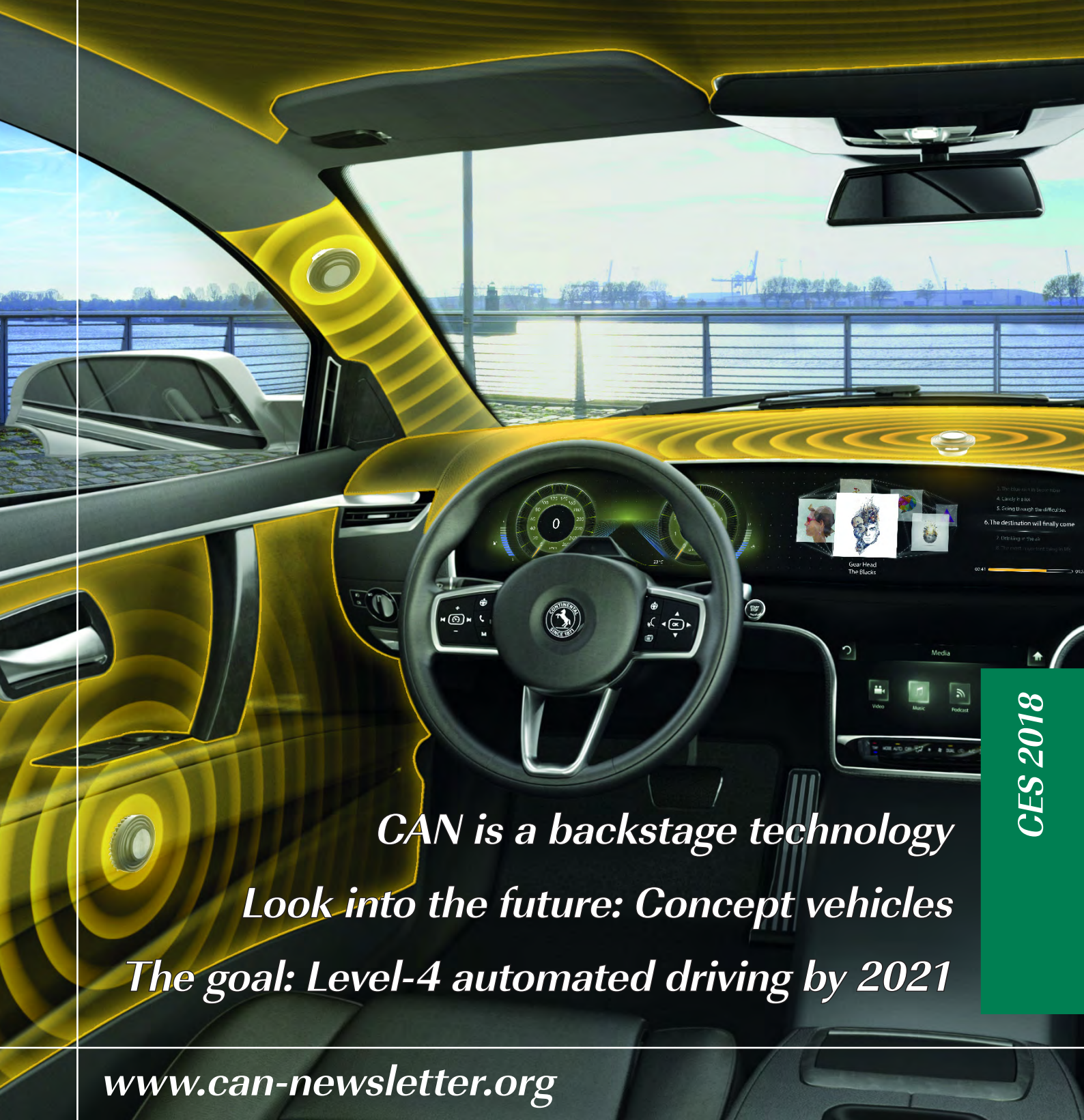# CAN *Newsletter*

Hardware + Software + Tools + Engineering

CES 2018

CAN is a backstage technology

Look into the future: Concept vehicles

The goal: Level-4 automated driving by 2021

www.can-newsletter.org

Mobile CAN FD Diagnosis

NEW

■ PCAN-Diag FD

Mobile Diagnostic Device for CAN and CAN FD Busses

The new PCAN-Diag FD is a handheld diagnostic device for CAN 2.0 and CAN FD busses that allows the examination on the physical and on the protocol layer. A funded analysis is done by the scope function and further measuring functions for voltage and termination. The examination of the CAN communication can be done by the display of CAN and CAN FD messages, a bus load measurement, or the recording and replay function for the CAN traffic.

Specifications
- High-speed CAN connection (ISO 11898-2)
  - Complies with the CAN specifications 2.0 A/B and FD (switchable support for ISO and Non-ISO)
  - CAN FD bit rates for the data field up to **12 Mbit/s**
  - CAN bit rates from 20 kbit/s up to 1 Mbit/s
  - CAN bus connection via D-Sub, 9-pin (in accordance with CiA® 303-1) with switchable CAN termination
- Display with 800 x 480 pixel resolution
- Device operation via a push dial and 4 buttons
- Memory card for saving projects, traces, and screenshots
- Power supply via the internal rechargeable batteries or the provided supply unit

Overview of functions
- Clear display of the CAN traffic with various information
- Configurable symbolic message representation
- Transmitting individual messages or CAN frame sequences
- Recording of incoming CAN messages
- Playback of trace files with optional loop function
- Automatic bit rate detection based on a fixed value list
- Switchable listen-only mode and silent startup function
- Measurement of the CAN bus load and termination
- Voltage measurement at the CAN connector for pin 6 and 9

Oscilloscope functions
- Oscilloscope with 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
- Decoding of CAN frames from the recorded signal trace
- Display of various properties and of measuring data of the decoded CAN frame

CES 2018

Applications

Devices

System design

Weekly update on new articles

The CAN Newsletter Online is our sister publication. It provides regularly latest product news regarding CAN. Because online-media does not come to the users automatically, we provide an email service called CiA's Weekly Telegraph. If you are subscribing to it on the homepage, you get a weekly overview of all articles published in the CAN Newsletter Online. This keeps you up to date. Additionally, the CiA's Weekly Telegraph provides information on the CiA Product Guides and when the next issue of the CAN Newsletter magazine is available for download.

CAN is a backstage technology

The 51st CES (Consumer Electronic Show) is in the books. What remains except heavy rain and power cuts: Automated driving with e-cars, smart homes, and of course gadgets.

The Consumer Electronic Show (CES) has changed its face. When established in 1967, it was dominated by commercial audio and video equipment. Nowadays, the focus is on next generation technology. Samsung presented its view of smart homes, carmakers and suppliers showed concept vehicles and automated driving prototypes, and lot of other electronic equipment. CAN technology was not a hot topic. Nevertheless, you found it on the backstage doing its job deeply and very deeply embedded in particular in many of the exhibited automated driving vehicles and the concept cars. At

Figure 1: CES 1967 – 51 years ago, the show started in New York City (Photo: CTA)

the end, you always have to communicate reliable and robust just a few bits and bytes. CAN is a very proven network technology for such tasks. But it was nearly invisible for the shallow visitor. You needed to dig a little bit deeper to find the CAN-based embedded networks on the exhibition in Las Vegas.

In this issue, we try to inform about the CES trends in automated driving and next generation's vehicles. Although CAN was not in the main focus and not in the headlines, it was so-to-say below the sea-level, like an iceberg, sometimes looking a little bit out of the water. Still most of these embedded CAN networks were based on the Classical CAN protocol. In the following years, we will see increasingly CAN FD solutions.

This years CES saw more than three centimeter of rain, which was a record for the desert city. Additionally, a two-hour blackout in many parts of the Las Vegas Convention Center stopped ▷

Figure 2: CES 2018 – 51 years later, the exhibition is spread out in entire Las Vegas including hundreds of private events (Photo: CTA)

the high-tech show partly and reminded us that innovative high-end technology still depends on some functioning low-tech infrastructure. Let us take the cap in hand and look, how a low-priced communication technology such as CAN does its job on the backstage and in the backstreets not always visible for the consumers. "CES 2018 will be remembered as the year where the wattage of innovation was so huge that it caused a blackout!" said IBM's Bridget Karlin. "CES 2018 once again demonstrated that this is the world's premiere showcase for technology innovation with unparalleled diversity from international public officials to industry leaders to entrepreneurs."
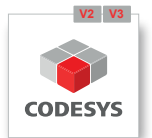
What becomes also clear, the first generation of autonomous driving vehicles will be not purchasable for everyone. Firstly, they will support on-demand ride serves, deliveries, and some commercial transportation. ◀

Author

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

Look into the future: Concept vehicles

The CES is not the place to announce cars that you can buy today. But concept vehicles are shown – some of them will drive on the roads very soon.

Figure 1: The Snap concept car comprises a chassis, the "skateboard", and the passenger cell, the "pod" (Photo: Rinspeed)

These concept vehicles are a look to the far future. But also vehicles for the next generation are exhibited. One highlight of the CES 2018 was the electric concept car by Rinspeed called Snap. The idea is simple: The concept vehicle comprises two parts. One part is the skateboard, which carries the durable mechanical and the fast-aging IT equipment. They will be recycled after a few years of intensive use once they have reached the end of their design life, while the much less stressed pod, the other part, is able to remain in service for much longer, before it also must be sent to recycling. This benefits the environment, because it plays a significant role in conserving natural resources.

Combing technology and creating new features

Frank Rinderknecht, head of the Rinspeed company, has already developed 23 concept cars. The name Snap really says all: everything fits together and can be snapped together. The concept car from Rinspeed was again designed at the Swiss company 4erC (Switzerland) and technically executed at Esoro (Switzerland). The electric vehicle – as always when Rinderknecht is at work – is full of technical and visual finesse, contributed by a worldwide network of companies. The two steering axles along with the integrated electric powertrain came from ZF. They allow the Snap to turn practically on a small coin and produce no emissions in urban traffic. Optionally, there is a 'personal assistant' in form of an autonomous, intelligent robot to accompany the occupants. It will also be happy to help with running errands, carrying purchases, or handle other tedious tasks.

The Snap, an SAE level-5 automated driving vehicle, uses a lot of electronic technology from third parties: ZF has contributed its ProAI control box (see insert "Artificial intelligence computing platform") as well as radars and cameras, and NXP supplied its Bluebox and several semiconductors, for example. The domain controller architecture has been developed by NXP. It uses different communication technologies including CAN.

Lidar sensors by Ibeo, owned partly by ZF, ensure that obstacles in the road are detected by means of real-time measurements of the light reflections. The products are 3-D solid-state sensors without rotating mirrors. Gentix delivered ▷

Artificial intelligence computing platform

The ZF ProAI control unit powers the Dream Car by ZF as well as the Snap concept car by Rinspeed (Photo: ZF)

Nvidia and ZF have joined forces to provide an artificial intelligence (AI) computing platform. On CES 2017, the companies launched the ZF ProAI system based on Nvidia's Drive PX 2 AI platform to process inputs from multiple cameras, lidars, radars, and ultrasonic sensors. ZF has integrated this control box in its Dream Car and demonstrated it this year in Las Vegas. The solution is nearly ready for volume production stated ZF's CEO, Dr. Konstantin Sauer, in Las Vegas. The German Tier-1 supplier uses a network of partnerships and co-operations to integrate additional features to the ZF ProAI control unit. A visible example at CES was the Snap concept car by Rinspeed.
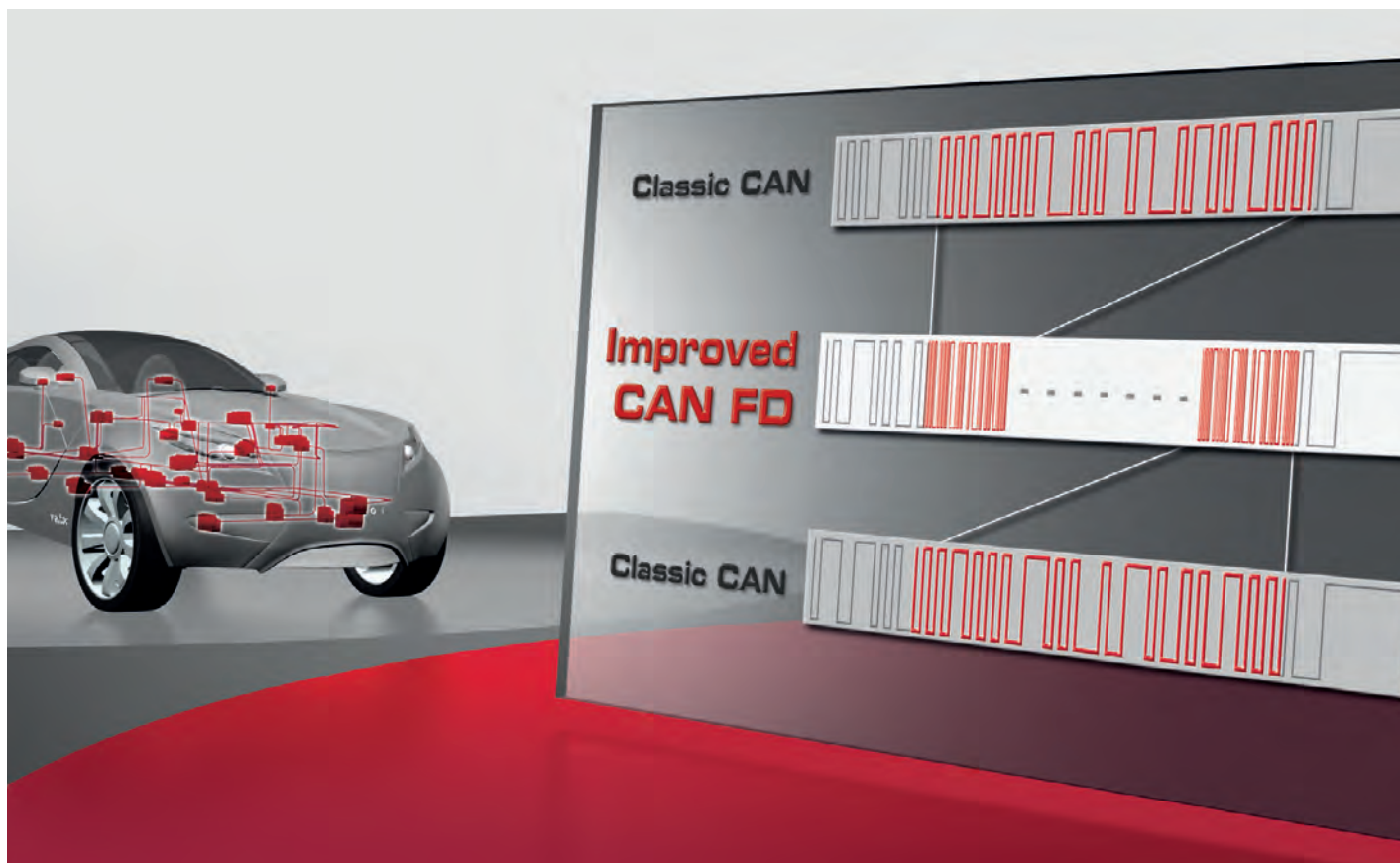
Statements at CES 2018

Jensen Huang, Nvidia's CEO: "In the future, every car will be self driving. There will be 100 million cars built each year, millions of robo-taxies, and several hundred thousand trucks. All of it will be autonomous. On top of this,

(Photo: Nvidia)

what will define the driving experience is the AI. The complexity of autonomous driving, the complexity of the software of future cars is incredible. It starts with, of course, building a brand new type of processor we call the Drive Xavier, an autonomous machine processor that is able to do deep learning, perception, has the ability to do parallel computing and also computer vision and high performance computing at very, very energy-efficient levels."

