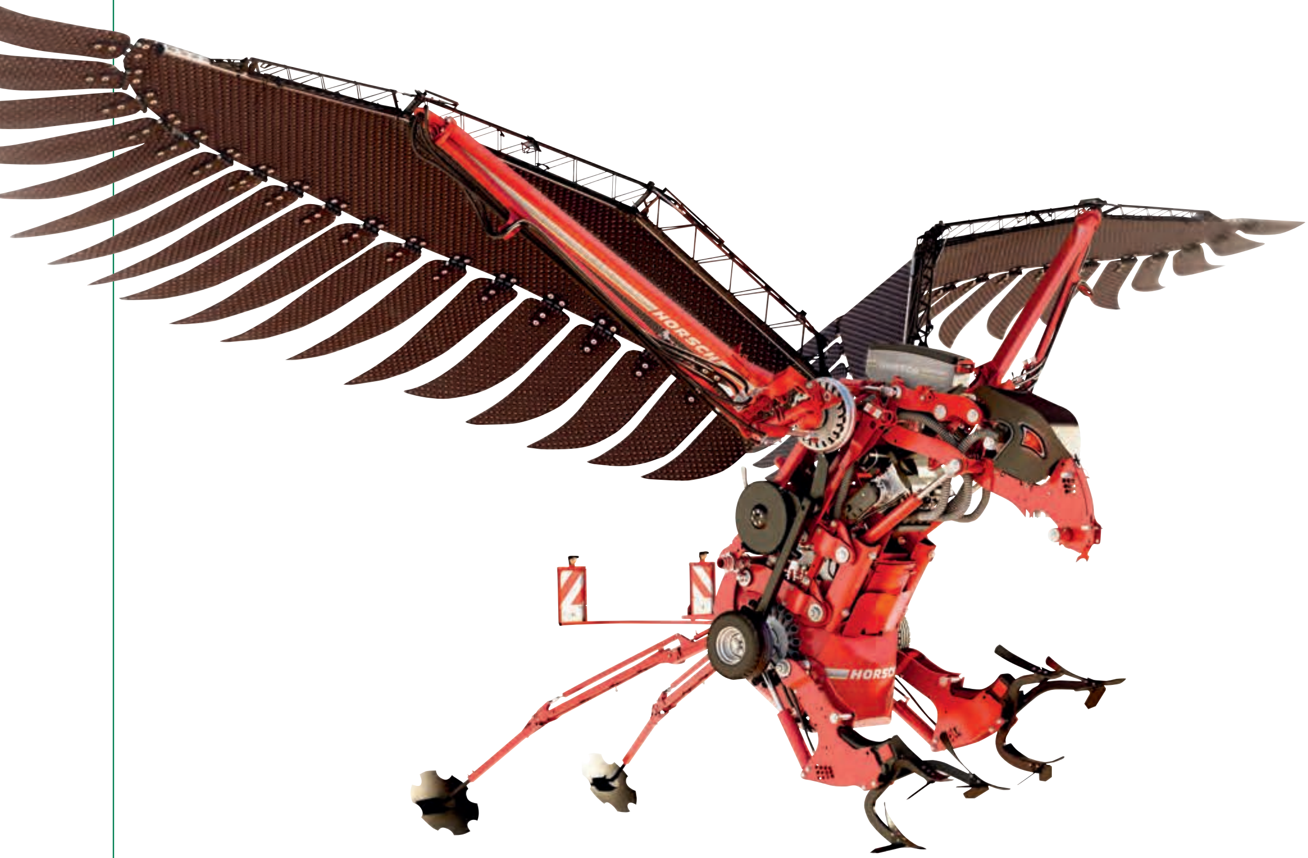
March 2014 B 25361

CAN Newsletter

Hardware + Software + Tools + Engineering



Farming with passion: CAN is set

To the light tower

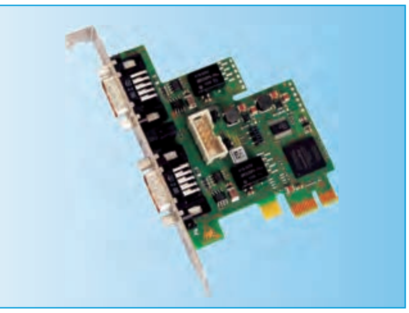
Detecting car damages with CAN networks

Tumor treatment with a CANopen motor

Embedded

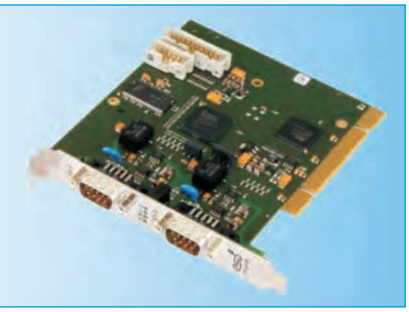
www.esd.eu

CAN-PCIe/402

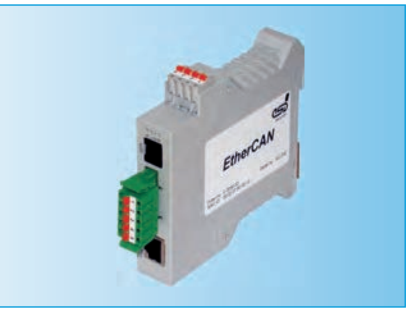


CAN-USB/400

CAN-PCI/400



Ethernet



CAN-USB/2

Gateways

All you CAN plug

CAN-PCIe/402
- up to 4 high performance PCI Express CAN interfaces
- DMA busmaster
- Powered by esd Advanced CAN Core (esd-ACC)
- MSI (Message Signaled Interrupt) support
- Electrically isolated
- Provides high resolution hardware timestamp

CAN-USB/400
- 2 high performance CAN-USB interfaces
- Powered by esd Advanced CAN Core (esd-ACC)
- USB 2.0 with high speed data rates of 480 Mbit/s
- Electrically isolated
- Provides high resolution hardware timestamp
- Error injection for advanced diagnostic
- IRIB B timecode as option

CAN-PCI/400
- up to 4 high performance CAN interfaces
- Powered by esd Advanced CAN Core (esd-ACC)
- Electrically isolated
- Provides high resolution hardware timestamp
- Error injection for advanced diagnostic

CAN-PCI104/200
- PCI104-CAN interface
- One or two CAN interfaces for PCI104 bus

EtherCAN
- 10/100 BaseT ETHERNET-CAN Gateway
- Electrically isolated
- Configuration and Diagnostics by webbrowser

CAN-USB/2
- CAN-USB interface
- Intelligent CAN interface with ARM 7
- USB 2.0 with high speed data rates of 480 Mbit/s
- Electrically isolated
- Provides high resolution hardware timestamp

Gateways
- EtherCAT-CAN
- PROFINET-CAN
- PROFIBUS-CAN
- PROFIBUS-DeviceNet
- EtherNet/S7-CAN

Operating Systems
