> c = CAN()
>>> cp = CANPico(c)
>>> cp.mon()
CANFrame(CANID(id=S123), dlc=1, data=b3, timestamp=
```

```
MPY: soft reboot
MicroPython v1.16-canpico on 2021-07-13; Raspberry Pi Pico with RP2040
Type "help()" for more information.
>>> from rp2 import *
>>> ch = CANHack()
>>> ch.set_frame(can_id=0x123, data=bytes([0xf0]))
>>> ch.print_frame()
0001001000110...1R11111111111
>>> ch.set_frame(can_id=0x123, data=bytes([0xb3]), second=True)
>>> ch.print_frame(second=True)
0001001000110...1R11111111111
>>> ch.send_janus_frame()
>>>
```

Figure 2: Setup of the two CANPico boards and the CANHack board in the middle. The CANHack tool kit has a function to show the bit patterns of both halves of a Janus frame. (Source: Canis Automotive Labs)

Updated CANPico firmware released

The CANPico firmware has been updated to the latest release of Micropython v. 1.16. The update fixes some bugs and adds robustness to SPI (serial peripheral interface) noise (for example, if SPI pins accidentally pick up noises from logic analyzer probes where the logic analyzer is not grounded). Thus, corrupted values could be written to or read from the CAN controller. The firmware keeps counters for the number of corrupted values with a new method ***get_diagnostics()***.

The documentation has been updated to reflect this API (application programming interface) call. There is also a new version of the ***canpico.py*** file of example functions that are useful when trying out different things on the CANPico board. This file can be copied to the CANPico board using the ***rshell*** utility.

There is a Janus bitstream test function called ***is_janus()*** included in the latest version of the Python CAN frame tool in the CANHack repository, plus a simple brute force algorithm to look for Janus payloads (no doubt, other smarter algorithms exist as well). This can be used to create CAN frames to show how the attack works. It would also be possible to attack devices with sample points that were more similar if the CANHack toolkit would use the output-compare-timer hardware present in most microcontrollers to make the CAN Tx transitions more accurately. But the goal with the CANHack toolkit is not to make it easy to attack a CAN bus but to prove that there is vulnerability that must be defended against.

How to defend against Janus attack?

Firstly, an intrusion detection system (IDS) with dedicated hardware should be used to detect these transitions. An IDS that uses a conventional CAN controller cannot detect this (it also cannot detect many other CAN protocol attacks). Secondly, devices should have sample points set as close to each other as possible: Ideally, this would be a part of an acceptance test when integrating devices together on to a CAN network. There are other protections too. Using the CAN-HG Bus Guardian hardware prevents a Janus frame from being sent and allows an IDS to shut down an attack. Protecting a payload with a cryptographic message authentication code (MAC) makes it much harder for an attacker to find a valid Janus payload, even if the attacker has the ability to sign messages with the necessary shared cryptographic key. ◀

Author

Ken Tindell
Canis Automotive Labs
ken@canislabs.com
canislabs.com

Facts & Figures

5%

Compound annual growth rate (CAGR) for fire trucks between 2021 and 2026 (source: Mordor Intelligence). Most of the market-leading suppliers use multiple CAN-based networks for the body applications. DIN standardizes the CAN interfaces for some fire-fighting equipment in DIN 14700, which complies partly to CANopen. CiA has established a SIG (special interest group) to initiate further standardization of fire-fighting device interfaces.

Standardization is somehow important, but do not waste our best engineers.
I will find someone, who can do the job.
Have you some staff for standardization meetings?
You know, we are short in good technicians.
You are retiring, soon. I have some tasks in standardization groups for you.
I am not educated for this. But I will do it, if this includes oversea travellings.
There are many standards, which we might be interested in.
Why you have printed out all of them?
I did not, we bought them as hardcopies.
Don't give such a job to someone, who is close to be retired.

CiA 604-1

The CAN FD Light specification has been released as Draft Standard Proposal. The 16-pages document specifies the CAN FD Light responder node. Bit-rate switching is not supported, which limits the bit-rate to 1 Mbit/s. The commander/responder communication scheme is optimized for price-sensitive sensor/actuator systems. It is used as deeply embedded network in smart headlights for road vehicles. But it is also suitable for industrial application due to its robustness and reliability.

As usual, CiA exhibits on the SPS tradeshow in Nuremberg (November 23 to 25). The CiA booth is in hall 5 at stand 410 showing CANopen products from some member companies and informing interested parties about CAN technologies.

sps

smart production solutions

More than ...

CiA has uploaded on Youtube many videos in English, Chinese, and Russian language. Most of them are records of CiA webinars, CiA technology days, and iCC papers. Most watched are the "CAN FD from a view point of an OEM" and the "Bit time requirements for CAN FD" iCC presentations.

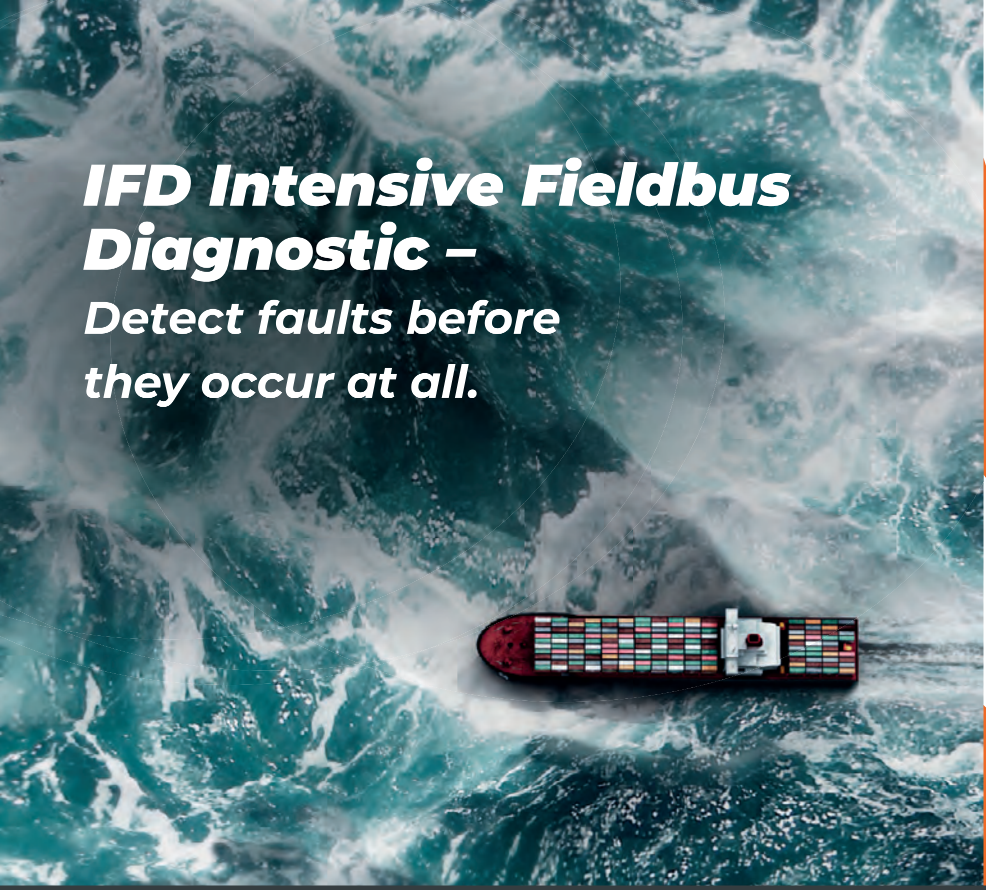
... 127 videos

Three out of four

About 75 % people in the European Union live in cities and the trend is rising. Many of them would like to use pedelecs and e-bikes for the inner-city journeys and the weekend travels. This is why the Bosch Ebike Systems participated for the first time at the IAA Mobility tradeshow. Bosch provides CAN interfaces for many of its pedelec devices. The company is one of the market-leading suppliers in Europe.

20 CAN FD ports

The Stellar SR6 P micro-controller series by ST Microelectronics provides up to 20 on-chip CAN FD nodes. One of the CAN FD nodes supports TTCAN (Time-triggered Controller Area Network). Based on six Arm Cortex-R52 cores, the MCU addresses ASIL-D (automotive safety integrity level) safety-related applications compliant with ISO 26262.



CANtouch®
Bus-status
Bus-fehler
Bus-spannungen
Gleichtakt-spannung
CAN Pegel Differenz
CAN Pegel Absolut
Bus-verdrahtung
Messung Teilnehmer
Online Trigger
Protokoll-monitor
GEMAC
IFD
INTENSIVE FIELDBUS DIAGNOSTIC

GEMAC
GEMAC Motus XC
XC6MZ360-0
Order No.: PR-2/116-30
Serial No.: 27116-30/000001
7.5...36 VDC • IP6K7/IP6K9K
Interface: CANopen
GEMAC Chemnitz GmbH
Made in Germany
CE
POWER IMU

Automated sewer cleaning with CANopen

Components used in municipal vehicles are exposed to extreme temperatures, humidity, dust, dirt, and vibrations. With the Ecomatmobile series, ifm offers CANopen-capable automation products for these harsh environmental conditions. Bucher Municipal uses them for its sewer cleaning vehicles.

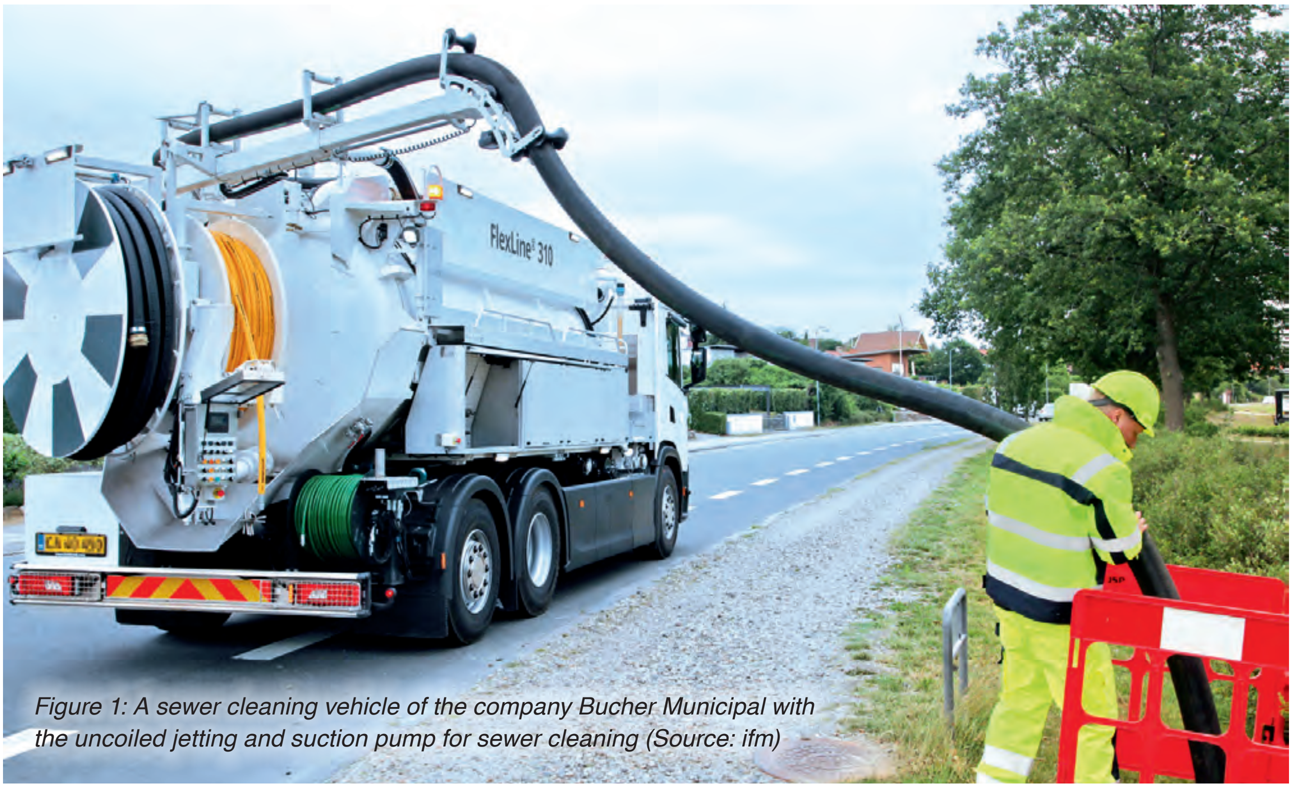


Figure 1: A sewer cleaning vehicle of the company Bucher Municipal with the uncoiled jetting and suction pump for sewer cleaning (Source: ifm)

Bucher Municipal is a global supplier of special vehicles such as refuse collection vehicles, sweepers, and winter maintenance equipment. In the Danish city of Silkeborg, the company manufactures sewer cleaning vehicles. Brian Munk Andersen, R&D Manager at Bucher in Denmark, explained the structure and function of this vehicle type: "Sewer cleaning units from Bucher feature two pump systems. The jetting pump cleans sewers and tanks. With the vacuum pump, we can suck sludge and industrial waste into the tank mounted on the vehicle."