Qi Lu, Group President and COO of Baidu: "Apollo is an example of 'China Speed', demonstrating the rapid pace of China's innovations and development in the global autonomous driving industry. Artificial Intelligence and

(Photo: Baidu)

innovation are borderless. We're facing a historic moment with immense opportunities for people around the world, which requires big countries and great enterprises, including China and Baidu, to lead and explore together. We are very pleased to be at the center of this large-scale innovation and stand together with each partner at the forefront of this momentous time."

Aido Toyoda, president of Toyota Motor: "The automobile industry is clearly amidst its most dramatic period of change as technologies like electrification, connected, and automated driving are making significant progress.

(Photo: Baidu)

Toyota remains committed to making ever better cars. Just as important, we are developing mobility solutions to help everyone enjoy their lives, and we are doing our part to create an ever-better society for the next 100 years and beyond. This announcement marks a major step forward in our evolution towards sustainable mobility, demonstrating our continued expansion beyond traditional cars and trucks to the creation of new values including services for customers."

Video: Toyota at CES 2018

Research platform for automated driving

Highly equipped with lidar sensors: Self-driving Lexus LS 600hL (Photo: Toyota)

Toyota introduced in Las Vegas its "Platform 3.0", which is able to fuse many sensors. The Japanese carmakers demonstrated it in a special Lexus LS 600hL. The number of connected sensors was not disclosed, but it was said that the car was equipped with more than fifteen. This included four lidar (light imaging detection and ranging) sensor systems by Luminar with a 200-m range tracking the forward direction. They enable to detect objects in the environment including difficult-to-see dark objects. The connected sensors enabled a 360-degree perimeter. Additional shorter-range lidar sensors are positioned low on all four sides of the vehicle—one in each front quarter panel and one each on the front and rear bumpers. These can detect low-level and smaller objects near the car like children and debris in the roadway. Production of the platform starts this spring. It has been developed in the Toyota Research Institute (TRI) located in California. Of course, the platform provides also CAN connectivity to communicate with the other ECUs (electronic control units).

the Iris scanner for occupant detection and dimmable front and rear glass elements, which also can be found on Boeing's Dreamliner.

MaaS – Mobility as a service

Automated driving enables that what is called mobility as a service abbreviated as MaaS. Toyota introduced at CES 2018 its e-Palette concept vehicle, which is dedicated for such services. The Japanese carmaker will cooperate closely with partners. This includes Amazon, DiDi, Mazda, Pizza Hut, and Uber, who will collaborate on vehicle planning, application concepts, and vehicle verification activities. This alliance will create a broad-based ecosystem of hardware and software support designed to help a range of companies utilize advanced mobility technology to better serve customers. In the near term, the alliance will focus on the development of the new e-Palette concept vehicle, also unveiled at CES.

The concept reflects one of Toyota's visions for automated mobility including MaaS applications. Of course, these vehicles based on the Mobility Services Platform (MSPF) announced already in 2016 will be battery powered. Toyota plans to conduct feasibility testing of the e-Palette concept in various regions, including the United States, in the early 2020s. The carmaker hopes to contribute to the success of the Olympic and Paralympic Games Tokyo 2020 by providing mobility solutions like the e-Palette and other innovative mobility offerings. There are three sizes of the e-Palette concept ranging from 4 m to 7 m. Due to a flat and extensive barrier free interior space layout designed with a low floor, equipment can be installed in accordance with the ▷
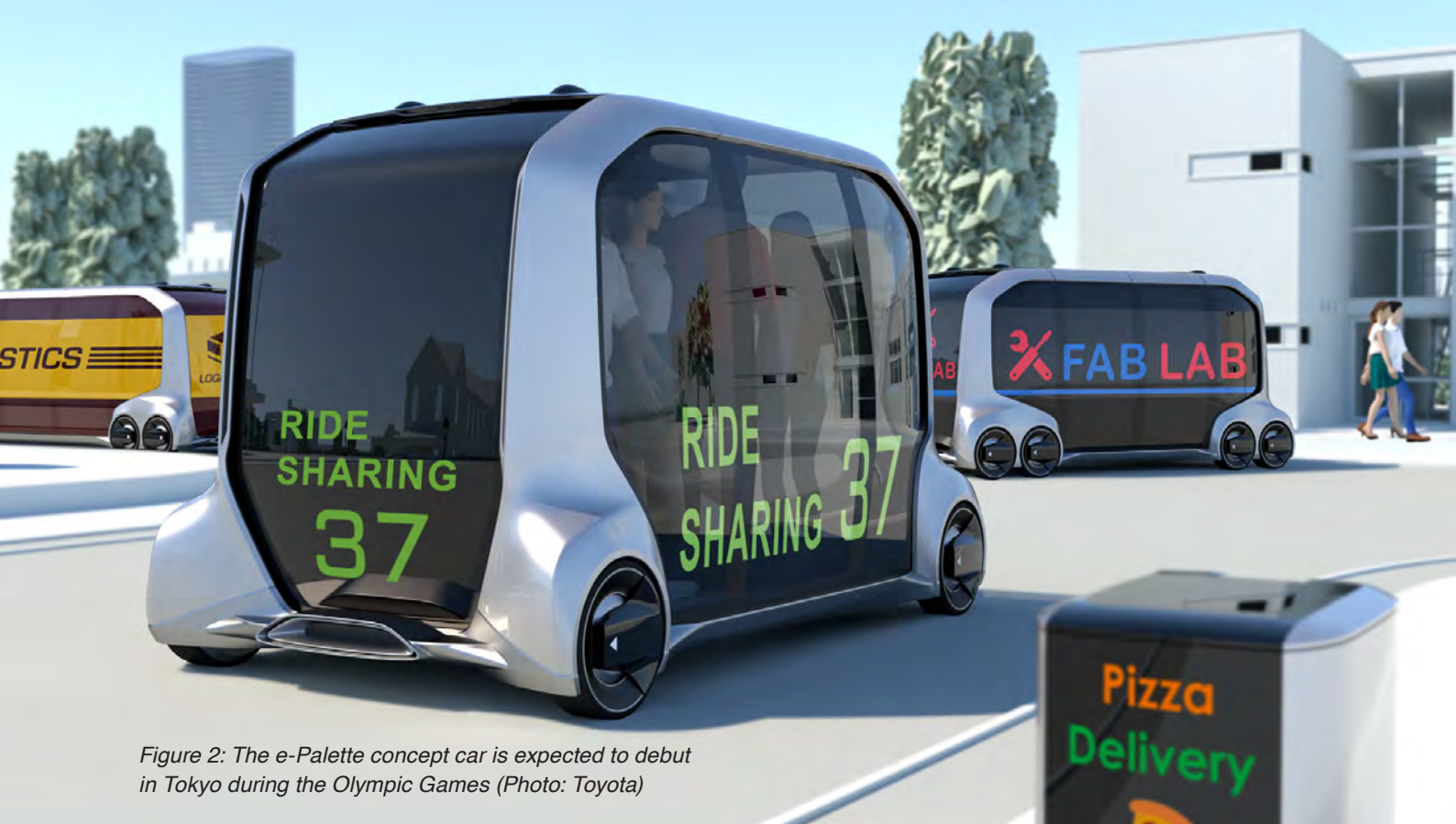
Figure 2: The e-Palette concept car is expected to debut in Tokyo during the Olympic Games (Photo: Toyota)

user's needs, such as ride sharing, hotel room, and retail shopping specifications. Toyota president, Akio Toyoda, mentioned in a press conference Apple, Facebook, and Google as competitors for its mobility initiative, but not the other OEMs (original equipment manufacturers). He said: "My goal is to transition Toyota from an automobile company to a mobility company."

Vehicle information is gathered from the Data Communication Module (DCM) fitted to the e-Palette concept and accumulated in the Toyota Big Data Center (TBDC) through a global communication platform. DCMs are currently different depending on the region and country, but will be standardized by 2019. Besides the telematics interfaces, the DCM also provides connectivity to the in-vehicle networks including CAN-based sub-systems. Already last year, Toyota submitted a patent application (US 20170208074A1), which describes a method to detect unauthorized access attempts by device using the DCM's CAN interfaces (e.g. the OBDII interface).

There is already competition to the e-Palette approach: The Chinese bus maker King Long will operate self-driving L4 shuttles, e-Palette look-alikes, using Baidu's Apollo platform ().

Production-ready ADAS solutions

At CES 2018, Renesas demonstrated ADAS (advanced driver assistance system) solutions based on its R-Car H3 SoC (system-on chip) featuring among other connectivity options two CAN FD on-chip modules. The Dodge Ram 1500 truck used the SoC in its cockpit. Also the Lincoln MKZ model implemented the chip, which processed data from nine cameras to detect other vehicles, pedestrians, lane markings, stop signs, speed-limit signs, traffic lights, and parking spaces. After processing all of this information, the results are shown on the dashboard or leads to commands transmitted via CAN, for example, to the related ECUs (electronic control units) to perform acceleration, deceleration, steering, etc. The SoC was also used in the exhibited Cadillac SRX for the 3-D surround view.

Prototype implementations of ADAS solutions using SoCs (Photo: Renesas)

E-cars keep the city clean

Look under the hood: The GXE Corvette is a battery-powered car reaching 250 km, when not running at the highest speed of 330 km/h (Photo: Genovation)

To keep the still growing megacities clean, it is necessary to power the cars electrically. Of course, not all of the electrical energy generation will be green and CO_2 neutral. This "dirty" generation of electrical energy happens in remote areas, not visible for those living in urban areas.

Look under the hood: The GXE Corvette is a battery-powered car reaching 250 km, when not running at the highest speed of 330 km/h (Photo: Genovation)

Many of the in Las Vegas launched vehicles were electric-powered cars. Genovation presented at CES its GXE Corvette sports car, which achieved a record speed of 330 km/h. The development started four years ago. Just 75 units will be produced. The price is US-$ 75000. The e-car is based on the C7 Corvette and retains all the stock safety systems and onboard LAN communications but adds a dedicated CAN network to connect the eleven control modules and the instrumentation, which includes a Volvo-like vertical touchscreen. The CAN network is fed just enough information to trick it into thinking there's a perfectly functioning powertrain onboard.

In particular, the Chinese government forces foreign OEMs to manufacture e-cars. In Las Vegas, the Chinese start-up Byton deputed an all-electric SUV (service utility vehicle). The company plans to roll-out the US-$ 45000 SUV already next year in China. Two models will be offered, a 268-hp rear-wheel drive version and a 469-hp dual-motor all-wheel drive version.

Autonomous driving is possible now

Google and others do it since some years. In dedicated areas, self-driving prototypes are driving on normal roads. Of course, a human driver has to sit behind the steering wheel – so-to-say just in case that electronics fail. In Las Vegas, Lyft provided together with Aptiv the largest fleet of robotic cars, BMW 5-series models (see also page 12). ◄

Author

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

The goal: Level-4 automated driving by 2021

One of the hot topics in Las Vegas was automated driving. Besides traditional carmakers and suppliers, new players from the consumer and IT business throw their hats into the ring.
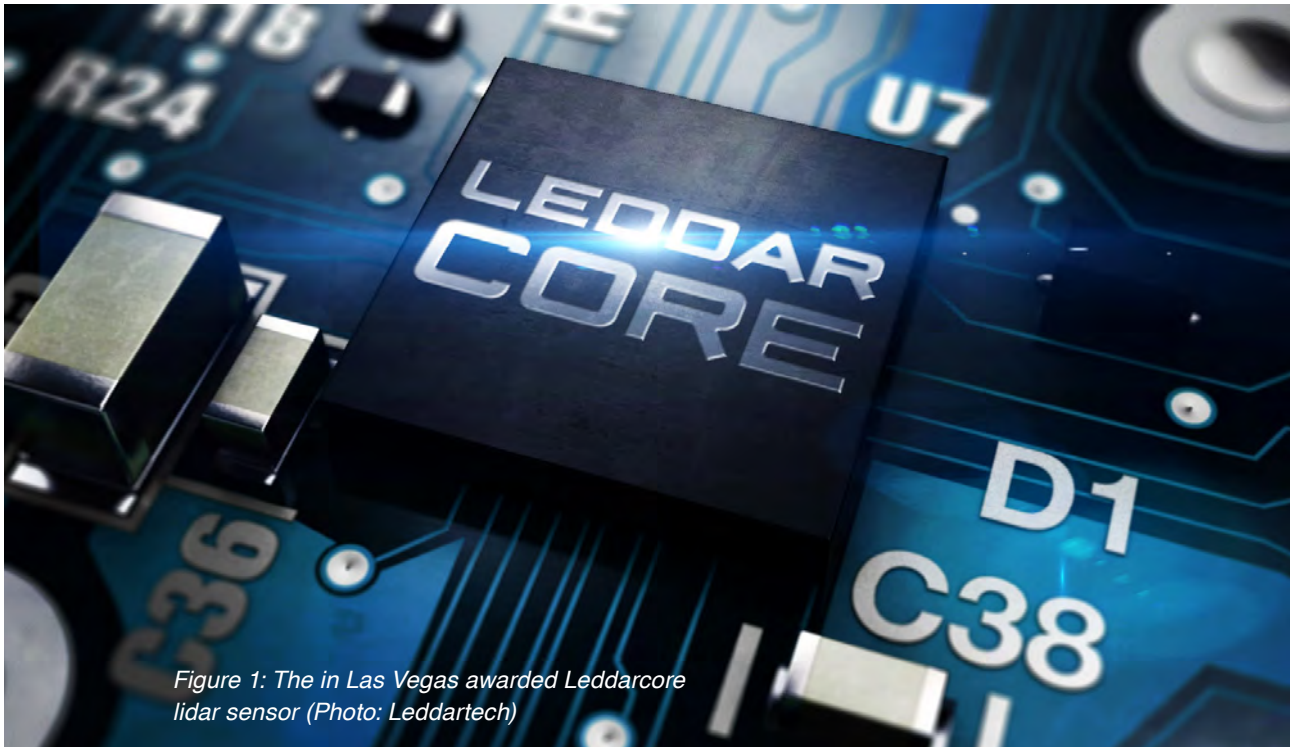

Figure 1: The in Las Vegas awarded Leddarcore lidar sensor (Photo: Leddartech)

Automated driving is an old dream: Already back in the 1960s, some enthusiasts conducted some first experiments with self-driving cars. At CES 2018, automated driving was a main trend. SAE Level-3 automated driving is already possible. This means the automated vehicle monitors already the driving environment. But the human driver still needs to be hot stand-by, ready to respond appropriately to a request to intervene. Next level is expected for 2021: Level-4 systems do not need drivers responding appropriately, when intervention is requested.

