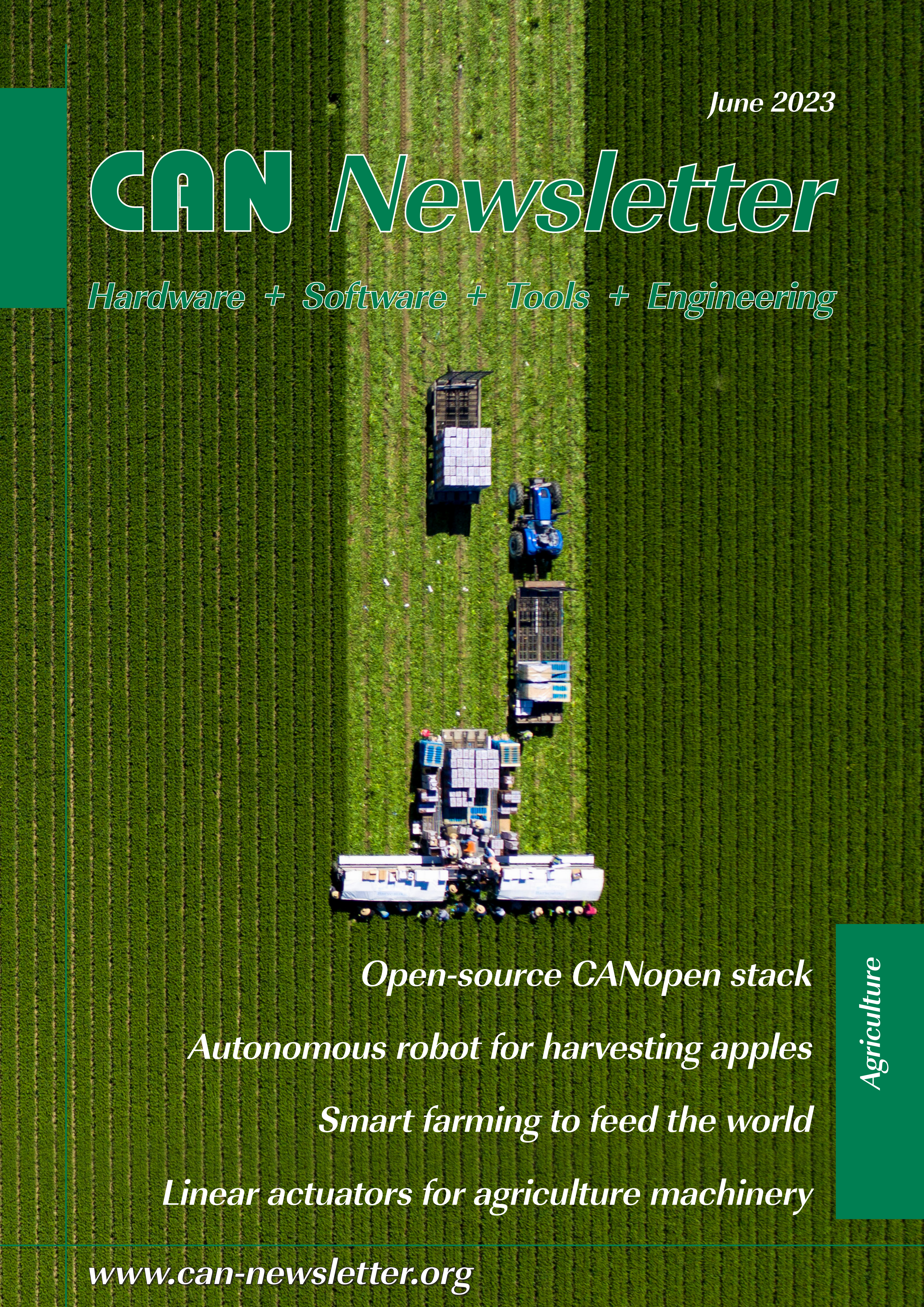
June 2023

CAN Newsletter

Hardware + Software + Tools + Engineering



Agriculture

Open-source CANopen stack

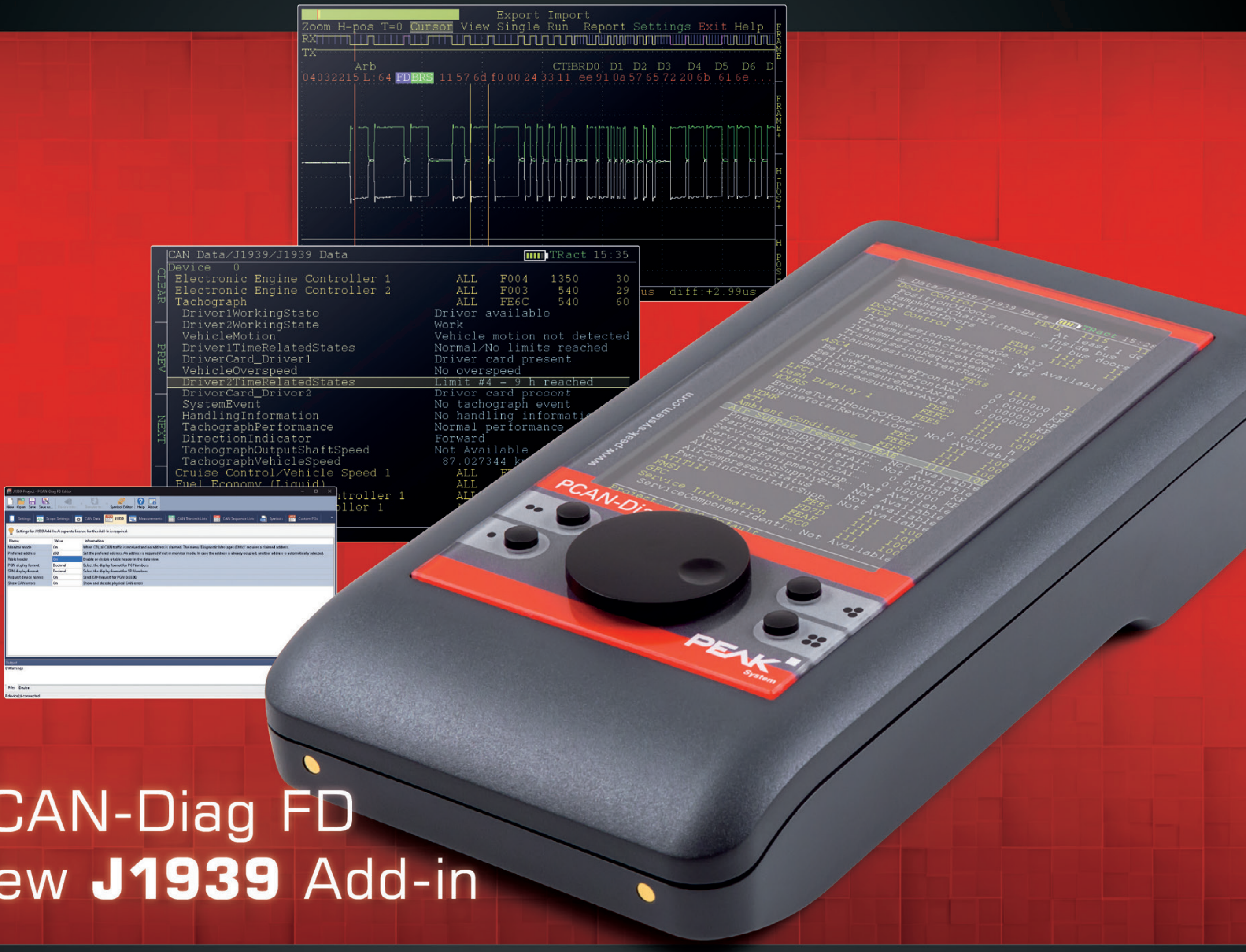
Autonomous robot for harvesting apples

Smart farming to feed the world

Linear actuators for agriculture machinery

www.can-newsletter.org

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



```
Export Import
Zoom H-pos T=0 Cursor View Single Run  Report Settings Exit Help
RX
TX
      Arb                           CTIBRD0  D1  D2  D3   D4  D5  D6  D
04032215 L:64 FDBRS 11 57 6d f0 00 24 33 11  ee 91 0a 57 65 72 20 6b 61 6e ...
```

```
CAN Data/J1939/J1939 Data                              TRact 15:35
Device    0
 Electronic Engine Controller 1            ALL   F004   1350     30
 Electronic Engine Controller 2            ALL   F003    540     29
 Tachograph                                ALL   FE6C    540     60
  Driver1WorkingState                     Driver available
  Driver2WorkingState                     Work
  VehicleMotion                           Vehicle motion not detected
  Driver1TimeRelatedStates                Normal/No limits reached
  DriverCard_Driver1                      Driver card present
  VehicleOverspeed                        No overspeed
  Driver2TimeRelatedStates                Limit #4 - 9 h reached
  DriverCard_Driver2                      Driver card present
  SystemEvent                             No tachograph event
  HandlingInformation                     No handling informati
  TachographPerformance                   Normal performance
  DirectionIndicator                      Forward
  TachographOutputShaftSpeed              Not Available
  TachographVehicleSpeed                   87.027344 k
 Cruise Control/Vehicle Speed 1            ALL
 Fuel Economy (Liquid)                     ALL
```

PCAN-Diag FD: CAN & CAN FD Diagnostic Device

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

- High-speed CAN connection (ISO 11898-2)
  - Complies with CAN specifications 2.0 A/B and FD
  - CAN bus connection via D-Sub, 9-pin (CiA® 106)
  - Switchable CAN termination for the connected bus
- Power supply via rechargeable batteries or a supply unit
- Clear listing of the CAN traffic with various information
- Transmitting individual messages or CAN frame sequences
- Configurable, readable CAN ID and data representation
- Recording of incoming CAN messages
- Playback of trace files with optional loop function
- Measurement of the CAN bus load and termination
- Voltage check at the CAN connector for pins 6 and 9

Oscilloscope

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

Now available with J1939 support

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

Features

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

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

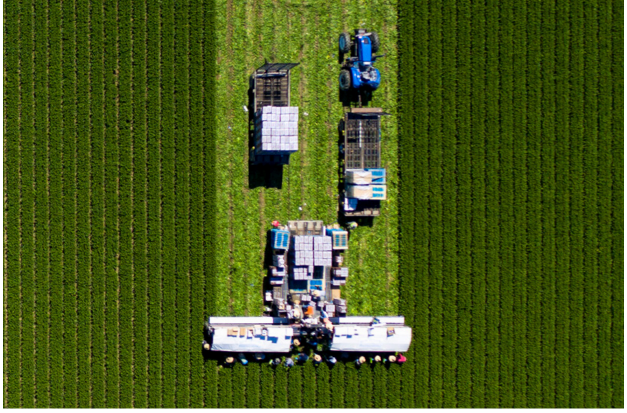
www.peak-system.com

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

PEAK-System Technik GmbH

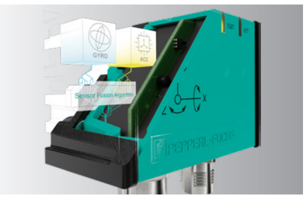
Otto-Roehm-Str. 69, 64293 Darmstadt, Germany
Phone: +49 6151 8173-20 - Fax: +49 6151 8173-29
E-mail: info@peak-system.com

Table of contents



Agriculture

Cybersecurity



Devices

Engineering

Brief news

Imprint

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

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

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

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

Layout
Nickel Plankermann

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

Downloads March issue
(retrieved May 22, 2023)
4542 full magazine

The views expressed on CAN Newsletter magazine are not necessarily those of CiA e. V. While every effort is made to achieve total accuracy, neither CiA e. V. nor CiA GmbH can be held responsible for any errors or omissions.

CAN in agriculture

Agriculture communities were developed about 10 000 years ago. From the beginning, tools and equipment have been used to cultivate, harvest, and process plants. Also, the livestock production dates back about 10 000 years, when humans started to domesticate sheep. Domesticating animals has been supported by tools and equipment for a very long time, too.

Nowadays farming is supported by a lot of machines, stationary ones as well as mobile ones. The introduction of robots is still an ongoing topic. Of course, many of this agriculture equipment is electronically controlled. When multiple micro-controllers are used, communication between them is needed. CAN is one of the suitable communication technologies for embedded control as well as for open network approaches.

Already mid of the 90ties, the CAN-based LBS (Landwirtschaftliches Bussystem) was developed within the DIN standardization body. It was internationalized by ISO and released in the ISO 11783 standard series. In the meantime, this approach, also known as Isobus, is internationally widely accepted and used to connect tractors and implements (e.g. harvesting equipment).

Other CAN applications in the agriculture industry include milking plants, feeding systems, greenhouses, etc. In such applications, embedded and deeply embedded CAN networks are applied. Often non-standardized higher-layer protocols are in use. But there is a trend to apply CANopen or J1939 as higher-layer protocols including the specified process data for dedicated devices. *hz*

Throw the CANfetti: Open-source CANopen stack

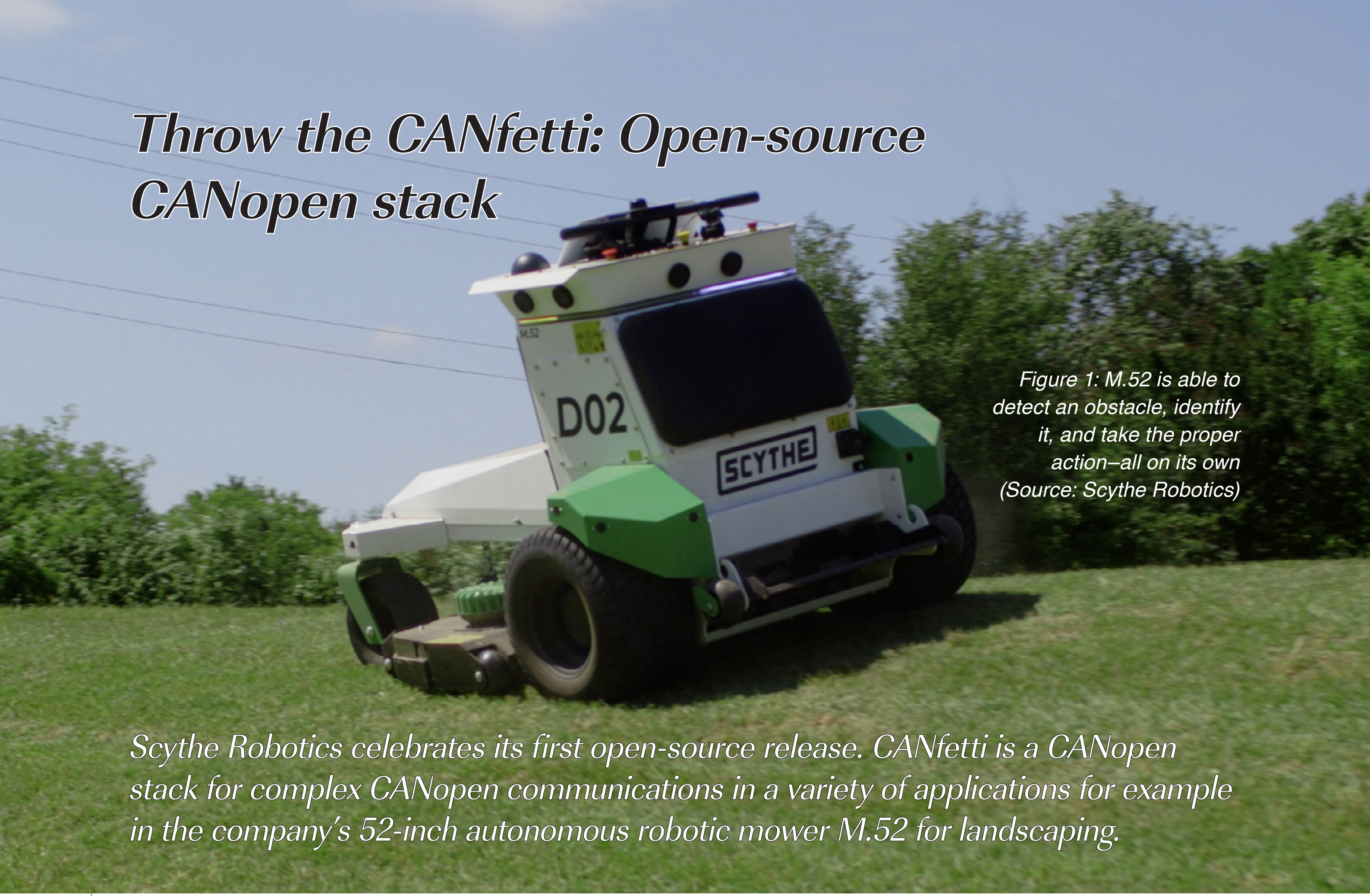


Figure 1: M.52 is able to detect an obstacle, identify it, and take the proper action–all on its own (Source: Scythe Robotics)

Scythe Robotics celebrates its first open-source release. CANfetti is a CANopen stack for complex CANopen communications in a variety of applications for example in the company's 52-inch autonomous robotic mower M.52 for landscaping.

Scythe Robotics, developing advanced, commercial-grade autonomous solutions for the professional landscape industry, announced its first open-source release. CANfetti is a CANopen-compliant stack developed to overcome the limitations of existing libraries. Written and refined over the past several years by Scythe's firmware and software teams, CANfetti significantly lowers the barrier to entry with an open-source, easy-to-use, and production-grade library for robust CANopen communications in fields such as on- and off-road vehicles, industrial devices and, of course, robotics. "Given the complex communication needs across the range of specialized components in Scythe M.52, we knew we'd have to leverage a higher-level CAN protocol," said Matt Quick, lead firmware engineer at Scythe. "A number of our vendors already support CANopen, making it a great fit for us. But as advantageous as CANopen is, the available open-source libraries were frankly a headache to integrate and had severe functional limitations, so we built our own solution."

Self-driving mower for landscaping

Just like the car industry, the transition to electric power is the most prominent shift in landscaping equipment today. Clients are demanding it and local governments are requiring it as consumers and communities pursue greater environmental sustainability in their everyday lives. Technology is rapidly developing to meet these needs, and Scythe is excited to usher in the electric era.

With the company's first commercial mower Scythe M.52 self-driving technology meets commercial-grade equipment to expand the capacity and performance of landscape crews. M.52 follows contours, tackles slopes, and automatically adjusts striping patterns on its own for a consistently cut. The mower's eight HDR cameras and advanced sensors enable it to identify obstacles on a property and safely navigate around them. And since it's all-electric, M.52 can be charged overnight and run all day with zero emissions and substantially less noise than gas-powered mowers. The mower can handle the demands of commercial mowing, like large-scale areas, sloped landscapes, and constantly changing obstacles. With M.52 on their trucks, landscape crews will be freed up to do higher value work and focus on the details that take a property from good to great. They will also be able to use real-time data from the mower to identify additional service opportunities including adding seasonal color, pruning, and preventive lawn and shrub care. Software updates are included. M.52 is only available as a usage-based rental. While reservation ensures earlier access to M.52 mowing service, it does not represent ownership. This also means there is no equipment to buy. No big up-front costs and latest technology because Scythe handles updates and repairs.

CANfetti for mower robot

The autonomous commercial mower uses a robust, automotive-grade CAN as a backbone of its communications system. To unify the range of specialized components in the mower – like advanced sensors, battery modules, and custom boards – and to handle the complex communica-

▷

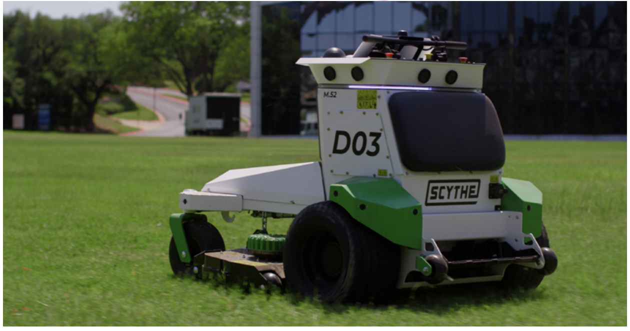


Figure 2: Scythe Sight, M.52's computer vision, uses rich visual data from the mower's eight cameras to understand the world around it (Source: Scythe Robotics)

tion needs between them, Scythe knew they have to leverage a higher-level CAN protocol, like CANopen, Devicenet, or DroneCAN.

The Scythe team found the APIs (application programming interface) and designs of current open-source frameworks too constraining for integrating into M.52 in a consistent manner across both firmware and software. To overcome the rigidity of other options, CANfetti introduces the ability to use dynamic Object Dictionary types that allow easier integration of complex runtime behavior. And with a significantly more flexible API, CANfetti provides engineers with a drop-in CANopen stack that doesn't get in the way and simply lets them build their system around it. Most open-source CANopen libraries are no longer actively being developed, with many abandoned libraries sitting in various states of disrepair and becoming rapidly outdated without community or commercial support. CANfetti represents Scythe's first step in its commitment to updating and expanding the open-source firmware ecosystem.