With two ifm control units for mobile applications installed outside the vehicle, the vehicle operator can perform a variety of work steps: rotate the boom, unwind, and rewind the hose, switch the pumps or empty the sewage water tank. The displays of the dialog modules show the relevant system parameters and process values and assist the user in performing the work steps. A control unit inside the vehicle – also supplied by ifm – ensures that the individual processes run smoothly. "The intelligent control of our sewer vehicles ensures efficient processes and enables maximum focus on the task, guaranteeing the highest possible added value for our end users," said Andersen.

Ifm as a partner

For several years now, the automation specialist ifm has been supporting Bucher Municipal as a partner for sensor components and control technology. Brian Munk Andersen: "At Bucher, we have a constant focus on innovation and development. That's why we use automated and intelligent solutions. When we entered into a cooperation with ifm in 2016, we were looking for a reliable supplier of control solutions. Ifm offers a wide range of components for our product – from sensors to displays and I/O systems to controllers.

Throughout the development phase, we worked closely with ifm to develop a solution and choose the ideal products. Our vehicles have to operate reliably in very varied conditions such as cold, heat, dust, and dirt. This places particularly high demands on the components. Together with ifm, we have created a good and reliable solution with many automated features that offers the operator high quality and safety standards when our machines are on the road."

▷

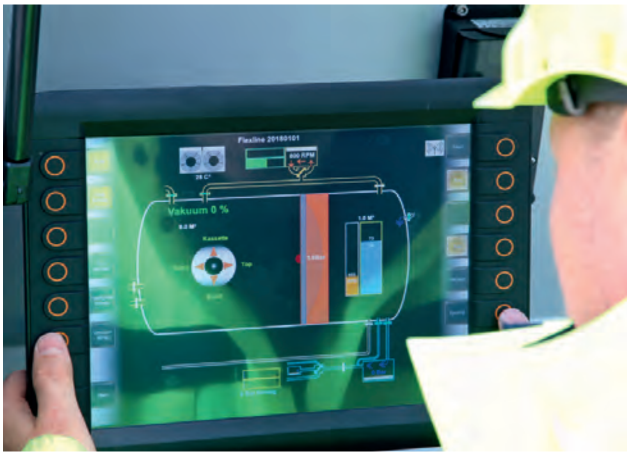


Figure 2: The robust 12-inch display CR1200 installed in the external control cabinet of the vehicle for visualisation and setting of all machine parameters (Source: ifm)

The central CAN products in detail

The core element of the system is the Ecomatcontroller CR711S, a robust PLC (programmable logic controller) for mobile applications. What makes it so special is that it has two independent internal PLCs – one of them a certified safety controller. Powerful integrated multi-core processors allow even complex control functions to be processed quickly. The application programs can be divided between the two internal PLCs if necessary. Consequently, the safe program part can be executed without interference from the general program execution. This ensures reliable operation even with complex control functions. The controller can be used in safety-related applications up to ISO 13849 PL d and IEC 62061 SIL CL 2.

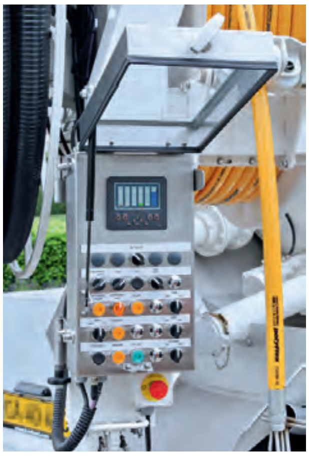


Figure 3: The Basicdisplay CR0451 indicates the most important parameters on the control panel (Source: ifm)

In addition to its many multifunctional inputs and outputs with diagnostic capabilities, the Ecomatcontroller features four CAN interfaces and two Ethernet ports. The CAN interfaces support all important protocols such as classic CANopen, CANopen Safety, and J1939 as well as the transparent and preprocessed data exchange. The CiA 301 CANopen application layer and communication profile version 4.2 as well as CiA 401 device profile for generic I/O modules version 1.4 are supported. The control functions are easily integrated into the application program thanks to Codesys programming (version 3.5).

At Bucher, the controller is additionally connected to a GSM (global system for mobile communications) radio module. Andersen: "In many cases, our remote connection

▷

Interview with ifm: “CANopen is our preferred network”

Dietmar Brüss (ifm)

Dietmar Brüss, Product Manager Control Systems at ifm explained the CAN Newsletter why the company relies on CANopen and spoke about the possible future connectivity developments for ifm’s devices.

Q: CANopen is your preferred network technology. What are the main benefits?

A: If customers have to decide which CAN-based higher-layer protocol they should use in their application, ifm advices to use CANopen. CANopen is internationally standardized (EN 50325-4), widely used, and accepted. Also the ifm tool chain for programming and configuration supports CANopen as one of the standard communication channels. Additionally, the available CiA CANopen device profiles (e.g. for I/O modules, inclinometers, encoders) are implemented in the related sensors. This simplifies the task of integrating the devices in a CANopen system. The freely-programmable controller can be flexibly configured via CANopen off-the-shelf tools.

Q: Are new CANopen device profiles needed?

A: For devices offered by ifm the CANopen device profiles are already available.

Q: Is cybersecurity an issue for future applications?

A: This is increasingly an issue for applications in which a wirelessly-connected device has to access/control in-vehicle networks. I think, because of the cost reasons, the application securing functionality would reside in the Edge gateway (e.g. HMI, IPC, modem) allowing access to the in-vehicle application network. Thus, no additional effort would arise for single devices (sensors, controllers, etc.).

Q: Would it be helpful to standardize gateways to in-vehicle networks?

A: Due to the free-programmability of our controller and displays, we can react on customer’s requirements. For the application engineers integrating our devices into the vehicle, it would be a huge benefit. Standardized CANopen gateways would allow a unified access/control of the in-vehicle networks. No adaptations to a specific vehicle would be required. This saves development time and costs.

Q: Are you planning to migrate to CANopen FD?

A: Currently, neither ifm nor our customers are realizing any project using CAN FD or CANopen FD. All of our new products are capable to support CAN FD and CANopen FD. When the market in general or a big customer would require to support a corresponding solution, implementation in the hardware would be relatively simple. Regarding software, to realize a commonly-used tool-based solution would be a challenge. Such programming environments as e.g. Codesys do not support CAN FD at the moment.

Q: Does CAN XL provide features you like to use?

A: At the moment, we see no customer demands on a higher bandwidth. Formerly, in some (very few!) projects, we considered to implement an additional Ethernet-based two-wire network (Broadr-Reach). Finally, the customers decided against it, because effort and gain are not in a reasonable relation to each other. For diagnostics, maintenance, and programming all current devices provide a four-wire Ethernet interface as a standard. This is a clear market requirement and is also used by all our customers.

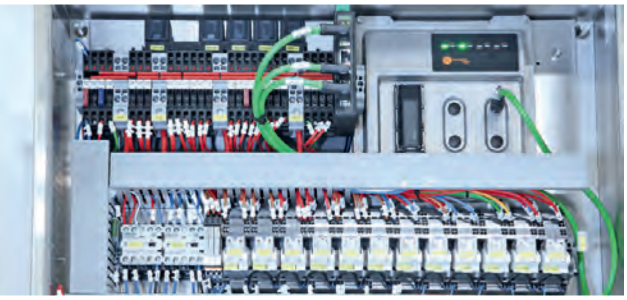


Figure 4: The core element at the top right of the control cabinet: the powerful Ecomatcontroller CR711S with two integrated PLCs (1x standard, 1x safety) (Source: ifm)

allows us to solve issues while the vehicle is still on the road. This saves our customers a lot of time. Only in cases where remote troubleshooting is not possible the municipal vehicle needs to be checked at one of our many service centers."

I/O modules

Various sensors and actuators are installed on the sewer cleaning vehicle to monitor and control the different work steps and process values. Using decentralized I/O modules, they communicate with the controller via CAN. Brian Munk Andersen explained the benefit: "With CAN units installed at different positions on the truck, we reduce wiring and also achieve greater reliability and an easier operation of the equipment."

The type CR2032 control modules each have 16 ports that can be configured multifunctionally, for example as digital inputs or outputs or as PWM outputs for controlling proportional valves. A controller integrated in the modules enables decentralized evaluation of the sensor signals in advance. This pre-filtering of the data not only reduces the data flow on the CAN network to the controller, but also simplifies the application program on the PLC. The robust metal housing is designed specifically for the harsh outdoor use of mobile machines and offers protection rating IP67 for high ingress resistance of the connectors. The CR2032 supports the CiA 301 CANopen application ▷

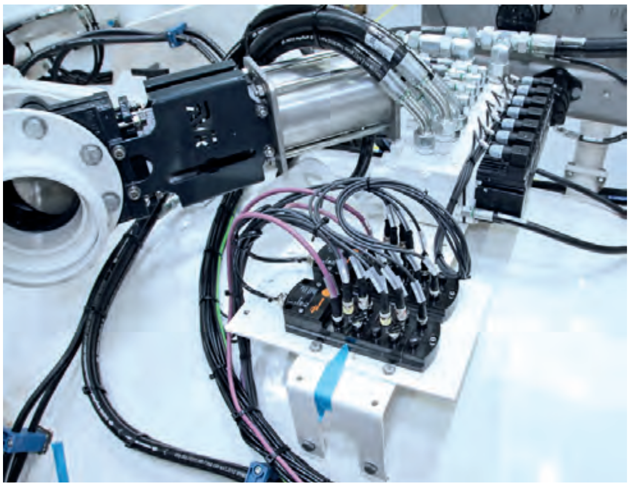


Figure 5: Decentralised CAN I/O modules outside the vehicle connect the sensors and actuators to the controller (Source: ifm)

layer and communication profile version 4 as well as the CiA 401 CANopen profile for modular I/O devices version 2.1

Dialog modules

A range of displays for mobile applications are mounted outside the vehicle as human-machine interfaces. Brian Munk Andersen: "On the large display in the main cabinet, the operator can control the entire system and make the basic settings. After this, the system can be operated via the remote control or the operating panels."

Dialog modules are programmable graphic displays for controlling, parameter setting, and operation of mobile machines and installations. They can be used in conjunction with a mobile controller or as a stand-alone solution. Data and device functions are safely transferred via CAN interfaces. The displays feature many freely programmable backlit function keys. The units offer increased EMC (electromagnetic compatibility) levels and an e1 type approval for operation on public roads. Thanks to the high protection rating of the housing, the modules are suited for outside panel and surface mounting as well as for cabin installation. Just like the other ifm components for mobile applications, the displays are vibration resistant and have protection rating IP67. The CR1200 and CR0451 (name: Basicdisplay) displays come with TFT LCD colour screens. The CR1200 provides a resolution of 1024 pixels x 768 pixels while the CR0451 provides 320 pixels x 240 pixels. Both displays come with a CAN interface and support CiA 301 CANopen application layer and communication profile version 4 as well as CiA 401 CANopen profile for modular I/O devices version 1.4, or J1939.

Conclusion

Ifm offers a comprehensive portfolio of products for efficient and reliable automation of functional units on municipal vehicles. Brian Munk Andersen concluded: "With ifm's solution, we can create a highly automated system that offers us superior reliability and makes the lives of those operating our equipment a lot easier." All of the named products are part of the Ecomatmobile series. ◀

Author

Andreas Biniasch
ifm electronic
info@ifm.com
www.ifm.com

Migration to CAN FD

In 2011 efforts were made to overcome the existing limits of the Classical CAN in terms of the maximum achievable bit rate – the idea of CAN FD was born. But is it actually worth migrating to CAN FD?

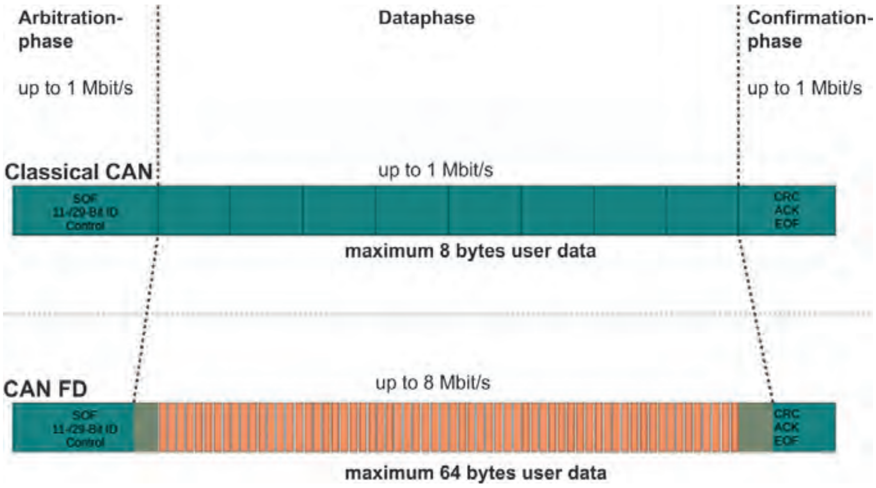


Figure 1: The comparison of protocol framework (Source: ESD Electronics)

As with the Classical CAN protocol it was the automotive industry that stood as a driving force behind the development of the CAN FD protocol (CAN with flexible data rate). In cooperation with some other experts Bosch began working on a solution in 2011 to shift the existing limits set by Classical CAN regarding the maximum available bit rate respectively the maximum achievable data throughput. At the same time, it was a declared aim to preserve the proven concepts of Classical CAN, such as real-time bus arbitration, event control, 11-bit and 29-bit CAN-Identifier, and multi-manager capability. Moreover, a high robustness against interference, low power consumption and the use of existing topologies were further advantages that needed to be maintained.