The base: Sensor fusion

Monitoring the driving environment requires a lot of sensors. Multiple radars, lidars, and cameras are needed. In Las Vegas, the Leddarcore LCA2 by Leddartech achieved two innovation awards. The solid-state 3D lidar is intended for high-volume applications. "The LCA2 truly is a breakthrough innovation that brings lidar technology to the mass markets. It delivers unique added value, reduces inherent risks at all levels of the value chain, and accelerates the path toward commercial deployments of semi- and fully-autonomous driving solutions," said Charles Boulanger, Leddartech's CEO. "These two CES awards are an ac-

knowledgement of our technology excellence and Leddarcore IC business model geared toward mass production of SSL sensors by Tier-1 manufacturers for deployment by automotive OEMs as early as 2020," he added. Leddartech cooperates with several Tier-1 suppliers to integrate the lidar ICs to board-level products and in electronic control units (ECU). Some of them provide connectivity to CAN-based in-vehicle networks.

To produced lidar sensors for reasonable costs is one of the keys for the success of automated driving. Besides Leddartech, Luminar, Quanergy, Velodyne, and other start-ups battle to supply the car industry as well as other applications fields. This includes service robots and automated guided vehicles (AGV) for industrial applications. Also agriculture and construction machinery is going the way to self-driving. In many of these applications, CAN connectivity of sensors is desired.

In general, sensor data can be fused in decentralized units or by a centralized computing system. The discussion on decentralized or centralized data processing is ongoing: one time distributed computing wins, and next time central computers are ahead. In Las Vegas, Continental presented its Open Computing Language (OpenCL) framework developed in cooperation with Xilinx. The introduced ▷

TTControl
HYDAC INTERNATIONAL

HY-TTC 32 - Compact Control Unit for Cost-Sensitive Applications, Smaller Machines and Implements

Flexibility and User Friendliness

- Extensive I/O set (30 Inputs / Outputs with various options for configurability by software)
- CAN with automatic baud-rate detection
- Programmable in C/C++ or CODESYS® including support for CANopen® master
- 1 x CAN bus termination configurable via connector pin

Safety

- Certified according to EN ISO 13849 PL c
- CANopen safety protocol (CiA 304) according to EN 50325-5

Robustness and Availability

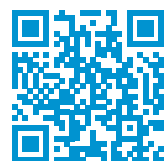- Aluminum die-cast housing for extremely rough work conditions
- Maximum current up to 24 A

Connectivity

- 2 x CAN 125 kbit/s up to 1 MB/s
- CANopen conformity

Performance

- Infineon XC22xx CPU running at 80 MHz
- 768 kByte int. Flash, 82 kByte int. RAM, 8 kByte EEPROM

www.ttcontrol.com/HY-TTC-32-ECU

Safety Certified ECUs

General Purpose ECUs

Safe I/O Modules

Ethernet Switches

Operator Interfaces

Chinese platform for automated driving

Nvidia cooperates with Baidu, China's search engine giant, and ZF, Germany's number three Tier-1. Baidu has introduced in Las Vegas its Apollo 2 "open" platform for automated driving vehicles. The previous Apollo version comprised a vehicle computer with recommended CAN interface board from ESD. "Open platforms and ecosystems are the best way to accelerate the transition of AI technologies toward commercialization," said Qi Lu from Baidu. Apollo has gathered more than 90 partners. Baidu said that it supports four main computing platforms from Nvidia, Intel, NXP, and Renesas in 2018. An additional cooperation with ON Semiconductors was announced in Las Vegas. Ross Jatou from ON Semiconductor said: "We are delighted to be partnering with Baidu on their Apollo platform. We believe that the value of such a platform to automotive system designers will be tremendous. It is underlined by the number of industry leaders already engaged and looking to utilize it. Image sensors are fundamental components of ADAS implementations throughout the vehicle, and they will become even more relevant as the industry moves towards fully autonomous cars. Joining forces with Baidu by providing the image sensor solution for the Apollo platform is further validation of ON Semiconductor's leading position in automotive image sensing." The chipmaker provides also CAN transceiver chips. Infineon is also a partner of the Apollo program. The German chipmaker supplies its Aurix family of 32-bit micro-controllers featuring Classical CAN and CAN FD modules. These products are made for sensor fusion, gateway, and domain controller applications. In addition, the company provides a variety of other integrated circuits (IC) for autonomous driving. This

Baidu's Apollo program is very ambitious: Many market-leading chipmakers participate to develop an "open" platform for automated driving (Photo: Baidu)

includes sensors, actuators, and transceivers, for example for CAN.

"Apollo is more than just open-sourcing code and technology – it is evolving from technology innovation to product innovation and enabling more implementation scenarios," said Jingao Wang, Head of Apollo Platform and Senior Director of Baidu. Chery Automotive, a Chinese brand will produce in series Level-3 autonomous vehicles based on the Apollo platform by 2020. Baidu also plans to mass-produce driverless buses for designated areas by the end of July 2018 with King Long, a Chinese vehicle manufacturer situated in Xiamen. Additionally, co-operations with JAC Motors and BAIC Motor are planned. Production of self-driving vehicles will begin with the next two to three years.

The Apollo project goes abroad, too: The first overseas expansion to Singapore was announced already. The joint venture is called Apollo Southeast Asia and is financed by US-$ 200 million fund.

platform provides heterogeneous computing options such as a Central Processing Unit (CPU), Graphics Processing Unit (GPU), Digital Signal Processor (DSP), and now with the help of Xilinx's all programmable technology a customizable hardware acceleration solution. This provides developers the ability to optimize software for the appropriate processing engine or to create their own hardware accelerators. "Xilinx is proud to collaborate with Continental in the development of the Assisted & Automated Driving Control Unit, enabling the creation of an ecosystem for automated driving. We embrace the spirit of a hardware platform that invites collaboration, rather than tying companies to a proprietary architecture," said Willard Tu.

"Our Assisted & Automated Driving Control Unit will enable automotive engineers to create their own differentiated solutions for machine learning, and sensor fusion. Xilinx's All Programmable Technology was chosen as it offers flexibility and scalability to address the ever-changing and new requirements along the way to fully automated self-driving cars," said Karl Haupt, Head of Continental's Advanced Driver Assistance Systems business unit.

The jointly developed platform offers a scalable product family for assisted and automated driving fulfilling

the safety requirements (ASIL-D) by 2019. This platform will provide a variety of communication ports for the necessary data flow. During development, Continental distinguishes between an Assisted Driving Control Unit and an Automated Driving Control Unit. The first product of this scalable family is a module for advanced driver assistance systems that offers a complete, cost-optimized package connecting sensors and actuators with complement of central processing, safety, and security. The control unit for automated driving follows closely behind as a powerful computer that meets the requirements of highly automated driving, with special focus on new digital structures for comprehensive environment modeling, ASIL-D, and real-time performance, while providing a heightened ease of use to developers by offering an OpenCL path into every chip present.

The workhorse: Number-crunching hardware

Sensor fusion and combining the results with information from electronic maps and weather forecasts using artificial intelligence (AI) methods requires a lot of computing power. This means, special hardware is needed. Specialized companies such as Nvidia and Mobileye (recently ▷
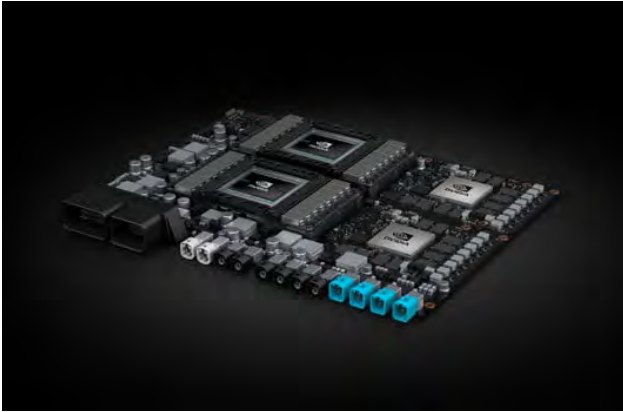
Figure 2: The Drive platform powered by the Xavier system-on-chip (Photo: Nvidia)

acquired by Intel) are the top dogs. Nvidia introduced in Las Vegas the next generation of its autonomous driving board powered by Xavier system-on-chip (SoC). It was developed for SAE Level-5 self-driving vehicles. The chip has more than nine billion transistors with an 8-core CPU, a 512-core GPU, a video-processor, a deep-learning accelerator, and a computer-vision accelerator. It can perform 30 trillion operations per second and consumes just 30 Watt. This number-crunching hardware is the base of two software platforms, Drive IX and the recently announced Drive AR.

Nvidia cooperates with 320 partners regarding self-driving. This includes Tier-1 suppliers such as ZF and OEMs such as Volkswagen (VW). ZF uses Nvidia's platform for its ProAI car computer. VW will implement the Drive IX technology by 2022 in its automated driving vehicles. During the CES, Jensen Huang, Nvidia's CEO, and Herbert Diess, VW's CEO, enter jointly the stage to discuss how AI and deep learning will shape the next generation of vehicles. This was a meeting of two business cultures: Dressed in a leather jacket and in traditional suit. Jensen Huang behaved more like a preacher man, while Herbert Diess presented himself a bit starchy.

Nvidia partners also with Baidu's Apollo project developing an open platform for automated driving vehicles (see insert "Chinese platform for automated driving"). It comprises four major modules: reference hardware, software platform, cloud computing services, and last but not least a vehicle platform.

But there is not just Nvidia offering number-crunching hardware. Mobileye is the toughest competitor. Recently acquired by Intel for US-$ 15,3 billion, Mobileye has launched the EyeQ5 system-on-chip, indicating by its name to support the development of SAE Level-5 self-driving vehicles. The company has a similar long list of partners comprising OEMs and Tier-1s. At the CES show, the company announced a co-operation with Chinese automaker Saic motors. The SoC combined with Intel's Atom processor is competing Nvidia's Drive platform. Besides the computing power, the power consumption is essential. The Mobileye/Intel solution features also CAN connectivity to integrate the ▷

Statements at CES 2018

Brian Krzanich, Intel's CEO: "As driverless cars become a reality, we must start thinking of the automobile as a new type of consumer space. We have barely scratched the surface in thinking about the way cars will be designed, the interaction among passengers, and how passengers will spend time while they are riding and not driving. In this respect, autonomous driving is today's biggest game changer, offering a new platform for innovation from in-cabin design and entertainment to life-saving safety systems."

(Photo: Intel)

Michael Xie, president and CTO of Fortinet: "Connected vehicles are the next major technology innovation disrupting the automotive industry. With 3D mapping, sensor processing, smart device integration, cloud-based services, advanced LAN/CAN networks, and autonomous driving defining the connected car of the future, the cyber risks are enormous. And with IoT devices connecting to the car network to access content and applications, the attack surface is even larger."

(Photo: Fortinet)

Peter Schiefer, president of Infineon's the automotive division: "With our profound expertise in automotive applications as well as the premium products and services, Infineon significantly contributes to the breakthrough of autonomous driving. It is in this regard that we look forward to supporting Baidu in taking the Apollo initiative to the next level."

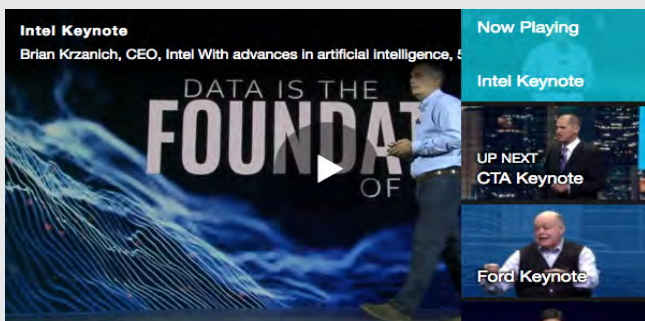*(Photo: Infineon)*

Watch CES 2018 Keynote Addresses

Brain-to-vehicle communication

(Photo: Nissan)

At CES 2018, Nissan launched a driver-to-vehicle device. Of course, you cannot buy it today. The driver wears a cap, which reads his brain waves and uses them to help improve the reaction times of the vehicle's electronics. The Japanese carmaker selling vehicles under the brands Nissan, Infiniti, and Datsun is one of the first of conduct research on brain-to-vehicle (B2V) communication. The company also owning partly Mitsubishi Motors and cooperating with Renault said that the B2V cap can predict driver behavior to shorten reaction time, when a driver is in control, for instance by making steering wheels turns or braking 0,2 to 0,5 second faster. Of course, copying a human's driving style is not ideal in all cases. The last thing you would want is an autonomous car that speeds and makes erratic lane changes. Nissan's goal is to maximize driver safety during autonomous driving without departing too much from the driver's own style. This technology is hopefully far away from implementation in serial production, but Nissan said they like to show the potential of combining human and artificial intelligence.

supercomputer into the in-vehicle network architecture. The production of the EyeQ5H system-on-chip will start in August 2018. Volume production is expected for 2020, when first OEMs will use the SoC in their series cars. In Las Vegas, the chipmaker introduced in a keynote speech its 100-vehicles test fleet.

Some call this competition the "chip war". Intel claims to be ahead with over two million Mobileye installations. But not just Mobileye and Nvidia are in the contest: Qualcomm is the third in the ring. The company likes to acquire NXP's mother Broadcom. Jaguar Land Rover announced to use Qualcomm's Snapdragon computing platform for its next generation of automated driving vehicles. Additionally, Ford and Qualcomm announced to cooperate.