"Creating a much more robust CANopen stack at Scythe allowed us to integrate critical components that weren't previously compatible," said Davis Foster, Scythe's head of hardware. "With CANfetti, we've been able to integrate more sophisticated components – like advanced sensors, battery modules, and motor controllers – into M.52, resulting in much better machine performance. By publishing CANfetti, we hope to support more companies that are building exciting, cutting-edge machines of all kinds and promote innovation across the field of robotics at large." Other open-source frameworks only partially implement the CANopen specification and have architectures that made extension to the rest of the spec a herculean effort, said Scythe on their blog. Not only is CANfetti a cleaner architecture and built using modern C++, but it supports a broader set of CANopen features like block mode which allows users to efficiently transfer larger contiguous blocks of data.

To make it as robust as possible, the company designed CANfetti as a multi-platform CANopen stack that works across a wide range of architecture, from bare metal micro-controllers to multi-threaded Linux systems. Within M.52, CANfetti integrates with these platforms and more. Beyond M.52, CANfetti can be used for applications as diverse as railway logistics, maritime electronics and building automation. "By publishing CANfetti, we hope to help more companies that are building exciting, cutting-edge machines of all kinds by opening new possibilities for them."

Scythe Robotics provides the commercial landscape industry with commercial-grade, all-electric autonomous equipment solutions for more sustainably maintaining outdoor environments. The company is headquartered in Longmont, Colorado. Find CANfetti on Github. ◀

Source

Scythe Robotics
contact@scytherobotics.com
www.scytherobotics.com

CAN Newsletter Online

In the CAN Newsletter, we already reported about several open-source projects:

CAN Newsletter magazine

CAN FD open-source IP core

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

Read on

CAN Newsletter magazine

Open-source CANopen protocol stack extended

CANopennode is a free and open-source CANopen protocol stack available on Github. Recently, it was extended by a CANopen stack example running on STM32 micro-controllers.

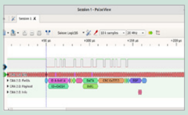
Read on

Open source

CAN FD interface for Arduino

CANFDuino is an open-source project for Arduino. It is available on Crowdsupply as part of the Microchip-Get-Launched design program, using the ATSAMC21G18A micro-controller.

Read on

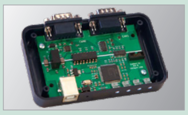


CAN Newsletter magazine

CAN decoder warns for malicious attacks

The open-source Sigrok project is a set of drivers and tools. It provides a desktop oscilloscope and logic analyzer UI (user interface) that can control different instruments (from Siglent, Rigol, and others).

Read on

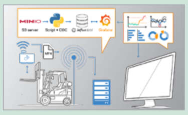


CAN-to-USB adapter

Open-source product supports CAN FD

CANtact Pro from Linklayer Labs (Canada) is an open-source CAN-to-USB dongle with two integrated CAN FD interfaces (flexible data-rate).

Read on



Open-source

Visualizing CAN data in telematics dashboards

CSS Electronics have recently enabled to visualize CAN data in free, open-source telematics dashboards.

Read on

cd

Autonomous robot for harvesting apples

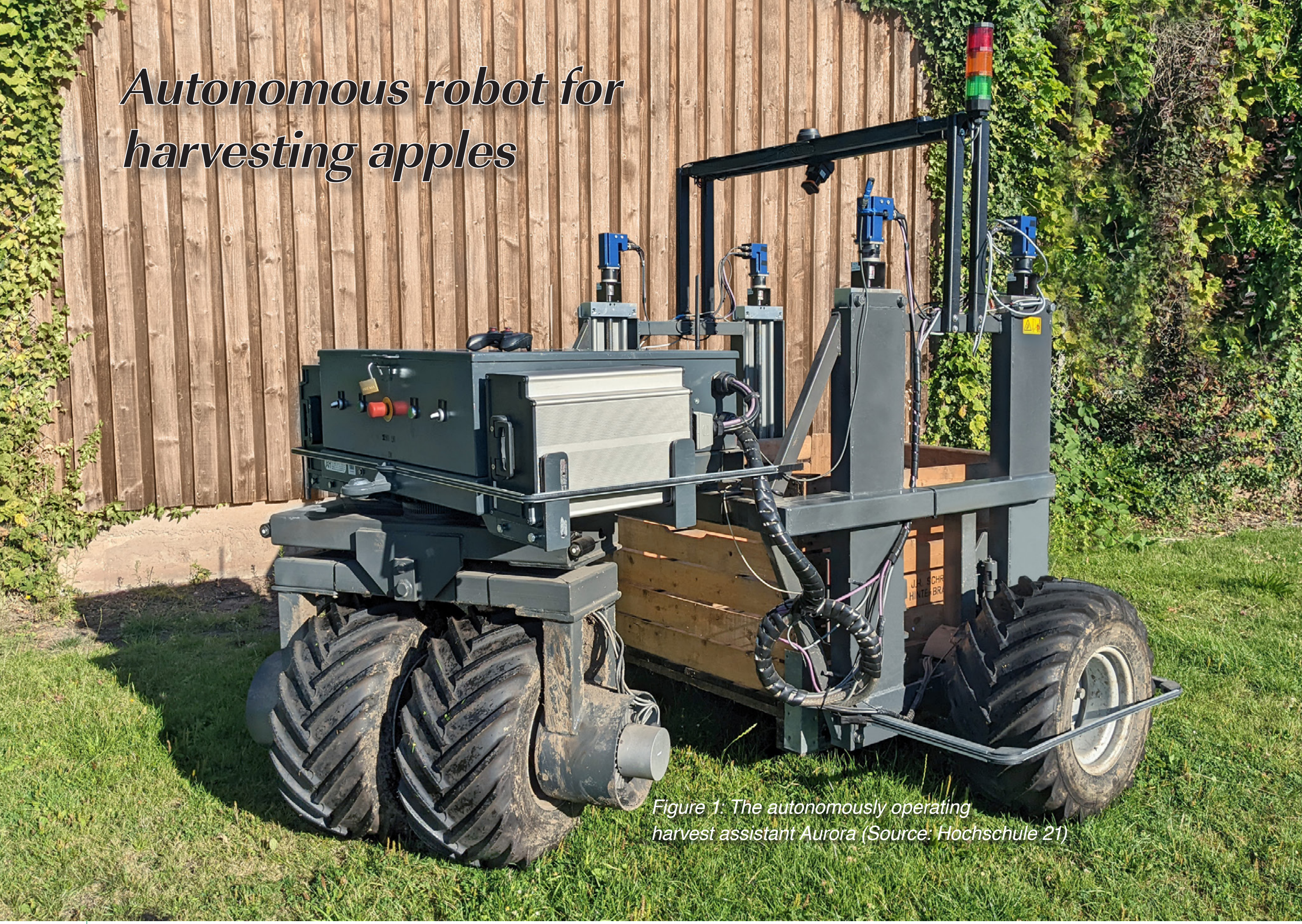


Figure 1: The autonomously operating harvest assistant Aurora (Source: Hochschule 21)

CANopen measurement and sensor solutions from Siko are not only found in industrial applications. Currently, the company supports an agricultural research and development project for an autonomously operating harvesting vehicle in fruit orchards with rotary encoders from its range for mobile machines.

Aurora (autonomous orchard assistant altes land) is a small autonomous vehicle which in future will move independently around fruit orchards and detect full fruit boxes, pick them up, and take them to a defined unloading point. The robot eases the burden on harvest workers and allows them to concentrate on more challenging tasks. Technology and automation should increasingly help to avoid monotonous, tiring activities, and is set to make the job of fruit growers significantly easier. The idea for the project comes from practice: fruit farmer Johann Schröder from Jork in the "Altes Land" region south-west of Hamburg asked Hochschule 21 in Buxtehude for help in developing an autonomously operating vehicle of this sort. The project was launched in collaboration with the agricultural equipment manufacturer PWH from Jork in February 2020. The demand for technical support is high among fruit orchard owners and the project is therefore intended to turn into a market-ready, profitable product in the medium term. The concrete objective of the project, however, was to deliver a functioning prototype by January 2023 in the first instance, which will demonstrate its practical feasibility. The project is funded through the ZIM funding program of the Federal Ministry for Economics.

Second milestone: robot drives autonomously

The project is currently in the last third of the planning stage, having achieved its second milestone: the robot can already operate largely autonomously in an orchard. Work is still being carried out on avoiding collisions and detecting the ground conditions, to avoid getting the wheels stuck in muddy ground, for example, or drifting off course into a ditch. Milestone number three will then be actually to pick up a box and transport it.

A development project of this sort always poses particular challenges, starting with coordination of the interests of various fruit farms, which often have very different harvesting processes, through problems with the infrastructure, such as a stable cell phone standard so that

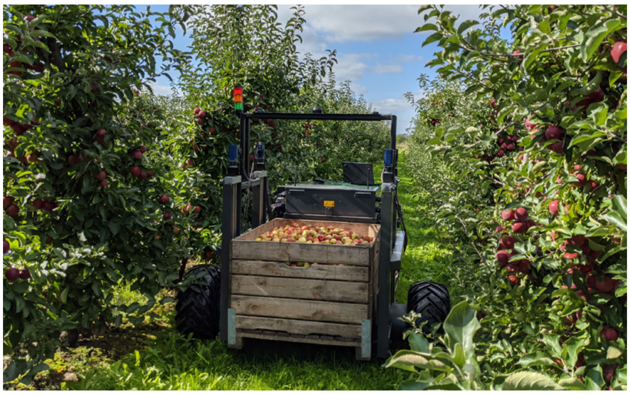


Figure 2: The Aurora harvest assistant will navigate through the rows of trees in an apple orchard and detect and pick up fruit boxes and transport them to a defined unloading point autonomously in future (Source: Hochschule 21)

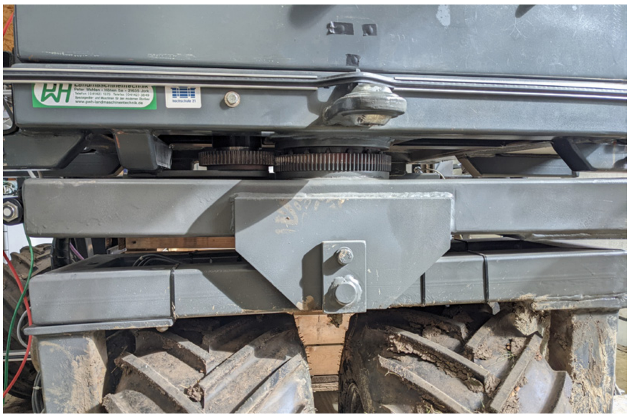
the robot can receive GPS data and communicate with the operator, to practical difficulties in day-to-day outdoor operation (weather conditions, snow, rain, sunshine, ground conditions).

Rotary encoder for tough environmental conditions

Sensors that carry out various measuring tasks are needed for a vehicle that operates autonomously. Measurement and sensor specialist Siko was called in to work on the steering angle detection and positioning of the box holders. With many years of experience in mobile machines and agricultural machine technology, Siko was able to contribute its expertise to the planning phase and ultimately came up with two suitable rotary encoder types that support these important functions. One of them supports CANopen. Alexander Kammann, research assistant at Hochschule 21, appreciates the work of the SIko experts: “We were pleasantly surprised by the willingness of Siko to support future-oriented projects and how committed they were in offering their advice. In the beginning, we were not even sure what requirements we actually had of the sensors. We worked all this out and defined it together.”

First of all, potential sensors must be extremely robust and resilient in the face of tough outdoor conditions (mud, dust, rain, strong sunshine, unevenness in the ground). Components in the Pure.Mobile range of sensor modules from Siko are particularly suitable for use in mobile machines under harsh environmental conditions. A couple of the products in this range support CANopen, CANopen Safety, or J1939.

A double wheel is fitted to the back of the vehicle, which can rotate and thus control the steering. The steering angle is recorded, processed, and sent to the controller by the CANopen WV5800M magnetic rotary encoder. This is a multiturn rotary encoder by means of which even multiple rotations can be detected absolutely. If the power supply is interrupted, because the batteries are flat for ▷



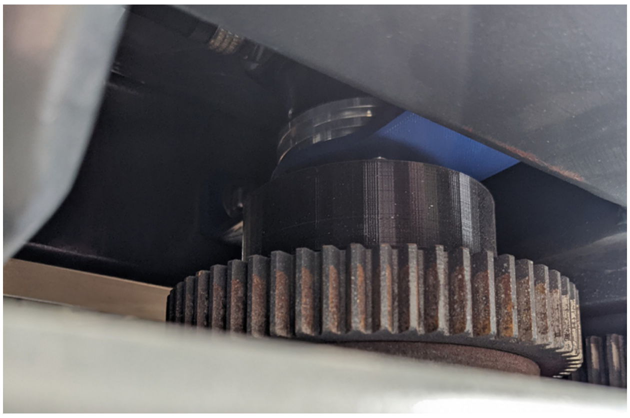


Figure 3 + Figure 4: Important details of the steering: The CANopen WV5800M multiturn rotary encoder records the steering angle so that the vehicle can follow its defined path (Source: Hochschule 21)

example, the steering angle previously set is still present. Without an absolute encoder, this would incorrectly be set as the zero degrees angle when the vehicle is started up again. The magnetic measurement principle meets the requirements of robustness and resilience. The high precision and reliability of the rotary encoder also impressed the team, meaning that the vehicle always adjusts its steering angle so that it keeps to its defined path – without failures or unacceptable deviation from tolerances. In order to increase safety in interaction with the people working in the orchard still further, the WV58MR safety variant (CANopen Safety) of the rotary encoder with redundant position detection will be used for future vehicles to reliably prevent failures. In the development phase, the focus was initially on technical feasibility, so that the rotary encoder without the safety standard was adequate. The plus point of the Siko models: the two rotary encoders are identical in design, so that no mechanical adjustments need to be made to the application when swapping them. A CANopen interface was required for the steering angle detection system so that as many standard electronic components as possible can be used, replaced quickly, and integrated into the system bus.

Details of the CANopen WV5800M/WV58MR magnetic rotary encoders

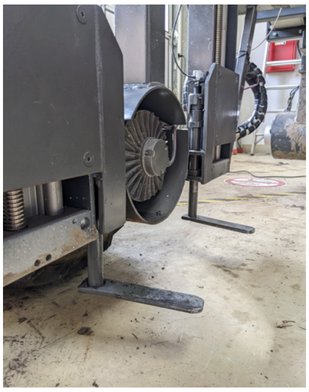
The WV5800M rotary encoder is a magnetic absolute rotary encoder with solid shaft, which has been specially developed for use in mobile machines. It is available optionally with a CANopen or J1939 interface and records the absolute travel information.

The WV58MR rotary encoder is a magnetic safety rotary encoder with redundant position detection, also custom-designed for use in mobile machines. It can be employed in safety-critical applications up to Performance Level PLd. It provides an optional redundant CANopen or CANopen Safety interface.

Both encoders can be parameterized and read out via the CAN interface using the CANopen protocol. For diagnostic purposes there are 3 LEDs in the encoders (yellow, red, green), which indicate error or status information for diagnostic purposes (CiA 303). The encoders support the following CAN in Automation (CiA) specifications: CiA 301, CiA 303 Part 3, CiA 305, and CiA 406. The safety variant additionally supports CANopen Safety (EN 50325-5).

- CiA 301 CANopen application layer and communication profile specifies the CANopen application layer. This includes the data types, encoding rules and object dictionary objects as well as the CANopen communication services and protocols. In addition, this specification specifies the CANopen network management services and protocols. This specification specifies the CANopen communication profile, e.g. the physical layer, the predefined communication object identifier connection set, and the content of the Emergency, Timestamp, and Sync communication objects.
- CiA 303-3 device and network design – Part 3: CANopen indicators. This recommendation describes the communication-related indicators. Additional application-related indicators are either described in the appropriate device profile or are manufacturer-specific.
- CiA 305 CANopen layer setting services (LSS) and protocols specifies the layer setting services (LSS) and protocols for CANopen. These services and protocols are used to inquire or to change the settings of three parameters of the physical layer, data link layer, and application layer on a CANopen device with LSS server capability by a CANopen device with LSS manager capability via the CAN network.

▷



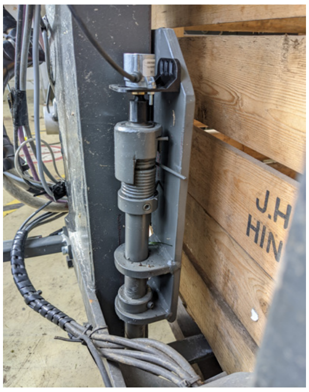


Figure 5 + Figure 6: The position of the box holders, the so-called flippers, is detected by the robust AH25S miniature rotary encoder (the rotary encoder is located at the top of the structure) (Source: Hochschule 21)

- CiA 406 CANopen device profile for encoders specifies the communication and application parameters for different types of linear and rotary encoders such as incremental and absolute, normal, and high resolution, single and multi-sensor (linear only) encoders. The document provides also operating principles of the encoders and specifies encoder output process values such as position, speed, acceleration and jerk. The document specifies also encoder CAM parameters. This document also specifies CANopen Safety parameters such as Safety position and Safety speed for encoders with CANopen Safety functionality (see EN 50325-5).

CAN Newsletter Online

The CAN Newsletter Online already reported on further CANopen sensors from Siko:

SPS 2021

Sensor family for mobile machines

The wire-actuated encoders of the Pure. Mobile family from Siko (Germany) measure position, speed, and inclination due to an integrated single-axis inclination sensor.

Read on

SPS Connect 2020

Sensors and actuators for harsh environments

Siko introduced several devices at the SPS Connect 2020 digital fair. The AP10 position indicator, AG03/1 actuator, IKM360R inclinometer, and WH5800M encoder are connectible via CANopen.

Read on

Machine on wheels

Siko and STW cooperate regarding sensors

The two companies have agreed on a strategic partnership with the aim of further opening up the market for mobile machinery. This includes joint developments of sensors.

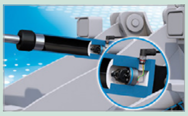
Read on

Position sensor

Wire-actuated encoder for 12-m measuring length

The SG121 wire-actuated encoder from Siko is suitable for measuring lengths up to 12 m. It comes with an installation depth of 70 mm x 8 5mm x 105 mm and supports CANopen, J1939, and CANopen Safety interfaces.

Read on

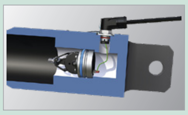


For hydraulic cylinders

Position sensor with +105 °C temperature range

Siko updated its SGH10 position sensor. The product has been certified by the German Federal Motor Transport Authority in accordance with UN ECE R10 and now has E1 certification for road vehicles.

Read on



CAN Newsletter magazine

Encoders for hydraulic and telescopic cylinders

Draw-wire sensors based on rotary encoders have some advantages compared to other solutions. Matthias Roth, Siko's Industry Manager Mobile Automation explains them on the example of the SGH series.

Read on

cd

Position sensors for the "flippers"

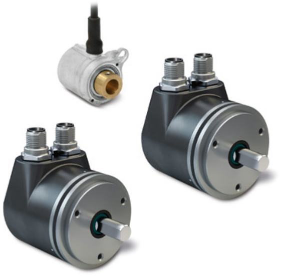


Figure 7: The AH25S, WV5800M, and WV58MR encoders described in the article (Source: Siko)

The second Siko rotary encoder (not CANopen capable) used in the project is the AH25S. It is a single turn rotary encoder which monitors the position of the box holders, the so-called flippers. The filled fruit box is picked up at four points by one flipper for each. When the robot moves over the box and the spring-loaded holders touch it, the flippers swivel to the side, then open automatically and are then located under the four corners of the box for pick-up. In order to be able to transport the box safely, the position of each flipper must be known: has it really swiveled back or has it jammed? Are all four flippers under the box to ensure that it is picked up correctly? The space is very restricted, so a miniature rotary encoder was required which could be used directly without a special holder. An analog encoder is adequate here, as the data is less critical than that provided by the steering angle sensor.

A harvesting tool with real added value

Many little cogs have to interlock in a development project of this sort to turn a vague idea into a technically perfect product, which in future can be used with a balanced cost-benefit ratio in numerous orchards. In order to offer farms genuine added value, the intention is to use Aurora for other maintenance work, too, such as mulching and mowing or as support for planting new trees. Effective use virtually throughout the year is therefore possible and is not just restricted to harvest time. ◀

Source

Siko
info@siko-global.com
www.siko-global.com

Smart farming to feed the world

Figure 1: Targeted use of fertilizers and herbicides reduces soil contamination (Source: Adobe Stock)

CANopen-connectable DC micro-drives are deployed in many industrial, medical, transportation, aerospace, and other applications. But what are the benefits of deploying them in smart farming and agriculture?

The agricultural industry faces a major challenge regarding the feeding of growing world's population: Crop cultivation and livestock farming must produce more without endangering the life-sustaining resources. Smart farming concepts are critical to enable it in an ecologically feasible manner over the long term. The increasingly automated agricultural industry relies on micro-drives deployed e.g. in robotic equipment. These drives are compact, high-torque, and dynamic. Networked via CANopen in agriculture environments, they can be precisely actuated and meet the reliability and long-service-life requirements.