The desired objectives were achieved:

- Maintaining the Classical CAN concepts of arbitration and confirmation phase as well as error management
- Increasing the bit rate during the data phase from a maximum of 1 Mbit/s up to 8 Mbit/s and more
- Increasing the number of transferred data bytes transmitted in a CAN frame from maximum 8 bytes to maximum 64 bytes

The new protocol has been published as an international standard since 2015 with all CAN FD controllers being backwards compatible and still supporting the Classical CAN protocol. A wide range of dedicated CAN FD controllers, micro-controllers with integrated CAN FD interfaces, and FPGA-based (field-programmable gate array) solutions are nowadays available.

Protocol details

In Classical CAN the transmission of a frame can be divided roughly into three phases: bus arbitration, data transfer, and confirmation. During all these stages, bits are being transferred with an identical bit rate, while all network participants resynchronize constantly in order to compensate for phase noise and phase drift of independent local oscillators. This is especially important during the arbitration and confirmation phases, since all nodes must be broadcasting simultaneously on the network, and each individual node must be able to compare its sent bit with those of other participants. This property of the Classical CAN protocol determines the physical limits for the maximum possible bit rate or cable length.

The idea behind the CAN FD protocol is to send data with a second, usually much higher bit rate during the data phase. Post-synchronization is suspended during this phase since, due to the principle, there should be only one transmitter on the bus. Furthermore, the payload of a frame has been increased from 8 byte to 64 byte ensuring a considerable improvement in the ratio between protocol and user data. Bit rates with a ratio of 1:4 between arbitration phase and data transfer phase result in an increased ▷

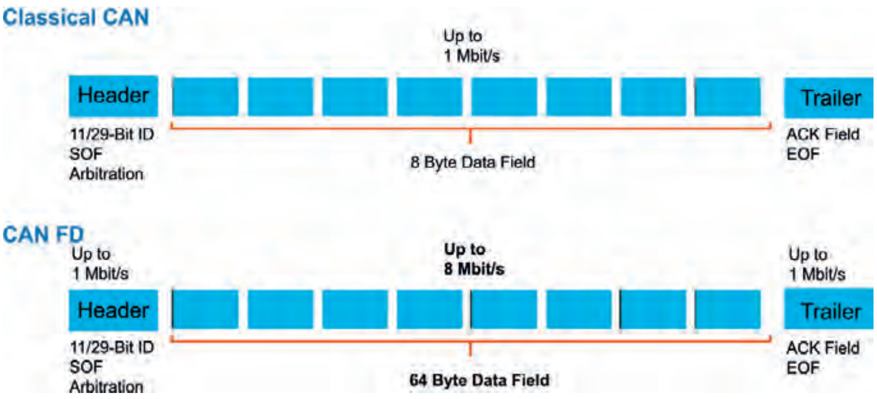
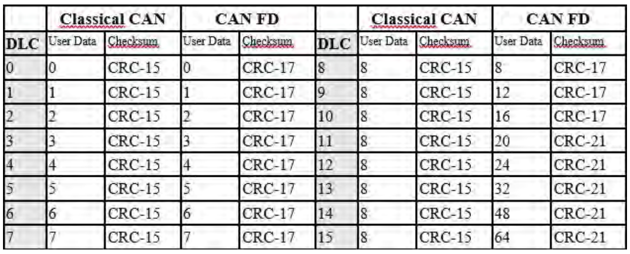


Figure 2: The data fields in comparison (Source: ESD Electronics)

Table 1: A comparison of the data length code (DLC) for CAN and CAN FD



	Classical CAN		CAN FD			Classical CAN		CAN FD	
DLC	User Data	Checksum	User Data	Checksum	DLC	User Data	Checksum	User Data	Checksum
0	0	CRC-15	0	CRC-17	8	8	CRC-15	8	CRC-17
1	1	CRC-15	1	CRC-17	9	8	CRC-15	12	CRC-17
2	2	CRC-15	2	CRC-17	10	8	CRC-15	16	CRC-17
3	3	CRC-15	3	CRC-17	11	8	CRC-15	20	CRC-21
4	4	CRC-15	4	CRC-17	12	8	CRC-15	24	CRC-21
5	5	CRC-15	5	CRC-17	13	8	CRC-15	32	CRC-21
6	6	CRC-15	6	CRC-17	14	8	CRC-15	48	CRC-21
7	7	CRC-15	7	CRC-17	15	8	CRC-15	64	CRC-21

net data rate by the factor of 2 up to even 5 depending on the payload size.

To implement the CAN FD protocol a previously reserved bit within the control field of the CAN frame was used, respectively two more bits were added:

- Extended data length (EDL)
- Bit rate switch (BRS)
- Error state indicator (ESI)

A CAN controller will recognize the CAN FD format with the help of the recessive EDL bit (dominant and unused in the Classical CAN protocol). The newly-added BRS bit determines whether the higher bit rate will be used in the data phase or the frame continues to be sent at the arbitration bit rate. Finally, the ESI bit with its dominant status indicates that the sender is in the error active state. On grounds of efficiency the size of the DLC (data length code) field with 4 bits has been left unchanged so that CAN FD frames with more than 8 data bytes can only be sent in discrete quantities. In order to achieve the same degree of robustness against communication errors despite prolonged payload sizes, in CAN FD a 17-bit checksum (frames with up to 16 bytes of user data) or a 21-bit checksum (frames with more than 16 bytes of user data) is used to check correctness instead of the usual 15-bit checksum (Classical CAN).

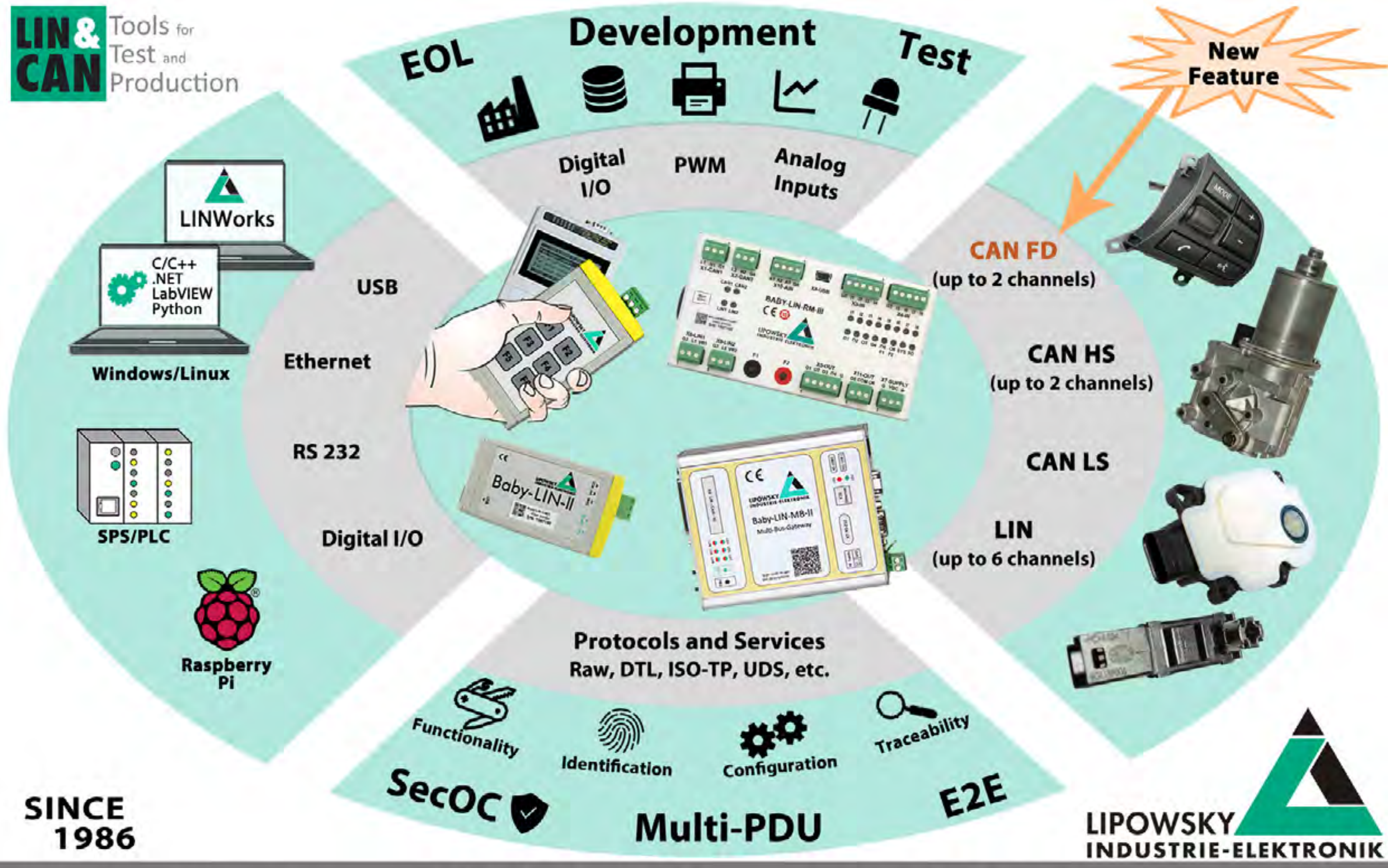
Table 1 provides an overview regarding the assignment of the DLC to the amount of data transferred and the checksum used in each case. However, the RTR (remote transmission requests) feature is no longer supported in the CAN FD protocol. Due to the backward compatibility, the use of RTRs is still supported by CAN FD controllers for the Classical CAN protocol.

Advantages of CAN FD

Both main innovations introduced by the CAN FD protocol – higher bit rate in the data phase and frames with up to 64 data bytes – can be used in a wide variety of ways in applications:

- Improved data throughput is particularly noticeable when transferring large data sets (such as firmware updates)
- Improved real-time behavior (reduction of latency) with higher bit rates during the data phase and unchanged protocol
- Reduced bus load with higher bit rates during the data phase and unchanged protocol allows extensions in

▷



systems that otherwise would not be expandable due to the current bus load and might have required an additional CAN network.

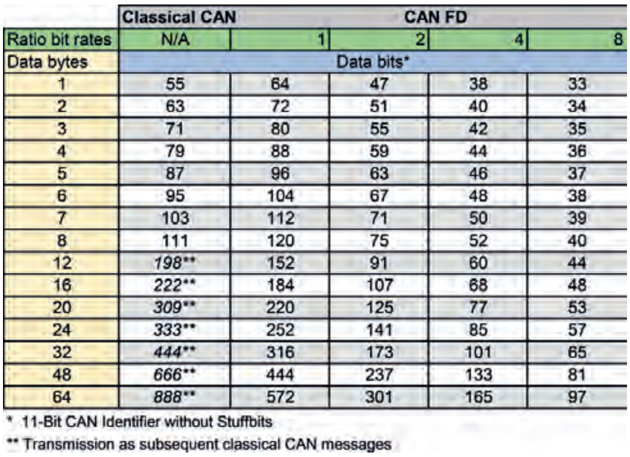
- Simple safeguarding of data consistency regarding process data of more than 8 data bytes that can now be sent in a frame with more data bytes
- Possibility to extend existing CAN networks that are already operating at their physical limit regarding the bit rate. This is done by reducing the arbitration bit rate and using a higher bit rate in the data phase, so that an identical or even larger net data rate is achieved.

While the CAN protocol itself is already quite robust the improved protection against transmission errors by means of extended checksums as well as the indication of the sender's state (error passive or error active) are additional advantages that make the communication even more secure.

Performance gain

Any statement regarding the expected gain in throughput or the reduction of latency when switching from Classical CAN to CAN FD is not easy. It basically depends on the type of implementation and the higher-layer protocol used as well as on other boundary conditions. For a better estimate, Table 2 shows the bits required for the transmission of frames with 11-bit CAN-Identifiers at different data lengths and different ratios between the bit rate in the CAN FD arbitration and data phases. The number of data bits refers to bit times of the arbitration phase: i.e. this number indicates the CAN frame length (time) expressed in multiples of 1 arbitration-phase bit time. Based on Table 2, two extremes will be considered when trying to estimate the effort involved for switching from CAN to CAN FD.