The challenge: Safe and secure

Besides the Apollo platform, several other approaches were presented in Las Vegas. It is not just computing power what counts in the automated driving business. Important features are functional safety and cyber-security. Already serious production in mind, ZF presented its ProAI hardware and software developed jointly with Nvidia (see ▷

insert "Chinese platform for automated driving"). The German Tier-1 showcased the Dream Car development vehicle equipped with this solution. It is nearly ready for volume production, said Dr. Konstantin Sauer, ZF's CEO. Rinspeed's Snap concept car uses the ProAI () platform, too. In virtual test drives, the Dream Car travelled already 9 000 km. The same distance as I drove with my younger daughter a couple of years ago from San Francisco to New York within six weeks.

Continental presented in Las Vegas its Safety Domain Control Unit (SDCU). This unit is used as a fallback path for just in case. This SDCU stops the vehicle safely, even in the event of a functional failure in the primary path. There are one or more fallback paths for every central system and they are independent of each other. Since the SDCU also acts as the airbag control unit, its priority availability – including energy reserve and a crash-proof installation location in the vehicles – is guaranteed. With the additional fallback path of the SDCU, the supplier ensures that the vehicle can still be brought to a safe stop, if the main automation functionality fails. This increases the availability of the vehicle's electronic. "It is precisely this fallback path that may not be available in highly automated vehicles, since the driver is allowed to focus on other things and cannot be requested, in a fraction of a second, to take control of the vehicle immediately after a possible failure," explained Maged Khalil from Continental. Every highly automated vehicle must therefore be able to stop automatically. Level-4 vehicles such as Cruising Chauffeur from Continental are prepared for this.

Besides functional safety, cyber-security is an issue. Developed in cooperation with Renesas, Fortinet demonstrated its Fortios security operating system. Both companies presented an implementation on Renesas' R-Car H3 SoC installed in prototype car exhibited in Las Vegas. Mock cyber breaches were demonstrated including intrusion-preventing system (ISP) attacks and distributed denial-of-service (DDoS) attacks. The SoC by Renesas features two CAN FD ports besides Ethernet, Most, USB, and other serial interfaces.

The FEV Group demonstrated at CES 2018 a self-driving vehicle using its cyber-security solution, the Cyber-Security Gateway (CSG). The company is known as powertrain supplier and vehicle engineering provider. The launched CSG is linked to the CAN-based in-vehicle networks, to detect and to prevent malicious attacks, and can also function as a firewall between the external interfaces such as WLAN, Bluetooth, Cellular, and the CAN-based OBDII port, to protect the vehicle from these potential remote security threats.

Karamba Security (Israel) announced in Las Vegas its Safecan security software. It protects CAN-based networks from hacking by authenticating in-vehicle communications with zero protocol overhead, claimed the company. It can be implemented without overtaxing the car's internal communications to protect and authenticate CAN communications. There is no need to change network protocols, or add any additional network packets to ensure the authenticity of source-destination authentication and overall in-vehicle network authentication. By offering seamless encryption for ECU communication, Safecan ▷
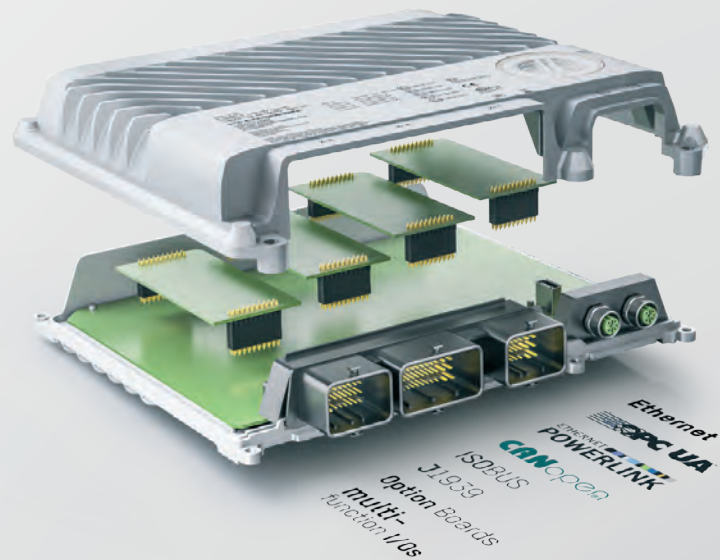
Infineon supports Nvidia's Pegasus platform

Infineon has expanded its safe automated driving collaboration with Nvidia, announcing that its Aurix TC3xx series automotive MCU will be used in the Pegasus AI car computing platform. The supercomputer for autonomous vehicles meets the requirements of Level-5 autonomous driving as defined by the Society

Ritesh Tyagi *(Photo: Infineon)*

of Automotive Engineers (SAE). "Nvidia's Drive AI vehicle supercomputers deliver up to 100-times more computational horsepower than the most advanced cars on the road today," said Gary Hicok from Nvidia. "Their multiple levels of redundancy and safety functionality demand a proven, widely deployed safety architecture, like that of the Aurix TC3xx series."

The German chipmaker now supplies the safety MCUs, safety power supply IC, and selected vehicle communication interface ICs for several the Nvidia hardware platforms. The devices support increasing levels of autonomous driving capability, ranging from auto cruise functionality to auto-chauffeur and full autonomy.

The collaboration enables users of the platform to access Aurix capabilities through an Autosar-compliant software stack. This potentially allows re-use of higher-level application code and can likely reduce development time by 20 percent to 40 percent compared to traditional platforms.

Ritesh Tyagi: "Collaboration between Infineon and Nvidia through multiple generations of Drive car computers provides the automotive industry with a consistent platform for development and market deployment across all classes of driver-assist and fully autonomous systems."

The multicore MCUs help the platform to meet the functional safety requirements according to ISO 26262 ASIL-D for Advanced Driver Assistance Systems (ADAS) and self-driving systems. The products support among other communication options also CAN FD. In Las Vegas, exhibited several Aurix solutions for ADAS systems.

hardens the network leading to and from the car's safety systems and ensures that only legitimate commands are received by the car's safety systems. Commands originating from invalid sources are ignored.

In addition to hardening the car networks against physical attacks, Safecan enables secure OTA (over-the-air) updates from the cloud to any ECU in the car. OTA products use secure channels from the OEM cloud to the primary ECU, which serves as the OTA's entry point in the car. However, due to lack of network authentication, attackers may hack the car, impersonate an OTA update

and deploy malicious software on safety ECUs. By hardening the network between the OTA primary ECU to the in-vehicle safety systems, target ECUs will not accept changes, unless it was authenticated by the security software. The software complements and extends Karamba's Carwall autonomous security product to provide end-to-end in-vehicle security. Carwall hardens externally connected ECUs by sealing their binaries according to factory settings. This prevents cyber-attacks and in-memory attacks from compromising the car ECU's, while eliminating false positives that risk consumers' safety.

The backstage network: CAN

At the end, when all sensor data is fused and combined with other information coming from the CAN-based in-vehicle networks, you have the same simple commands as in non-automated driving vehicles. This means, most of the carmakers will use CAN as an embedded or even as a deeply embedded network – so to say not visible for the original equipment manufacturer. All the above-mentioned hardware platforms provide in minimum optionally CAN connectivity. The reliability and the robustness are unique features of CAN. Of course, there are other INV technologies on the "backstage": Automotive Ethernet and LIN have also a great future. But they were also not hotly discussed in Las Vegas. They are as CAN not visible to the consumer – and it is still a consumer event. ◄

Author

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

Reliable mobile machine control

Standard and SafetyController in one unit

Modern vehicles and mobile machines require powerful control electronics.
The new ecomatController has two independent, powerful 32-bit PLCs – one of them an independent safety controller (SIL2 / Pl d).
In addition to a variety of configurable I/O ports, two Ethernet and four CAN interfaces with CANopen, CANopen Safety and J1939 protocol are available.
Robust, reliable and powerful. ifm – close to you!

www.ifm.com / de / en / ecomatcontroller
Phone +49 800 16 16 16 4

Compact drives with CAN interface

EBM-Papst is continuously expanding its product range of electrical drive systems for industrial applications. This series includes CANopen.

Our customers in the mechanical and plant engineering sector are looking for compact and powerful drive systems that can receive commands from higher-level controllers via standard network interfaces and return actual values and status messages to the control system. A new addition to our range is the new ECI 63.xx K5 series in the power range from 180 W to 370 W. Based on a BLDC internal rotor motor with integrated electronics module, this series includes a standard CANopen interface.
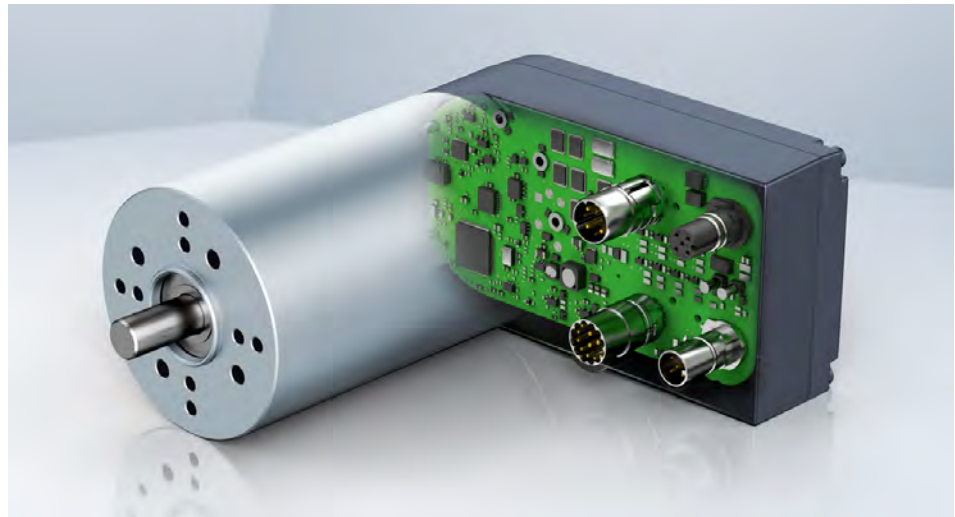

Figure 1: A BLDC internal rotor motor with integrated electronics module includes a standard CANopen interface (Photo: EBM-Papst)

With the integrated, freely programmable sequence control (PLC functionality), technology functions can be implemented directly in the drive; the previously required PLC is thus either unburdened or can ideally be dispensed with altogether. The drive can be controlled via the digital and analog inputs and outputs — our range of Industry 4.0-capable drive systems has thus been expanded to include an additional electronic module.

These compact drive systems offer a cost-optimized alternative to conventional AC servomotors in many applications. Compared to AC standard motors with frequency converters, this series offers increased efficiency and a higher power density.
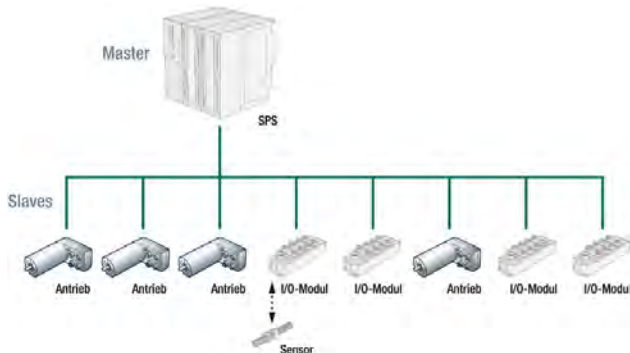
Although Ethernet-based bus systems are now required in many applications, CANopen remains a popular option when the number of nodes in a system increases. This is because systems with CANopen offer considerable cost advantages in terms of hardware and implementation. The performance of the CANopen protocol is more than adequate for many industrial applications.

The ECI 63.xx K5 supports the communication and motion profiles in accordance with IEC 61800-7 (CiA 402). This means that the drive can be operated with positioning, speed, current, or torque control. Interpolated positioning with cyclic set value requirement is also implemented. Referencing of the drive position can be carried out using normalized homing methods, as well as via a gentle movement onto a blocker/mechanical stop.

In addition, thanks to the integrated intelligence, the drive can be freely programmed in a similar manner to a PLC. For example, the drive's functions are implemented in such a way that it can be controlled virtually at will via the integrated I/Os without the need for motion commands via CANopen. Thanks to the integrated PLC functionality, the drive can also be used as a CAN master. As a result, in less complex applications, networks can be set up that operate as a standalone application ▷
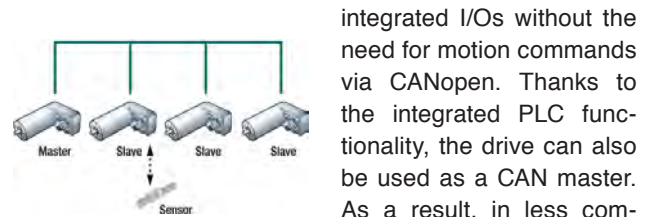

Figure 2 and Figure 3: before/after comparison - Thanks to the integrated intelligence, the drive can be freely programmed in a similar manner to a PLC, what offers the possibility of dispensing with a higher-level PLC (Photo: EBM-Papst)
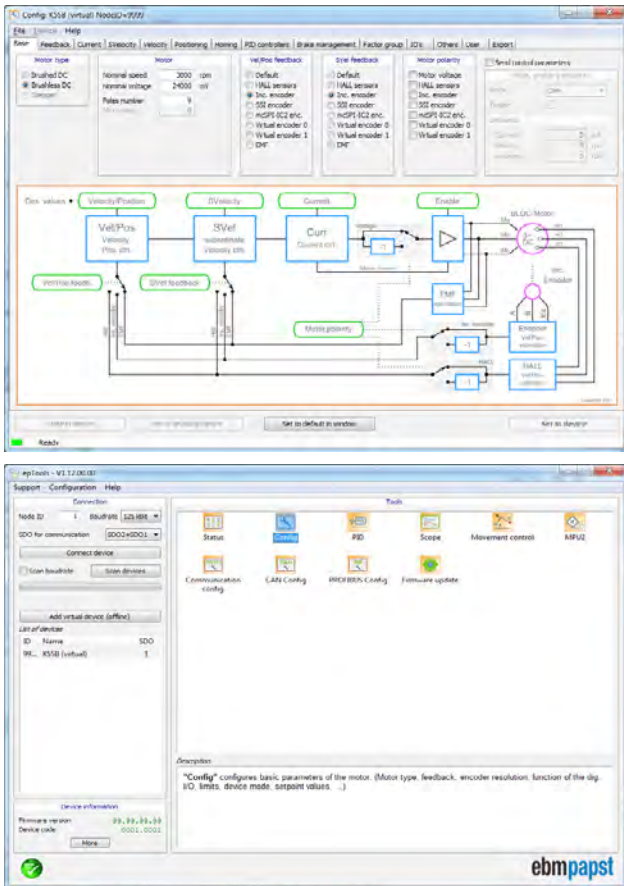
Figure 4 and Figure 5: With the easy-to-use commissioning and parameterization software Eptools, the drive can be conveniently operated directly from a PC via CANopen (Photo: EBM-Papst)

without a higher-level PLC. The possibility of dispensing with a higher-level PLC has a positive effect on the cost situation.