Smart farming for efficiency

Most work steps in arable farming such as sowing, fertilizing, and crop protection have so far been carried out over entire areas, meaning the machines distribute the substances with a corresponding throughput. Thus, instead of fertilizer working right on the plant, it partially ends up in the groundwater. Also, tasks such as pruning of fruit trees or harvesting of vegetables require costly manual labor, while more and more companies suffer from a personnel shortage.

Smart farming (also precision, digital, or e-farming) concepts use modern technologies to increase efficiency, spare resources, relieve people from monotonous work, and to produce higher yields. With computer-aided, networked processes, machine learning, and tailor-made robot functions, it is possible to focus the measures on individual plants instead of on the entire area (see Figure 1). For example, use of herbicides could be significantly reduced, fruits and vegetables could be harvested by robots in continuous passes, always at the optimum ripeness (see Figure 2).

Field robots instead of large machines

Large agricultural machines weigh up to ten tons and compact the soil, so it can barely absorb any additional water and air. The growth and health of the crop plants in the areas near travel paths are also impacted. Lightweight, autonomous field robots can help contribute to healthier soil and increased biodiversity.

Many of these applications currently only exist as studies or prototypes. A practical example is precision planting, originally developed for research and seed breeding. Applied machines can plant individual seeds at precisely defined intervals. Each plant receives enough space to grow, and the acreage is optimally utilized. At the same time, the seeds are used efficiently. The machines use a separating module with an electric drive for each row. A motor drives a slotted or toothed disk that transports the individual seeds to the outlet. The control precisely sets the optimal distance depending on the type of seed. The different radii of the individual rows can be compensated when driving along curves. The feeding of the seeds to the disks is controlled using closures that are also motorized.

Robotics in greenhouse

With vegetable and flower cultivation in greenhouses, many plants are first sprouted in small pots and later replanted in larger pots or in beds. In modern horticultural enterprises, machines perform the sorting and handling of plants and pots. Their machinery is similar to that used in industrial production and logistics (see Figure 3). There are conveyor

Figure 2: Continuous, automated harvesting ensures perfect ripeness (Source: Adobe Stock)

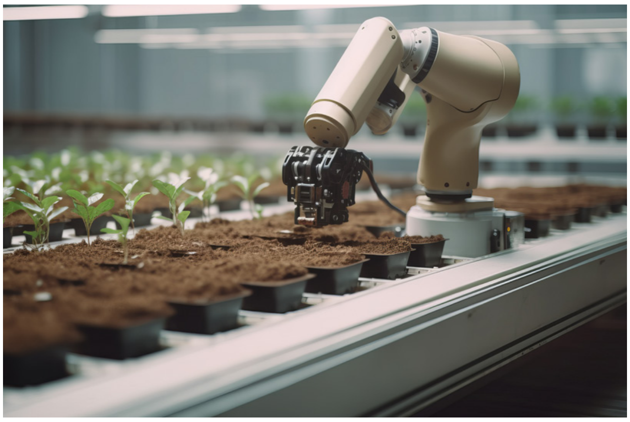


Figure 3: Modern automation technology sorts and handles the seedlings in greenhouses (Source: Adobe Stock)

Company background

Faulhaber is specialized in the development, production, and deployment of high-precision, miniature drive systems, servo components, and drive electronics with up to 200 W of output power. This includes customer-specific packaged solutions as well as an extensive range of standard products, such as brushless motors, DC-micro-motors, encoders, and motion controllers. The motion control solutions are used in such application areas as medical technology, factory automation, precision optics, telecommunications, aviation, aerospace, robotics, and others.

belts and roller conveyors, on which trays with products in various stages are transported, sorted, and repotted. The grippers used in other industries differ only in terms of shape. Driven by micro-motors, they perform automatic handling of the individual pots and root balls.

These micro-motor types will also play a key role in self-propelled fruit and vegetable harvesters, which have not yet reached series maturity. Here, camera-assisted sensors detect the ripeness degree of strawberries or peppers on basis of color and shape, and record their exact position. The on-board computer uses these data to control a robot arm, which is equipped with a type of shears and a collection device. The prototypes of this technology are full of electric motors, from the single-wheel drive and the robot arm to the cutting apparatus and the collection system for the harvested produce.

Requirements for small electric drives

Unlike the traditional large agricultural devices, the machines and components used in smart farming are more compact and lighter with little space available for motors. Nevertheless, as drives of sowing disks, flaps, grippers, robot arms or shears, they must supply sufficient power to reliably perform the respective task over countless cycles. At the same time, they should operate efficiently, as autonomous units usually draw their energy from batteries. It is also important to integrate the drive electronics into the

▷

Figure 4: Drive technology used in agriculture must work reliably, even in tough environmental conditions (Source: Adobe Stock)

networked structures and enable smart control. Moreover, the drives must be robust to function reliably and for long term under demanding conditions such as large temperature fluctuations and high mechanical loads. And, last but not least, the costs must remain reasonable.

The drive specialist Faulhaber provides various motor and drive device series to address these issues. For example, the BXT brushless and compact DC flat motors enabling short designs in the axial direction. The motors are 14 mm, 16 mm, and 21 mm in length, but deliver torques up to 134 mNm, within a diameter of 22 mm, 32 mm, and 42 mm respectively. For precise speed control and high positioning accuracy, diameter-compliant magnetic encoders or speed controllers are fully integrated into the housed motor variants, whereby the drive length is increased by just 6,2 mm. The matching metal planetary gearheads of the GPT series are characterized by a robust, short design, high torque, and fine graduations of the numerous reduction ratios. Another suitable drive solution is the copper-graphite CXR motor line along with the matching gears. Their commutation system is durable and is suited to dynamic, high-performance applications with fast start/stop operation, as is required for automatic sorting. Optional incremental encoders enable precise positioning. Various controllers, e.g. with a CANopen interface, are available for the networking of the company's drive systems.

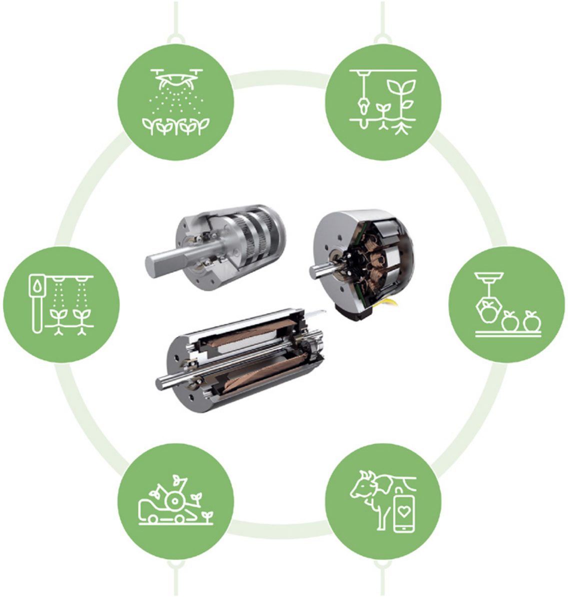


Figure 5: The CANopen-connectable BXT compact flat DC-micro-motors, the robust CXR copper-graphite motors, and the GPT gearheads are well-suited for smart farming applications (Source: Faulhaber)

CANopen communication

CANopen is a higher-layer protocol for Classical CAN. It is pre-destined for networking of micro-drives. Because of its size, a CAN interface can be integrated in small electronic modules. Further CAN benefits include real-time and multi-drop capabilities, robustness regarding EMC (electromagnetic compatibility) disturbances, and reliable communication due to very low residual error probability. Each year, more than two billion CAN nodes are sold e.g. for use in automotive and heavy-duty transportation applications. Thus, CAN is well-proven and the price for CAN protocol controllers is very reasonable.

The CiA 402 CANopen device profile specifies the configuration parameters, process parameters, and diagnostic information for drives and motion controllers in a standardized manner. CiA 402 series is a de-facto standard for motion control applications and is also internationally standardized in IEC 61800-7-201/-301.

Faulhaber's CANopen-connactable device versions provide the common operating modes as defined in CiA 402. All parameters are stored directly in the CANopen object dictionary. Thus, configuration of the drives can take place both via the Faulhaber Motion Manager tool or via off-the-shelf CANopen configuration tools from other providers. The CANopen version is particularly suitable for users who already use different CANopen devices or who want to operate the motion controller on a PLC (programmable logic controller). The dynamic PDO (process data object) mapping enables efficient networking with the connected devices. Many of CANopen systems are already in use today in smart farming applications and will continue to contribute to advancing technology in this area, which is essential to feeding the world's population. ◀

Authors

Kevin Moser
Faulhaber
redaktion@faulhaber.com
www.faulhaber.com

Ellen-Christine Reiff
Redaktionsbüro Stutensee
kontakt@rbsonline.de
www.rbsonline.de

18th international CAN Conference

iCC

Baden-Baden (DE), May 14 and 15, 2024

Call for Papers: 18th international CAN Conference

CAN in Automation (CiA) announces the 18th international CAN Conference (iCC), the premier platform for showcasing the latest advancements in CAN technology. The conference aims to foster collaboration, knowledge exchange, and networking among professionals at the forefront of CAN technology. Join us as experts from around the world, spanning diverse application fields, gather to share insights, discuss trends, and explore cutting-edge developments in CAN-based networking.

- CAN implementations
- CAN device design
- CAN system design
- CAN diagnostics
- CAN higher-layer protocols
- CAN-related research studies
- CAN applications in vehicles
- CAN applications in industry
- CAN in general-purpose applications
- Other CAN-related topics

Submit an abstract showcasing your latest developments, whether they are based on Classical CAN, CAN FD, or the emerging CAN XL.

Important date:

- Abstract Submission Deadline: **September 15, 2023**

Please consider that the iCC Program Committee, chaired by the CiA Managing Director H. Zeltwanger, considers technical-oriented papers only.

Enhance your visibility in the CAN community, and demonstrate your commitment to technological advancements:

- Tabletop exhibition for showcasing products and services
- Sponsorship opportunities available

For submission guidelines, tabletop exhibition details, sponsorship opportunities, and further information, please contact CiA office: conferences@can-cia.org

CAN in Automation e. V.

Linear actuators for agriculture machinery

(Source: Adobe Stock)

Timotion has developed J1939-connectable linear drives that are designed for agriculture equipment.

The linear actuators come in an IP69K-rated enclosure. This makes them compatible with high-pressure cleaning, which is common in agricultural machinery maintenance. They are robust and have a high-load capacity of up to 16 000 N. According to the supplier, they are leak-free and maintenance-free. They can also be equipped with various position sensors allowing feedback and thus synchronizing two devices. The products are compatible with several control systems and communicate with them via the CAN interface supporting the J1939 application layer.

The products are configurable by the system designer. They are preconfigured to a 100-percent speed. An H-bridge motor drive circuit can adjust this to fulfill the PWM (pulse-width modulation) speed control. The recommended value is between 60-percent and 100-percent speed, as lower values could reduce the actuator performance. With the implemented T-Smart solution, the user can set up to eight actuators in synchronous movement. Without worrying about different loads and complicated cabling, the actuators stay aligned when moving. The T-Smart actuator can set a distance to begin decelerating before the end of the stroke (0 mm to 20 mm). The deceleration ensures that the actuator reaches zero velocity at the point of contact with the end of the stroke, preventing any impact loading at the end of the stroke.

There is also a configurable virtual stroke function, which limits the movement in the middle of the stroke, in extending or retracting direction. Once the virtual stroke limit has been set up, the actuator will stop and won't surpass the designated position. With soft start and soft stop, the actuator slowly accelerates to the full speed or slows down from the full speed. This helps to provide smooth operation of the application. Apart from using the default current limit value for overcurrent protection, the current limit value can also be down-adjusted to let overcurrent protection occur in lighter applications. And, it could set up different values for extending and retracting directions.

The MA2T drive with integrated T-Smart controller allows for integration in SAE J1939 networks. It is compatible with the supplier's PGMA programming environment. In addition to configure the drive, the PGMA also provides status monitoring, capturing usage and performance data for development or maintenance purposes.

The MA2T electric linear actuator for agricultural machinery can push up to 8000 N. The MA3 actuator features up to 16000 N. The MA4 electric drive for agricultural vehicles can push up to 2000 N. It is particularly compact and fits into small spaces. The actuators can also be used in the cabs of agricultural machines. Because of the difficulty of the tasks and the danger of the machines, the profession of farmer involves a significant number of possible accidents. Ergonomics is, therefore, an essential aspect of modern agricultural machinery cabs in order to optimize the safety of farmers. By allowing the adjustment of seats, ▷

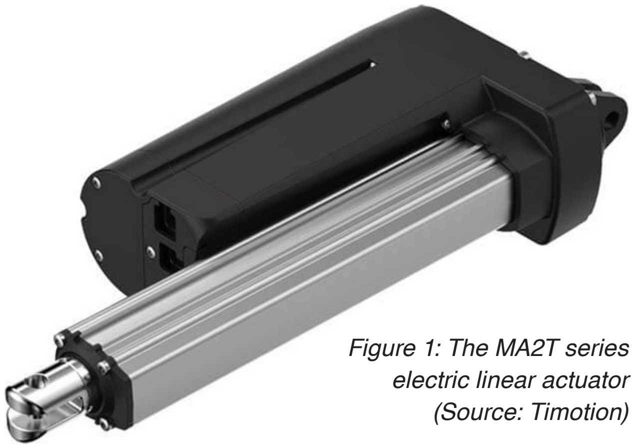


Figure 1: The MA2T series electric linear actuator (Source: Timotion)

steps, hoods, windows, and hatches in an automated way, electric linear actuators for agricultural cabs bring more comfort and safety to farmers and improve their working conditions.

Usage benefits of linear actuators

Electric linear actuators are also used in automated agricultural machines. They made a significant contribution to the automation of agricultural machinery. They have been integrated into balers, combines, seeders, sprayers, fertilizer spreaders, and tractors. One of the benefits is that they do not leak oil, which could pollute the soil. Without a hose or compressor, they are particularly easy to install, explained the supplier.

Electric linear actuators for modern agricultural machines can precisely operate spreading systems and spouts. The programmable opening systems allow the precise release of the desired amount of products and optimize profitability by reducing losses. With a high level of control, they can also operate agricultural wrappers, crop blades, and agricultural AGVs (automated guided vehicles). Traditionally equipped with pneumatic or hydraulic actuators, agricultural equipment is gradually seeing its systems replaced by electric actuators. Such electric solutions are also maintenance-free. This is particularly appreciated in the context of more environmentally friendly agricultural practices, stated the drive supplier. ◀

hz (based on information from Timotion's website)

Predictive maintenance in CANopen Lift

Predictive maintenance in CANopen Lift is a number of measures to determine condition of devices in an operational lift facility and to estimate the maintenance needs for these devices or for the whole facility. Condition monitoring is a continuously-performed measure of predictive maintenance to estimate the equipment condition.

(Source: Adobe Stock)

CANopen Lift is not the first application where predictive maintenance applies. There are numerous applications involving equipment evaluation for the very same purposes and so multiple methodologies are deployed to achieve the maintenance goals.

It was an imperative thought for the CAN in Automation (CiA) special interest group (SIG) lift control to start the development of condition-monitoring handling for CANopen Lift applications. The SIG even assigned a separate task force (TF condition monitoring) with dedicated experts to address this issue. As a base for specifying the parameters and functionality of condition monitoring, the task force used the VDMA 24582 standard sheet. The German-language VDMA 24582 document “Feldbusneutrale Referenzarchitektur für Condition Monitoring in der Fabrikautomation” means translated “Fieldbus-independent reference architecture for condition monitoring in factory automation”. It considers the goals of approved and standardized condition monitoring methodology for automation in embedded networks, such as CANopen networks.

The CANopen-based communication in lift control networks is well established for about 15 years. In context of predictive maintenance, it is used to collect interconnected device’s condition data and to transfer it via the CANopen network to the equipment evaluating the maintenance needs and suggesting the next action steps.

Estimating the maintenance needs

The VDMA 24582 provides a concept for collection of condition monitoring data to effectively estimate the maintenance needs. The CiA 417 CANopen Lift specification developed by CiA, adopted this concept for lift applications. The base concept idea is to identify the functions to be monitored with regard to the function, application, and automation-function location reference (see Figure 1).

The function-based view classifies the functions in a system, e.g. counter (electrical: trip counter), timers (electrical: hour meter, mechanical: life cycle door drive), temperature (electrical: motor temperature). The application-based

▷

Function-based view

Application or component-based view

Automation-based view

Figure 1: VDMA 24582 function identification viewpoints (Source: CAN in Automation)

view identifies which part of the system or sub-system has to be monitored, for example a car door unit (door controller temperature, etc.). Finally, the automation-based view serves to identify the function location, e.g. light barrier, frequency inverter, etc.

CANopen Lift monitoring

Due to the Classical CAN data link layer specifics, such as the 8-byte process data payload, the SIG lift control has defined a small pool of monitored functions. These functions can be delivered by the most of lift devices to minimize network traffic. For example, the hour meter information can be measured by a lift host controller and also by the inverter. This practice allows individual information about each device state, whereas the door drive temperature should be provided by a door controller only.

Subsequently, the function viewpoint leads to the VDMA 24582-based CANopen Lift monitoring function block with the structure given in Figure 2. The standardized approach to the system state, function identification, and input data including thresholds leads to certain output data. The output data is used to identify the status of the lift device and to decide which maintenance mode should be selected. It is also used to indicate the current condition of the device e.g. with help of the so-called visual traffic lights (status lights).

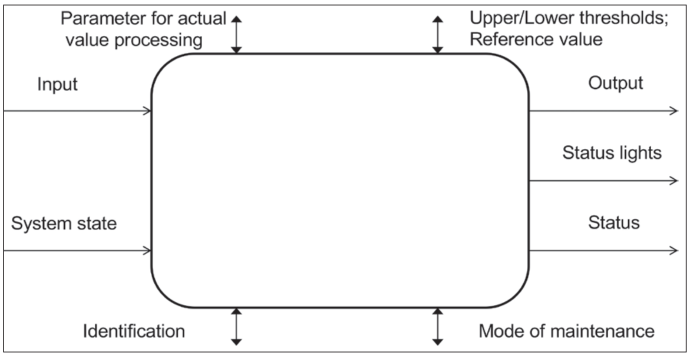

Parameter for actual value processing
Upper/Lower thresholds; Reference value
Input
Output
Status lights
System state
Status
Identification
Mode of maintenance

Figure 2: Simplified VDMA 24582-based CANopen Lift monitoring function block structure (Source: CAN in Automation)

Conditional monitoring example

To understand how the CANopen Lift conditional monitoring practically works, an example is necessary. The example shown in Figure 3 should help to understand the CANopen Lift condition monitoring principles. CiA 417 already specifies parameters (data objects) for condition monitoring, which can be seen in Figure 3.

In the UML (unified modeling language) activity diagram, the objects 6080_h and 6081_h provide identification and location of the monitored function (data point). For instance, the motor temperature is a monitored function defined in the object 6081_h. It is submitted using MPDO 1 (multiplex process data object) for the door 3 by a car door unit, which is located in the 3rd floor in the lift 1.

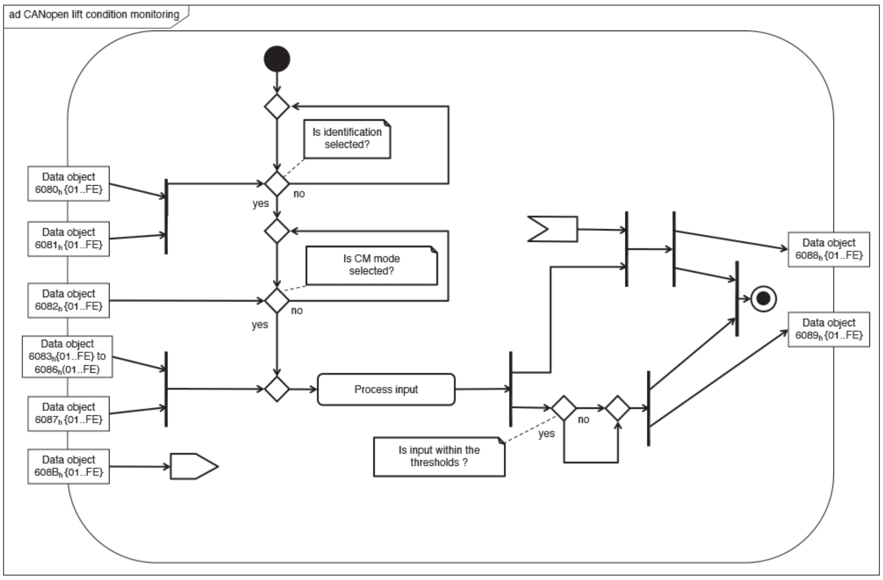

ad CANopen lift condition monitoring
Data object 6080$_h${01..FE}
Data object 6081$_h${01..FE}
Data object 6082$_h${01..FE}
Data object 6083$_h${01..FE} to 6086$_h$(01..FE)
Data object 6087$_h${01..FE}
Data object 608B$_h${01..FE}
Is identification selected?
yes
no
Is CM mode selected?
yes
no
Process input
Is input within the thresholds ?
yes
no
Data object 6088$_h${01..FE}
Data object 6089$_h${01..FE}

Figure 3: UML activity diagram example of the simplified CANopen Lift monitoring (Source: CAN in Automation)

The condition monitoring mode is an internal operation mode (see object 6082$_h$) at which the status and the function data is acquired e.g. manual, learning, simulation, etc. If it is selected, the input can be processed resulting with the output value (see object 6088$_h$) and checking the threshold conditions for the motor temperature. The lift operator selects the maintenance mode on its own. Does the temperature exceed a threshold (see objects 6083$_h$ to 6086$_h$), then the certain status light condition (see object 6089$_h$) is generated depending on the reached threshold type, e.g. yellow for warning and red for critical. If the temperature remains within the thresholds, then the green light status condition is generated. The object 6089$_h$ provides not only the status lights but also the maintenance strategy that can be set by a lift operator i.e. condition monitoring only or also preventive and predictive maintenance measures.