Table 2: Performance of CAN and CAN FD for various bit ratios



	Classical CAN	CAN FD			
Ratio bit rates	N/A	1	2	4	8
Data bytes	Data bits*				
1	55	64	47	38	33
2	63	72	51	40	34
3	71	80	55	42	35
4	79	88	59	44	36
5	87	96	63	46	37
6	95	104	67	48	38
7	103	112	71	50	39
8	111	120	75	52	40
12	*198***	152	91	60	44
16	*222***	184	107	68	48
20	*309***	220	125	77	53
24	*333***	252	141	85	57
32	*444***	316	173	101	65
48	*666***	444	237	133	81
64	*888***	572	301	165	97

* 11-Bit CAN Identifier without Stuffbits

** Transmission as subsequent classical CAN messages

Conversion from CAN to CAN FD

Without changing the protocol: Besides the need to purchase CAN FD capable hardware, the (software) effort is in the best case limited to setting the increased bit rate in the data phase. With a ratio of 1:4 between arbitration and data phase bit rate and with a protocol based primarily on frames with 8 data bytes, one can expect to improve the throughput by a factor of more than 2 or to halve corresponding latency times.

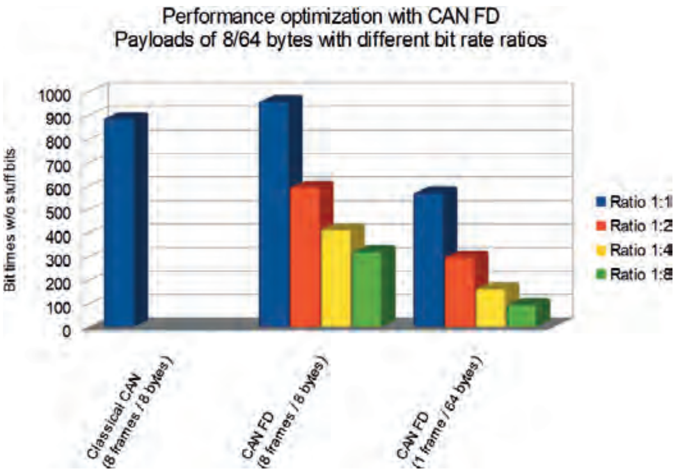


Figure 3: Performance optimization for CAN FD frames with 8-byte and 64-byte payloads sent with different bit rate ratios (Source: ESD Electronics)

With changing the protocol: Even greater performance gains can be achieved if, besides increasing the data rate, the protocol is adapted with additional software effort. In this way the higher number of possible CAN FD data bytes is fully exploited.

Based on the previous example, a protocol (e.g. for firmware update), which was previously based on CAN frames with 8 data bytes, is to be converted to CAN FD frames with 64 data bytes. Figure 3 considers transmission of 64-byte data blocks.

The graph shows that with the protocol unchanged and a ratio of 1:4 between arbitration and data phase bit rate (as in the previous example), the throughput has more than doubled. Using the full 64 bytes of CAN FD user data, the data throughput will increase even fivefold and with a further increase in the bit rate ratio to 1:8 the throughput increase will be more than nine times higher. In the latter case, the transmission of the CAN FD frame with 64 data bytes takes even less time as for transmitting a single CAN frame with 8 data bytes. Under these conditions an additional reduction in latency is achieved.

Migration to CAN FD

For hardware developers: For new hardware developments the support of CAN FD has become quite easy. As with Classical CAN, driven by the automotive industry, one or more CAN FD interfaces are replacing the Classical CAN interfaces in current micro-controllers. Up to a certain ratio of the bit rate (arbitration bit rate to data phase bit rate), CAN FD accepts the same oscillator tolerance as CAN, but it is advisable to use a transceiver specified for CAN FD. Even if a customer continues to only use Classical CAN they will benefit from these advantages. If existing designs are to be extended by a CAN FD connection this is easy to implement with now available standalone controllers or by using an FPGA IP core.

For software developers: The effort involved in migrating an application to CAN FD depends heavily on the ▷

Vector Testing Solution
It's Good If Your Software Runs.
And Even Better If It Conquers
Every Challenge.

Outstanding Software Quality Demands Rigorous Testing.

For embedded software to be successful, it must meet the highest demands. Our comprehensive test solution enables your software project to effortlessly pass every efficiency test. From the design and implementation of the test to its execution, along with the centralized administration and analysis of your test data – we cover the whole gamut, whether for unit or system tests, SIL or HIL. This allows you to always be on the safe side and identify potential improvements for your software at an early stage. And to conquer every challenge with ease.

Vector brings your software development a giant leap forward.

vector.com/testing-solution

VECTOR

Interview: Why migrate to CAN FD?

Dirk Flege (ESD Electronics)

Due to the backward compatibility of CAN FD technology, Classical CAN applications can be migrated to CAN FD or can be used as a basis in new applications. Dirk Flege, Head of Sales at ESD Eelectronics, explained in an interview what makes a migration to CAN FD worthwhile.

Q: The CAN protocol is characterized by great robustness against interference. How can this property be preserved in CAN FD?

A: The CAN FD protocol is designed in such a way that keeping Classical CAN concepts is possible in the arbitration and confirmation phase as well as in error handling. In order to achieve the same robustness against communication errors even in the longer data phase, the protocol uses a 17-bit checksum (frames with up to 16 bytes user data) or a 21-bit checksum (frames with more than 16 bytes user data) instead of the usual 15-bit checksum.

Q: The CAN FD protocol is backwards compatible with the Classical CAN protocol. What are the opportunities of this advantage for industrial automation?

A: Thanks to the backward-compatible design, CAN applications can be easily converted to the more powerful CAN FD communication without having to change the existing wiring. Alternatively, CAN FD components can also be used as a basis in current CAN applications and simply be switched to CAN FD communication later on.

Q: In addition to standardized CAN FD controllers there are also FPGA-based ones available on the market. They have greater flexibility in terms of performance and functional density. What exactly are the advantages of FPGA-based CAN controllers?

A: The write and especially the read access to standard controllers is rather slow compared to the cycle time of modern CPUs (central processing unit). Therefore, we have developed an FPGA-based CAN controller, which all our CAN interfaces are based on. The Advanced CAN Controller (esdACC) has an interface of up to 32 bits wide and supports 64-bit timestamps. Furthermore, it can generate a 100-% busload. These are the features where the CAN FD controller for FPGA is derived from supporting the CAN FD protocol in accordance to ISO11898-1:2015.

Q: What are the specific advantages the FPGA offers for the CAN FD interfaces?

A: The CAN interface "CAN-PCIe/402-FD", for example, is a universal board that was developed for the PCIExpress bus and has one or two CAN FD interfaces in accordance with ISO 11898-2. It uses bus mastering for data transfer to the host storage. This reduces latency during I/O transactions, especially due to the higher data rate and the reduction of CPU load. By using MSI (message signaled interrupts), the PC board can work in hypervisor environments, for example. It also supports high-resolution hardware timestamps.

API (application programming interface) previously used for Classical CAN. If the API remains unchanged for the CAN FD hardware, a migration can take place in three steps.

1. All participants use the CAN FD interfaces as before with the Classical CAN protocol.
2. Conversion of all participants in the data phase with all using a higher bit rate, which with an unchanged protocol will immediately lead to a reduction in latency and bus load respectively to an increase in throughput. The developer must first check whether his protocol requires the sending of RTR frames, since this is no longer supported with CAN FD.
3. Modification/extension of the protocol by transferring more than 8 user data bytes.

In addition to a data throughput gain, the last step facilitates the solution of data consistency problems for transmission of more than 8 user data bytes. Moreover, it is possible to implement protocols, for example in the area of safety and security, which are often difficult or impossible to implement using CAN frames with only 8 user data bytes. Especially in step 3, however, the developer must check whether the desired real-time properties of his implementation (latency times) have still been preserved.

For system integrators: The advantage for system integrators when migrating to CAN FD lies in the fact that the network participants with a Classical CAN controller can initially be exchanged by network participants with a CAN FD controller, even if this takes place in several stages. Due to the backward compatibility, the Classical CAN protocol can still be used for the time being. If there is a need for more bus bandwidth and/or lower latency at a later time, the application can be changed accordingly. Switching back to the Classical CAN state can be done at any time if problems with CAN FD communication arise due to the wiring having been left unchanged. The only limitation to a migration is that a switch to CAN FD can only take place if all network participants support the CAN FD protocol, since Classical CAN controllers will interpret the CAN FD frames as protocol errors.

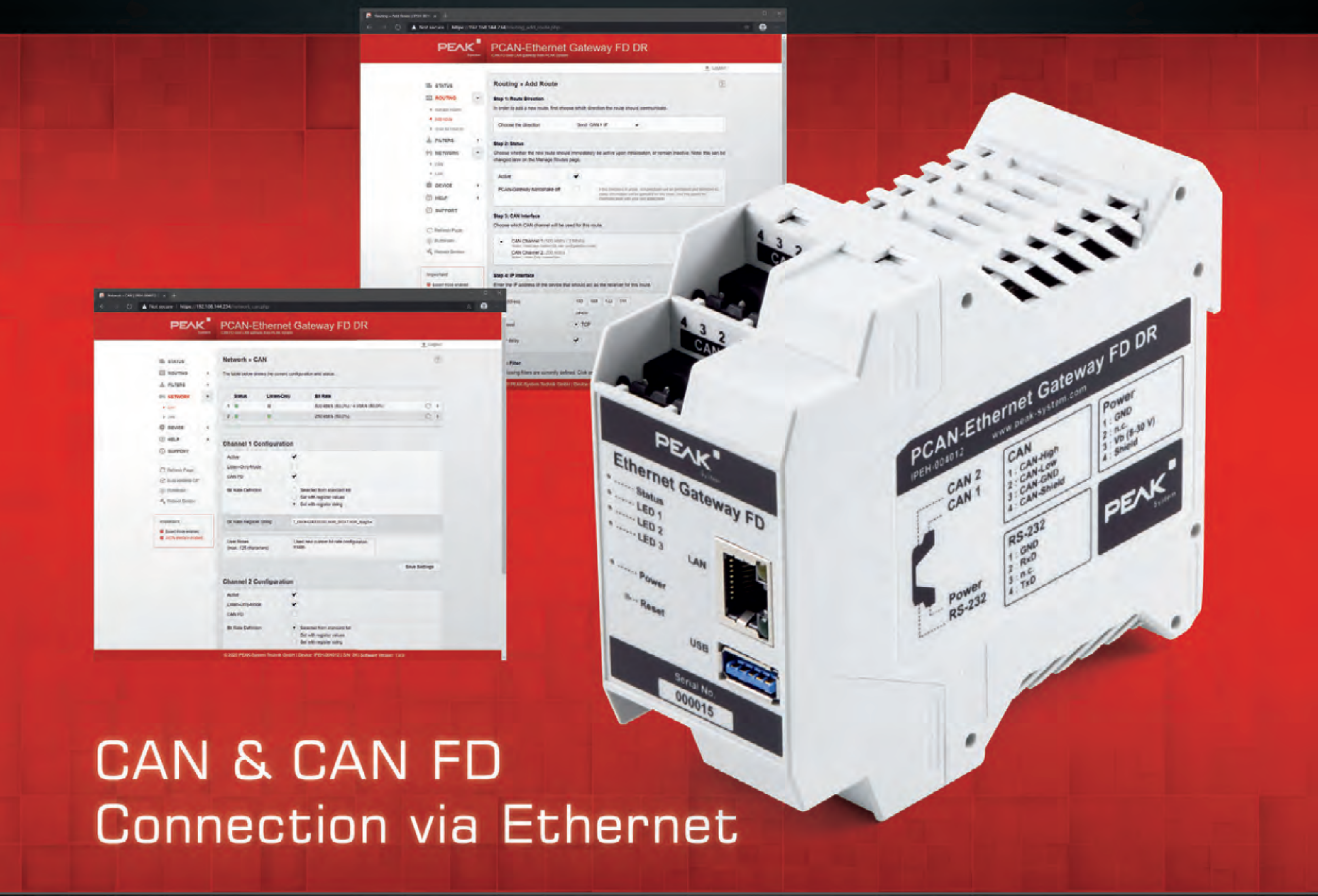
Higher-layer protocols

After the publication of the standard in 2015, several Classical CAN-based higher layer protocols from different industry sectors were adapted to the CAN FD extensions or are now about to be released. Examples are ISO TP and J1939 (automotive industry), CANopen FD (automation), or Arinc 825 (aviation). ◀

Author

Oliver Thimm
ESD Electronics
info@esd.eu
www.esd.eu

This article was originally published in German language in the magazine "Computer & Automation 8/21".



PCAN-Ethernet Gateway FD DR

The PCAN-Gateway product family from PEAK-System is designed for the transmission of CAN messages over IP networks. With a single gateway connected to a CAN bus, users can access the CAN bus using the LAN interface of their computer. In addition, different CAN buses can be connected over IP using this technology. The devices are configured via a convenient web interface. Alternatively, the JSON interface allows access via software.

The PCAN-Ethernet Gateway FD DR is the first model supporting the modern standard CAN FD in addition to classic CAN.