The ECI 63.xx K5 incorporates an integrated encoder system as standard, which resolves the position of the output shaft to 12 bits. This achieves a high degree of positioning accuracy. Even slow speeds and standstill can be smoothly controlled, thus permitting the use of a very wide speed range. With EBM's commissioning and parameterization software Eptools, the drive can be conveniently operated directly from a PC via CANopen. The most important parameters are displayed in the tool's configuration window. Any number of additional parameters can be added to the interface and uploaded to the drive. The entire parameter set can also be saved on a PC. The software is available free of charge. The status window in Eptools enables the relevant measurement values and drive status information to be visualized. As a result, controllers can be quickly optimized and commissioning simplified. The control window in Eptools lets the user operate the drive in different operating modes and directly specify both controller release and setpoints. Digital inputs and outputs can also be set manually in this window. An application-specific program for the integrated PLC can be compiled in another Eptools window and uploaded to the drive.

Those interested in learning more can view the documentation for the new drive solutions (technical data, drawings, and 3D models) in the EBM-Papst online-portal, and print or download them as required. Of course, the ECI 63.xx K5 preferred types, both as solo and gear motors, will be included in the online-portal and will be available for dispatch within 48 hours from receipt of order. ◀

Author

Patrick Schumacher
EBM-Papst
patrick.schumacher@de.ebmpapst.com
www.ebmpapst.com

CAN Newsletter Online: Drives

The CAN Newsletter Online reports briefly about products and services.

SPS IPC Drives 2017
CANopen drive features 180 W to 370 W
EBM-Papst (Germany) presents its ECI 63.xx K5 drive system based on a brushless DC motor.
Read on

Heater and valve
System solutions for gas condensing
EBM-Papst has presented its products and system solutions for gas-air ratio assembly at the ISH trade fair. Both a gas-air system and a gas valve come with a CAN port.
Read on

BLDC motor drive
Permanent output power of 1100 W
With the BG 95 dPro CANopen, Dunkermotoren has launched a drive based on a brushless DC motor (BLDC). It has an output power of over 1 kW.
Read on

Stepper motor
Configurable via USB or Bluetooth
Camozzi (Italy) has introduced the DRCS series of CANopen drives. The product can be configured wireless and by means of USB.
Read on

Nema-17 stepper motor
Optionally with CANopen interface
JVL Industri Elektronik (Denmark) has released the Servostep integrated stepper motor family (MIS171 to MIS176). They provide an embedded multi-turn encoder.
Read on

Devices

Security expectations vs. limitations

In part 1 of this article series, we examine the security limits of various embedded applications. What kind of security levels can realistically be achieved by developers, integrators, and users of embedded systems.

Sometimes the perception about embedded security still seems to be that it is either "there" or "not there" but in fact, security is not a binary "on" or "off". There are various levels and if your customer expects 100 % security, then you first need to help them to review their expectations.

When it comes to the security of embedded systems we still see a lot of unrealistic expectations. With this article we would like to give developers, integrators, and users of embedded systems an overview about what kind of security levels can realistically be achieved. Let's look at traditional secure communication models as illustrated by the individuals Alice and Bob exchanging messages in Figure 1. The security goal here is to provide a private messaging system, which is both encrypted and authenticated in a way that no third party can read or manipulate the communication between them.

The attack vectors potentially available to a third party like Chuck (assuming he can make use of them) are illustrated in Figure 2 and include:

◆ intercepting the messages and trying to decrypt them
◆ accessing Alice's or Bob's computer or message device to extract keys or messages
◆ directly tricking Alice or Bob into revealing keys or messages

It shouldn't be a surprise that it is more difficult to maintain a fully private channel if the third party has easy access to multiple attack vectors. If Alice and Bob are embedded devices within the same machine and Chuck has unlimited physical access to it, then it means he has direct access to the entire communication channel including both the transmitting and receiving computing devices.

Before selecting any application-specific security method, one needs to review the possible attack vectors and draw a line between those attacks that we can protect a system from and those that are beyond our control, like attacks involving extortion, personal threats and such. For many embedded systems the "unlimited physical access" is an important criteria. If we can say that the attacker can never have physical access because the machine is locked inside some building, then the required security levels can focus on protecting remote access. By securing the internal communication between the devices in
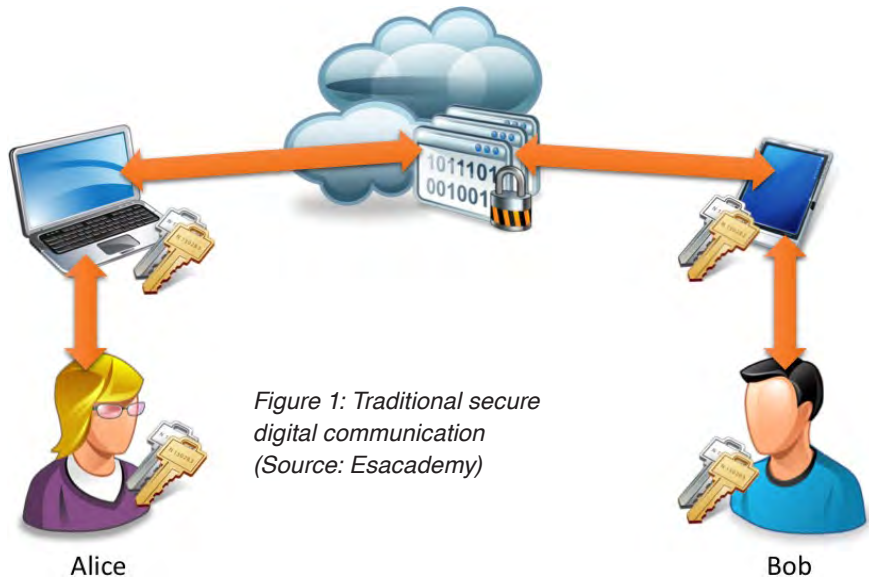

Figure 1: Traditional secure digital communication (Source: Esacademy)

Alice

Bob

the machine against manipulation, an attacker who gains remote access to it, for example through some gateway, won't be successful in gaining further control. In this article series, we examine the security limits of various embedded applications. For part 1 we start by examining the fare calculation of a taxi.

Limits of embedded security

Can you ever be sure to pay the correct taxi fare?

Over the last years, we have been involved in various security projects and learned that for specific security expectations there doesn't seem to be a realistic solution available. In this article we take the application of taxi fare calculation to show that sometimes even sophisticated security methods can only provide a somewhat moderate security level overall.

Today, a taxi fare calculation is based on a wheel pulse counter. One could now engage in the discussion whether today's average phone with all its sensors wouldn't be better suited to do a more reliable calculation of the fare. Currently, the only method that has gained official approval from the governing bodies is calculations based on direct input from the wheels. Other methods such as ones based on GPS combined with acceleration measurements have not yet passed the approval process.

The security challenge in this application is: how can we as customers ensure that a rogue taxi driver or company does not manipulate the way fares are calculated or presented to the passenger? Can we ensure overcharging becomes impossible?
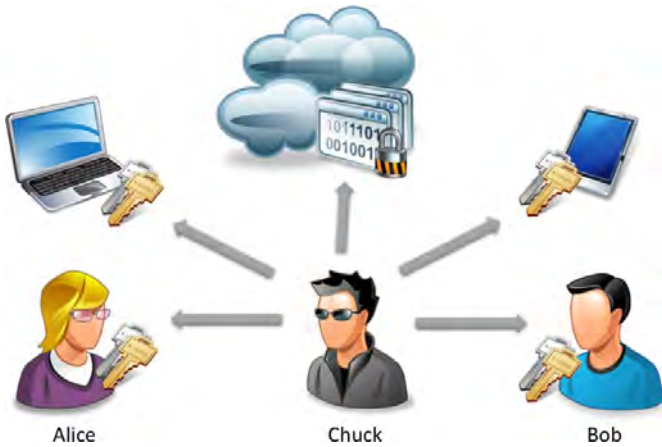
▷

Figure 2: Possible attack vectors (Source: Esacademy)

On a technical level, the wheel pulse counter sensor detects magnets rotating/passing by its sensor. With every pass, the counter is incremented. How many pulses are counted per rotation can vary in different cars, this is one of the many parameters a meter needs to know when making its calculations. The wheel pulse counter value is transmitted via a Controller Area Network and, after passing through one or multiple bridges or gateways, finally reaches the meter where the fare is calculated.

One potential method for manipulating the system is illustrated in Figure 3. The rogue driver/owner connects a CAN device that implements a man-in-the-middle manipulation. The CAN cable is cut somewhere between the sensor and the meter. The manipulating device is then inserted in between the network branches and acts as a bridge. It passes on all CAN messages – but when passing on the wheel pulse counter value it inserts its own value that is always a certain percentage higher. This would result in a higher fare being calculated.

To prohibit the use of such a manipulating device, some say that end-to-end security from wheel pulse counter to the meter is needed. The idea is that the meter only accepts authenticated wheel pulse data. Then a man-in-the-middle device would only work if it knows the security methods and keys involved.

The security challenge here is, that potential manipulators of such a system (rogue taxi drivers or companies) have full, unlimited physical access to the entire system – from message producer (wheel pulse sensor) to the consumer (meter).

A security system that uses the same master key(s) shared among multiple vehicles would be unsuitable here. The rogue party could simply report a car as stolen and then send the sensor and the meter to a third party "data and code recovery or extraction service" (there are multiple companies offering such services starting at below one hundred Euro). The extraction would give them access to all code and data stored in these embedded devices. Even if keys are hidden and encrypted, with access to all code, hackers will be able to retrieve the keys eventually. If these keys are used in multiple cars, it is then easy to still build a man-in-the-middle attack device.

There are dedicated security hardware chips/microcontrollers that make such an extraction more difficult, but choice and price of these have not yet reached a level where they can easily replace common micro-controllers. ▷

Figure 3: Man-in-the-middle attack between wheel and meter (Source: Esacademy)

A higher security level would require that keys are random and unique in every taxi. In Figure 4 this is illustrated with Alice, the manufacturer of the wheel pulse counter and Bob, the taxi meter manufacturer. Each wheel pulse counter and meter require their own individual pairing key (silver) – and a potential master key (golden) to reset/erase/revoke these keys.

The issue with such master keys is: they provide a back door that could also be used by hackers. Yes, also the back door would have security mechanisms. However, the motivations for hackers to break it grows with the number of installed devices.

As with many security systems, the key generation/ distribution logistics remains one of the biggest challenges: whose responsibility would it be to generate and install keys or make the initial pairing? And when and where would this happen?

Even worse, looking at the entire system, manipulating the communication between the sensor and the meter is only one of several options available to manipulate the system. Let's do a review from wheel to meter:

◆ Wheel: A 3 % variation in the tire diameter results (multiply by Pi) in a 10 % variation of the measured distance. As far as we know, a 5 % variation in measured distance is therefore generally accepted as "within parameters" to allow for variations in tires.

◆ Communication: Today, manipulation of the communication between wheel pulse counter and meter could be achieved by inserting a man-in-the-middle CAN device. As the potentially rogue parties have full physical access to both producer and consumer, this could only be prohibited by using a security method based on individual, non-revocable keys.

◆ Meter: In the end, it is the meter that displays the fare. How difficult would it be to manipulate the meter itself to show a different fare? Well, as previously mentioned, code can potentially be extracted and in a next step could be manipulated to display a different fare, not impossible for a motivated hacker. To prohibit such manipulations, meters are sealed.

But now think about the manipulations already performed today to banking machines. Additional

keyboards and card readers can be tacked-on to banking machines in a way that users don't recognize the difference. In the same way a meter-like display could be designed to clip onto or fully around an existing meter. The original meter "vanishes" inside a fake meter that can display whatever the taxi driver would like it to display.

Reviewing this list, prohibiting any type of manipulation becomes very challenging. Adding authentication and possibly encryption to the communication between sensor and meter only addresses one of many attack vectors. When the possible attacker has full physical access to the car, the keys used to protect the communication and possibly a back door for a system reset must all be individual and may not be shared, requiring a complex key infrastructure.

In the long-term, the entire process on how taxi fares are calculated needs a review. Busses, trains, ferries, and planes primarily charge by destination. Can you imagine an airline or train transport system trying to surcharge their passengers on detours or delays? Somehow that is common practice with taxi cabs – with a taxi you may pay more, when you get into a traffic jam or detours are taken.

I fully understand that historically these rules have been established to protect the drivers and cab owners: make a passenger pay if they want to make stops or want specific routes to be taken. However, other industries, too, have faced re-structuring challenges or even (industrial) revolutions in the past and survived.

Even without being a fortune teller it looks obvious to us that self-driving vehicles will arrive sooner or later. If these are used for passenger transportation, possibly even with some hop-on/hop-off support, then the current (taxi) fare calculation can hardly be maintained.

An intermediate solution might be to remove the manipulation incentive: If the base fare is calculated on the theoretical distance (based on a current map, start and end coordinates), then this is a fixed, transparent value that all parties: owner, driver, and the passenger can verify. If the map used includes current road closures, then most detour reasons are already taken into account. If ▷

Figure 4: End-to-end security between wheel and meter (Source: Esacademy)

needed, there could still be surcharges added for passenger-caused waiting time.

In summary, reviewing this application has taken an interesting twist: we started off with the request of adding security features to the CAN communication used for the fare calculation of a taxi meter. And in the end, the recommendation for this specific application is: do not use that very CAN communication at all to calculate the fare. Sometimes being a CAN security consultant requires to also recommend solutions outside of CAN.   ◄

Preview to the next article of the series

In the next issue, the authors will have a look at security requirements for applications that are being discussed, driven by now-possible scenarios that could be taken out of a Hollywood blockbuster: A swarm of flying drones intersecting planes and trucks or ships with hazardous goods on collision course. The self-driving car of a prosecutor is taken over by a hacker on the payroll of organized crime and driven straight off the cliff. One can expect that lawmakers won't stand by while such scenarios become a reality.

Regulations that mandate security in place "at all levels" of such machines and devices are likely. Will they be technically detailed and allow exceptions for less-vulnerable levels of communication within the machine? Probably not. The long-held argument that a CAN bus is often within a closed system not accessible from the outside andtherefore does not need security might become moot once tough regulations become law.

Authors

Olaf Pfeiffer
Christian Keydel
EmSA (Embedded Systems Academy)
opfeiffer@esacademy.de
ckeydel@esacademy.de
www.esacademy.de

Using CAN the Swedish way

Miunske in collaboration with Tekplus realized a CAN-based unit to control two such disparate functions as a tipper truck and a snow plough with only one device.