The condition monitoring strategy specified in CiA 417 is considered as a check up of the component/device status at regular or irregular time intervals. Depending on the status, a manufacturer-specific predictive maintenance entity decides what to do with the lift device or the whole lift facility. The preventive strategy is a scheduled data point acquisition of the output value for exceeding thresholds over a period of time or in case of a monitoring state change. The predictive strategy, on the other hand, is used when the device maintenance is required. Both preventive and predictive maintenance require collection of the monitored data in the style of conditional monitoring strategy.

Use of the status lights offers the lift operator a simple way to decide either to dispatch a technician for the motor maintenance or to replace the motor due to according ▷

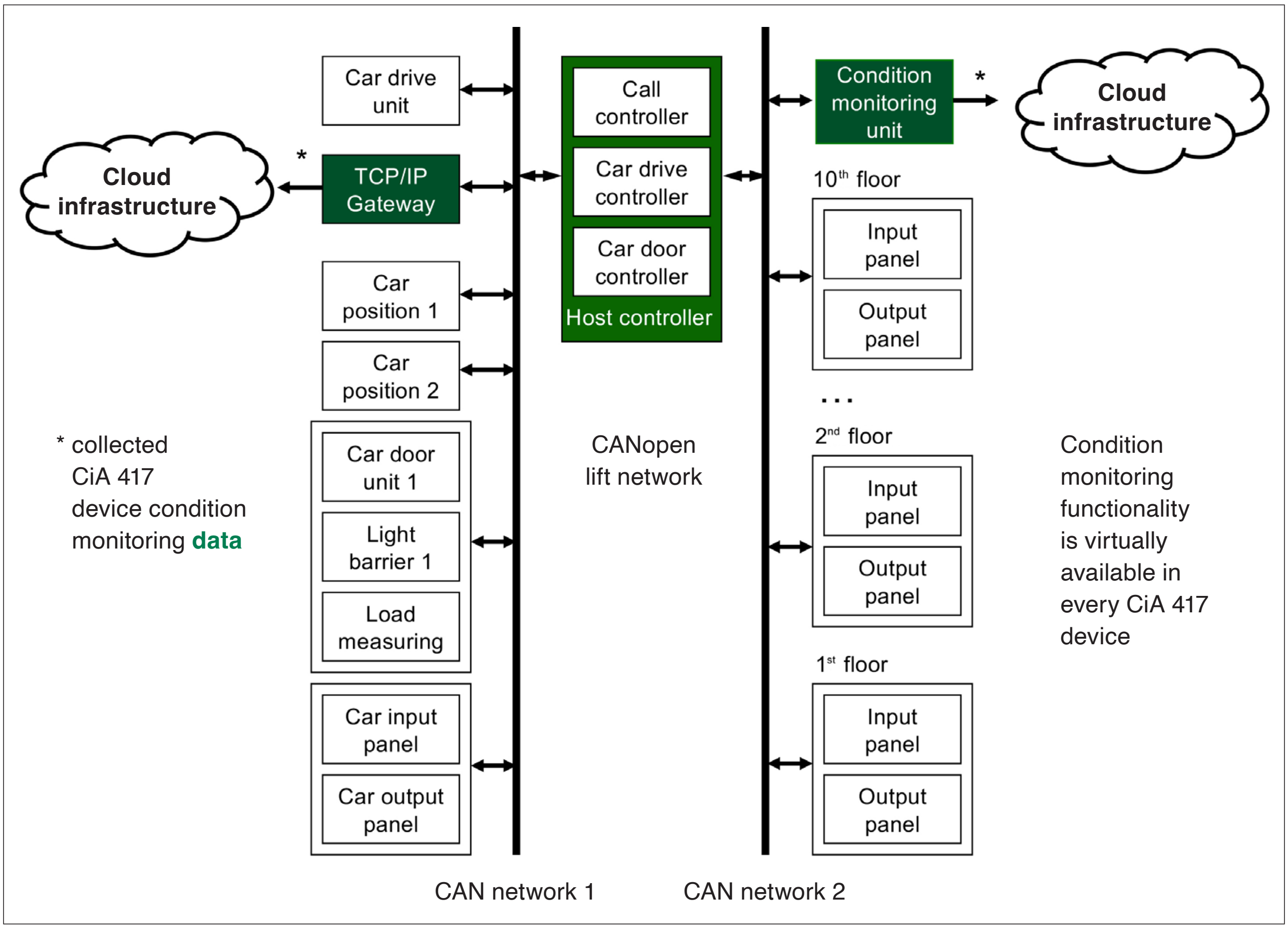


Figure 4: Example of a simplified CANopen lift network (Source: CAN in Automation)

visual traffic light indication. The CANopen Lift profile (CiA 417) provides also a status indication, whether the whole lift application is OK or not. This is indicated by the value 0000_h in object 6081_h. CiA 417 also provides a specific configuration for each monitored function, so the user can decide which data points are monitored and have to be submitted via CAN. This is possible using the object $608B_h$.

Example lift application

An example lift application network is shown in Figure 4. The monitored function can be submitted by the related lift device or the lift host controller. The data can be collected by the lift host controller and provided to the end user via an edge gateway into the cloud infrastructure. Independently, there is a condition monitoring unit as a virtual device (software or hardware) that is able to collect the data in parallel to the lift host controller and transmit it independently to the higher-level hierarchical networks or IoT (Internet of Things) infrastructure. The CiA 309 document specifies a data interface (gateway) between CANopen embedded networks and TCP/IP-based networks. Such a getaway device can be used as a monitored-data collector if neither the lift host controller nor the condition monitoring unit do not support any communication beyond the embedded lift network. Many lift host controllers already provide an Ethernet interface or even wireless and/or mobile connections. Even an edge-gateway capable condition monitoring unit (if designed in a hardware) may offer such external connections. Thus, the condition data of the lift devices and the host controller can be acquired in different ways and the lift operator can meet a maintenance strategy based on the collected data.

Conclusion

Collection of big data amounts from the CANopen lift sensors and control devices was initially discussed by the CiA TF (task force) conditional monitoring, but rejected. It is not in the scope of the SIG lift control, because it would require higher data throughput as it is possible with Classical CAN. The upcoming technologies such as CAN FD and CAN XL are capable to overcome the Classical CAN throughput limitations and allow instant data collection. For the moment, more than 30 specified condition monitoring functions in CiA 417 seem to cover the predictive maintenance requirements of the CANopen Lift community.

Author

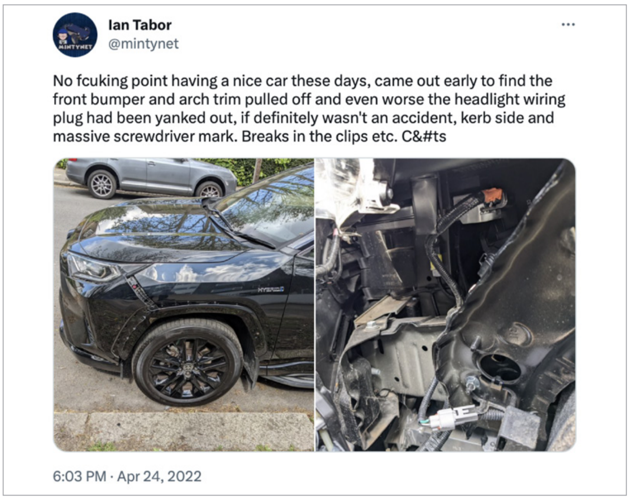
Oskar Kaplun
CAN in Automation
headquarters@can-cia.org
www.can-cia.org

Miniature Pressure Transmitter
CMP 8271
CANopen®
• Small and rugged construction
• CANopen bus protocol DS301/DS404 supports CAN 2.0A/B
• LSS (DS 305 V2.0)
www.trafag.com/H72619
www.trafag.com | trafag@trafag.com
trafag
sensors controls

The CAN Injection attack

The attack has been reported widely in the media. This article focuses on the special properties of the CAN Injector and explains them for "CAN insiders". Methods for defeating the attack are discussed as well.

A few weeks ago, I published on my blog a detective story [1]. It describes in detail how Ian Tabor, an automotive cybersecurity researcher, had his Toyota RAV4 stolen. It was clearly a sophisticated crime: the thieves managed to override the engine immobilizer without using the keys and drive the vehicle away. A few weeks earlier they had tried to steal the car and failed. Ian tweeted pictures at the time of the damage they had caused.



Ian Tabor
@mintynet

No fcuking point having a nice car these days, came out early to find the front bumper and arch trim pulled off and even worse the headlight wiring plug had been yanked out, if definitely wasn't an accident, kerb side and massive screwdriver mark. Breaks in the clips etc. C&#ts

6:03 PM · Apr 24, 2022

Figure 1: A tweet from Ian Tabor a few weeks before the car was stolen, showing how the 'vandalism' was actually an attempted CAN Injection attack (Source: Ian Tabor, Twitter)

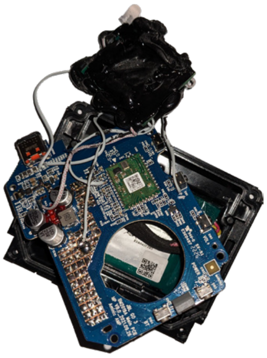


Figure 2: CAN Injector hidden inside a JBL Bluetooth speaker case (the device is powered by the speaker's battery and hidden in resin) (Source: Ian Tabor)

After the car was stolen, Ian used the Toyota 'MyT' telematics service to examine vehicle diagnostics remotely and very quickly focused on diagnostic trouble codes (DTCs) related to the CAN network. He suspected the thieves had accessed the car's CAN network to override the immobilizer and open the doors. After some research on the dark web, he found that devices were being sold to thieves to inject CAN frames for specific brands and models of cars. He bought one of these devices for Toyota and Lexus cars – hidden inside a JBL Bluetooth speaker case (Figure 2) – and asked me to help reverse engineer the device.

The device has CAN_H and CAN_L wires that are attached to a vehicle's CAN network and then CAN frames are injected on to the network. To steal a RAV4, thieves remove a panel and access CAN_H and CAN_L lines in the headlight connector – just as the damage to Ian's car showed (from the earlier failed attempt to steal the car). After some investigation we named this the CAN Injection attack and notified the Automotive Security Research Group (ASRG). It now has an official common vulnerabilities and exposures (CVE) identifier: CVE-2023-29389. This vulnerability applies not just to Toyota or Lexus models: the dark web sites selling these theft devices list many models of cars from many manufacturers.

The core of the CAN Injection attack is Classical CAN frame spoofing, exploiting the way the vehicle is architected according to the perimeter defense concept (i.e. only the outer perimeter of a system is protected on the assumption that nothing can get to the unprotected part). Figure 3 is a simplified schematic of the RAV4's CAN networks.

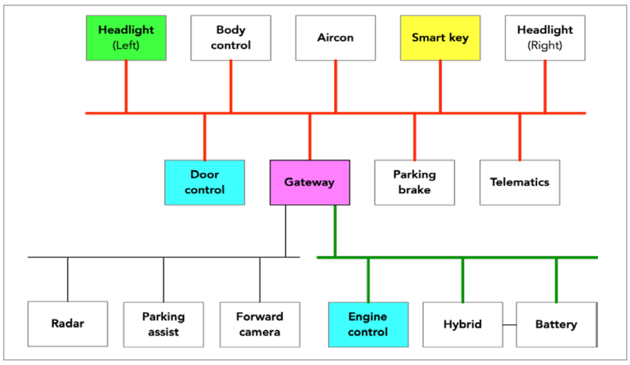
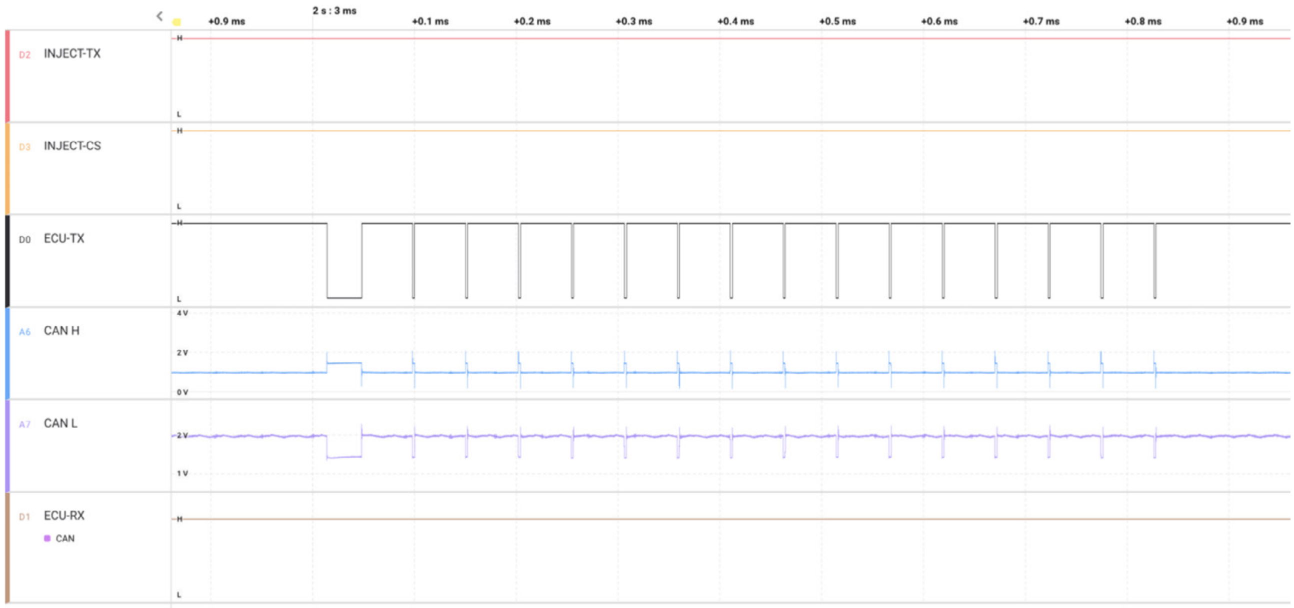


Figure 3: A simplified schematic of the Toyota RAV4 CAN networks (Source: Canis Automotive Labs)

Three CAN networks are shown. The network marked in red connects multiple electronic control units (ECUs) together (there are many others on these networks that are not shown). The thieves broke into the connector near the left headlight ECU. The injected CAN frames spoof the frames that normally come from the smart key ECUs. This ECU has very sophisticated cryptographic messaging over a wireless link to the owner's key, but the CAN messaging from the smart key ECU to the engine ECU (via a gateway) and the door ECU is unprotected.

CAN details

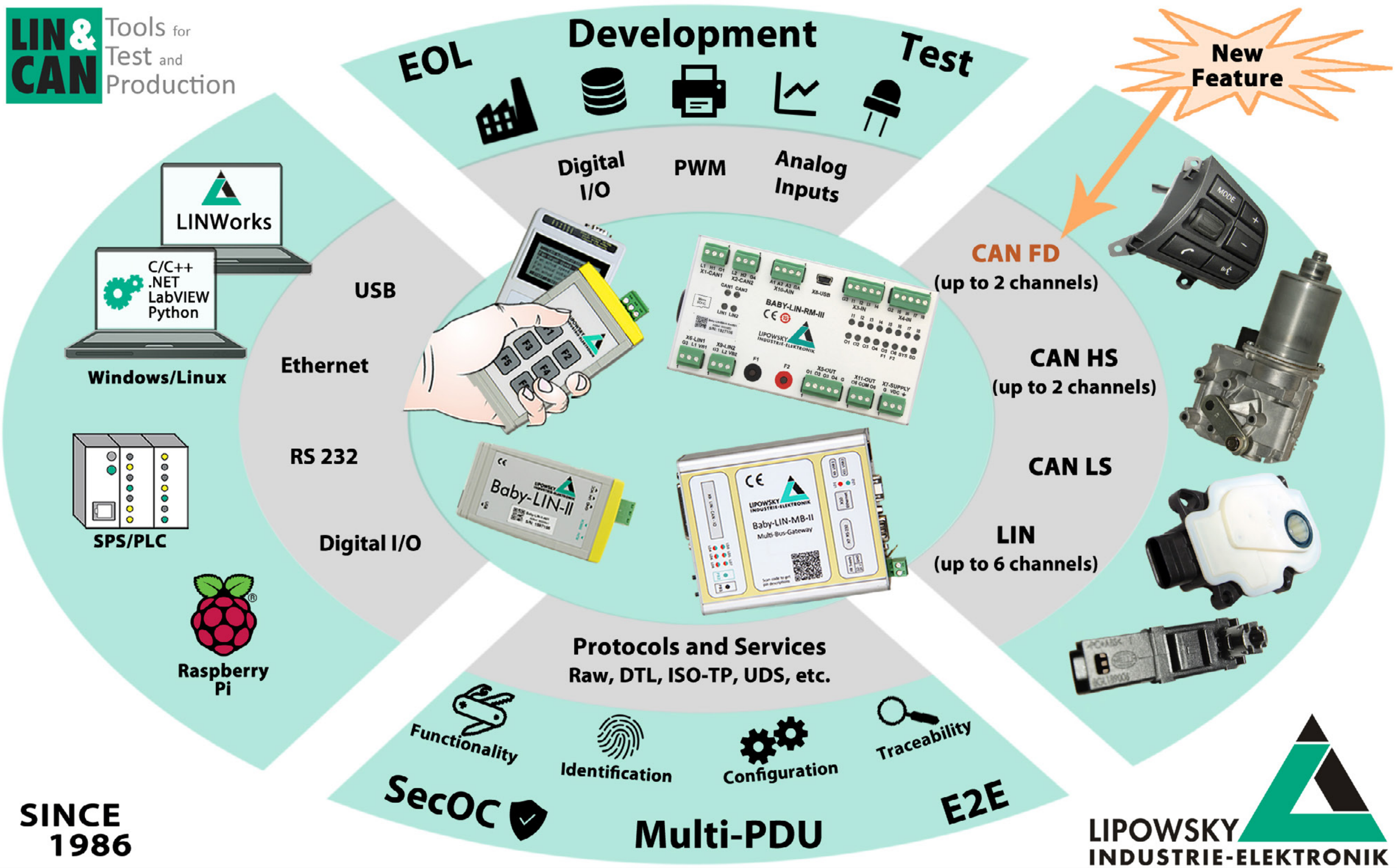
The attack has been reported widely in the media but very few reports focus on the most important property ▷



INJECT-TX	**The line representing CAN TX of the CAN Injector device**
INJECT-CS	**The circuit select for the dominant-override**
ECU-TX	**CAN TX of the CAN controller in the ECU**
ECU-RX	**CAN RX of the CAN controller in the ECU**
CAN H	**CAN-High line**
CAN L	**CAN-Low line**

Figure 4: A logic analyzer trace showing an ECU trying to send a CAN frame when the dominant-state-override function is triggered (Source: Canis Automotive Labs)

of the CAN Injector: *it contains a modified CAN transceiver.* When enabled, this transceiver can actively drive the recessive state on the CAN network, overriding other controllers that try to assert a dominant state. This means that other ECUs cannot transmit frames, leaving the CAN Injector as the only transmitter. Figure 4 shows a logic analyzer trace of a CAN controller trying to send a CAN frame.