Specifications:

- AM5716 Sitara with Arm® Cortex® M15 core
- 2 GByte Flash and 1 GByte DDR3 RAM
- Linux operating system (version 4.19)
- Two High-speed CAN channels (ISO 11898-2)
  - Comply with CAN specifications 2.0 A/B and FD
  - CAN FD bit rates for the data field (64 bytes max.) from 20 kbit/s up to 10 Mbit/s
  - CAN bit rates from 20 kbit/s up to 1 Mbit/s
- Galvanic isolation of the CAN channels up to 500 V against each other, against RS-232, and the power supply
- Connections for CAN, RS-232, and power supply via 4-pole screw-terminal strips (Phoenix)
- LAN interface
  - Data transmission using TCP or UDP
  - 10/100/1000 Mbit/s bit rate
  - RJ-45 connector with status LEDs
- Monitoring and configuration of the devices via the web interface or JSON interface
- Software update via the web interface
- Reboot or reset of the device to a previous software version with a reset button
- Plastic casing (width: 45.2 mm) for mounting on a DIN rail (DIN EN 60715 TH35)
- LEDs for device status and power supply
- Voltage supply from 8 to 30 V
- Operating temperature range from -40 to 70 °C (-40 to 158 °F)

Further PCAN-Gateway Models:

- PCAN-Ethernet Gateway DR - CAN to LAN gateways in DIN rail casing with Phoenix connectors
- PCAN-Wireless Gateway DR - CAN to WLAN gateways in DIN rail casing with Phoenix connectors
- PCAN-Wireless Gateway - CAN to WLAN gateways in casing with flange and D-Sub or Tyco connectors

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

Achieving correct ESD protection for CAN FD

Connectivity, autonomous driving, and electrification are driving the evolution of automotive wiring harnesses. This results in a growing demand for high-speed data transmission and bandwidth required for ADAS. All of these must be protected from ESD spikes and surges.

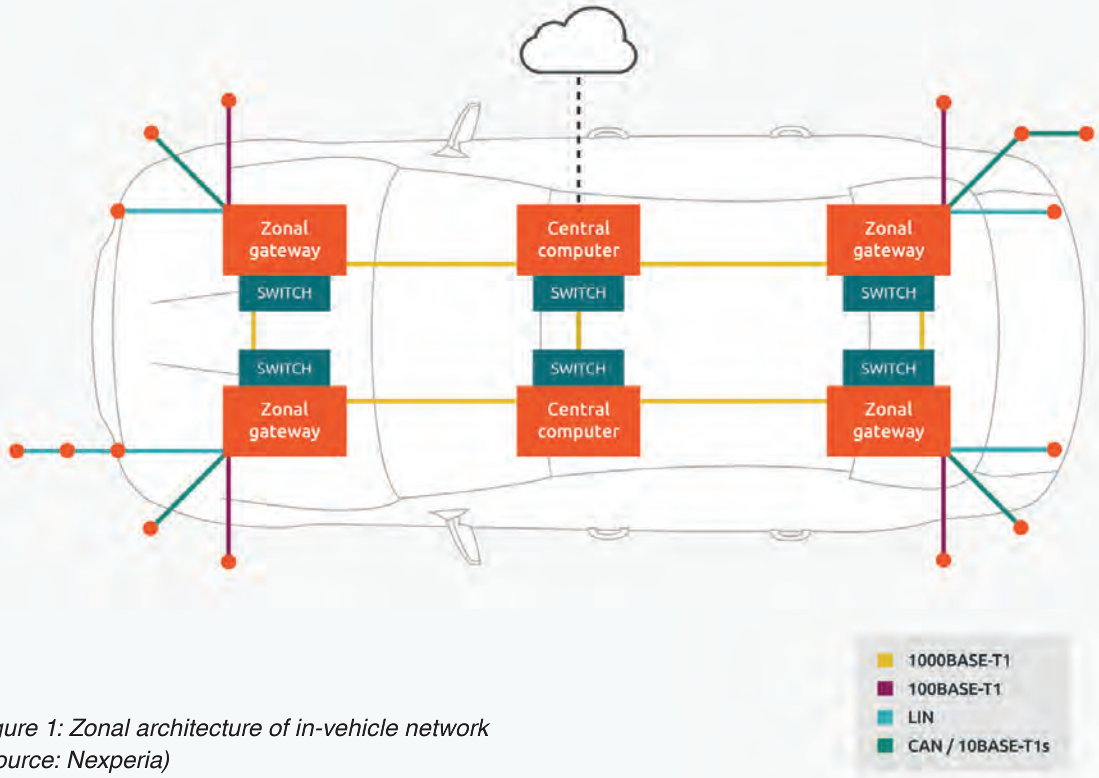


Figure 1: Zonal architecture of in-vehicle network (Source: Nexperia)

Expectations surrounding travel and human interaction with vehicles are changing dramatically. The mega-trends of increased connectivity, autonomous driving, and electrification are driving the evolution of automotive wiring harnesses and fueling the growing demand for high-speed data transmission and bandwidth required for advanced driver-assistance systems (ADAS). Protection of ESD (electrostatic discharge) spikes and surges is essential.

Traditional wiring looms and in-vehicle networks have been undergoing a significant transformation. The classic flat architecture wiring harness is changing to a domain and zonal architecture (Figure 1) with Automotive Ethernet as the backbone. However, peripheral buses still need to transmit more data, so new versions of existing protocols are finding their way into vehicle networks. The CAN network is synonymous with in-vehicle networks but was limited to 1 Mbit/s until the launch of CAN FD, which covers speeds up to 12 Mbit/s and offers critical advantages necessary for future ADAS (advanced driver assistance systems) applications.

2 Mbit/s is the typical implementation limit suitable for many applications that do not require higher data rates. CAN FD uses the same differential signal levels as Classical CAN. The increased data rate is achieved by shortening the dominant and recessive states of a 'send' ▷

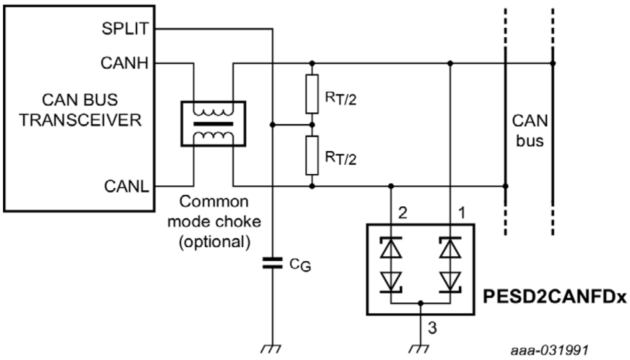


Figure 2: Circuit diagram showing Nexperia's improved PESD2CANFDx ESD protection diode in a CAN FD application (Source: Nexperia)

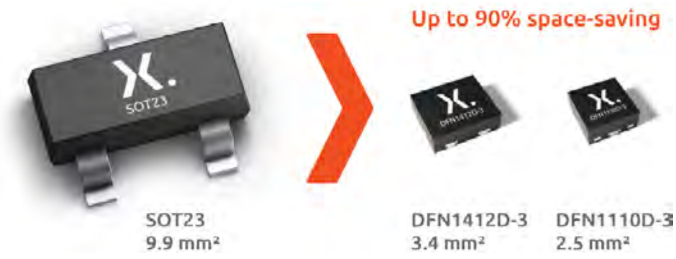


Figure 3: Leadless DFN packages reduce PCB space (Source: Nexperia)

frame. This technique increases the requirements on the physical layer and, as systems become more sensitive with regards to EMC (electromagnetic compatibility) and ESD, this requires additional, discrete ESD protection to improve system ESD robustness to a reliably acceptable level.

Besides OEM (original equipment manufacturer) car makers' requirements, ESD protection devices must fulfil automotive industry standards such as IEC 61000-4-2 and ISO 10605. For Classical CAN and CAN FD, ESD devices must be short-to-battery and jumpstart robust according to ISO 16750-2 (26 V) or internal norms (28 V). Compliance with IEC 62228-3 in combination with a CAN transceiver (emission, immunity: DPI, pulses, ESD) is also necessary. In addition, common requirements for CAN are diode capacitance of 17 pF to 30 pF and for CAN FD 6 pF to 10 pF, as the data speed is greater and signal integrity, as well as capacitance matching are more critical. Therefore, Nexperia has improved its IVN ESD protection diode product range and developed a new generation tailored to CAN FD requirements. The new PESD2CANFDx series comes in different voltage, capacitance, and packages configurations while being twofold AEC-Q101 qualified.

The advantages of leadless packages

Advantages of leadless CAN FD in DFN packages over classic SOT packages are not only significant PCB (printed circuit board) space savings but, especially, the improved signal integrity, which is critical for ESD protection. For signal integrity, routing is a crucial concern. Even though parasitic capacitance reduces the signal quality, at very low capacitances, the routing that is required to connect the package, plays an important role. The most important general conclusion agrees with best-practice signal integrity design: avoid switching layers; avoid using stubs.

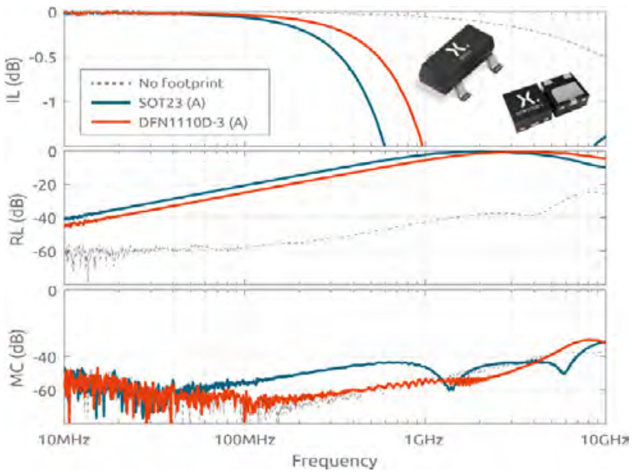


Figure 4: S-parameters comparison of no footprint, PESD2CANFD24V-T and PESD2CANFD24V-QB (Source: Nexperia)

S-parameters are a common way to measure the signal integrity. The parameters shown in Figure 4 are differential insertion loss (IL, S21dd), return loss (RS, S11dd), and differential to common mode conversion (MC, S21dc). The measurements were conducted using a VNA (vector network analyzer) and the system was calibrated to the probe tip, so the traces before and after the footprint are not de-embedded. Figure 4 shows the same routing schemes with a PESD2CANFD24V-T in SOT23 and PESD2CANFD24V-QB in DFN1110D-3, both with maximum diode capacitance of 6 pF. The dashed lines plot the results of straight traces without any footprint. It can be seen that the very similar performance of the empty footprints starts to deviate when devices are mounted. Here, the leads of the SOT23 package appear as stubs and the larger structure inside the package adds greater parasitics. As such, the DFN solution shows better signal integrity especially for insertion loss and common mode conversion compared to the leaded alternative. ◀

Author

Lukas Droemer
Nexperia
lukas.droemer@nexperia.com
www.nexperia.com/esdprotection

People counter enables social distancing

RS Components (RS) and Barth Elektronik unveil People Counter maker project to help social distancing efforts during Covid-19 pandemic. The used display and PLC (programmable logic controller) are CAN-based, while the PLC is also CANopen-capable.

RS, the trading brand of Electrocomponents, a global multichannel provider of industrial and electronic products and solutions, has joined forces with miniature PLC manufacturer Barth Elektronik to develop a maker project that aids social distancing in the effort to prevent the spread of Covid-19. Barth Elektronik provided the idea and the necessary parts, which can be ordered from RS.

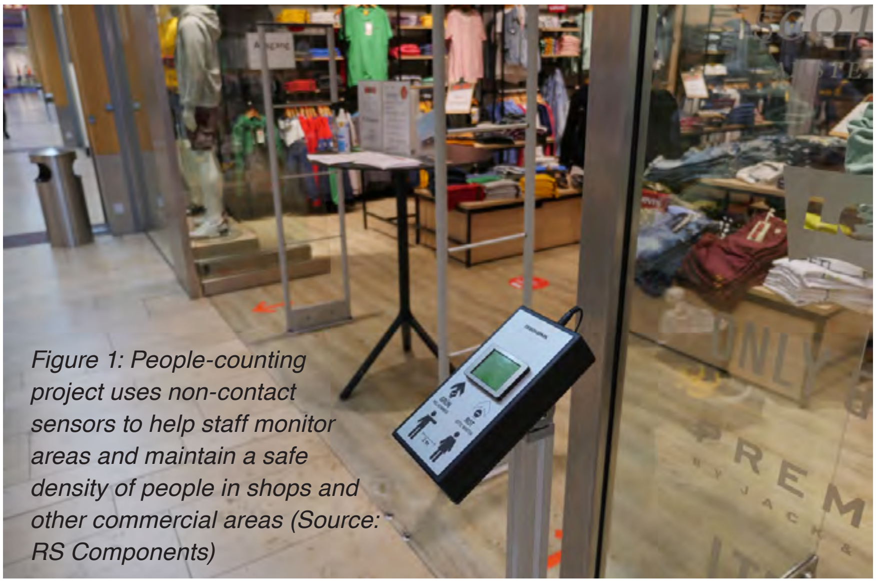


Figure 1: People-counting project uses non-contact sensors to help staff monitor areas and maintain a safe density of people in shops and other commercial areas (Source: RS Components)

The project, called People Counter, can be assembled in less than an hour and records the number of people entering and exiting a room, indicating when it is safe to allow more people to enter while still maintaining the recommended distance from others. This is particularly effective in retail environments where safe social distancing can be difficult to control.