(Photo: Fotolia)

Transporting goods on pallets in the morning, logs at mid-day, and bulk goods in the evening – three possible uses for one and the same lorry. What makes it so special is that it is possible to control the different swap bodies using just one central control unit. Although such a scenario is current-ly still a pipe dream, a major step forward in terms of imple-mentation has already been taken in Scandinavia. Such tech-nologically sophisticated systems are of particular interest to smaller companies in Scandinavia, the reason being that they often have only one chassis, but various attachments and superstructures.

Lastvagnsmontage i Eda, based in Charlottenberg in Sweden, has specialized in retrofitting lorries in line with customer-specific requirements. It can, for example, even carry out subsequent installations of loading cranes or snow ploughs. Equipped in this way, the vehicles are prepared for different assignments, depending on summer or winter operations. Swapping attachments and super-structures, however, has involved enormous effort up to now: no device that can be used to control two such disparate functions as a tipper truck and a snow plough has yet existed.

Together with Tekplus, Miunske has now implemented a CAN-based control unit. This unit is enhanced to include a radio remote control that makes external operation possible. This is particularly advantageous when it comes to function controls or attaching or removing individual components such as push plates. The CAN network control modules by Miunske offer multiple possibilities for individual project design. They are designed for use in mobile control systems in electrical systems of 9 V to 36 V and certified with E-certification. All

CAN products from the company use the communication standard ISO 11898 layer-2 and freely selectable bit rate.

The three companies have already had initial experience of working together on other projects. There was also a clear division of tasks in terms of snow plough control. While Tekplus, as the local partner, analyzed the installation space and designed the housing, Miunske developed the electronics including the software. The first prototypes were completed within six months and have since proved their worth in everyday use. Sara Jonsson, from P-M Anderssons Akeri, was one of the first to be allowed to test the German-Swedish solution. Her conclusion: "This new system has significantly improved the working environment, as all functions are located together directly on the armrest. This gives me a more comfortable sitting position instead of constantly having to bend forward to the dashboard, where the control unit used to be located."

Potential buyers for this new control unit, which is based on an I/O module, already exist, as the installation overhead is significantly reduced, because two devices are now housed in the same box. Thanks to the bus system, cable harnesses can also be kept slimmer, while many more options are possible in technological terms.

Another feature is the special control unit: to be able to clean and grit the roads in the same work process in winter service operations, the loading area may be tilted while driving in Sweden. The grit then falls into a trailer, which carries out even spreading. Mattias Wennerstrand, project manager at Lastvagnsmontage responsible for the technical ▷

Figure 1 + 2: Retrofitted customer vehicle from the inside and outside (Photo: Lastvagnsmontage i Eda)

Figure 3: The CAN-based snow plough control on the right and its remote control for external operation on the left (Photo: Klaus Nachtigall, Tekplus)

implementation, gave a positive review. "By modernizing our control unit, we have taken an important step towards the future. We had a strong sense that we would receive a good product from Miunske and Tekplus. And that's what we now have." Klaus Nachtigall, technical contact person and long-standing sales partner for Miunske in Sweden, was also visibly pleased: "There is a different mentality here in the North; it is not so much the price, but above all the result that matters in terms of collaboration here. And the result is impressive. We already have ideas for the next generation of control units, such as linking them to smartphones." Such remote diagnostics would obviate the need for service engineers to travel hundreds of kilometers to fix a minor error. It is not possible to provide a conclusive description of all the other possibilities. The one certainty is that many

possibilities are conceivable. Ultimately, it is the market that decides what, if anything, is implemented. Adopting a wait-and-see approach, however, does not sit well with any of the participants. "There are many options", said Nachtigall. "Further projects are being planned." ◄

Contact

Bettina Miska
Miunske
b.miska@miunske.com
www.miunske.com

Recommendation for the CAN FD bit-timing

The CiA 601-3 CAN FD device and system design recommendation will be released soon. It provides guidelines for the bit-timing settings in the arbitration as well as the data-phase.

(Photo: Fotolia)

The CAN FD standards, ISO 11898-1 and ISO 11898-2, do not include device and system design specifications. The new editions of ISO 11898-1 and ISO 11898-2 address only semiconductor manufacturers. Device and system designers need additional guidelines and recommendations for the CAN FD device interface. Normally, the device designer needs to fulfill the device design requirements given by the OEM.

The ISO 11898-1:2015 document does not specify the interface to the host controller in detail. It just gives some basic information, which is not sufficient for interoperability and system design aspects. For example, the oscillator frequency is not specified, because this is a device design issue. The CiA 601-2 CAN controller interface specification recommends using 20 MHz, 40 MHz, or 80 MHz. Other frequencies should not be used. Another recommendation in this document is the number of bit-timing registers to be implemented. The ISO standard just requires a small register, which is sufficient for some bit-rate combinations. The CAN FD protocol may use two bit-rates: one for the arbitration phase and another one or the same for the data-phase. In case of using a large ratio between arbitration and data-phase bit-times, the standardized size of the bit-timing registers is not appropriate. Therefore the CiA 601-2 document recommends for the arbitration phase a register programmability of 5 time-quanta (*tq*) to 385 *tq*. The configurability for the data-phase register should be in the range from 4 *tq* to 49 *tq*. Additionally, the CiA 601-2 specification contains some recommendations regarding interrupt sources and message buffer behaviors.

In order to understand the ISO 11898-2:2016 standard from a device designer's point-of-view, the CiA 601-1 specification provides some useful information about the transceiver loop delay symmetry, the bit-timing symmetry, the transmitter delay compensation (TDC). This document explains how to interpret and consider the parameters given by the transceiver chip suppliers.

As said, the ISO 11898 series does not specify device or system design aspects. In order to achieve interoperability of devices, bit-timing should be the very same in all nodes. This is nothing new for engineers familiar with Classical CAN network designs. However, in Classical CAN networks there are some tolerances allowed regarding the bit-timing settings. They are necessary, when nodes with different oscillator frequencies are in the same network. Typically, the sample-point (SP) is given as a range such as 85 % to 90 % with nominal value of 87,5 % (CANopen). The SP is between the phase segment 1 and the phase segment 2 of a bit-time. The bit-time comprises the synchronization segment (always one time-quantum), the propagation segment, the phase segments 1 and 2.

In CAN FD networks, the rules and recommendations needs to be more strict, because higher bit-rates bring the network closer to the physical limits. Of course, when not using the bit-rate switch function, the bit-timing is like in Classical CAN. But when using two bit-rates, the system designer should take care that all nodes apply the very same bit-timing settings.

The nonprofit SAE (Society of Automotive Engineers) International association developed two recommended practices for CAN FD node and system designers. The SAE J2284-4 document specifies a bus-line network running at 2 Mbit/s with all necessary device and system parameters including the bit-timing settings. The SAE J2284-5 document does the same for a point-to-point CAN FD communication running at 5 Mbit/s. The given parameter values are mainly deriving from General Motors CAN FD first system designs. If you read between the lines, you can adapt the specification also for other topologies and bit-rates.

The Japan Automotive Software Platform and Architecture (Jaspar) association develops also guidelines for CAN FD device and system design. The Japanese nonprofit group cooperates with CAN in Automation (CiA). Both associations exchange documents and comment them each other. Recently, there was a joint meeting to discuss the ringing suppression, in order to achieve higher ▷
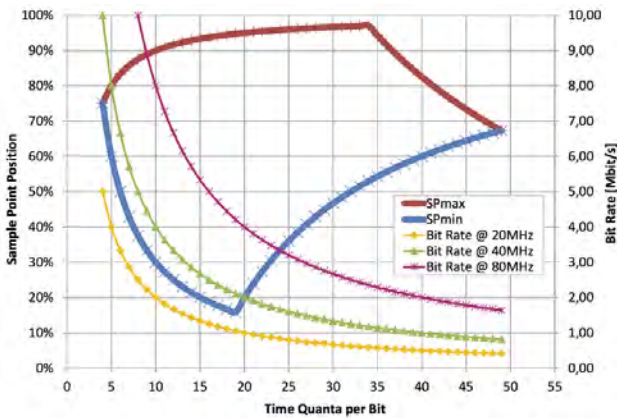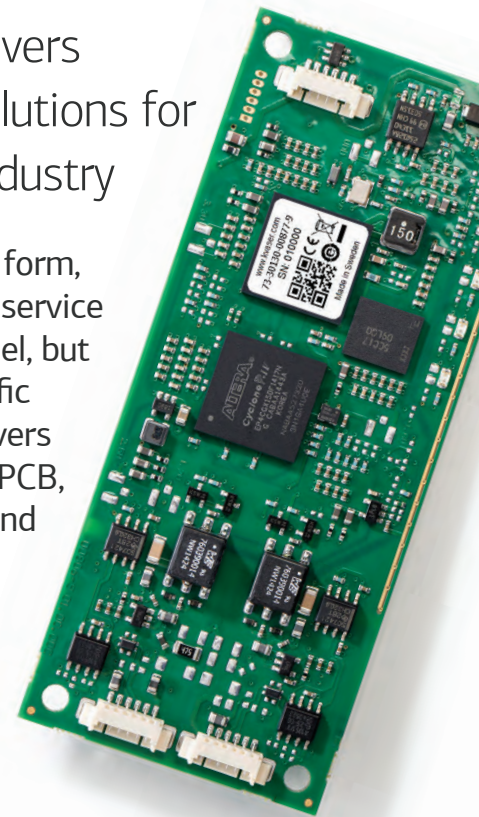
Figure 1: Possible data bit rates and SP positions (min/max); this is a graphical representation of values given in CiA 601-3 (Photo: CiA)

bit-rates or to support hybrid topologies such as multi-star networks.

Recently, CiA has released its CiA 601-3 document. Besides the oscillator frequency (see above), it recommends the bit-timing configuration and some optimization hints for the phase margin. This includes recommendations for the topology, the device design (especially limiting parasitic capacitance).

The bit-timing configuration has two aspects: Setting the nominal time-quantum for the arbitration phase and the data time-quantum for the data-phase as well as setting of the related sample-points including the secondary sample-point (SSP) in the data-phase, when the TDC is used.

Six recommendations

The recommendations given below consider that with each resynchronization, a receiving node can correct a phase error of sjw_D in the data-phase and sjw_A in the arbitration phase. The larger the ratio $sjw_D{:}BT_D$, the larger the resulting CAN clock tolerance in the data-phase. The same holds for the arbitration phase with $sjw_A{:}BT_A$. The absolute number of resynchronizations per unit of time increases towards higher bit-rates. However, the absolute value of sjw_D or sjw_A decreases proportionally with the bit-time. In other words, a higher bit-rate leads to more, but smaller resynchronizations. A CAN FD node performs the bit-rate switching at the SP of the BRS (bit-rate switch) bit and the CRC (cyclic redundancy check) delimiter bit. All three available SPs are independent of each other: arbitration phase SP, data phase SP, and data phase SSP. They can be chosen independently.

In the arbitration phase, the nodes are synchronized and need the propagation segment as a waiting time for the round-trip of the bit-signal. In the data-phase, the nodes are not synchronized. Therefore, no delays need to be considered. Nevertheless, the phase-segment 1 should be large enough, to guarantee a stable signal.

For the data-phase bit-timing settings all the following recommendations should be considered. For the arbitration phase just recommendation 3 and 5 apply.

◆ Recommendation 1: *Choose the highest available CAN clock frequency*

This allows shorter values for the *tq*. Use only recommended CAN clock frequencies (see above).
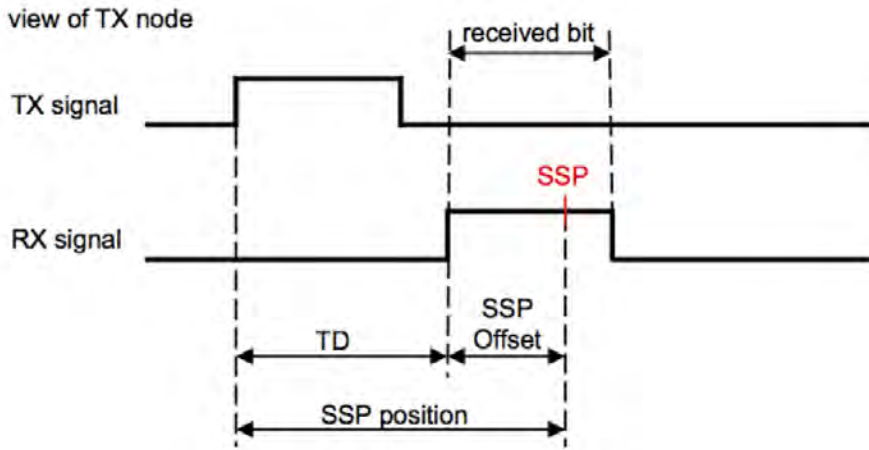
▷

Figure 2: Definition of the SSP (secondary sample-point) position (Photo: CiA)
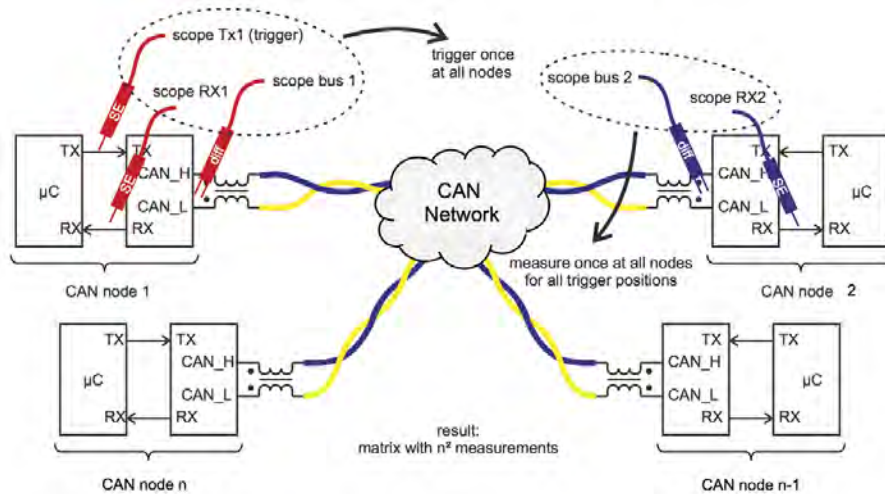

Figure 3: Measurement setup for the evaluation of the asymmetry introduced by the topology (Photo: CiA)

◆ Recommendation 2: *Set the BRP$_A$ bit-rate prescaler equal BRP$_B$*

This leads to identical *tq* values in both phases. This prevents that during bit-rate switching inside the CAN FD data frame an existing quantization error can transform into a phase error.