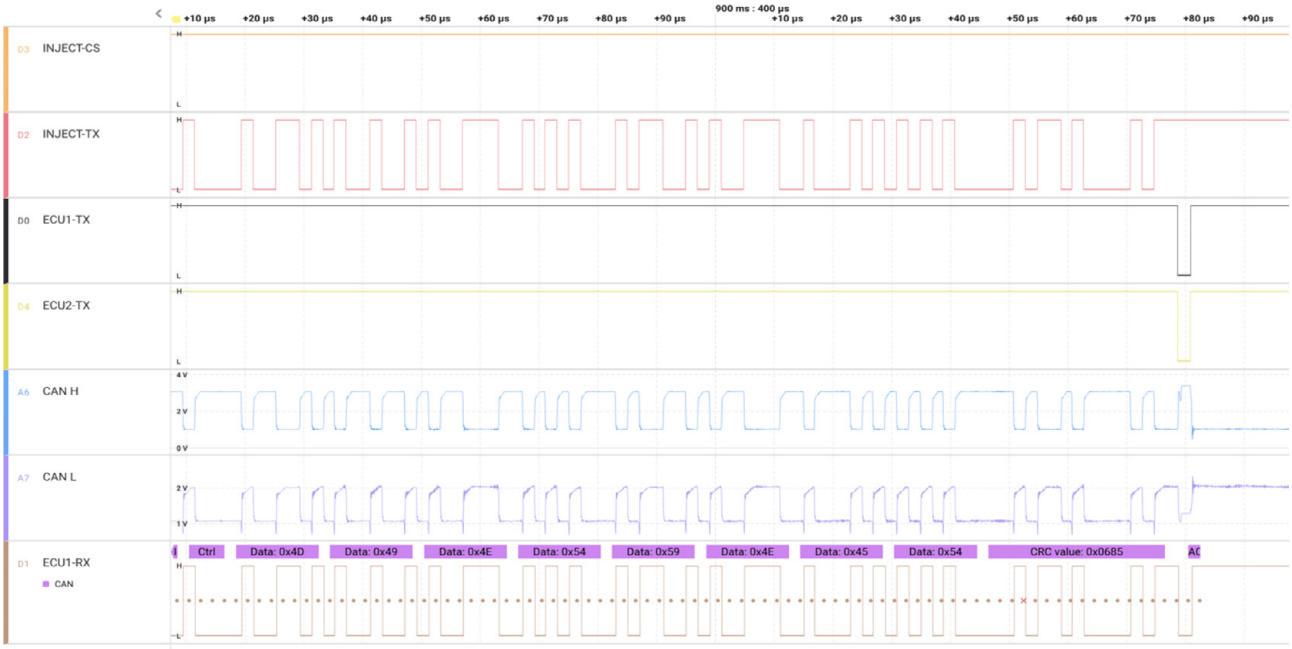


Figure 5: Multiple CAN controllers asserting a dominant state when the CAN Injector dominant-override transceiver circuit is engaged (Source: Canis Automotive Labs)

Figure 4 shows how an ECU CAN controller attempts to assert a dominant state on the CAN network. But the CAN Injector device holds the voltages below the thresholds needed for any CAN transceiver to recognize a dominant state. The transmitting CAN controller goes through the error rules of the CAN protocol (since sending a 0 but reading a 1 is a CAN bit error) and then goes “Bus Off”. The specific pattern seen for CAN TX from the ECU CAN controller is explained in the answer to a recent CAN Quiz Question [6].

The specific CAN Injector uses a Microchip PIC18F with an on-chip CAN controller. To transmit a CAN frame correctly, the acknowledge field must be read back as 0: receivers must assert a dominant bit in this field. If a CAN controller cannot assert a dominant state, then this would cause the spoof frames to fail to be received. However, the transceiver circuit in the CAN injector is designed so that when *multiple* CAN controllers assert a dominant state *at the same time*, then the combination does force a dominant state and the receivers all accept the spoof CAN frame. Figure 5 shows this happening.

This is important because of how it affects state-of-the-art CAN security hardware that is used to detect and destroy spoof CAN frames. For example, CAN-HG augmentation [2] can automatically identify spoof frames (by using out-of-band data added to Classical CAN frames, containing physical address information) and destroy them by asserting a CAN error (i.e. sending six dominant bits). The ‘Stinger’ secure CAN transceiver from NXP [3] contains Block/Pass lists of CAN-IDs and any frames with CAN-IDs on the Pass list that are sent from elsewhere on the network are deemed spoof frames and are destroyed. But dominant override transceivers can neutralize anti-spoofing hardware.

References

[1] https://kentindell.github.io/2023/04/03/can-injection/
[2] https://canislabs.com/canhg/
[3] https://www.nxp.com/products/interfaces/can-transceivers/secure-can-transceivers:SECURE-CAN
[4] https://can-newsletter.org/hardware/gateways/230308_implementation-requirements-for-secured-gateways_canis-labs_cnlm/
[5] https://canislabs.com/cryptocan/
[6] https://kentindell.github.io/2023/03/29/can-quiz-2-answer/

Defeating the CAN Injection attack

There are in practice only two ways to defeat a CAN Injection device with a dominant override transceiver: (1) Partition a CAN network into trusted and untrusted segments with a security gateway [4] between, or (2) use cryptographic protection for CAN frames. The problem with the security gateway approach is that it relies on there being no physical access to the trusted network. This leaves just cryptographic protection to defeat CAN Injection. The Autosar SecOC framework for Classical CAN uses four payload bytes to contain authentication information and four bytes of application payload. The CryptoCAN [5] scheme from Canis Labs uses a pair of CAN frames to carry an encrypted and authenticated version of the original CAN frame. Both schemes rely on the cryptographic primitives provided by the Secure Hardware Extensions (SHE) Hardware Security Module (HSM) standard. It is possible to emulate an SHE HSM in software for micro-controllers without HSM hardware – and this provides a way to defeat CAN Injection for existing vehicles by updating ECU firmware.

There is an adage that says “Cryptography is a machine for turning any problem into a key management problem” and this is certainly true for defeating the CAN Injection attack: there must be tools and infrastructure for the secure creation, distribution, re-programming, and storage of keys. Fortunately, the SHE HSM standard ▷

Inferring the sender of a CAN frame

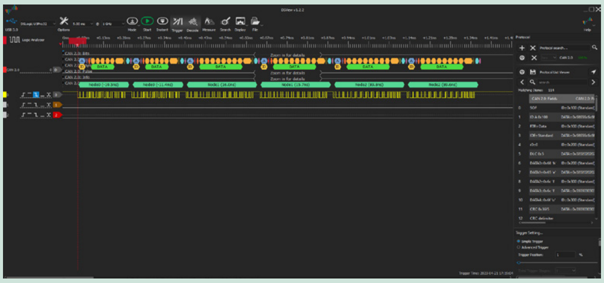


Figure: The decoder uses tiny variations in timing of CAN recessive pulses to automatically infer which CAN frames come from which nodes on the CAN (Source: Canis Automotive Labs)

The latest update of the open-source can2 protocol decoder by Canis Automotive Labs is able to automatically infer the sender of a CAN frame. It uses the method of deterministic distortion of CAN signals that result in frames from a given node on the network having consistently shortened or lengthened recessive pulses. The differences can be quite small - just 10 ns or 15 ns - but they can be picked up by a suitably accurate logic analyzer.

The decoder shows more information about what's happening on the CAN than the usual protocol decoders in logic analyzers. It already warns about unusual CAN events (such as error frames, overload frames, or a double-receive), which might be low-level CAN protocol attacks. Upgrading it to automatically infer the sending node for each frame means that the decoder can passively analyze a CAN network: there is no need to unplug nodes to see which frames no longer appear (which anyway disrupts the behavior of a running system). As it maps CAN-IDs to nodes, it can help to build up a detailed picture of a CAN system. This is useful for debugging (e.g. to see which node sends an unexpected CAN frame), for reverse engineering an unknown system, and even for detecting spoof frames. A spoof frame is one with a CAN-ID normally sent from another node, and is a common technique for hacking the CAN network. The CAN Injection attack used to steal cars is an example of a spoofing attack. Read here {1} how to use the protocol decoder.

{1} https://kentindell.github.io/2023/04/21/can2-decoder-update/#fn:4

defines not only cryptographic operations but also a secure key distribution protocol, and this at least allows standardized tools and processes to be used to address the problem. ◀

Author

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

CAN XL plugfest in April

(Source: CiA)

CAN in Automation (CiA) has organized the third CAN XL plugfest, it took place in Troy, Michigan. IP cores from Bosch, Kvaser, and Vector were tested on interoperability as well as CAN SIC XL transceivers from Bosch, Infineon, NXP, and Texas Instruments.

Across from the SAE office in Troy, CiA members tested CAN XL nodes on interoperability. About 30 attendees started early in the morning of April 24 to setup their CAN XL products. After some difficulties to configure the same bit-timing, the morning session started with testing the CAN XL protocol. The FPGA implementations by Bosch and Vector had been tested successfully in the first two plugfest in Nuremberg in 2021 and 2022. In these previous plugfests also the IP core by Fraunhofer/Cast was successfully participating. This time, the IP core by Kvaser was the newcomer. “The CAN XL plugfest was not just about connecting first prototypes of protocol controllers and transceivers from different vendors around the world. The general objective was to test protocol features, the performance of physical layer implementations and potential network designs. It is also an initial and very important step towards the interoperability of CAN XL and a platform to connect engineers with different backgrounds, opinions, and ideas," explained Patrick Isensee from the C&S group.

Morning session: CAN XL protocol testing

Dr. Arthur Mutter (Bosch) led the plugfest. He is also the chairperson of the CiA SIG (special interest group) CAN XL developing the CAN XL specifications. In the plugfest preparation meeting, different bit-timing settings were agreed as well as a 2-pin AKL connector. The selected cable was a twisted Flexray-style cable with a 100-Ohm impedance. The C&S group provided the cable with connectors.

After all nodes to be tested were connected, the morning session started. The tests included receive error cases and transmit error cases. These tests were performed with error signaling enabled as well as disabled. Each bit of the valid CAN XL frame was corrupted and the transmitting node as well as the receiving node reaction was proofed on correct behavior. All three IP core implementations behaved accordingly to the CAN XL specification (CiA 610-1). In the meantime, CiA 610-1 has been integrated into the ISO DIS 11898-1 standard, which will be voted, soon.

▷

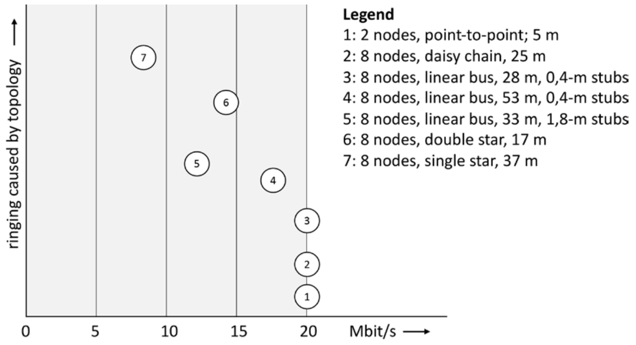


Figure 1: The maximum data phase bit rate depends on the ringing caused by the topology – the more ringing limits the data phase bit rate (Source: CiA)

Afternoon session: CAN XL physical layer testing

In the afternoon several topologies were used. The maximum achieved data phase rate bit-rates are shown in the figure. The arbitration bit rate was 500 kbit/s. The tested CAN SIC XL transceiver compliant with the CiA 610-3 specification were provided by Bosch, Infineon, NXP, and Texas Instruments. NXP used its 2nd generation stand-alone transceivers. The selected topologies (see the figure) were calculated and simulated in advance. The calculated, simulated, and measured results for the selected topologies were nearly identical. This confirmed the robustness and reliability of CAN XL communication.

For the first time, the CAN SIC XL transceivers by Texas Instruments were tested in a CiA plugfest. The results are impressing: 20 Mbit/s seemed to be possible for linear bus topologies with short stubs connecting eight nodes with heterogenous transceivers. But even, if more challenging topologies are needed (i.e. stars and double-stars) high data phase bit rates can be achieved. The wiring harnesses used in plugfest were not optimized. To be serious, the 20 Mbit/s bit rate is the limit for the specified PWM (pulse-width modulation) coding.

Oscilloscopes from different suppliers (Keysight, Pico Technology, Rohde & Schwarz, and Teledyne) were used to decode the CAN XL frames and to measure the bit waveforms on the network lines. All these products provided trigger and decoder functionality. In addition, Vector used its CAN XL tools to analyze the protocol and to generate erroneous CAN XL frames.

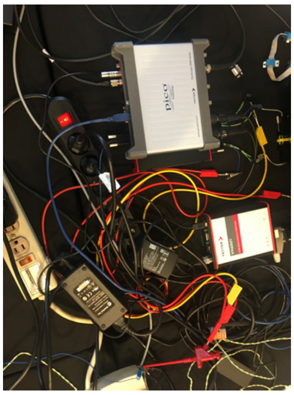


Figure 2: Even though the cabling looks chaotic, the performed interoperability tests worked fine (Source: CiA)

The participating companies were more than satisfied. Dr. Arthur Mutter (Bosch) stated: “It was a great success, as it showed that a significant number of implementations are available and all are interoperable! We successfully performed extensive layer-2 tests (reaction on transmit and receive errors) and layer-1 tests.”

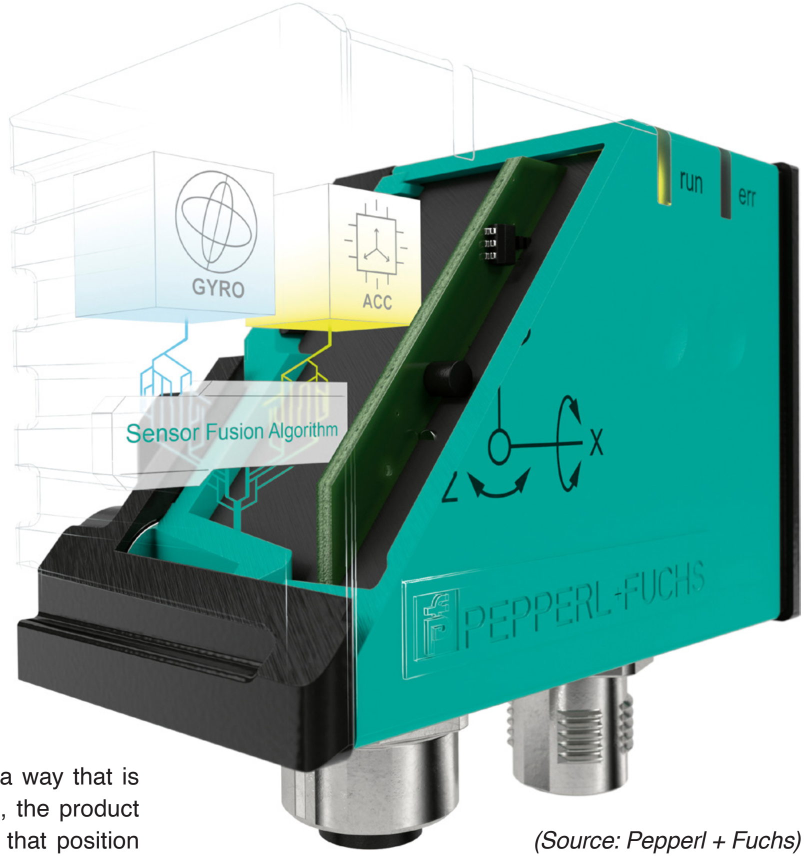
“The plugfest proved that the interest in CAN XL and the ecosystem of controllers, transceivers, and tools are developing quickly”, said Teun Hulman from NXP. “Our 2nd generation of CAN SIC XL prototype transceivers once again proved to be a robust implementation and able to reliably achieve bandwidths up to 20 Mbit/s in complex topologies, also in combination with other implementations. This paves the way for adoption of CAN XL technology in future vehicle and industrial networks.” Vikas Thawani from Texas Instruments (TI) added: “We have successfully demonstrated our 8-pin stand-alone CAN XL transceiver performance in multiple topologies. TI’s transceiver supports low-power standby mode and highest bus fault (±58 V) compared to other solutions currently available.” ◀

Author

Holger Zeltwanger
CAN Newsletter
pr@can-cia.org
www.can-newsletter.org

Dynamic inclinometer with angular stability

Pepperl + Fuchs has developed the IMU F99 sensor providing J1939 connectivity. It features reliable inclination values for dynamic applications, because it is able to filter out external interference (e.g. potholes). The software adjustment configurable via the CAN-based interface ensures a high angular quality, even when the driving behavior of machines varies greatly.



(Source: Pepperl + Fuchs)

Static inclination sensors reach their limits, when used with machines that move dynamically, such as wind turbines, AGVs (automated guided vehicles) as well as construction, agriculture, and forestry machinery. This is because static inclination sensors detect a change in angle based on gravitational acceleration that is always on the same axis. Any additional accelerations triggered, e.g., by braking or travelling over a pothole, cause significant interference, which makes reliable angle measurement impossible.

The IMU F99 dynamic inclination sensor has been developed for this type of dynamic application. At its core, rotation rates and acceleration are both measured in all three spatial directions and are then merged in the smart algorithm to produce an angle value. This makes it possible to achieve a reliable angle output. Nevertheless, it is clear that the different types of machine movements mean that the rotation rate and acceleration need to be merged in a way that is adapted to the particular machine. Therefore, the product comes with adjustment setting capability, so that position measurements can be performed on a wheel loader, bulldozer, crane, etc., using just one device.

The IMU F99 inclinometer also provides the rotation and acceleration rates for each of the three axes in parallel to the angle output. This means that the product can be used in a wide range of applications. For example, the device can be used to determine the rotation speed of wind turbines. At the same time, it can also monitor the blade acceleration rates, which may fluctuate when unwanted ice forms are on the blades. In this way, it is possible to control rotation speed and perform predictive maintenance on the wind turbine.

Acceleration sensor and gyroscope

The inertial measurement unit (IMU), combines an acceleration sensor and a gyroscope into a single device. This device is optimized to provide gyroscopic-stabilized inclination and acceleration data as well as rotation rate data. Heart of the IMU is the adaptive sensor fusion algorithm. It is developed and implemented for inclination measurement with effective compensation of external acceleration disturbance.

Triaxial acceleration sensor and triaxial gyroscope outputs are used as input of the fusion system. The adaptive sensor fusion algorithm is designed to compensate the measurement errors by combining accelerometer and gyroscope data adaptively to the current situation. The Figures 1 to 4 show the orientation and assignment of the axis for which the sensor can be used depending on the parameterization of the angle output system.

The IMU measures the acceleration, yaw rate, and angle in each of the three axes. Regardless of the current position of the sensor in space, the acceleration and yaw rate values equal the rotation rate values. A reliable angle output per measuring axis depends on the current position of the sensor in space. A change in angle around the gravitational vector, which is always vertical, can't be measured. If a measuring sensor axis is parallel to the gravitational vector (±5°), then this axis does not provide reliable angle values and must be ignored. The implemented Gravity Flag (GF) offers help for this. The sensor automatically detects whether a sensor axis is parallel to the gravitational vector and shows this in the status of the Gravity Flag (GF). ▷

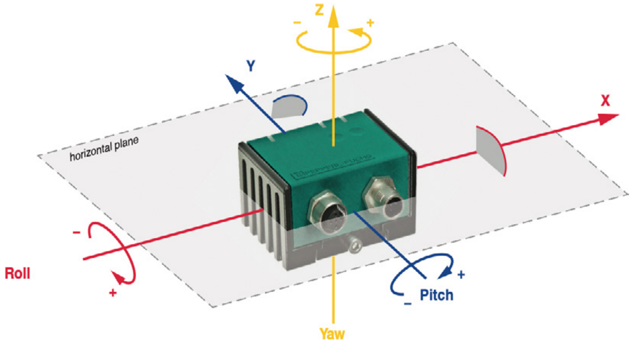


Figure 1: Spatially fixed coordinate system (extrinsic reference to the horizontal plane) for the angles INX or INY (Source: Pepperl + Fuchs)

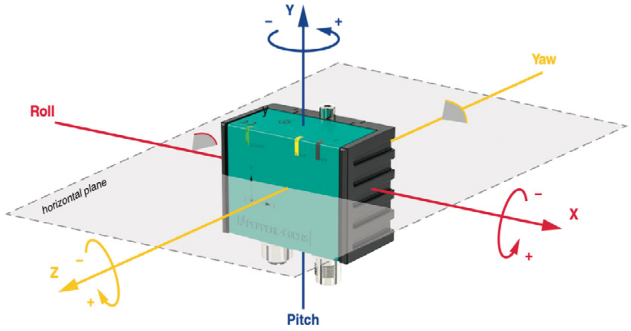


Figure 2: Spatially fixed coordinate system (extrinsic reference to the horizontal plane) for Euler angle (Source: Pepperl + Fuchs)

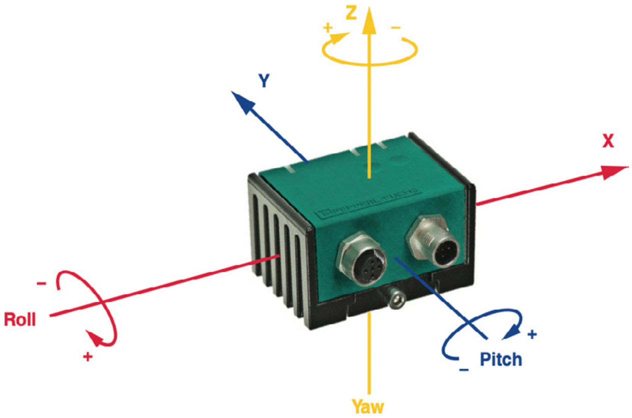


Figure 3: Body fixed coordinate system (intrinsic or co-rotating) for Euler angle zy'x'' (Source: Pepperl + Fuchs)

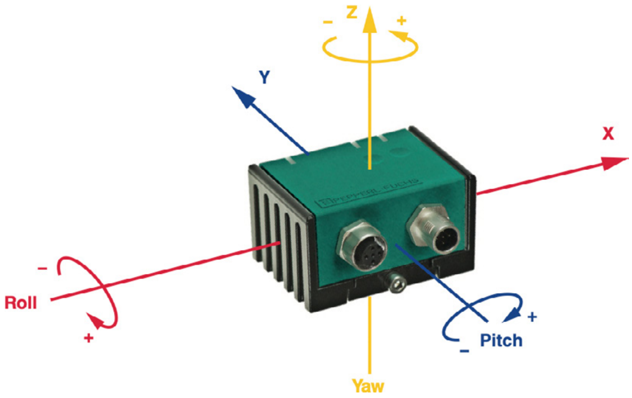


Figure 4: Body fixed coordinate system (intrinsic or co-rotating) for P+F angle INZ (Source: Pepperl + Fuchs)

CANopen profiles mapped to J1939

CiA supports the mapping of device profiles originally developed for the CANopen application layer to the J1939-21 higher-layer protocols. This includes the CiA 510 document specifying the mapping of SDO (service data objects) and EMCY (emergency message) to J1939 parameter groups (PG). This means you can configure and diagnose the J1939 device similar to CANopen. CiA provides additionally a mapping of CANopen-PDOs (process data objects) to standardized PGs. The CiA 406-J document specifies the encoder profile mapping to J1939. The CiA 410-J document does the same for inclinometers, but is not yet released.