Two photoelectric proximity sensors, or light barriers, detect the direction of movement, while a miniature PLC calculates the number of people in and out of the store in real time. A password-protected CAN touchscreen display is used to pre-set the maximum people limit and also serves as a traffic light system, illuminating green when access is granted and red when access is denied. There is also an audio alert. The miniature PLC processes the data and controls the display.

CAN touch display

The DMA-15 is designed as HMI (human machine interface) for universal measuring, controlling, and regulating applications. The IP65-rated 2,4-inch CAN display allows connection to any Lococube mini-PLC via CAN interface. It's bright 240 pixels x 320 pixels TFT display integrates resistive touch technology. Supply voltage is 7 V_{DC} to 32 V_{DC} and dimensions 69 mm x 50 mm x 69 mm. Both, display design and menu can be selected out of a variety of templates with one single CAN frame.

This feature ensures that no display programming is necessary. The DMA-15 can be fully integrated within the graphical Micon-L Software Suite supporting any Barth mini-PLC with CAN interface. With the open-source programming option the DMA-15 can be user-customized within the powerful Keil µVision software suite. Several open source "C"-programming templates are available for free download. The DMA-15 is also available as customer-tailored OEM (original equipment manufacturer) version within eight weeks. The communication between the mini-PLC and the DMA-15 is ensured via CAN, setting a fixed bit rate of 250 kbit/s.

CANopen mini-PLC

As already mentioned, the CAN display can be directly connected to any Barth mini-PLC providing a CAN interface. In case of the People Counter project, it is connected to the STG-800 PLC. The controller comes with a 32-bit ARM Cortex core and features a rugged CAN/CANopen/J1939/NMEA 2000 interface with intuitive graphical programming capability. The Cortex core provides two high speed event, pulse and frequency counter inputs and one 16-bit PWM output combined with a internal voltage reference for the 12-bit analog inputs. The CAN/CANopen/J1939/NMEA 2000 interface is able to operate in noisy environment and allows the user to connect a variety of network com-

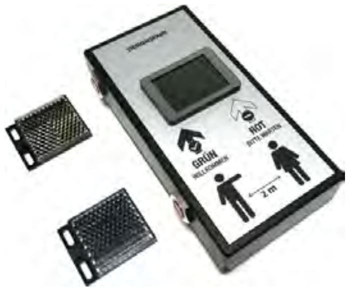


Figure 2: A password-protected CAN touchscreen is used to preset the maximum person limit (Source: RS Components) ▷

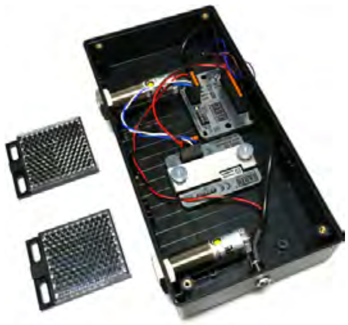


Figure 3: The miniature PLC processes the data and controls the display (Source: RS Components)

ponents to the PLC, explained the manufacturer. The CAN interface communicates with data rates at 50 kbit/s, 100 kbit/s, 125 kbit/s, 500 kbit/s as well as 1 Mbit/s.

The STG-800 does not need any peripheral components to operate. Both, inputs and outputs feature integrated and rugged protection circuits to operate the PLC in harsh environment. Application fields include industrial, automotive, and 12-V/24-V battery-powered applications.

The IP20-rated PLC with dimensions of 60 mm x 45 mm x 11 mm can be programmed using graphical function blocks. This block design meets graphical standards of the latest graphical programming languages. The Micon-L software suite features programming, simulation, and test in one software design tool. The CAN programming option offers a variety of possibilities in industrial, automotive, and maritime applications. The STG-800 can also, just like the CAN display, be programmed as open-source PLC using the Keil µVision software suite.

Project design

The project design is very simple according to RS. All of the parts required are available to purchase from RS, and the full bill of materials, 3D data, software, and manuals can be downloaded from the RS Designspark engineering website. A short video also gives instructions on how to build the system.

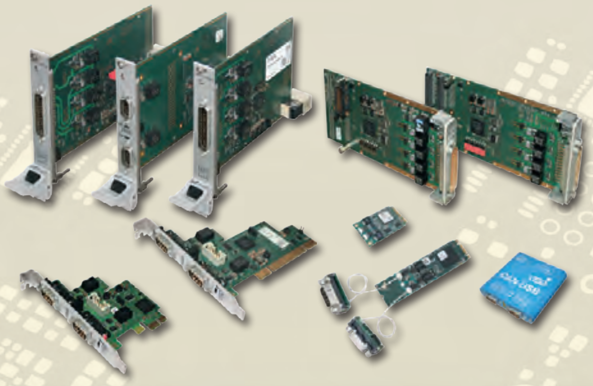
Daniel Barth, CEO of Barth Elektronik, who devised this project, commented: “The idea came from the challenge that many businesses currently face when restricting the number of people in shops. Maintaining a reasonable maximum can reduce the likelihood of the virus spreading further through human contact. It was important to find a precise, contactless solution that could protect public health, while avoiding the costs associated with employing extra staff to monitor numbers manually.”

Mike Bray, VP of Innovation at RS, added: “This is a simple project that could have a huge, positive impact on the way retailers help protect customers from Covid-19 while they are out shopping. We would encourage any makers keen to help combat the virus to look at this project and consider how it could support businesses in their area, and then perhaps help those retailers to implement it. Makers really can make a difference.” ◀

cw

Source

RS Components
info@rs-components.com
de.rs-online.com



Generic CAN (FD) security requirements

This article gives an insight into the CAN (FD) security issue as asked by several companies participating within the CiA's (CAN in Automation) interest group IG safety and security.

In the past 5 years we have been reporting about various security threats and solutions for CAN and CAN FD. It is interesting to see that security requirements can differ quite a bit depending on the application, and that therefore the solutions developed also differ. An access control system has a high focus on authentication but might not care about encryption. A custom high-tech machinery in a somewhat closed housing might not worry about authentication but more about protecting the intellectual property and encryption of the data exchanged, making re-engineering more difficult. From the security viewpoint, the toughest applications are those where the system owner or user is considering the security threat. For example, when an owner is trying to bypass a machine's safety limitations such as a maximum weight, speed, or RPM (rotations per minute).

Usually, adding security to the CAN (FD) communication level is not sufficient, a more detailed view at the entire system is required to address all potential attack vectors. Nevertheless, secure CAN (FD) communication is an important "piece of the security puzzle" in more and more applications. As is, CAN (FD) systems are too easy to manipulate once an attacker has access to the CAN (FD) wiring. Adding a sniffer or even a contactless CAN interface allows recording and replaying of CAN frames, often allowing full control of a system. If such access is gained remotely because of a weak gateway, multiple systems can be at risk of misuse.

Current developments

There are currently multiple working groups at CAN in Automation (CiA) addressing security issues. The SIG (special interest group) CAN XL TF Security works on adding security to CAN XL (the third CAN generation), directly on the data link layer so that it can become part of the hardware, the CAN XL interface.

In September 2021, the IG safety and security decided to also review security options for CAN and CAN FD. The Hochschule Offenburg (Institute for reliable Embedded Systems und communication electronics) and Embedded Systems Academy (Emsa) currently work together on a proposal that defines a generic security layer for secure group communication in lightweight broadcast networks such as CAN (FD).

Being of general interest, the approach is pursued by defining the generic objects, parameters, and roles required in such a way, that they can be mapped to multiple network technologies. Although optimized for CAN and CAN FD (also covering CANopen and CANopen FD) the methods could also be mapped to I2C or EIA-485 based communication.

Key requirements

The key elements and requirements of the proposal are:

- The underlying communication system exchanges communication blocks with data and meta data (such as a CAN frame using a CAN-Identifier, DLC (data length code), and data field).
- The underlying communication system shall have a method to identify devices (e.g. using a node ID).
- To secure these communication blocks a security object is added to or associated with them.
- A manager role supervises the secure communication and initiates key refresh cycles.
- A synchronized date and timestamp with one-millisecond resolution is used for uniqueness and to prohibit replay attacks.
- If required, ALL communication blocks can be secured.

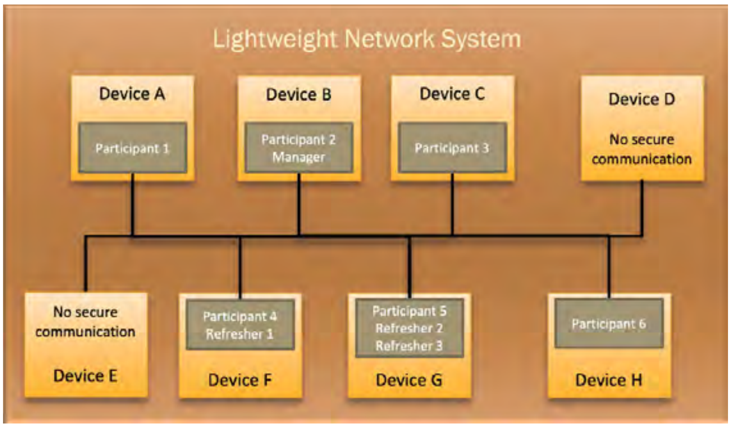


Figure 1: The various security roles that need to be assigned in the network system (Source: Emsa)

Figure 1 illustrates the various roles that need to be assigned in the network system. All devices that need to be able to produce or consume secure communication blocks need to implement the "participant role". One device must implement the "manager role" and a total of three "refresher roles" are required. These are helpers to the manager in the current communication key refresh cycles.

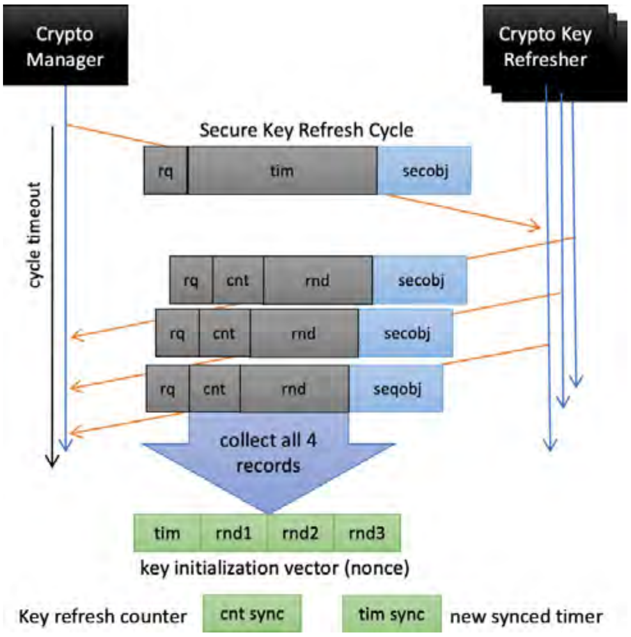


Figure 2: Basic elements of the current communication key refresh cycle (Source: Emsa)

The basic elements of the current communication key refresh cycle are shown in Figure 2. The manager role initiates the key refresh cycle and shares the current date and time value. The three refresher roles reply with an updated key refresh counter and a random value. All these messages are secured with the security object using a cryptographic checksum based on the previous key.

Once the cycle is completed, all participants build a nonce (number used once) using the timer and the random values. The nonce and the current session key is then used to generate a new communication key used to secure all communication blocks until the next refresh cycle. In addition, all participants synchronize their timers and key refresh counters.

Security object

Let us have a closer look at the security object used to protect each communication block. As a minimum, the security object contains the following data:

- The truncated timestamp (such that participants can restore the full value)
- A truncated key refresh counter (to determine which key is currently in use) and
- The cryptographic checksum for authentication

If and how many bits are used for the individual values is specified by the mapping document profiling the security layer for a specific network technology. For CAN FD, the security object could be made part of the data field, requiring only limited truncation. For CAN it could be part of the CAN-Identifier (using 29 bits instead of 11 bits) or located in an additional CAN frame if no other options are available.

Limitations

The effectiveness of the generic security layer depends on the specific cryptographic methods chosen and how its objects are mapped to the underlying communication system. The security offered provides a "secure grouping" or "point-to-multipoint" security. For each participant the security ends in the software layer implementing the participant role.

Receiving a properly authenticated communication block means that the participant determines that the transmitter sent the exact data received and that it was not manipulated during transmission or that it did not originate from an alternate source (such as an additional device injecting communication blocks to the physical media).

However, it cannot guarantee that the data was not manipulated on higher layers within the transmitting device. This could be the case if the application in the transmitter device is compromised, or sensors connected have been manipulated.

When and how the initial primary keys are installed is application-specific. Often these would be installed on the system integration level when powering up a network for the first time. The authors recommend that a change of the primary keys is only allowed through a public key certificates method.