◆ Recommendation 3: *Choose BRP$_A$ and BRP$_D$ as low as possible*

Lower BRPs lead to shorter *tq*, which allows a higher resolution of the bit-time. This has the advantage that the SP can be placed more accurately to the optimal position. The size of the synchronization segment is shorter and reduces the quantization error. Additionally, the receiving node can synchronize more accurately to the transmitting node, which increases the available robustness.

◆ Recommendation 4: *Configure all CAN FD nodes to have the same arbitration phase SP and the same data phase SP*

The simplest way to achieve this is to use the identical bit-timing configuration in all CAN nodes. This is not always possible, when different CAN clock frequencies are used. The arbitration phase SP and the data phase SP can be different, without any impact on robustness. Different SPs in the CAN FD nodes reduce robustness, because this leads to different lengths' of the BRS bits and CRC delimiter bits in the different nodes and a phase

error introduced by the bit-rate switching. The SSP can be different in the CAN nodes, without influencing robustness.

◆ Recommendation 5: *Chose sjw$_D$ and sjw$_A$ as large as possible*

The maximal possible values are min (ps1$_{A/D}$, ps2$_{A/D}$). A large *sjw$_A$* value allows the CAN node to resynchronize quickly to the transmitting node. A large *sjw$_D$* value maximizes the CAN clock tolerance.

◆ Recommendation 6: *Enable TDC for data bit-rates higher than 1 Mbit/s*

In this case, the BRP$_D$ shall be set to 1 or 2 (see ISO 11898-1:2015). It is not recommended to configure the TDC with a fixed value, because the large transmitter delay variations.

Location of sample-points

The SP locations of the arbitration phase and the data-phase may be different. If in the arbitration phase the SP is at the very far end of the bit-time, the maximum possible network length can be achieved. Sampling earlier reduces the achievable network length, but increases robustness. A value of higher than 80 % is not recommended for automotive applications due to robustness reasons

The SP location in the data-phase depends on the maximum possible bit asymmetries. There are two asymmetries, one for the worst lengthening of dominant bits (A1) and another for the worst shortening of dominant bits (A2) in a given network set-up. Both values are given normally in ns. Both values are the sum of asymmetries ▷
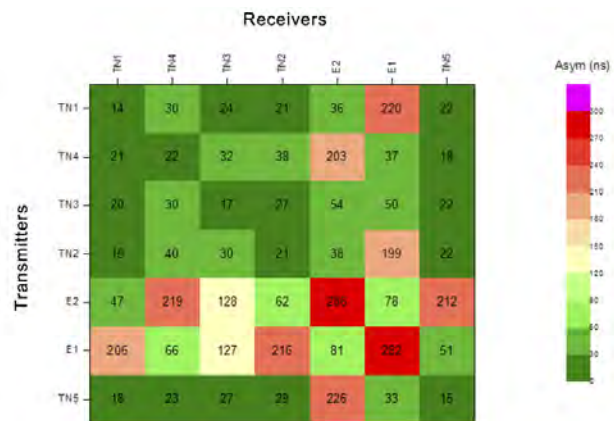

Figure 4: Example of worst-case A1 values for all communciation relationships (Photo: CiA)

caused by the physical network elements including transceiver, cabling, connectors, and optional circuitry (e.g. galvanic isolation). In order to avoid compensations, absolute values are added. ISO 11898-2:2016 specifies the asymmetry values for 2 Mbit/s and for 5 Mbit/s qualified transceivers. The asymmetries caused by the other physical network components are given by datasheets or needs to be estimated or measured. The system designer selects the worst-case connections in network and calculates or measures the both asymmetry values. Another option is to simulate it. There are providers offering such simulation services.

A1$_{topology}$ and A2$_{topology}$ values are different for every communication relationship. This means in a setup with n CAN nodes there are n^2 values for A1$_{topology}$ and n^2 values for A2$_{topology}$. To represent the worst-case, the maximal A1$_{topology}$ and the maximal A2$_{topology}$ values are used to calculate A1 respectively A2. CiA provides with the CiA 601-3 specification a spreadsheet to prove the robustness of the chosen bit-timing settings and the sample-points.

The PM is the allowed shift of a bit edge towards the SP of the bit, at a given tolerance of the CAN clock frequency (df_{used}). In other words, this is the edge shift caused by physical layer effects that is still tolerated by the CAN protocol.

The worst-case bit sequence, i.e. that leads to the lowest PMs, is when the transmitting node sends five dominant bits followed by one recessive stuff bit (for details see /CiA601-1/). This is the longest possible sequence of dominant bits followed by a recessive bit inside a frame. Current transceiver designs cause the largest bit asymmetry at this bit sequence, i.e. the recessive bit is typically shorter than its nominal value. Further effects additionally raise the asymmetry: e.g. asymmetric rise and fall times, bus topology, EMC jitter, etc.

The PM1 and PM2 values for the RX direction given in s (aecond) can be calculated by the following equations:

$$PM1 < \frac{6 \cdot BT_D - PS2_D - tq_D}{(1 + df_{used})} - \frac{5 \cdot BT_D}{(1 - df_{used})} \qquad (1)$$

$$PM2 < \frac{5 \cdot BT_D}{(1 + df_{used})} - \frac{5 \cdot BT_D - PS2_D}{(1 - df_{used})} \qquad (2)$$

with *PM1* = phase margin 1, *PM2* = phase margin 2, BT_D = data-phase bit-time, $PS2_D$ = data-phase phase segment 2.

Additionally, *PM1* and *PM2* for the TX direction needs to be calculated and considered.

Optimizing the system design

The transceiver chips or the SBCs cause a significant part of the overall asymmetry. Therefore it is recommended, to use always components qualified for higher bit-rates. Even if for 2-Mbit/s CAN FD networks, 5-Mbit/s qualified chips should be chosen.

The "badly" designed wiring harness can add many asymmetries. The following recommendations should be considered:
- Use a linear topology, terminated at both ends.
- Reduce the total bus length.
- Limit the number of CAN nodes.

▷

- Avoid long, not terminated stubs, which are branches from the well-terminated CAN lines; use stubs of "cm-range" instead of "m-range". Consider a high-ohmic termination of not terminated stubs.
- Optimize the low-ohmic termination (resistor position and resistor value). Another option is to increase the low-ohmic termination resistance (e.g. 124 Ω instead of 120 Ω) to compensate for the high-ohmic terminations in systems with many nodes.
- Reduce the number of stubs per star point. The more stubs are connected to one star point, the higher the reflection factor gets.
- In case, a star point with many branches is required due to mechanical constraints, avoid identical stub lengths per star point.
- In case, multiple star points are required, keep a significant distance between the two star points.
- Cable cross section: increase it to approximately 2 x 0,35 mm of the CAN_H and CAN_L wire.

Besides these system design recommendations, the device designer should consider the following hints:

- Limit the parasitic capacitance of the device. The parasitic capacitance of the device includes the following parameters: additional ESD protection elements; parasitic capacitance of the connector; parasitic capacitance of the CAN_H or CAN_L wire; parasitic capacitance of the CMC; the parasitic capacitance of the transceiver input pins. All this parasitic capacitance should be below 80 pF per channel.
- CAN_H and CAN_L PCB tracks from connector to transceiver should be of equal distance and parallel.
- Keep the TXD and RXD PCB tracks between host controller and transceiver short.
- Configure the host controller TXD output pin with strong push-pull behavior: a pull-up or pull-down resistor behavior can cause additional asymmetries and propagation delays.
- Avoid any serial components like logical gates or resistors within the TXD and RXD connection lines between host controller and transceiver. In case galvanic isolation is required, take care of the potential additional asymmetry and select components accordingly.
- Use a CAN clock source with lower clock jitter.
- Avoid galvanic isolation, or use a galvanic isolation solution that adds only a small asymmetry.
- In order to optimize the PM, the following hints should be considered:
- Optimize the bit-timing configuration by reducing the *tq* length. This increases PM1 by reducing the quantization error.
- Use a CAN clock with lower tolerance (dfused). This improves PM1 and PM2.

Further recommendations under development

Besides galvanic isolation, there are some other options, which system and device designers may consider. European carmakers often use common-mode chokes, for example. Further add-on circuitry includes a split-termination (two 60-Ω resistors) with a capacitor to ground.

References

[1] Arthur Mutter: "Robustness of a CAN FD bus system – About oscillator tolerance and edge deviations", 14th international CAN Conference (iCC 2013), Paris, France, 2013
[2] Florian Hartwich: "The configuration of the CAN bit-timing", 6th international CAN Conference (iCC 1999), Turin, Italy, 1999
[3] Marc Schreiner: "CAN FD system design", 15th international CAN Conference (iCC 2015), Vienna, Austria, 2015
[4] Y. Horii, "Ringing suppression technology to achieve higher data rates using CAN FD," 15th international CAN Conference (iCC 2015), Vienna, Austria, 2015
[5] CAN Newsletter magazine 2012 to 2017 (several articles), Nuremberg, Germany.
[6] CiA 601 series, Nuremberg, Germany

The CiA community discusses a ringing suppression option, which will be specified in the CiA 601-4 document. It is still under development. In general, such ringing suppression circuitry changes dynamically the network impedance to reduce the ringing in the beginning of the bit-time. Before the SP, the impedance is dynamically switched back to the nominal value. There are two approaches discussed:

- Ringing suppression circuitry on the critical receiving nodes (CiA 601-4 version 1.0)
- Ringing suppression circuitry on the transmitting nodes

The updated CiA 601-4 will just specify the requirements and not the implementations. The automotive industry is highly interested in ringing suppression. It would allow achieving higher bit-rates (desired is 8 Mbit/s) or to allow higher asymmetries caused by the network topology.

The common-mode choke specification for CAN FD networks will be given in CiA 601-6. Also this document is under development. It will mainly contain recommendations and how to measure the values to be provided in datasheets. It is the goal, to make datasheet values more comparable than today.

CiA members are also working on a cable specification (CiA 110). It is intended to define parameters and how to measure them, in order to make datasheets comparable. ◄

Author

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

Sensors for ship cranes

TTS NMF was founded as Neuenfelder Maschinenfabrik in Hamburg in 1970. Today, it is a leading manufacturer of ship cranes, focusing on heavy deck cranes.

With lifting capacities (SWL) of up to 1 000 t and 2 000 t, the cranes manufactured at TWK are the most powerful in the world when operated in tandem. The fact that complex technology is used in these mighty systems is clearly revealed by the control technology, and particularly the sensor system that is implemented. Important parameters that have to be registered include e.g. the boom angle, the turret position (azimuth), and the winch speed for the lifting speed. The ship's heel (list) is additionally registered by means of an inclinometer. If the ship reaches a specific limit value when "rolling" around its longitudinal axis and a corresponding boom angle is registered, the function is limited due to safety reasons. TWK has

been supplying TTS NMF with sensors since 1986. Type PP27 potentiometric angle of rotation encoders were initially supplied. These encoders use contacts for sampling, and have a limited electrical working range. These small, robust rotary encoders that are suitable for industrial use were used primarily in smaller deck cranes to determine the distance between the load on the crane hook and the revolving crane (working radius). Type TBA50 contactless absolute rotary encoders are now increasingly being used. They come with CANopen Safety option and support CiA 301, Version 4.1, CiA 406 Version 3.0, as well as CiA 305.

The T series rotary encoders operate internally using Hall technology, i.e. magnetically. They are designed in ▷

Applications

Figure 1: Sensor model TBA50 (Photo: TWK)

Front chamber with ball bearings

Main chamber with electronic circuit

Figure 2: Cross-section of a rotary encoder from TWK (Photo: TWK)

dual-chamber which e.g. enables the electronics to be cast. The extended temperature range of -40 °C to 85 °C is standard. Thanks to its wall thickness of 5 mm to 10 mm, the housing, which is manufactured from aluminum or, in this case, stainless steel, is extremely robust. With a diameter of 12 mm, the stainless steel shaft can cope with loads of up to 250 N axially and radially. A Simmer-ring seal ensures leak tightness. Protection class IP69K can be achieved by casting the electronics in the housing. This encoder series is particularly suitable for harsh environments that are characterized by wet conditions and extreme temperatures.

It can be networked together with other sensor system and actuator system subscribers in e.g. CANopen using a network interface. SIL2 and TÜV-certified variants are also available (CANopen Safety). In automating complex assemblies, these perform a number of tasks as position feedback sensors and speed sensors.

Rotary encoder

One further rotary encoder that has been developed specifically for cranes is an absolute multiturn encoder with slewing ring functionality. These enable the number of teeth of the slewing ring and rotary encoder pinion to be set directly in the rotary encoder. As a result, all conceivable gear ratios can be implemented, and the rotary encoder can be adapted precisely to the respective slewing ring by the customer. The rotary encoder then supplies the position of the slewing ring in degrees (resolution adjustable) and its speed in degrees/unit of time (unit of time adjustable) as output values. An optional play-free gear ZRS from TWK is available for coupling to the slewing ring. Manufactured from special, permanently elastic plastic, this gear is particularly resistant to temperature influences, moisture, aggressive substances, and permanent mechanical stress. The special tooth shape guarantees that a tooth's flanks are constantly in contact with the gear that is to be measured. This prevents falsification of the measurement signal on switching between forwards and backwards rotation (backlash).

In the field of inclinometers, TWK has developed the NBx65 model series based on so-called Mems technology.
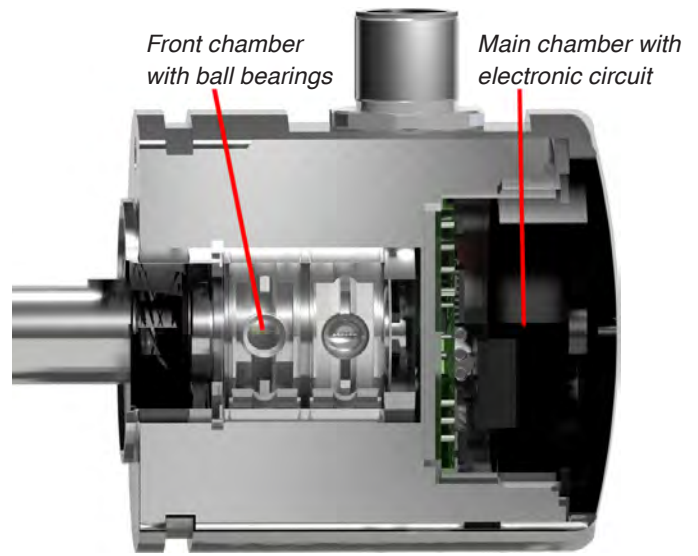
Registration over +/- 90° for one or two axes and signal output with all relevant industrial interfaces are possible. TÜV-certified safety variants are also available in this case. Thanks to the solid housing made of seawater- resistant aluminum or stainless steel, with wall thicknesses of up to 5 mm, these encoders are particularly suitable for maritime use. ◄

Author

Gerd Schulz
TWK-Elektronik
info@twk.de
www.twk.de

CAN Newsletter Online: TWK

The CAN Newsletter Online reports briefly about products and services.