The CiA inclinometer base document (CiA 410-B) specifying the process and configuration parameters currently does not support smart inclinometers such as the IMU F99 by Pepperl + Fuchs, for example. If this is desired, the inclinometer profile needs to be improved by means of additional configuration parameters setting the filter options. This would improve device interoperability and partly interchangeability. *hz*

Accordingly, it is always displayed for each angle value as to whether it can be used.

Independent limits can be configured for the X, Y, and Z axes of the acceleration, rotation rate, and angle measurement axis. If these limits are exceeded, this is indicated in the switching status of the Application Flags (AF).

Several selectable output values such as acceleration, rotational speed, inclination (Euler angle, Euler value, quaternions), and programmable filters allow users to adapt the measuring system to the application. Parameterization and data transfer take place via the CAN-based SAE J1939 interface.

The J1939 interface

The CAN interface supports a default bit rate of 250 kbit/s. It implements an application layer compliant with J1939-21. As specified in J1939/81, the sensor supports the dynamic address claiming starting with default address 128. If this feature is not desired, it can be deactivated.

The J1939 inclinometer communicates by means of proprietary Parameter Groups (PG). The payload is similar to the PDOs (process data objects) used in the CANopen variant of this inclinometer. The above-mentioned configuration of the J1939 sensor is performed by means of dedicated PGs. This configuration is mainly the setting of filters, which determines the measured signal filtering. This enables the suppression of vibration frequencies. These vibrations could be triggered by a running engine or gearbox, for example. In this way, the quality of the angle output can be adjusted despite disturbing vibrations. The filter type, the filter order, and the width of a low-pass filter are configurable. The filter settings can be defined in the filter-settings parameters.

hz (based on information by Pepperl + Fuchs)

J1939-based networks vulnerability to Address Claim Hunter cyberattack

This article explores a particular weakness in CAN networks based on SAE J1939, which use the self-configurable address mechanism. Mitigation strategies are given to eliminate the vulnerability from an Address Claim Hunter cyberattack.

Cybersecurity in control systems is now receiving a lot of attention. A lot of the network technologies that are successfully used in many control systems have been found to be susceptible to attacks from malicious parties. This article explores a particular weakness in such J1939-based CAN networks as:

- SAE J1939 for trucks, buses, heavy-duty vehicles
- NMEA 2000 for marine applications
- ISO 11783 (Isobus) for agriculture vehicles
- RV-C for recreational vehicles

There is also a number of other J1939-based higher-layer protocols that have been implemented in practice. Using J1939 mechanisms as a basis, these may also have the described vulnerability.

J1939-based networks using the self-configurable address mechanism for claiming a source address enjoy the ability to automatically set themselves up with no user intervention by a defined plug-and-play method. There are 252 or more unique source addresses available, and each device will attempt to claim a unique one of these dynamically. If a device is not able to claim a unique source address, it signifies this by a “Cannot Claim Address” message and then does not participate in any further network communication activity. Whilst this feature provides a lot of flexibility, it also means that devices that support the self-configurable address feature are susceptible to an attack by an Address Claim Hunter algorithm, resulting in a “denial of service” (DoS). Such attacks can leave many devices disabled or at worst case disable the entire network. Depending on how safety-critical the devices on the network are, the outcome could at a minimum be an annoyance or endanger life.

The particular weakness

The first studies known to report a vulnerability in the SAE J1939 Address Claim functionality was in 2018 [1, 2]. They found that the dynamic address claim mechanism could be used to upset the network. However, testing carried out by the author on a random selection of devices shows that this situation is in fact more serious, and most were susceptible to invalid Address Claim messages (i.e. those with invalid fields, that should not be allowed on the network).

This particular weakness in J1939-based networks involves the following steps:

- Gain access to the CAN network so that a malicious algorithm can be deployed;
- Disable a device (e.g. a water speed sensor in NMEA 2000 network) using an Address Claim Hunter algorithm;
- Claim the device’s old source address on the network and spoof the network by sending incorrect measured values (e.g. vessel water speed over the NMEA 2000 network).

To be able to attack one of these networks, the attacker just needs to be able to access the CAN network. Examples of these include:

- Physically add small device whose aim is to disrupt network (e.g. see Figure 1);
- Putting a USB key into a PC on the vessel. If the PC itself can reflash or reconfigure an ECU (electronic control unit);
- Via IoT-connected or Internet-connected type device.

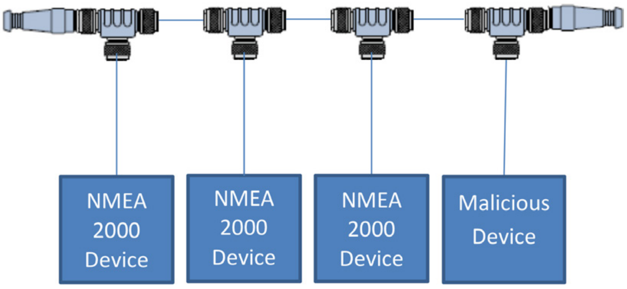


Figure 1: Typical installation for NMEA 2000 (Source: Warwick Control Technologies)

Figure 1 shows the typical configuration of an NMEA 2000 network in which off-the-shelf cables and connectors are simply screwed together via M12 connectors of the appropriate genders. It is easy just to add a T-connector and add the malicious device. NMEA 2000's easy wiring is an advantage for installation but also an advantage for hiding a malicious device behind a panel. Other networks such as J1939 on trucks could also easily have a malicious device added in secret.

There is no standard mechanism for detecting this and therefore the likelihood of this succeeding is quite high. An example of this could be that a malicious device could be installed on a vessel and wait for a trigger to occur before executing the attack. This could be a vessel location, speed, etc. When the trigger conditions are met, then the attack is initiated.

SAE J1939-based networks and address claim

The J1939-based networks support dynamic address claiming so that each ECU claims a unique source address. This feature is very flexible so that devices can be easily added to a network. However, this functionality is also vulnerable to a cyber-attack that can stop some or all nodes from working.

There are a few different address claim mechanisms defined in SAE J1939-81 for network management. The final of these is concerned with dynamic addressing and referred to as "self-configurable address ECUs", which enables a plug-and-play functionality. If two ECUs have the same source address, the clash is dealt with and the process re-assigns each source address automatically.

Whilst address claiming is taking place, a device or ECU cannot send its normal PGNs (parameter group numbers) onto the CAN network, therefore the system is disrupted at this time. Arbitration when two nodes claim the same source address is dealt with using the NAME field (or Address Claim field in RV-C), which is the 8-byte data field of the address claimed message. The lower numerical value of this 64-bit value wins the address claim and, in theory, a data field with all zeroes has therefore the highest priority and will always win the claim for a source address. The data field with all zeros (e.g. 0000 0000 0000 0000) is however an invalid setting. The following explains why. The NAME or Address Claim field across the four networks is compared in Table 1 to Table 4.

Table 1: SAE J1939 – NAME convention (Source: Warwick Control Technologies)

Arbitrary Address Capable	Industry Group	Vehicle System Instance	Vehicle System	Reserved	Function	Function Instance	ECU Instance	Manufacturer Code	Identity Number
1 bit	3 bit	4 bit	7 bit	1 bit	8 bit	5 bit	3 bit	11 bit	21 bit

Table 2: ISO 11783 – NAME convention (Source: Warwick Control Technologies)

Self Configurable Address	Industry Group	Device Class Instance	Device Class	Reserved	Function	Function Instance	ECU Instance	Manufacturer Code	Unique Number
1 bit	3 bit	4 bit	7 bit	1 bit	8 bit	5 bit	3 bit	11 bit	21 bit

Table 3: NMEA 2000 – NAME convention (Source: Warwick Control Technologies)

Reserved (set to 1)	Industry Group	System Instance	Device Class	Reserved	Device Function	Device Instance (Upper)	Device Instance (Lower)	Manufacturer Code	Unique Number
1 bit	3 bit	4 bit	7 bit	1 bit	8 bit	5 bit	3 bit	11 bit	21 bit

Table 4: RV-C – Address claim field (Source: Warwick Control Technologies)

Arbitrary Address Capable	Compatibility Field			Reserved	Compatibility Field	Function Instance	Node Instance	Manufacturer Code	Serial Number
1 bit	3 bit	4 bit	7 bit	1 bit	8 bit	5 bit	3 bit	11 bit	21 bit

The first part to examine why all zeroes in the Address Claim field is invalid is to look at the left-most bit, which is called "Arbitrary Address Capable" in SAE J1939 and RV-C. This should be set to 1 if to correctly indicate that the ECU supports self-configurable addressing. In NMEA 2000 it is called "Reserved" and should always be set to 1. For NMEA 2000, the "Industry Group" will always be set to 4 (which means a marine network). In SAE J1939, the "Manufacturer Code" of 0 is not allowed and is a reserved value. This means that a NAME field set to all zeros should not occur on these networks in practice. However, many devices in the market will lose the address claim process to a NAME field including all zeroes. According to NMEA 2000, Appendix D (D 4.3), NMEA 2000 does not support an unknown or not available state or value for any of the NAME fields. However, from testing carried out it is clear that this is not the case.

Address Claim Hunter algorithm and impact on a self-configurable device

The Address Claim Hunter algorithm is a simple method to force one or many devices from their source address so that they eventually run out of source addresses to claim. This results in the affected devices to not be able to claim an address, issue the "Cannot Claim Address" message and then no longer participate in (NMEA 2000) network communications. It is possible to use this method to attack all devices (all source addresses) or a specific manufacturer code. Example algorithms 1 and 2 illustrate the simplicity of this approach.

Example algorithm 1 running in malicious device

```
If (Address Claim Msg Received)
    THEN Send Address Claim Msg with
    NAME 00 00 00 00 00 00 00 00
```

The execution of the example algorithm 1 would trigger a sequence of events as shown in Figure 2. The process starts with an attempt by a device (device under attack) to claim source address (SA) as 0. This device is then attacked by a malicious device, which claims SA=0. Then the device under attack attempts to claim addresses 1 through to 251, but each time the malicious device claims the source address using a higher-priority NAME field. The process ends with the device under attack having tried to claim every possible source address, issues a "Cannot Claim Address" message with source address = 254. It then takes part in no further network activity. Once this has happened, it is usual that some kind of external intervention is needed to reset the device such as an ignition/power cycle.

Example algorithm 2 running in malicious device

Another Address Claim Hunter algorithm for an example attack on a fictional Warwick device is shown in Figure 3. This has a simple approach to attack a particular device manufacturer, e.g. send ISO request for address claimed to all devices:

```
If ((Address Claim Msg Received) AND (Manufacturer Code is Warwick))
    THEN Send Address Claim Msg with
    NAME 00 00 00 00 00 00 00 00
```

The result of this attack is that a device under attack:

- Will try to claim new source addresses thus upsetting the network;
- Whilst claiming a new source address, all control PGNs will normally be suspended, because the device does not know which source address it should be using and receiving devices do not know which source address to expect to receive the PGNs from;

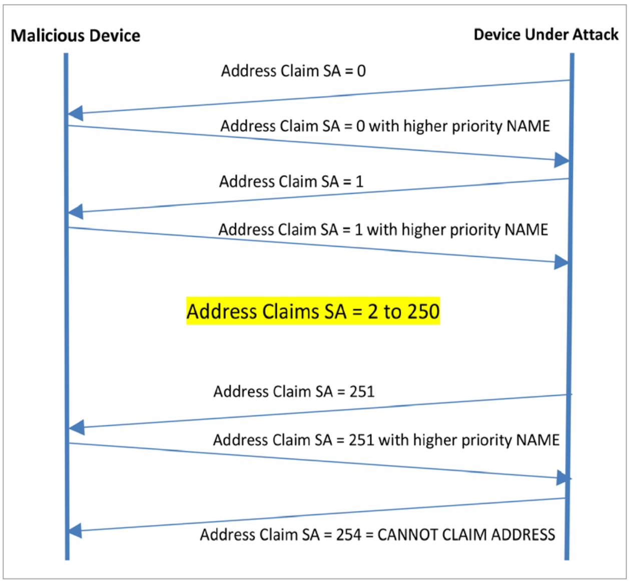

Malicious Device
Device Under Attack
Address Claim SA = 0
Address Claim SA = 0 with higher priority NAME
Address Claim SA = 1
Address Claim SA = 1 with higher priority NAME
Address Claims SA = 2 to 250
Address Claim SA = 251
Address Claim SA = 251 with higher priority NAME
Address Claim SA = 254 = CANNOT CLAIM ADDRESS

Figure 2: Address Claim Hunter algorithm 1 sequence (Source: Warwick Control Technologies)

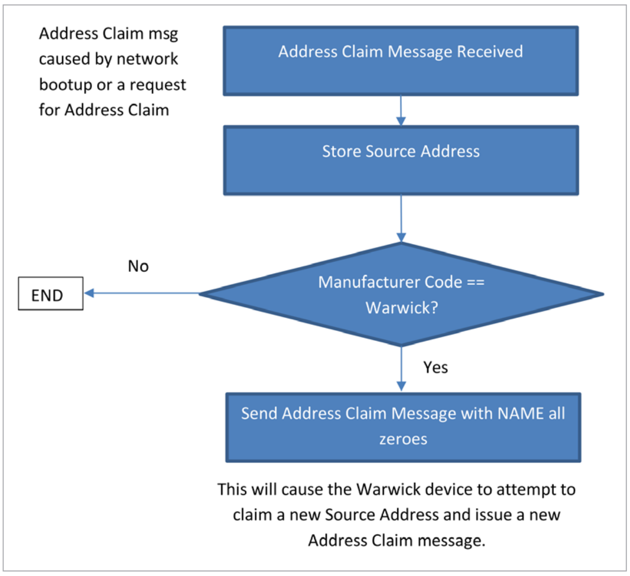

Address Claim msg caused by network bootup or a request for Address Claim
Address Claim Message Received
Store Source Address
Manufacturer Code == Warwick?
No
END
Yes
Send Address Claim Message with NAME all zeroes
This will cause the Warwick device to attempt to claim a new Source Address and issue a new Address Claim message.

Figure 3: An Address Claim Hunter algorithm 2 (Source: Warwick Control Technologies)

- Once all possible source addresses have been tried by the device, it will issue a "Cannot Claim Address" message (on the null address FE_h) and cease all communications. Usually, the only way to make this device to go online again is some kind of operator intervention.

Potentially the severity of this is dependent upon the type of device that is attacked. For example, does your system remain safe if it uses GPS location or water speed? What if a system providing Thruster feedback information is taken down, what will the system do?

Address Claim Hunter followed by a spoof attack

It is possible to use the Address Claim Hunter algorithm to spoof the network. The process for this is to take the device down using one of the previously described Address Claim Hunter algorithms. Once the device has been taken down, spoof PGNs can be sent, potentially using incorrect values with the intent of sending malicious damage. For example, actual vessel speed could be 3 m/s when it is actually 0 m/s.

Possible protection mechanisms

Protecting proposals outlined in this clause are by no means exhaustive but merely some initial suggestions for designer to consider.

NAME and Address Claim field plausibility checks

Here are some recommendations of plausibility checks that can be made on the NAME field:

- The fields "Reserved" (NMEA 2000), "Arbitrary Address Capable" (J1939, RV-C), and "Self-Configurable Address" (ISO 11783) should equal 1. This is the easiest of checks to carry out. In NMEA 2000, two of the fields in the NAME field are nominated as "Reserved" and should be set to 1.
- Creation of an Allow/Deny list of manufacturer codes, function code, and class: The more sophisticated protection can be achieved by a simple plausibility check of the fields "Manufacturer Code", "Function Code", and "Class" within the NAME field. A vessel manufacturer will know which combinations are valid for a specific model and from the NMEA organization a list of certified products and their attributes is available so that these can be cross-checked for plausibility using a combination of Allow/Deny lists. Upon receipt of an address claim message, it would be possible to check which combinations are valid from the published NMEA list of certified products. This approach reduces the openness, interoperability and plug-and-play capabilities of the NMEA 2000 protocol. Devices would need a firmware update to be able to accept a newly fitted device. However, this could be an important feature for safety-critical systems.

Fixed address for safety-critical devices

In SAE J1939 a number of devices have recommended fixed source addresses, e.g. source address 0 for the engine. Such devices do not take part in any dynamic source address assignment activity. There is usually a range of source addresses that are reserved for devices that take part in the dynamic source address assignment. As the networks grow with the addition of new PGNs considerable for safety-critical systems (e.g. electric propulsion, steering controls, etc.) then a limited area of recommended fixed addresses would protect such devices from attacks such as the Address Claim Hunter.

Wait then recover

A way for a device that "Cannot Claim Address" could be to wait for an application-specific time and then attempt to recycle again. The trigger could be a prompt on a mobile field device or tablet to allow user intervention or some automatic application software triggering to lead to an attempt to claim an address again (e.g. searching for a gap using ISO request).

Address claim NAME tracking

Apply an additional rule to the address claim process, e.g. has the same device (NAME) made another address claim, when no other device has requested that address? For example, Device A has address 10, it receives an ISO address claim from a device with NAME 00000000_h, which ▷

Device A relinquishes and gets an address 11. It then receives another ISO address claim from a device with the same NAME 00000000_h for address 11, but no other device requested the address 10, so it rejects the address claim and transmits a new alert PGN for "Suspicious Network Activity Detected". Therefore, a device would simply need to remember its last valid CAN address, the NAME of the device that requested it and if any other device has requested its last valid CAN address. This is a bit of an overhead but should be easy to implement.

Conclusion and recommendations

This article has highlighted a particular vulnerability that the J1939-based networks have to a cybersecurity attack that exploits part of the protocol that deals with dynamic address claiming for self-configurable ECUs and devices. The dynamic address claim feature is one of the benefits of these protocols that allows a plug-and-play type functionality for adding new devices to the network. However, it has been shown that this can be exploited and result in a complete network shutdown for susceptible devices. The impact of this can range from being an annoyance through to being a serious safety concern as these networks being used increasingly for more important control applications. Not all J1939-based implementations will be susceptible. The susceptibility will depend upon how the dynamic address claim functionality is implemented. The good news is that the implementation of some additional checks and balances can reduce the risk. Designers of J1939-based systems should consider implementing various address claim plausibility checks to ensure that this weakness cannot be exploited. ◀

Author

Dr. Chris Quigley
Warwick Control Technologies
enquiries@warwickcontrol.com
www.warwickcontrol.com

References

[1] Murvay P.S. and Groza B. (2018); "Security Shortcomings and Countermeasures for the SAE J1939 Commercial Vehicle Bus Protocol," in IEEE Transactions on Vehicular Technology, vol. 67, no. 5, pp. 4325-4339, May 2018

[2] Daily J. (2018); "Introduction to SAE J1939" Cybertruck Presentation, page 124

- SAE J1939-81, J1939 network management
- ISO 11783-5, Tractors and machinery for agriculture and forestry — Serial control and communications data network — Part 5: Network management
- NMEA 2000, Specification package v. 3.0
- RV-C, Recreation vehicle communications, clause 3.3.