esd supports the real-time multitasking operating systems VxWorks, QNX, RTX, RTOS-32 and others as well as Linux and Windows 32/64Bit systems

CAN Tools
- CANreal: Display and recording of CAN message frames
- CANplot: Display of online/offline CAN data
- CANrepro: Replay of pre-recorded CAN message frames
- CANscript: Python scripting tool to handle CAN messages
- COBview: Analysis and diagnostics of CANopen nodes

The tools are free of charge on the driver CD or can be downloaded at www.esd.eu

esd gmbh • Vahrenwalder Str. 207 • 30165 Hannover • Tel: (0511) 372 98-0 • Fax: (0511) 372 98-68 • info@esd.eu • www.esd.eu
esd electronics Inc. • 70 Federal Street • Suite 2 • Greenfield • MA 01301 USA • Phone: 413-7723170 • us-sales@esd-electronics.com • www.esd-electronics.us

Farming with passion: CAN is set

Dr. Matthias Rothmund leads the electronic development at Horsch, a manufacturer of agriculture machines. The company has a leading market position in innovations for seeding and spraying technology and was awarded with two Agritechnica silver medals in 2013.

Matthias Rothmund holds a Ph.D. in agricultural science. Since 2010, he has been working for Horsch, a company that developed its first own foil maize seed machine in 1981. His team comprises engineers and technicians, who are responsible for electronic system integration, programming embedded controllers, and testing.

The manor Sitzenhof, which nowadays is surrounded by the facilities of Horsch Maschinen, is still operated as a farm. Beyond that, today the Horsch family runs several big farms in Germany and in Czech Republic. Naturally, they use their own machines to farm their fields. Moreover Matthias Rothmund knows farming from his own experiences. The whole team knows farming not only in theory.