Outlook

The detailed proposal will be submitted to the CiA and IG safety and security, which will then review it. A first prototype implementation for CANopen FD is expected to be available in quarter 1, 2022. ◀

Authors

Olaf Pfeiffer
Emsa (Embedded Systems Academy)
info@esacademy.com
www.esacademy.de
Andreas Walz
Hochschule Offenburg
info@hs-offenburg.de
www.hs-offenburg.de

Matching CANopen drives for DC micro-motors

Small and powerful DC-motors are critical to the development of highly-integrated systems. Making the right choice is fundamental for reliable operation.

Figure 1: Micro-motors have especially stringent requirements on motion controllers (Source: Faulhaber)

The DC micro-motors are a driving technology in many different sectors, from medical and laboratory technology to aerospace, robotics, optics, and photonics as well as industrial machinery and equipment in general. But the small motors only mature to an application-relevant drive or positioning system when combined with other components, such as gearheads, encoders, and motion controllers. Making the right choice is fundamental for reliable operation. All components must be compatible with the motor and meet its requirements. In the worst case, selecting the wrong controller can destroy a motor in no time.

Fundamental questions

When selecting a suitable motion controller for a drive system, it is important to answer a few questions first. For example, the movements that are to be carried out must be established, and it must be defined what this means in terms of motor control requirements. Is the drive working continuously or in start-stop mode? Is precise positioning required? What type of load will the drive be moving? What are the load cycles? Is a gearhead required? Which motor is best suited for the application? The motion controller is then selected based on the answers. And it may get interesting, because not every motion controller suits every motor. DC-micro-motors in particular have unique requirements due to their design.

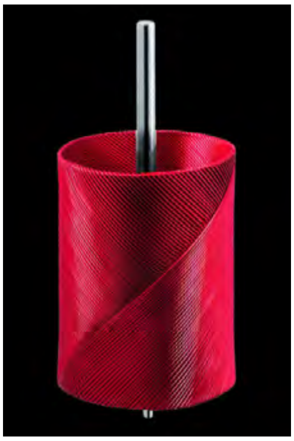


Figure 2: At the heart of the DC miniature and micro-motors is the patented, self-supporting, coreless rotor coil with skew-wound design, which rotates around a fixed magnet (Source: Faulhaber)

Risk of overheating

At the heart of the DC miniature and micro-motors from Faulhaber is the patented, self-supporting, core-less rotor coil with skew-wound design and brush commutation, which rotates around a fixed magnet. This motor is also often referred to as a bell-type armature motor due to its look. Its design not only has many practical benefits, it also influences the selection of the motion controller.

No cogging torque forms due to the symmetrical air gap, which enables precise positioning and excellent speed control. The ratio of load to speed, current to torque, and voltage to speed is linear. And as almost the entire motor diameter can be used for the winding, the motors achieve higher power and torques for their size and weight compared with conventional designs. The rotor's low inertia also guarantees an extremely low electrical time constant. The motors can thus be operated very dynamically and heavily overloaded. Triple continuous torque in overload mode is quite common and easily possible for servo applications, as long as the temperature of the motor winding is monitored. But motors with a diameter of only 22 mm or less do not have an integrated temperature sensor. There simply is not enough space. So, if just any controller is connected to a micro-motor, in the worst case the coil may be completely burnt up before any heat is even noticed on the outside.

Possible solution

Such problems can be avoided with motion controllers from Faulhaber, which were developed for the requirements of mini- and micro-drives and tested under real operating conditions. They estimate the winding temperature for the respective motor type using models of varying complexity. This means that the full dynamic range of the motor can be exploited, for example for fast positioning processes. The current is also limited before the winding overheats. The parameters required are transmitted to the drive controller with the “Motor selection dialogue” of the company's Motion Manager software.

▷

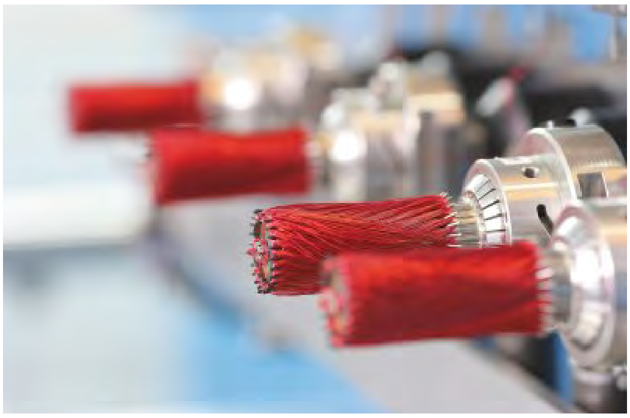


Figure 3: Motors with a diameter of 22 mm or less do not have an integrated temperature sensor. Without a matching motion controller, the coil may be burnt up before any heat is noticed on the outside. (Source: Faulhaber)

Additional information about thermal integration in the application can be used in the models that are stored in the controllers for further improvement. How well is the motor cooled? Is it necessary to limit power due to high ambient temperatures? Is a gearhead and encoder used? With such additional information, maximum motor power can also be used with, e.g. a drive that works cyclically in a climatic chamber, in that the motor controller keeps track of the ambient temperature parameters from the climatic chamber control within the models stored. The same applies if the load cycles are known. The motor can then often be smaller in design, which is an advantage especially when used in mobile devices.

Due to the low electrical time constant, which benefits dynamic processes, additional losses may occur due to the pulse width modulation (PWM) that is common in drive controllers. The typical electrical time constants of manufacturer's cbell-type armature motors are about 10 μs. For PWM frequencies below 50 kHz, the continuous torque specified in the data sheet is no longer achievable in many cases, or the motor may overheat. That is why it is important that the PWM frequency is sufficiently high when selecting a motor controller. For Faulhaber motion controllers, this is

Figure 4: The motion controllers 'estimate' the winding temperature of the respective motor type using models. The required parameters are transmitted to the drive controller using the Motion Manager software. (Source: Faulhaber)

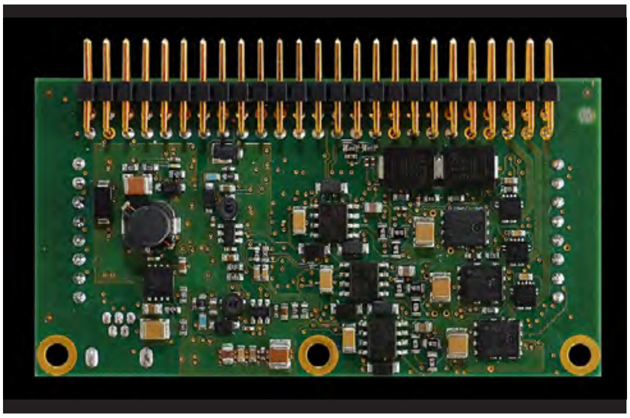


Figure 5: The MC 3001 B/P motion controllers are suited to smaller servo drives in terms of size and current measurement resolution (Source: Faulhaber)

between 78 kHz to 100 kHz, depending on the type. Due to the type of modulation, up to 200 kHz act on the motor, which suits the requirements of the small motors.

Miniaturized unhoused motion controllers

The motion controllers of the MC V3.0 family, which have been tried and tested for years, have limited usability for the company's micro-motors due to their size and the resolution of the integrated motor current measurement. This is where the recent MC 3001 B/P comes in: The first motion controller that is optimized for smaller servo drives, both in terms of its size and the resolution of the current measurement. With a maximum supply voltage of 30 V_{DC}, the motion controller sizing 16 mm x 27 mm x 2,6 mm achieves a continuous current of 1 A and a peak current of 5 A. At lower supply voltages, such as in 12- V_{DC} systems, continuous currents of up to 2 A can also be easily achieved. At the same time, they do not compromise on function compared with their large family members. The I/O options, and the encoder interface are the same as the rest of the product family. CANopen, USB, EIA-232, and optionally Ethercat are available as communication interfaces.

The controllers are designed for operation as CANopen devices with NMT (network management) server functionality. Via CANopen, they can be combined with a number of higher-level managing systems. Stand-alone operation using integrated sequence programs is possible. The devices support the profile position, profile velocity, and homing operating modes according to the CiA 402 profile for CANopen drives and motion controllers. CiA 402 is internationally standardized in IEC 61800-7-2/-3 and is further developed by CAN in Automation (CiA). Controllers' configuration can be performed with the Motion Manager software (version 6.8 and higher). Supported bit rates (up to 1 Mbit/s) and node-IDs are set via the CANopen layer setting services (LSS) as specified in CiA 305. Further, an SDO (service data object) server, four RPDOs (receive process data objects), and four transmit PDOs (TPDOs) with dynamic mapping are provided.

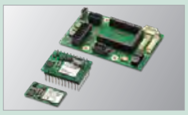
The controllers are available in two variants: The model with flat board-to-board connectors (MC 3001 B) is suitable when several drive controllers are combined on one carrier card. The MC 3001 P variant features a plug connector with a 2,54-mm grid over three sides. It is designed to be integrated into thecustomer's configuration, e.g. for multi-axis applications in laboratory automation. Thus, Faulhaber offers motion controllers for its smallest DC drives, matched to the micro-motors in terms of size and function. ◀

Author

Dr. Andreas Wagener
Faulhaber
redaktion@faulhaber.com
www.faulhaber.com

CAN Newsletter Online: CANopen drives

In the CAN Newsletter Online, CiA continuously informs about the recent drives and motion controller developments. A variety of drives with CANopen connectivity are available on the market:



CANopen motion controllers

Unhoused drives for space-limited applications

Miniaturized unhoused CANopen motion controllers can be embedded in small motors deployed in robot arms and other compact applications. These are available from diverse manufacturers.

Read on

Motion control

Servo drive series with CANopen

Celera Motion has announced the addition of the Capitan series to their line of Ingenia servo drives. The series offers CANopen communication with a bus latency down to two cycles.

Read on

Several applications

CANopen actuators

The actuators from ISP System are designed for integration of mechanic and electronic hardware. They are suitable for aeronautics, defense, railways, medical, and spatial devices. They communicate via CiA 301 CANopen application layer and general communication profile.

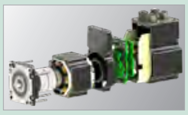
Read on

Servo-drive cylinder

For in-door, out-door, and under-water use

Ultra Motion's Servo Cylinders are available with CANopen and J1939 connectivity. The CANopen variant implements the CiA 402 CANopen device profile for drives and motion controllers.

Read on



Stepper motors

With integrated CANopen drive functions

JVL (Denmark) offers the Servostep integrated stepper motors with an updated implementation of the CANopen protocol.

Read on

CAN data logger case studies

Figure 1: A Ducati Diavel, the focus of Mr. Cobb's reverse engineering efforts (Source: CSS Electronics)

CSS Electronics offers complete CAN data logging solutions. Here are three data logging case studies from more than 40 provided on the company's website.

CSS Electronics (Danmark) develops CAN data loggers and sensor-to-CAN modules. The two-channel CANedge CAN/LIN data loggers (Figure 2) are used by automotive OEMs (original equipment manufacturers) in CAN (FD), CANopen, J1939, OBD2, NMEA 2000, and LIN applications. CANedge1 records data to an industrial SD card, while the CANedge2 also enables automatic log file upload via Wifi/4G to the end user's server. The recent CANmod sensor-to-CAN modules include the CANmod.gps and CANmod.temp. The first is a GPS-to-CAN module with a 3D IMU (inertial measurement unit). The second is a four-channel thermocouple-to-CAN sensor module. An input module with eight analog channels is under development. In addition, CSS offers three widely-used DBC files (data base CAN), including J1939 DBC, NMEA 2000 DBC, and OBD2 DBC. The files make it possible to decode CAN data to human-readable form.

The company's software tools are free and open source. Tools for the CANedge include the MF4 converters for turning MF4 log files into other formats (CSV, ASC, TRC, etc.). Another example is the Asammdf GUI (graphical user interface) for general-purpose analysis, DBC decoding, and plotting. Data from the CANedge can also be processed via the free Python API (application programming interface) and integrated with telematics dashboards (e.g. Grafana) for visualization. The MF4 data can be also processed in 3rd party tools such as the Matlab Vehicle Network Toolbox.

CAN data logger use cases span heavy duty, automotive, agriculture, electric vehicles, and marine industries. Applications include trucks, buses, cars, tanks, drones, submarines, and more. Offline logging, USB streaming, Wifi, and cellular telematics are the possible data acquisition options.

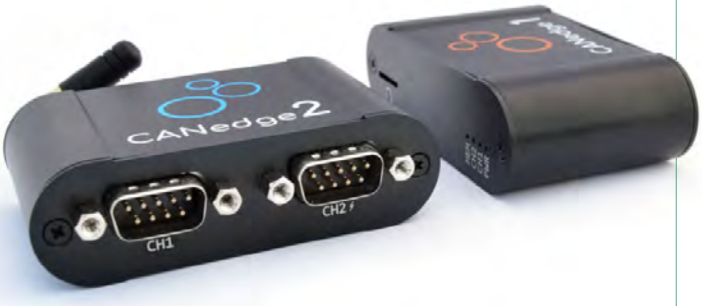


Figure 2: CANedge is a series of two-channel CAN/LIN data loggers (Source: CSS Electronics)

CAN dashboards and telematics for military UGV

Havelsan (Turkey) offers end-to-end technology solutions within defense, simulation, IT, homeland security, and cybersecurity. The company needed to record and collect data from unmanned ground vehicles (UGV). Normal data acquisition systems were too heavy (and expensive) for UGVs. Adding external sensors was not feasible. Hence a compact CAN data logger was required to collect all the data for analysis.