Virtual CAN FD network

Using the "Virtual CAN Bus" it is possible to separate the control tasks from other bandwidth-consuming tasks by modifying the physical layer i.e. the transceiver and the communication network without any impact on the control task.

The bandwidth required for pure control tasks is governed by the dynamics of the machinery to be controlled. CAN is a well-proven network for control tasks in a distributed embedded control system. For example in cars, it is not well suited for requirements that relate to the security of messages, transfer of raw data from advanced sensors and cameras as well as the re-flashing of ECUs (electronic control units) that demand a high bit rate. The primary reason for this is that CAN uses a very simple bit transfer method and a low bit rate at the arbitration phase.

A solution to this dilemma is the "Virtual CAN Bus" where signals to and from ordinary CAN controllers are multiplexed by smart transceivers that support one or more modern high-speed communication protocols running on the same physical layer. In this way, CAN is kept for control tasks and continuously the advantages of the newest technology for bandwidth-hungry tasks are used.

Proposed solution principles

CAN is, in a sense, a unique protocol: The transmitter uses 100 % of the network bandwidth but the receivers use just a fraction of it. The proposed solution takes advantage of this peculiarity. It introduces a "Virtual CAN Bus" (VCB), executed in a smart transceiver unit "Virtual CAN Converter" (VCC) connected to an ordinary CAN controller. The smart VCC transceiver encodes and transmits the CAN information on a modern high-speed communication. CAN signals are transmitted from the CAN controller to the VCC transceiver using the TX connection, according to the CAN standard. However, the signals are reduced to only dominant edges and the respective bit values (i.e. the only things CAN receivers identify), which are then passed to the lower layers of the transceiver unit. The communication in the final system runs on a modern physical layer where such reduced CAN bits are multiplexed and modulated. At reception, the encoded CAN dominant edges and bit values are received and the receiving VCC transceiver restores the CAN bits and signals these to the CAN controller's RX connection.

By using the VCB, the control task is separated from other tasks. The distributed embedded control system can be developed using standard CAN controllers and transceivers in a traditional way with well proven tools. Other tasks such as encryption, transmitter authentication, re-flashing, etc. can be developed by experts in these fields and carried out by using other protocols. With modern technology, the different tasks can run in parallel and simultaneously communicate on the same physical layer. It is a great advantage to separate the control problems from other problems. The control problem can be solved once and for all by the control experts and other problems by experts in their respective technology fields. Any solution to problems in those fields can be implemented at a later date by modifying the physical layer i.e. the transceiver and communication network without any impact on the control task.

CAN background

CAN was designed purposely to fit the needs of a distributed embedded controller network. The most important properties are:

1. No addresses. All nodes receive all CAN frames and determine if the frame should be received or not.
2. All nodes participate in error handling. No application receives a frame if all nodes have not found it to be correct.
3. Bit-wise arbitration at frame collisions. No frame is lost, and the maximum latency of any frame can be calculated.

These three properties solve some general control design problems in an efficient and elegant way.

- A first problem is data consistency within a system. All nodes shall have the same information at any given time. CAN takes care of this.
- A second problem is a predictable latency time. CAN allows the maximum latency time to be calculated, even for unscheduled frames.
- On top of that, the "No-address" feature makes the frames short as only a CAN-Identifier and a value are transported during the runtime. The required network bandwidth is minimized.

When CAN was developed in the early 80s, it was very efficient. It made maximum use of the technology at hand. CAN remains an excellent protocol for control systems. However, new tasks have been assigned to it. The first one was flashing of ECUs. The ECU software is continuously growing and using CAN for this purpose proved too slow. To remediate this problem, Bosch started in 2011 developing the CAN FD (CAN with flexible data rate) resulting in the ISO 11898-1:2015 standard. With the arrival of CAN FD, flashing could be done faster, but more requirements were then brought to the table. Fear for the system hacking requires encryption of the data and authentication of the transmitter and this creates more message overhead, ▷

i.e. longer messages. Another problem is that some safety standards require a Hamming Distance of a minimum of 4. Initially, CAN was said to have a Hamming Distance of 6, but it was later shown that a data bit mistaken for a stuff bit and vice versa might result in the same frame length and the same CRC (cyclic redundancy check) value, in which case the Hamming distance is only 2. This is true also for CAN FD and this might disqualify CAN for use in some safety critical systems.

In addition to distribution of control data in an efficient and reliable way (solved already by Classical CAN), CAN FD should also be capable of:

1. Encryption of messages.
2. Authentication of the message transmitter.
3. Fast file transfer for ECU flashing.

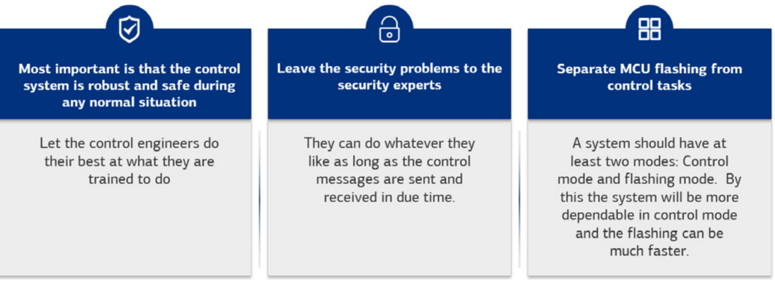
CAN FD does not seem to solve the additional problems and the Hamming distance issue remains.

The solution

CAN is used for feedback loop controls of systems involving mass. The bandwidth needed for control tasks is governed by the dynamics of the controlled items: the lower the mass, the higher the bandwidth needed. Most devices with CAN are related to humans. Since we can expect these ‘human-related’ devices to remain roughly the same size forever, we can safely say that the dynamic requirements of the future will be the same as today. Notably, many fourth-generation jet fighters are controlled by MIL-STD-1553 systems running at 1 Mbit/s. Does a car really need a faster control system than a high-performance, inherently unstable jet fighter? MIL-STD-1553 is less efficient than Classical CAN, so we can expect CAN FD to match any control demand of the future.

Figure 1: Modern, fourth-generation jet-fighters use MIL-STD-1553 at 1 Mbit/s, which is less efficient than CAN (Source: Adobe Stock)

CAN is more than adequate for control tasks. The driving force for a higher bandwidth for CAN is instead due to non-control issues. We should find a way to run an “old-fashioned” CAN system with a low bit rate on a modern physical layer, multiplexed with another protocol with a high bit rate that carries all the other information needed to satisfy any requirement on top of the control task. A starting point is an efficient system architecture with features given in Figure 2.



Most important is that the control system is robust and safe during any normal situation

Let the control engineers do their best at what they are trained to do

Leave the security problems to the security experts

They can do whatever they like as long as the control messages are sent and received in due time.

Separate MCU flashing from control tasks

A system should have at least two modes: Control mode and flashing mode. By this the system will be more dependable in control mode and the flashing can be much faster.

Figure 2: An efficient system architecture (Source: Kvaser)

Hence, let us:

- Separate control problems from other problems
- Use CAN for control tasks
- For other tasks, use better suited protocols
- Run multiplexed protocols on the same physical medium

This can be achieved by having the transceiver establishing a “Virtual CAN Bus” (see Figure 3).

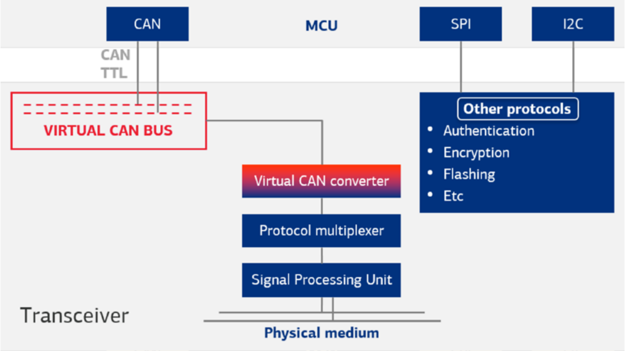


Figure 3: The transceiver establishes a “Virtual CAN Bus” (Source: Kvaser)

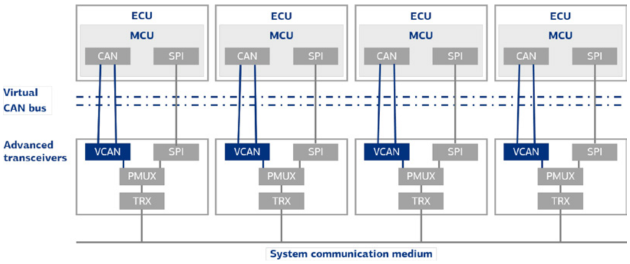


Figure 4: The respective CAN controller sends/receives the TTL signals according to the CAN FD standard (Source: Kvaser)

The physical layer carries two or more protocols in parallel and the transceiver multiplexes/demultiplexes the protocols. A “Virtual CAN Converter” in the transceiver processes CAN frames in a specific way.

Essential CAN features for a “Virtual CAN Converter”

The Figure 5 shows the construction of a CAN FD bit. ▷

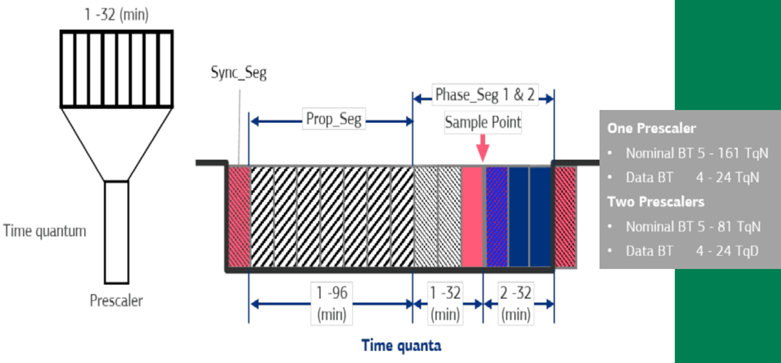


Figure 5: Construction of a CAN FD bit (Source: Kvaser)

According to the ISO 11898-1:2015, a CAN FD bit is constructed on time quanta. A time quantum (TQ) represents a number of clock cycles. A bit starts with a Sync_Seg of one TQ followed by a Prop_Seg, a Phase_Seg 1, and a Phase_Seg 2. The value of the bit is sampled at the sample point located between Phase_Seg 1 and Phase_Seg 2. The signal on the bus lines is the amplitude modulated in the simplest way: A zero is voltage, a one is no voltage. A CAN transceiver balances the outputs CAN high (CAN_H) and CAN low (CAN_L) around 2,5 V (see Figure 6).

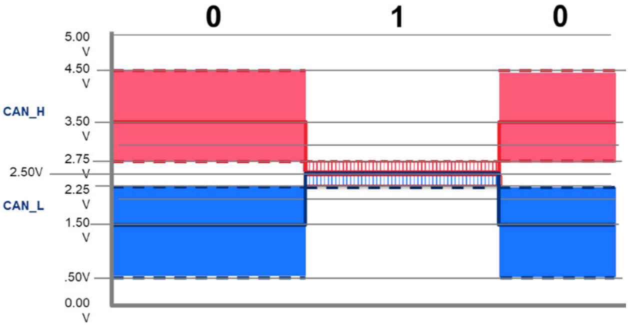


Figure 6: A CAN transceiver balances the outputs CAN high (CAN_H) and CAN low (CAN_L) around 2,5 V (Source: Kvaser)

At the sample point, the bit value is decided by the differential voltage between CAN_H and CAN_L (see Figure 7).

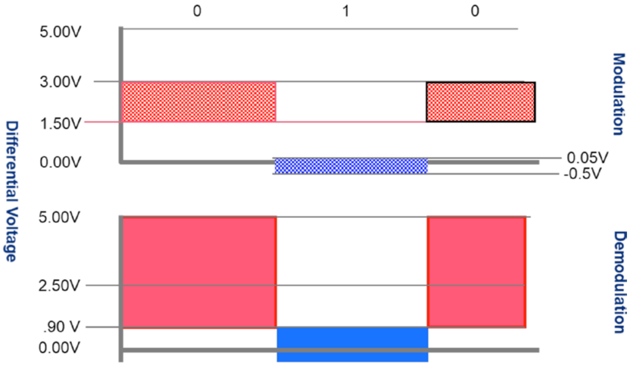
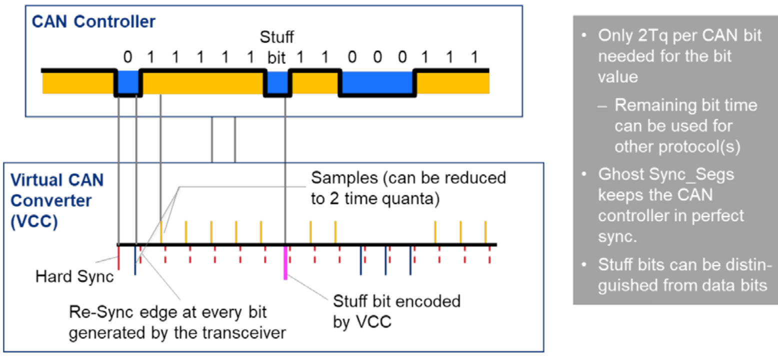


Figure 7: The bit value is decided by the differential voltage between CAN_H and CAN_L (Source: Kvaser)

A unique characteristic of CAN is that the transmitter occupies 100 % of the network bandwidth when transmitting but the receiver only a fraction of it at reception. The receiver only looks for flanks from an idle bus (recessive state, continuous value of 1) to dominant value (0), denoted as a dominant edge, where it makes a hard synchronization of the bit clock. If it samples the zero level at the sampling point, it regards the signal as a "start of frame" (SOF) and continues to look for dominant edges (where it resynchronizes its bit counter) and samples the bit value at each sample point. Any other signal is ignored. Thus, the receiver only uses two or three time quanta of every received bit. CAN uses a non-return-to-zero (NRZ) coding so consecutive bits of the same value are demodulated by dead reckoning of the sample points. Stuff bits with the opposite value are inserted when five bits of the value are transmitted in order to keep the bit clocks synchronized.

Reduced CAN Protocol (RCP)

Implemented in the "Virtual CAN Converter" is a "Reduced CAN Protocol" (RCP) that creates dominant edges at each Sync_Seg and the bit value at each sample point. This would take only one TQ for the Sync_Seg and two for the bit value. According to the CAN standard, a stuff bit of the opposite value should be transmitted after five consecutive bits of the same value. As described earlier, this causes some problems with the Hamming Distance. The "Virtual CAN Converter" could modulate the stuff bits and send an error frame if a stuff bit is detected in the wrong place.



CAN Controller
Stuff bit
0 1 1 1 1 1 bit 1 1 0 0 0 1 1 1
Virtual CAN Converter (VCC)
Samples (can be reduced to 2 time quanta)
Hard Sync
Re-Sync edge at every bit generated by the transceiver
Stuff bit encoded by VCC

- Only 2Tq per CAN bit needed for the bit value
  - Remaining bit time can be used for other protocol(s)
- Ghost Sync_Segs keeps the CAN controller in perfect sync.
- Stuff bits can be distinguished from data bits

Figure 8: Reduced CAN Protocol principle (Source: Kvaser)

The RCP also generates a dominant edge at the end of every bit, i.e. a "Ghost Sync_Seg" (see Figure 8 and Figure 9) at each bit instance where the CAN controller is not generating a recessive bit followed by a dominant bit (1/0). This keeps the CAN controller in synchronization with the VCC.

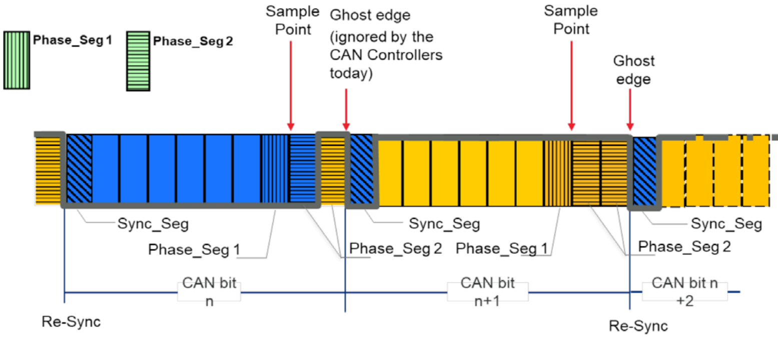


Figure 9: Injection of "Ghost edges" (Source: Kvaser)

According to the CAN protocol, Phase_Seg 2 should be no shorter than two TQ. Being so, the VCC can make a recessive TQ at the Phase_Seg 2 of a dominant bit and we have a dominant edge at every bit. However, the CAN controller ignores any dominant edge after sampling a dominant value, so such an edge will not cause a resynchronization. A worst-case scenario would then be six bits before the CAN controller resynchronizes (five consecutive 0 values and a stuff bit).

The VCC will receive full bits from the CAN controller but can reduce these to edges and bit-value signals at the sample points. The generation of "Ghost edges" after dominant bits could be of value to the "Protocol Multiplexer" (PMUX) but if not, this VCC feature can be omitted. ▷

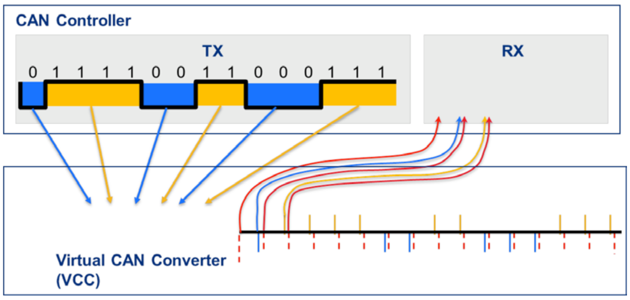


Figure 10: The VCC receives the full bits from the CAN controller on the TX line but transmits back only dominant edges and the bit values at the sampling point on the RX line (Source: Kvaser)

When the CAN controller transmits, the VCC receives full bits, i.e. differential voltage shifts when two consecutive bits have a different value, from the TX line of the CAN controller. The VCC creates at least a Sync_Seg and a bit value at the sample point at the respective bit and feeds them back to the RX line.

The information from the VCC to the "Protocol Multiplexer" can be further reduced. Already at the Sync_seg of bits from the CAN controller, the VCC knows the value of the bit. By applying some of the CAN specification rules, it can also know if it is a start of frame, any of the fixed value bits, end of frame (etc.) and add this information to the "Protocol Multiplexer" by a modulated signal. This can be done in a fraction of the CAN bit time.

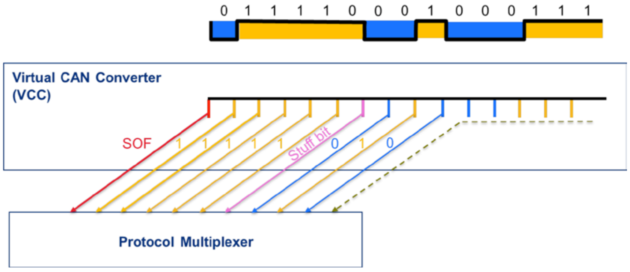
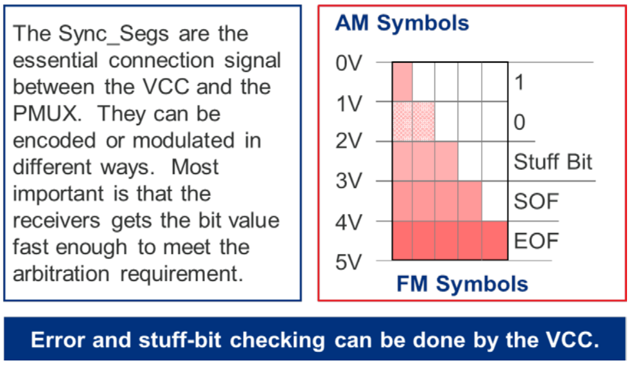


Figure 11: The VCC transmits only encoded Sync-Segs to the PMUX (Source: Kvaser)

The length of a CAN frame can be very important. It is therefore an advantage if the VCC in communication with the "Protocol Multiplexer" generates an encoded SOF bit at the beginning of a frame and an encoded EOF bit at the end of the frame. The RCP should then be capable of generating three specific encoded bits: SOF, EOF, and stuff bits. The encoding can be done in many ways, e.g. by amplitude modulation or phase modulation.



The Sync_Segs are the essential connection signal between the VCC and the PMUX. They can be encoded or modulated in different ways. Most important is that the receivers gets the bit value fast enough to meet the arbitration requirement.

Error and stuff-bit checking can be done by the VCC.

Figure 12: CAN bit modulation (Source: Kvaser)

The TQ on the CAN controller side can be different (longer) from the PMUX side (shorter), as the CAN controller side is limited by old technology but the PMUX can use modern and faster technology. Each Sync_Seg signal at the CAN controller side can be modulated on the PMUX side to immediately also carry the bit value. As the connection between the CAN controller and the VCC is a short point-to-point connection, the risk of disturbances is very low and the signal quality can be constantly supervised and acted upon.