The electronic team also designs CAN-based networks. Those include Isobus as well as embedded networks in implements. At the Agritechnica exhibition in 2013, the company received the silver medal for innovation for its single grain technology for seeding cereals. "The embedded CAN network connecting up to 80 brushless DC motors is based on the J1939 protocol," explained Rothmund. "We use proprietary PGNs, parameter group numbers." One control unit operates two motors. The awarded solution is able to meter cereals in single grain quality up to a frequency of 120 Hz, which adds up to 120 grains per second, thus to a seed quantity of 240 grains per square meter. The central hopper supplies the seed by means of a volume-metering unit. The pre-metered seed is pneumatically conveyed and transported to the respective seed row. The CAN-connected BLDC motors with high torque capability drive the metering units for grain singulation. The host controller for the prototype machine is from Mueller Elektronik, one of the main hardware suppliers. Similar metering systems were already used in seed drilling machines for corn, for example. In this machine, up to 24 motors with integrated controllers and CAN connectivity by Dunkermotoren are used.

"The embedded CAN network connecting up to 80 brushless DC motors is based on the J1939 protocol.

Their other silver awarded equipment is the Boom Control system. It is part of the spraying boom, which operates just above the crop. The Isobus-linked controller consists of STW hardware and Horsch software. The active boom control allows a low distance to the target area. As the boom has been separated from the chassis, an exact adaption of the boom to the field contour is possible. Due to this decoupling the rolling motions of the carrier vehicle are not transmitted to the boom. The adjustment speed of the contour adaption is high even under difficult conditions. Disturbing impacts like wind and thermal can thus be minimized. The necessary hydraulic devices are linked via the embedded J1939 network.

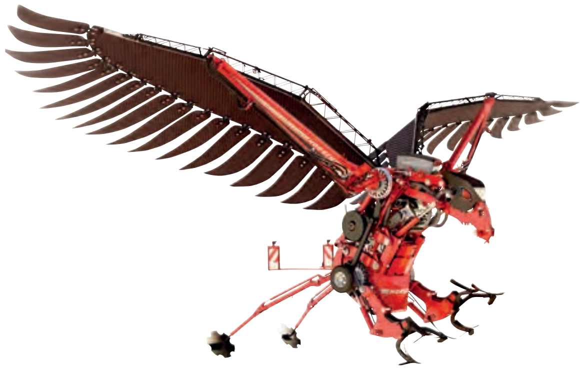
Some of the company's electronics are very dedicated. "We develop some devices by ourselves," said the head of the electronic department. "Of course, the production of this equipment is done by partners." One of them is Inmach, a German company partly owned by Horsch. Recently, this company introduced a CAN-connectable ultrasonic measurement unit, which comes optionally with Isobus software. "We also program some of the embedded controllers on our own," said Rothmund. "We program in C++, because we like object-oriented software."

"CAN communication is our daily business," said Rothmund further. "We install more than 7000 nodes per year." For development, diagnostics, and testing the CAN tools from Peak are used. Most of the CAN-based embedded networks run at 250 kbit/s.

All of Horsch's machines, which are using electronic control systems come with Isobus connectivity. They can make use of the virtual terminal installed in the tractors. "Teething trouble with Isobus virtual terminal is history," explained Rothmund, "with the Isobus task controller we have not yet solved all problems, and we already face challenges of automated Isobus implements, which control the tractor."

The company has established the electronic development team to determine the control architecture and to reduce dependency from electronic suppliers. So they always get first-hand information and to be prepared for the future, Horsch is member of the AEF, the Agriculture Industry Electronics Foundation. Matthias Rothmund participates in various technical working groups and he is also a member of VDMA's (German Engineering Association) technical committee for electronics. Both associations are involved in the Isobus development. ◀

Table of contents



Farming with passion: CAN is set

Dr. Matthias Rothmund leads the electronic development at Horsch, a manufacturer of agriculture machines. The company has a leading market position in innovations for seeding and spraying technology and was awarded with two Agritechnica silver medals in 2013.