Draw-wire sensor
Measures up to 10 m
The 125-D draw-wire sensor by TWK uses a CANopen encoder. It operates form -20 °C to +85 °C. The sensor based on rotary encoders is intended for outdoor applications.

Read on

CANopen
Safety sensor for wind power
The safety vibration sensor NVA115 from TWK has been developed to protect wind power plants from damage caused by oscillations and vibrations. Data output is carried out via the CANopen interface.

Read on

Vibration sensor
For SIL-2 applications
TWK (Germany) has added the NVA/S3 to its family of inclinometers and vibration sensors. It is able to output a safe vibration value between 0,1 Hz and 60 Hz via CANopen Safety or analog output.

Read on

Rotary encoder
Slewing ring functionality
TWK Elektronik (Germany) has equipped its rotary encoders of the TRT and NOCN model series with a slewing ring functionality. The encoders come with CANopen.

Read on

Inclinometer
With SIL2 certificate and CANopen Safety
The NBN 65 by TWK (Germany) is an inclination sensor supporting CANopen Safety. They are now also available with TÜV certification.

Read on

Encoder can be integrated into axle pins
TWK (Germany) has introduced the TBN 37. It is a sensor with a shaft loadability of up to 500 N radially and 100 N axially with a housing diameter of 25 mm. It can therefore be integrated within an axle pin.

Read on

SIL2 inclinometer with CANopen Safety
At the Sensor + Test 2013 TWK (Germany) has introduced the NBN/S3 inclinometer supporting CANopen Safety. The SIL2 certified sensors can be mechanically adjusted up to ±7,5° using elongated holes.

Read on

Display for chippers

Jenz introduced new CAN-based display control units from STW into their portfolio of chippers.

*Figure 1: The Jenz chipper
HEM 821 DQ Cobra+ hybrid (Photo: Jenz)*

Jenz is renowned for its chippers, used for chopping up shrubbery and heavy tree trunks, as well as for its top-class biomass processors. The company offers very different sizes and performance classes of vehicles and machines. Jenz has introduced new displays from the VSX family by Sensor-Technik Wiedemann (STW) into their products. They had been looking for a new product representative of the next generation of display control units, which combines robustness with high performance, and which could be used in different sizes for all construction series. It had to be possible to install these displays both into a cabin and into a control cabinet, and they should be available both with and without keys. Weiss Mobiltechnik, as a long-standing electronics development partner of Jenz, and specialists in display programming, control units, and telemetry, suggested the new VSX display product series by STW. One important aspect from Weiss' point of view was the further development of the display software established at Jenz. It should be possible to continue use of the existing software, and to add new functions without much effort.

The VSX family offered the optimum prerequisites for these requirements. Linux and the GUI Toolkit QT are available in the standard version of this display with its Cortex A9 dual-core processor. In order to support Weiss, STW also implemented a Codesys 3.5 runtime system on Linux. The interfaces between the Codesys runtime system and QT on the one hand, and the graphic library by Weiss on the other were implemented in a special "wrapper layer". This now permits Weiss to utilize its graphics library and all the applications based upon it immediately on the STW displays without source code adaptations or other changes being required.

For the first project, Weiss used the VSX-10 Professional Display for the cabin of the HEM 821 DQ Cobra+ hybrid chipper. In combination with an operating console, all the HEM 821 functions can be controlled here. The HEM 821 is a compact 4-axle-truck 8x6-4 with steered trailing axle for extreme off-road capabilities and high maneuverability. The rotatable and elevating driver's cabin provides an optimum overview, making it possible to change trucks at the location of operation even when the cabin is rotated and elevated and with the carrier vehicle under full tractive power. The chipper is suitable for shrubbery and heavy tree trunks up to diameters of approx. 800 mm, and permits high-performance chipping in extreme, continuous operations.

The display plays a central role in the HEM 821. Individual settings can be undertaken for the driver in different display menus. The operating elements are implemented as sliders or buttons. Limit values such as the maximum motor speeds can be defined in configuration menus, or certain advance selections can be made regarding working conditions or user profiles. Other menus permit the extension and retraction of the supports, the position regulation of the cabin itself, or depict work functions such as the speed control of the conveyor belt or the operation of the crane via touchscreen or buttons. It is therefore always possible to optimize the machine settings, and thus to guarantee maximum economic viability. Up to 2000 continuously-changing parameters including J1939 engine data, such as the speed or current fuel consumption are shown in special diagnosis menus ▷

Figure 2: The displays from the Interact-VSX family by STW (Photo: STW)

using various display instruments. The level of brightness also permits good legibility in direct sunlight. Regarding the presentation, the operator also profits from the performance capability of the display. Menu changes take place spontaneously; the display instruments run jerk-free so that pleasant operation with immediate feedback is possible.

The communication with the control units, in which in turn the work function is implemented using control and regulation algorithms, takes place via the CAN network. The Professional version of the VSX-10 offers four CAN interfaces, meaning that different networks are connected and gateway functions can also be implemented. It is even possible to wake up the display via defined CAN messages. The control units used are the STW ESX-3CM for the chipper itself and the STW ESX-2-4 for the crane.

Furthermore, the control units and the display can be connected with a combined data logger / telematic module, the TC3G by STW. A series of functions has been implemented by Weiss in the freely programmable Embedded

Linux available on this module. In this way, all operating data can be recorded and transmitted via USB, Wi-Fi or mobile communications into the company-specific data processing. Using the display enhancement possibilities, it is possible to depict this function, too, in the display itself.

In future, further Jenz vehicles are to be equipped with the VSX display. Here the family approach featuring different display sizes from 8 inch to 15 inch with the same platform is an advantage. Whereas the functionality does not have to be changed, the user interfaces can be adapted to the new dimensions through the Weiss graphic libraries. Regarding their use in control cabinets, not only the protection class IP67 is of benefit, but the resistive touchscreen also permits operation using gloves. "The typical utilization of the two CPU cores", says Mr. Mönninghoff from Weiss, "lies at maximum 20 %". This means that the display also provides sufficient space for new, improved algorithms, additional assessments, and indications.   ◀

Author

Hans Wiedemann
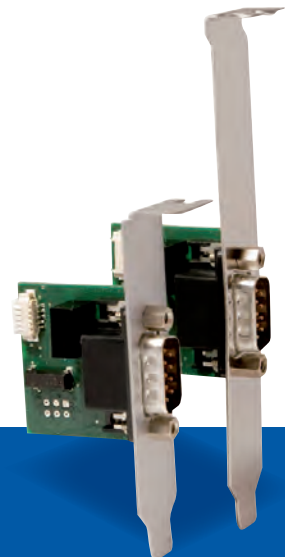Sensor-Technik Wiedemann
info@sensor-technik.de
www.sensor-technik.de

Open source Raspberry Pi with CANopen

Revolution Pi involves the idea of providing an inexpensive industrially viable version of the Raspberry Pi under "Open Source" conditions and making a "community based project".

Industry 4.0 and Internet of things (IoT) are changing the requirements for the control level dramatically. Firstly, the need for decentralized controllers (and communication in general) will increase considerably, and secondly, completely different applications will also be integrated gradually in higher-level networks.

Building technology, event technology, house technology, IoT requirements, private control tasks, surveillance technology, process automation, and of course automation technology as well, are moving closer together. Decentralized solutions are gaining in importance and thus the accompanying requirements for inexpensive, scalable, and industrially viable small control systems. Furthermore, there is a great need for connecting these small control systems to a CANopen network, for example. Even the desire for "Open Source" solutions is becoming greater and cloud solutions will already soon be the standard in the industry. But how could such a solution look like?

Revolution Pi

Revolution Pi is an open, modular and inexpensive industrial PC based on the established Raspberry Pi while meeting the EN61131-2 standard. It is supplemented by digital and analog I/O modules as well as by appropriate Ethernet and fieldbus gateways such as CANopen. The hardware and software is "Open Source" and all circuit diagrams and source codes are open to everyone.

It's a small computer based on the Raspberry Pi Compute Module that has USB, Ethernet, and HDMI connections. Robust 24-V industrial hardware is integrated into its DIN rail housing. As a result, this hardware meets all requirements for a fully-fledged, industrially viable small control system.

The Revpi Core is an open platform, on which everything from the operating system to applications can be installed, which also runs on a Raspberry Pi. A specially modified Raspbian version with a real time patch and approprate drivers for the expansion modules is available as an operating system. On this basis, the Soft PLC from logi.cals and Axel, Teamviewer, and Scada software Procon-Web-IoT can be used, for example. This means that the Revpi Core is a complete and operational PLC.

Through the modular design of the family, for example, CANopen can connect the Revpi Core to digital and analog input and output modules as well as certified gateways to all important fieldbuses.

Figure 1: Due to the gateway expansion module for CANopen, The Revpi Core 3 can be integrated into a CANopen network (Photo: Kunbus)

All cyclically exchanged process data stem from a central process image in the Revpi Core or are stored there. The central process image is a memory area, in which the process data are saved at predetermined addresses. Developers can write in the process image or read it from there by simply invoking the operating system. Connected gateways such as CANopen also exchange their data with the central process image of the Revpi Core.

The "Open Source" concept also allows users to use own software and program under Linux with Python. All drivers and operating software used as well as all process data can be accessed for this purpose. Developers can write their own application programs with Python, C+, or other programming languages and the well-known tools for Raspberry Pi and thereby use Linux functions to access the process image.

The I/O expansion modules come in four versions, which all have the same 28-pin I/O connector at the front:

◆ The standard version Revpi DIO has 14 digital inputs and 14 digital outputs
◆ The special version Revpi DI has 16 digital inputs and no outputs
◆ The special version Revpi DO has 16 digital outputs and no inputs
◆ Revpi AIO is the analog variant with four analog inputs, two analog outputs, and two RTD channels

In all four variants, the inputs and outputs are galvanically isolated from the logic component. All four versions are protected against disturbances, polarity reversal or surges according to EN61131-2 and can be operated (like the base module) between -40 °C and +50°C ambient temperature and up to 80 % relative humidity. The power ▷

supply unit works with 10,2 V to 28,8 V input voltage and only requires a maximum of 50 mA.

The previous task of the modular gateways was to connect industrial networks to different network protocols (e.g. a CANopen network to a Profinet network). The approach of accommodating the individual protocols in separate DIN rail modules ensures high flexibility because all available protocol modules are mutually compatible. One benefit of the modular design is the cost factor, among other things, during changes of the technical conditions in the field. Whereas normal gateways, for example, must be replaced entirely when a network is changed, with our system only the module of the network concerned is replaced. To do this, the CANopen gateway (slave) is simply inserted into a DIN rail next to the Revpi Core and connected by means of a jumper. The gateway is enclosed in a plastic casing measuring 22,5 mm x 101,4 mm x 115 mm (W/H/D). The module is supplied with an operating voltage of 24 V, whereby the power consumption is less than 3 W. The network is connected with a connector type D-SUB 9M. The max. bit rate is up to 1 Mbit/s and up to 512 bytes of I/O data can be exchanged with the Revolution Pi. The data are stored in the process image of the Revpi Core and are available to other applications. The complete system has the protection class IP20. The CANopen expansion module has been tested and certified at CAN in Automation.

Revolution Pi firstly involves the idea of providing an inexpensive industrially viable version of the Raspberry Pi under "Open Source" conditions and making a "community based project". Secondly, the Revolution Pi should advance the 4th industrial revolution. Thus, the Revolution Pi consists of many things. It is:

◆ A Raspberry Pi
◆ An industrial PC (IPC)
◆ A PLC
◆ An IoT gateway
◆ A web server
◆ A software platform
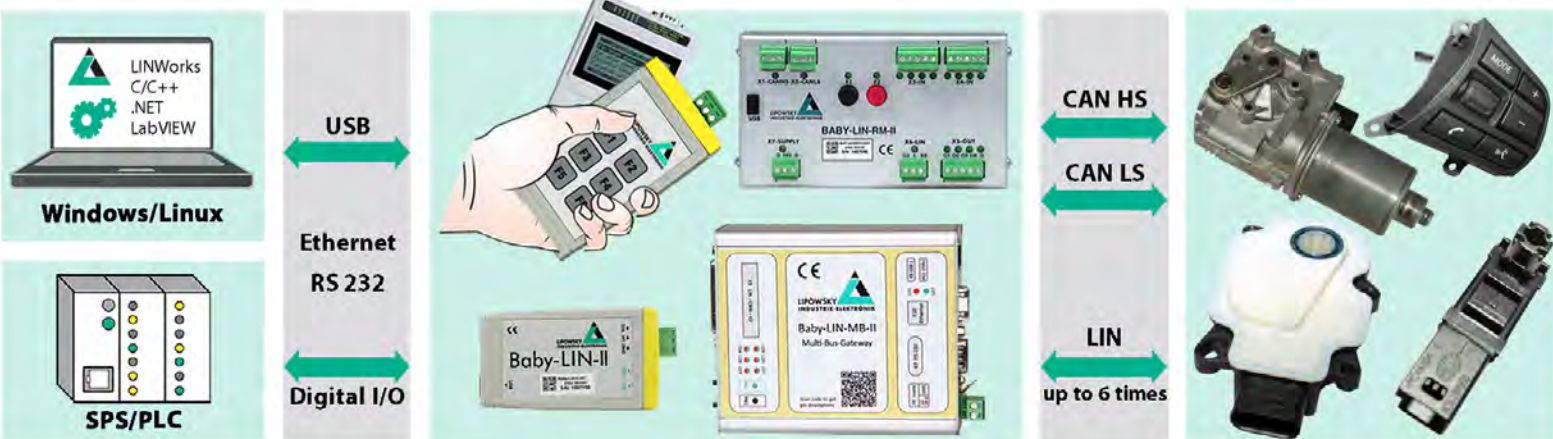◆ A small control unit for an HMI
◆ A cloud solution

And all that together with a certified CANopen connection. ◀

Author

Andreas Müller
Kunbus
a.mueller@kunbus.de
www.kunbus.de

CAN in Automation

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

Join the community!

▶ Initiate and influence CiA specifications

▶ Receive information on new CAN technology and market trends

▶ Have access to all CiA technical documents also in work draft status

▶ Participate in joint marketing activities

▶ Exchange knowledge and experience with other CiA members

▶ Get the CANopen vendor-ID free-of-charge

▶ Get credits on CANopen product certifications

▶ Get credits on CiA training and education events

▶ Benefit from social networking with other CiA members

▶ Get credits on advertisements in CiA publications

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

www.can-cia.org