Protocol multiplexing

The basis for the protocol multiplexing is the CAN frame generated by the RCP at the VCC. Such a frame is initiated either by the CAN controller or the "Protocol Multiplexer". It is essential that the timing of the RCP signals is kept by and through the "Protocol Multiplexer" and the "Signal Processing Units", so the VCCs can accurately create the "Virtual CAN Bus". A CAN frame (see Figure 13) starts with the dominant SOF bit followed by the CAN-Identifier field and one more bit (RTR bit in Classical CAN and RRS bit in CAN FD). These bits can be sent simultaneously from two or more CAN controllers. The ACK bit is sent from all receiving CAN controllers.

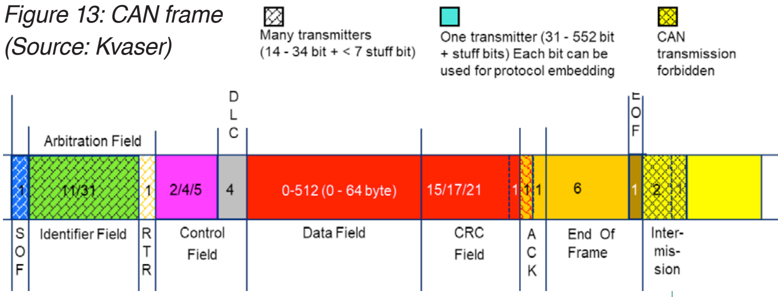


Figure 13: CAN frame (Source: Kvaser)

This can cause some difficulties for the "Protocol Multiplexer" and the RCP. When a bit value is received when more than one CAN controller is transmitting, the bit value can appear anywhere in the Prop_Seg of the CAN bit. The RCP has to catch it and transmit it to the CAN controller at the sample point. There are (at least) two ways to solve the problem:

1. The bit value is sent continuously on the communication in the part of the CAN frame where multi-transmissions are allowed. Any second protocol signal is blocked.
2. The CAN bit values and dominant edges are modulated in a way that they can be filtered out at the right time and position of the CAN frame.

Bit embedding

The CAN controller transmits a CAN frame to the VCC that reduces the bits to dominant edges, bit values, and bit type. When the "Protocol Multiplexer" receives an SOF Sync_Seg, it synchronizes the embedded protocol to the CAN bit timing. The time between the encoded Sync_Seg from the VCC is used for transmitting the second-protocol information. The symbol stream is sent to the "Sig-nal Processing Unit" (SPU) and transmitted on the physical medium.

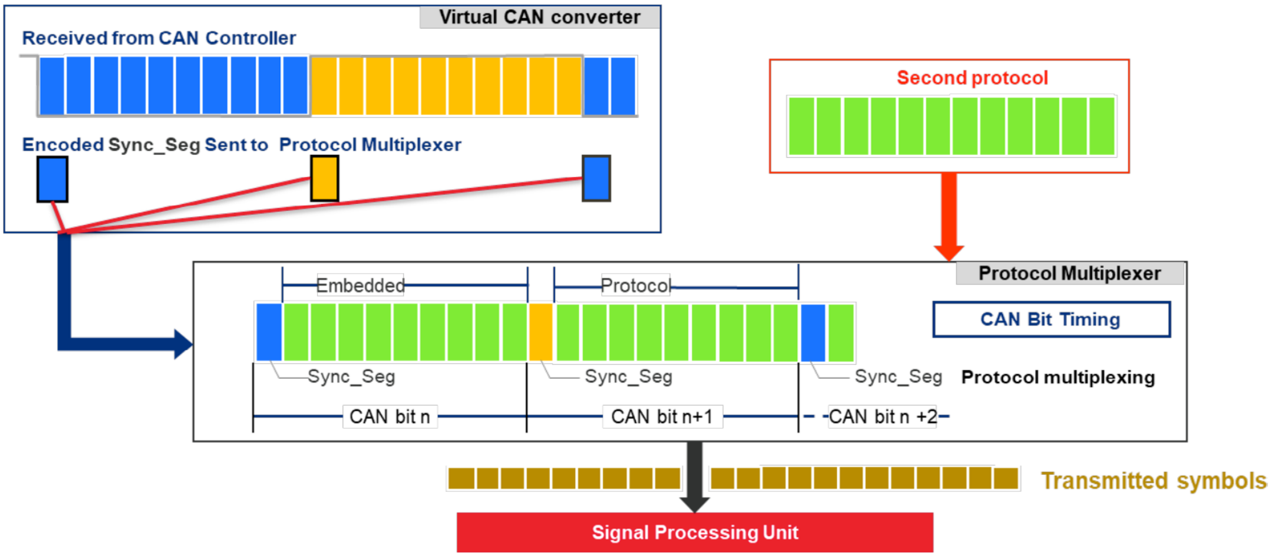


Figure 14: Integrated protocol multiplexing bit embedding transmission (Source: Kvaser)

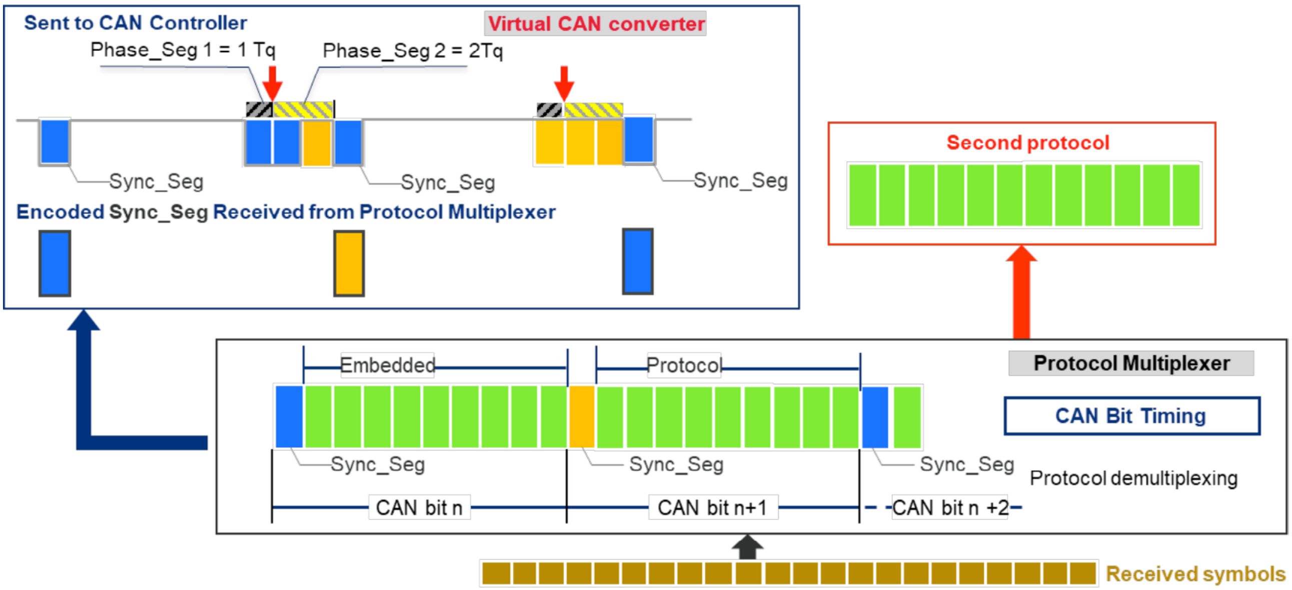


Figure 15: Receiving modules process the signals in reverse order (Source: Kvaser)

Receiving modules process the signals in reverse order (see Figure 15). A symbol stream is received from the SPU and demultiplexed by the "Protocol Multiplexer". The CAN symbols according to the RCP are fed to the VCC and the symbols of the second protocol to the second protocol handler. The VCC recreates the CAN bits by decoding the received Sync_Segs. A point-to-point connection between the CAN controller and the VCC (which is generating ghost edges) ensures that the CAN controller and the VCB are in perfect synchronization. This being the case, the sample point can be moved as far as possible to the end of the bit, i.e., the Phase_Seg 1 is one TQ and the Phase_Seg 2 two TQ long.

Embedding fake frames

Another method to embed a second protocol is to send a fake CAN frame. One CAN identifier is reserved for this purpose and known by the PMUX and the VCC. When the PMUX wants to transmit something from the second protocol, it starts the transmission as a CAN frame with the reserved CAN-Identifier and a DLC (data length code) that will create a time slot until the EOF that can be occupied by second protocol bits.

All VCCs will receive the first part and transmit it to their respective CAN controller (bit by bit). If the fake frame wins the arbitration, the respective VCC will create a fake frame and send it to its CAN controller. The PMUX will use the time until EOF for transmission of the second-protocol bits. More than one CAN-Identifier can be reserved and used to distinguish frames of specific kinds and addresses and/or to identify a third or fourth protocol, etc.

Longer time slots for second protocol frames

Sometimes the control system uses just a fraction of the available bandwidth. One way to make a window for the second protocol is to set up several dummy frames. These dummy frames are sent back-to-back to the CAN controller. If the dummy frame has the CAN-Identifier 0, it will block the CAN controller from any attempt to transmit a frame. During runtime of a control system, i.e. the CAN system, some frames require the highest priority ▷

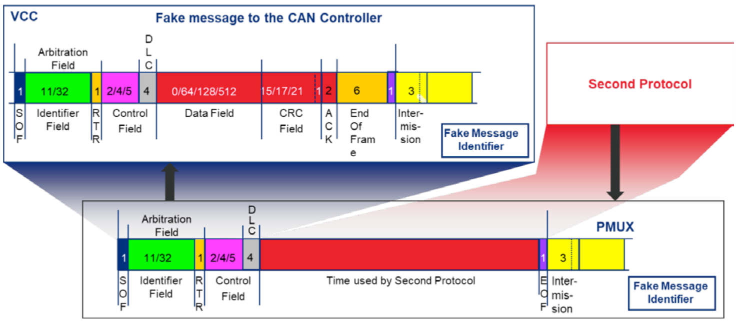


Figure 16: Integrated protocol multiplexing fake frame embedding transmission (Source: Kvaser)

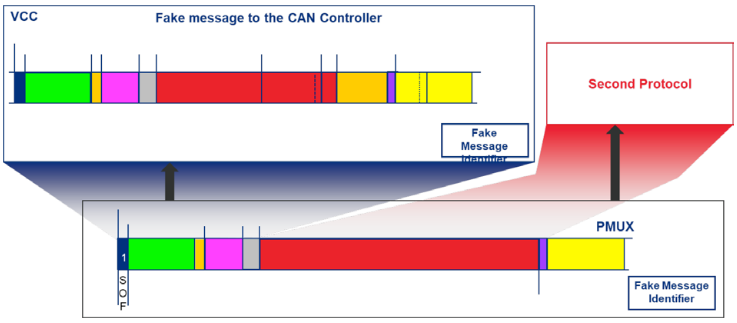


Figure 17: Integrated protocol multiplexing fake frame embedding reception (Source: Kvaser)

e.g., in catastrophic situations. The dummy frame should then have a lower priority. The VCC would then detect an attempt to transmit the alarm frame but too late for the PMUX to transmit it. The VCC then creates a bit fault to the CAN controller. The CAN controller will respond with an error frame and retransmission of the alarm frame. The PMUX will now get an SOF, abort the second protocol frame and continue transmitting the alarm frame.

Summary of the "Reduced CAN Protocol"

The RCP generates the position and values of the essential bit quanta in a CAN frame and the different frame structures from start of frame (SOF) to end of frame (EOF) according to the chosen CAN format for the actual system.

When the CAN controller transmits, the VCC mirrors the TX signal to the RX connection and conveys the following reduced CAN signals to the PMUX:

1. The Sync_Seg of every bit.
2. The bit value by one or more of the alternatives below
   a) modulating the Sync_Seg
   b) modulating the first TQ of the Prop_Seg
   c) last TQ of Phase_Seg 1 and first TQ of Pase_Seg 2
3. Encoded stuff bits
4. Encoded SOF
5. Encoded EOF

At reception, the PMUX transmits the CAN primitives according to the RCP to the VCC. The VCC converts the primitives to CAN bits on the go and feeds the signals to the CAN controller. The VCC also checks the bit flow according to the stuff bit rules. In case of a mismatch, it transmits an error flag both to the CAN controller and the PMUX.

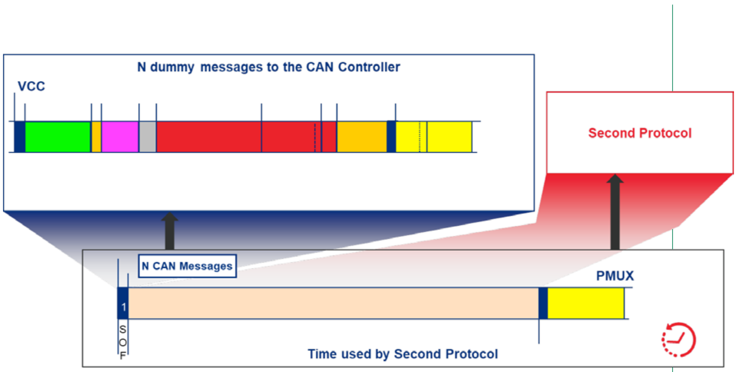

N dummy messages to the CAN Controller
VCC
Second Protocol
N CAN Messages
PMUX
1
SOF
Time used by Second Protocol

Figure 18: Integrated protocol time multiplexing (Source: Kvaser)

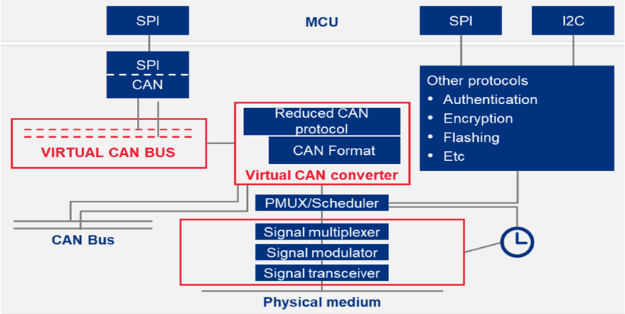


Figure 19: Further possible enhancements (Source: Kvaser)

A further enhancement

Until now it has been assumed that the ECU has a CAN controller. This makes it easy to apply the invention as old ECUs can be used without any modification. For completely new designs, it could be advantageous to move the CAN controller to the transceiver unit. There are already many such designs both for Classical CAN and CAN FD, denoted as standalone CAN controllers. In this case, the transceiver unit will have two modes, a "CAN only mode" and a "CAN embedded mode." In CAN only mode, the PMUX is bypassed and the signals according to the RCP are sent directly to the bus lines. In this way the kernel of the control system can be developed in a straight forward way using well proven CAN tools. As only the essential signals are transmitted on the CAN, detailed time analysis of the communication can be made. In a later stage of the development, when other features are added to the communication, the CAN control part can be verified by analyzing the "Virtual CAN Bus" by examining the RCP signals from the PMUX. Other features can be added such as frame schedulers, system clocks, etc. (see Figure 19). ◀

Author

Lars-Berno Fredriksson
Kvaser
lbf@kvaser.com
www.kvaser.com

Standards and specifications

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

Power-operated pedestrian entrance control equipment

The EN 17352 standard specifies requirements and test methods for power operated pedestrian entrance control equipment such as turnstiles, swing lanes, and retractable lanes. Such products can be operated electro-mechanically or electro-hydraulically. They are usually used in order to allow authorized persons to switch from one zone to another zone one at the time. This document covers safety in use of power-operated pedestrian entrance control equipment used for normal access as well as in escape routes and emergency exits. This document does not apply to power-operated pedestrian doors according to EN 16005 and EN 16361, doors according to EN 14351 1 and EN 14351 2, vertically pedestrian entrance control equipment, pedestrian entrance control equipment used in industrial processes as well as for people with special needs, and platform doors for subway as well as railway.

Boon Edam has upgraded its revolving doors, Tourlock 180 (4-winged) and Tourlock 120 (3-winged), to be compliant with EN 17352. The company has not disclosed, if the embedded network is CAN-based. But the CAN in Automation (CiA) member Dunkermotoren, a brand of Ametek, has announced to support EN 17352 in its CANopen-connectable motors. According to the company, it is a market leader in drive solutions for the door automation and is driving more slide and swing doors than any other motor manufacturer. At airports or metro stations for example, entry systems such as access gates ensure that only authorized persons get access to the airport terminal, or that the door to a platform is only released after the metro has stopped. Equipped with brushless DC motors and integrated or external motor control units, those access gates provide additional safety for passengers. Customized and parametrizable motion profiles contribute to smooth and safe airport operation.

Different types of access gates, such as a one-way corridor or automated passport control, provide different ▷

(Source: Adobe Stock)

installation spaces for the drive solution. The option to select from both, planetary as well as angular gearboxes such as worm or bevel gearboxes, allow Dunkermotoren to configure the suitable drive solution for each entrance system no matter the space constraints.

By publishing the EN 17352 standard, suppliers of power-operated access control devices such turnstiles, swing lanes, and retractable lanes have been confronted with additional requirements and test methods. Thus, manufacturers of such products are required to take further safety characteristics into account when designing their product. Additionally, the motor controllers, which are certified to EN ISO 13849-1 for Performance Level d (PL d), can safely switch off the drive torque so that no one is harmed on their escape route. *hz*

Do not double use terms!

A synonym is a word that has the same meaning as another word (or nearly the same meaning). In standards and specifications, which are translated into other languages, this could lead to misunderstandings and misinterpretations. Therefore, as a general role, it is wise to avoid synonyms. However, there are many standards and specifications using synonyms.

Even more critical is the double-use of terms. They are known as homonyms. In many automotive-related standards and specifications the term “signal” is used. The term “signal” is defined in the online Electropedia electrotechnical vocabulary by the IEC standardization body as “physical phenomenon whose presence, absence, or variation is considered as representing information”. The Oxford Learner’s Dictionary defines that signal is a “movement or sound that you make to give somebody information, instructions, a warning, etc.” In contradiction to these definitions, ISO 23150:2021 (Road vehicles — Data communication between sensors and data fusion unit for automated driving functions — Logical interface) defines “signal” as “entity consisting of one or more values and which is part of a logical interface (3.1.4). “Signal” is laboratory slang in the automotive industry. Synonyms are “parameter”, “suspect parameter”, “process data”, “variables”, etc. In J1939 documents, the term “suspect parameter (SP) is used as well as “parameter group (PG)”. Nevertheless, you find in the J1939 Digital Annex, several hundred times the term “signal”.

Newcomer can be confused, when we use synonyms and double use terms (homonyms). To help to understand more easily standards and specifications released by different authors, we should harmonize terminology. It seems impossible to do this for all technologies. Even in automotive applications we will not achieve this in one step, because there are multiple standardization bodies and industry consortia releasing documents. In a first step, we can try to harmonize terminology within each organization and providing translation tables, if different terms are used. The term “signal” used as synonym for “parameter” should be avoided, because it is also used as a physical layer term. Perhaps, the term “(process) variable” is in the long-term the best choice, “(process) data” is in my opinion also a good option. *hz*

CAN SIC XL standardized in ISO DIS 11898-2

The ISO DIS 11898-2 standard specifying the CAN physical medium attachments (PMA) has passed the Draft International Standard (DIS) ballot, but with comments. Most of comments were of editorial and general nature. However, some technical comments were submitted, too.

The most important change is the introduction of PMAs supporting the PWM (pulse-width modulation) coding as specified in CiA 610-1 (CAN XL). This coding allows data phase bit rates up to 20 Mbit/s. Of course, the achievable bit rate depends highly on the network topology and the selected cables as well as connectors. The CAN SIC (signal improvement capability) XL approach is able to suppress ringing on the cable. It uses the same mechanism as the so-called CAN SIC transceivers originally specified in CiA 601-4. This CiA specification has also been introduced into the ISO DIS 11898-2:2023 standard. *hz*

Further readings

Since 2022, the section “Standards and specifications” provides brief news in the CAN Newsletter magazine issues. Here’s an overview on all published ones until now:

- CAN Newsletter March 2022
- CAN Newsletter June 2022
- CAN Newsletter September 2022
- CAN Newsletter December 2022
- CAN Newsletter March 2023

CAN in Automation

CANopen Product Panels – Increase your visibility

Join CiA at Interlift 2023 and SPS 2023. Take advantage of the CANopen product panels and showcase your CANopen-based solutions. The CANopen panel wall is prominently displayed at the CiA booth. By participating in the CANopen panel wall you will increase the visibility of your CAN-based products, your company as well as your brand. Additionally, you present your company to tradeshow visitors as an CAN solution provider, connected to the CiA community.

- Targeted Audience: Present your CANopen solutions to a focused audience.
- Industry Collaboration: Fostering innovation and knowledge sharing in the CiA community.
- Market Positioning: Present your active involvement and expertise in the CAN application field.

- Increased Visibility: Showcase your company, CANopen-related products, and solutions.
- Enhanced Reach: Present detailed product information to an enhanced audience, based on your product's CiA Product Guide entry.

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

www.can-cia.org