Realized solution: The CANedge2 Wifi CAN logger was deployed to measure the general vehicle health as well as to benchmark different scenarios based on data changes. Havelsan installed the logger on the UGV, where it collected data during field operation to the SD card. When the UGV returned to the workplace, the data logger came into the range of a stationary Wifi router and automatically offloaded the log files to Havelsan's server. For some tests, Havelsan deployed the logger with a 4G cellular network router on the vehicle. Grafana/Influx dashboards software tools were used for visualizing of CAN data in the browser. If abnormal data patterns were detected, the relevant MF4 log files (found via CANcloud) could be analyzed in detail. This was possible via the Asammdf GUI (graphical user interface) using the appropriate DBC file.

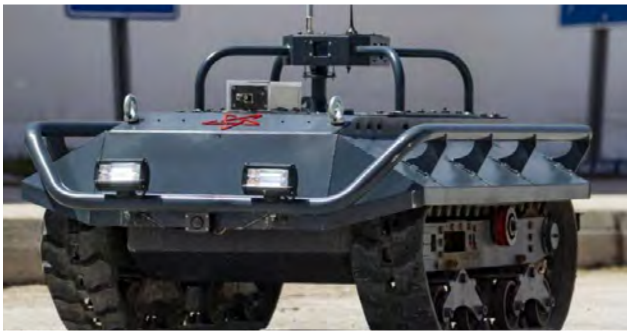


Figure 3: Havelsan's CAN-based unmanned ground vehicle (Source: CSS Electronics)

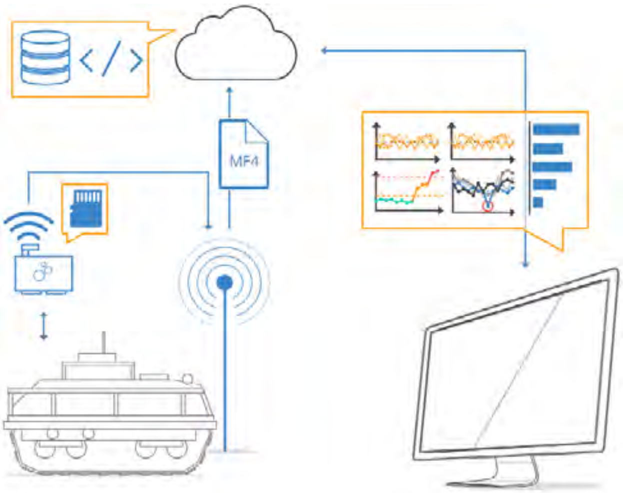


Figure 4: CANedge2 automatically uploads MF4 log files when the UGV gets within the Wifi range (Source: CSS Electronics)

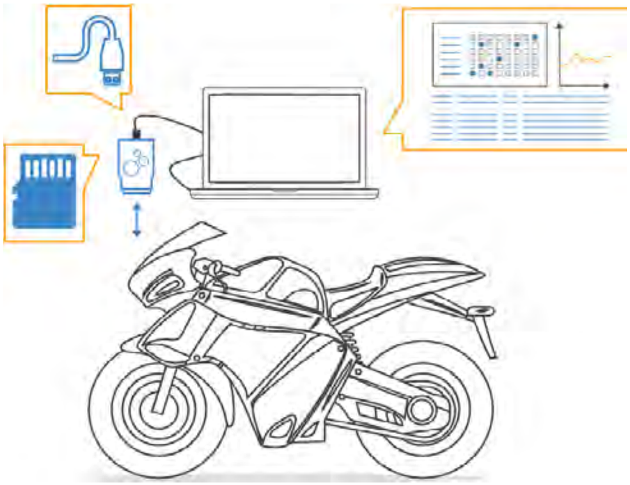


Figure 6: CL2000 enables real-time streaming of CAN data from/to SavvyCAN software tool (Source: CSS Electronics)

Benefits and choosing reasons: Sezer Kiral, Systems Engineer at Havelsan, explained: “The device helps us increase test/evaluation capability and enables us to take immediate action in response to technical parameters of the vehicle. The CANedge2 is an autonomous way to collect, transfer, and analyze data. Set it up - and watch the data from your office." Regarding the CANedge choice, he answered: “We were using Vector tools in the previous main battle tank project. During our search for an alternative and easy solution we found the CANedge. If we have any questions, the technical support is so fast and helpful.”

Reverse engineering a motorcycle's CAN

Thomas Cobb (a private person) used the CL2000 logger for CAN reverse engineering. Thus, he has been one of the first testers of the CSS’ recent CLX000-SavvyCAN integration. The challenge for Mr. Cobb was to tune his Ducati Diavel 2015 motorcycle. To do so he needed to log CAN data, decode the messages, and make changes based on real data.

Realized solution: Mr. Cobb reported: “Over all it was a steep learning curve when I started with Wireshark, but seeing the real-time data was great for identifying the relevant messages. SavvyCAN was my preferred software tool (also before it was supported by CSS Electronics), even if there was originally no support for a live data connection. I would log data and play it back in SavvyCAN, and the graphs and flow of data made it possible to slowly identify and interpret the changing bytes and bits. Now we have a CLX000-SavvyCAN integration that works great! Further, support has been great and any questions get answered very quickly.”

Benefits and choosing reasons: The mentioned tools have allowed Mr. Cobb to learn more about CAN data and to appreciate the work that goes into the reverse engineering process. Further, he has managed to decode most of the important messages of interest. “The CL2000 is compact, feature rich, and highly configurable. I chose the CL2000 as it had good reviews, the price was reasonable, it offered plug-and-play features, it required minimal configuration, and came with a real-time clock (RTC). Now, I often look at the CANedge ...”, added Mr. Cobb.

J1939 analysis for ship telematics

Vives is the largest university of applied sciences in West Flanders, Belgium. It has campuses in five student cities: Bruges, Ostend, Kortrijk, Roeselare, and Torhout. The university participated in a European funded project ISHY (implementation of ship hybridization) that wants to achieve 50 % of CO_2 reduction on medium ships. The project researches the possibility to use fuel cells, battery ▷

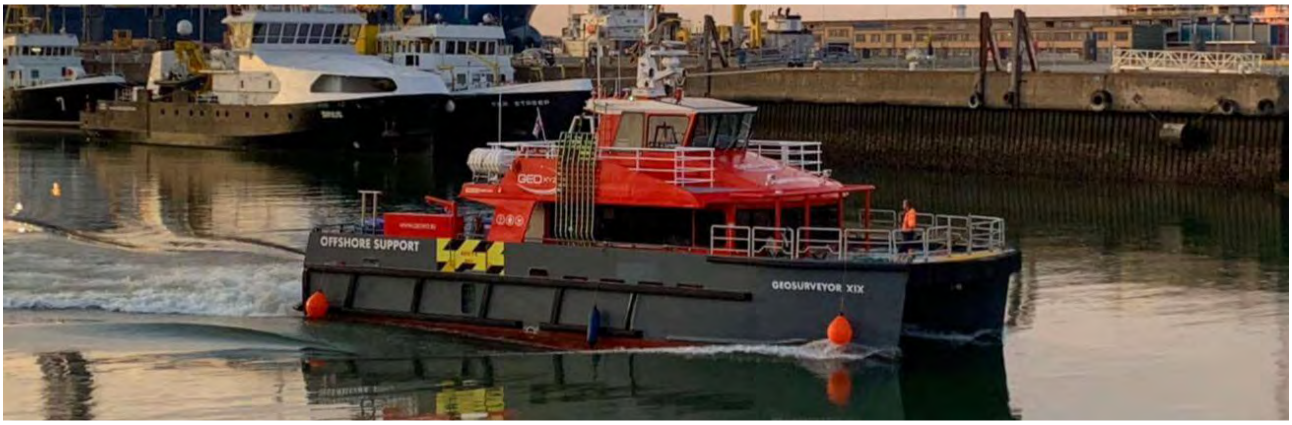


Figure 5: Vives recorded data from the GEOxyz maritime vessel (Source: CSS Electronics)

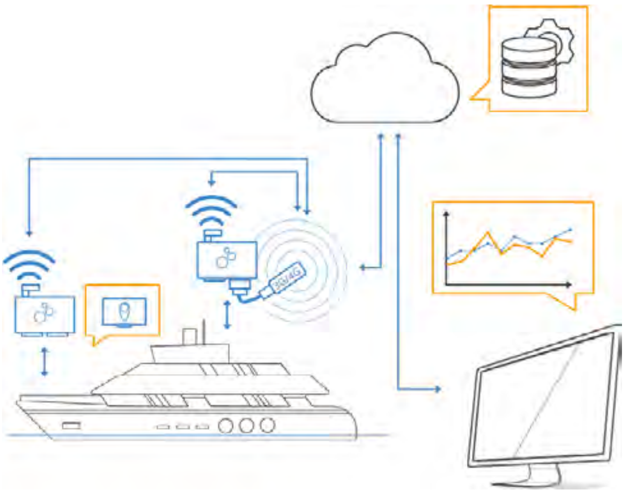


Figure 7: Two CANedge2 units upload MF4 log files from their SD cards via 4G to an AWS S3 server when connectivity is available (Source: CSS Electronics)

supply, and hydrogen in ships in place of heavy fuels. It was required to know how much power the combustion engines deliver in order to improve the power supply possibilities.

Realized solution: To calculate the size of the alternative power supplies exactly the project members needed to know how much power the combustion engines deliver at any time. On the in-vessel J1939 network the messages EngSpeed (engine speed) and ActualEngPercentTorque (actual torque in %) had to be monitored and logged. With those two parameters it was possible to make a power profile of the combustion engine. The boat has two engines (port and starboard) so one CANedge2 device was used for logging of parameters on those two networks. Further, the researchers wanted to know why the engine uses the amount of power it does. For this, a third network was set up and the data was logged by a second CANedge2 device. On this network a GPS (global positioning system) receiver, IMU (inertial measurement unit), wind speed sensor, wind direction sensor, wave sensor (and more) were implemented. The two CANedge2 units uploaded the MF4 log files from their SD cards via the 4G mobile network to an AWS S3 server. Finally, the data could be displayed on a monitor in the office using the Grafana dashboard software tool.

Benefits and choosing reasons: Arne Depuydt, Researcher ISHY and Lector of automotive technology itemized the benefits: “The benefits of this logger are the configuration simplicity and the 4G connectivity. In which the device also makes a difference is the data transportation to a third-party S3 server and not a server of the logger manufacturer. The reason is that AWS uses much better technologies than a manufacturer of logging devices can make.”

He also explained: “Last year we tested ten CAN logger devices and the CANedge2 has delivered good and stable results. It does not have the largest number of configuration settings (e.g. on-board database decoding, pull data over the air with a button, gateway, I/Os, GPS, etc.), but in return it is powerful in that it lets us set up a new installation quickly. The documentation and service enable non-IT people to set everything up - and that is a big plus! We have worked with big companies that deliver their products to huge car companies, with similar products (but more expensive) - and they do not have such a good service and documentation.” Interested parties are also welcome to contact Mr. Depuydt to get trainings on how to use the CANedge2 and set up dashboards. ◀

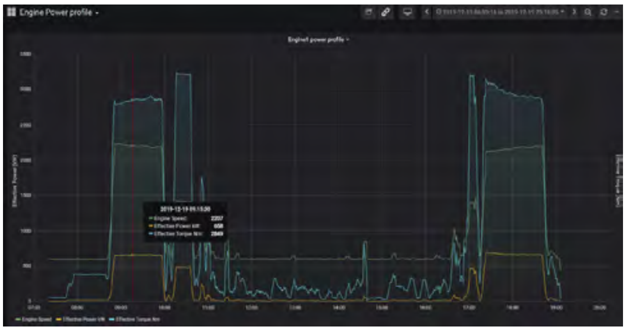


Figure 8: Vives deploy a Grafana telematics dashboard for visualization of their data (Source: CSS Electronics)

Author

Martin Falch
CSS Electronics
contact@csselectronics.com
www.csselectronics.com

CAN in Automation

The non-profit CiA organization promotes CAN and CAN FD, develops CAN FD recommendations and CANopen specifications, and supports other CAN-based higher-layer protocols such as J1939-based approaches.

Join the community!

- Initiate and influence CiA specifications
- Get credits on CiA training and education events
- Download CiA specifications, already in work draft status
- Get credits on CiA publications
- Receive the exclusive, monthly CiA Member News (CMN) email service
- Get CANopen vendor-IDs free-of-charge
- Participate in plugfests and workshops
- Get the classic CANopen conformance test tool
- Participate in joint marketing activities
- Develop partnerships with other CiA members
- Get credits on CiA testing services

For more details please contact CiA office at headquarters@can-cia.org

www.can-cia.org