Imprint

Publisher
CAN in Automation GmbH
Kontumazgarten 3
DE-90429 Nuremberg

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

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

CEO Holger Zeltwanger
AG Nürnberg 24338

Printed in Germany
Hard copies: 3000
Soft copies: 3000

Editors
(pr@can-cia.org)

Annegret Emerich

Cindy Weißmüller

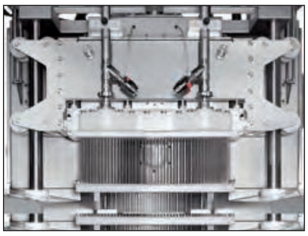
Holger Zeltwanger
(responsible according to the press law)

Layout
Nickel Plankermann

Advertising manager
Gisela Scheib
(responsible according to the press law)

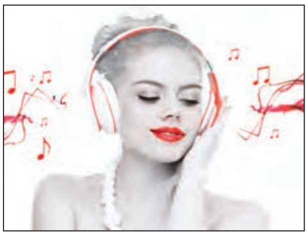
Distribution manager
Julia Adolf

Business



CANopen

Embedded



Engineering

Since the beginning of this year, Intel guarantees not to use such minerals (e.g. tantalum, tin, tungsten, and gold) in its products that were mined and sold by armed groups in the Democratic Republic of the Congo (DRC). Some of these groups use their gains to "finance conflict characterized by extreme levels of violence". CiA also supports the activities of the Conflict-Free Sourcing Initiative (CFSI). If you want to help, you can request your suppliers to support this initiative of the Electronic Industry Citizenship Coalition (EICC) and the Global e-Sustainability Initiative (GeSI). We hope this helps end the violence and child labor in DRC: No more "Blood CAN".

Solutions for Open Networks from one Source

Open CAN-based protocols are the basis of networking in commercial vehicles, avionics and industrial control technology. Vector supports you in all development phases of these systems:

> Systematic network design with CANoe, ProCANopen and CANeds
> Successful implementation with source code for CANopen, J1939 and more
> Efficient configuration, test and extensive analysis with ProCANopen, CANoe and CANalyzer

Multifaceted trainings and individual consulting complete our extensive offerings.

Thanks to the close interlocking of the Vector tools and the competent support, you will increase the efficiency of your entire development process from design to testing.

▶ **Further information, application notes and demos:**
www.vector.com/opennetworks

Vector Informatik GmbH
Germany • USA • Japan • France •
UK • Sweden • China • Korea • India

25 Years vector

Meeting point for the CAN community

The annual Embedded World tradeshow and the related conference is the first event of the year where the CAN community meets. Many leading chipmakers present their CAN transceivers and CAN micro-controllers.

Links
www.embedded-world.de
www.codesys.com
www.ems-wuensche.de

Exhibiting CiA members
3S-Smart Software (4-600)
Advantech (2-220)
AF Inventions (4A-130)
B-Plus (1-428)
Beckhoff (5-370)
Deutschmann (5-411)
Embedded Office (5-346)
EMS Dr. Wünsche (1-630)
Emtas (4A-310n)
ESD (4-141)
Etas (4-410)
Euros (5-344)
Fastwel (1-504)
Freescale (4A-210)
Frenzel + Berg (1-140)
Hilscher (1-348)
Hima (5-339)
HMS/Ixxat (1-540)
Infineon (4-550)
Janztec (2-308)
Kunbus (4-561)
MEN (2-230)
Microcontrol (5-454)
Mitsubishi (1-181)
NXP (4-240)
Peak (1-606)
Phytec (1-206)
Port (1-638)
Profichip (1-139)
Renesas (5-411)
Softing (1-360)
Sontheim (1-571)
Spansion (1-306)
Syslogic (1-479)
Systec (1-629)
Toshiba (1-306)
Vector (4-122)
Wago (1-309)
Xmos (4A-428)

Figure 1: The Embedded World is an international event, although the signs only carry the English translation as underlines (Photo: Embedded World)

Last year, more than 22000 visitors made their way to Nuremberg (Germany) to see the products of about 850 exhibitors. Approximately 1500 participants attended the conference. For the CAN community, especially for those involved in embedded control systems, this event is the prelude of the year. This year's conference keynote focuses on "Securing the Internet of Things".

The CAN community wonders if there will be announcements regarding CAN FD, the improved CAN protocol. Bosch, Freescale, NXP, and Texas Instruments have already introduced so-called CAN high-speed transceivers able to support bit-rates higher than 1 Mbit/s. STMicroelectronics samples its 32-bit micro-controller supporting CAN FD, but if this chip will be on the fairground is questionable: The CAN FD module only supports 8-byte payloads, even though the improved CAN protocol allows up to 64 byte per data frame. Of course, the French-Italian chipmaker will provide a full-featured CAN FD module in the near future. Other semiconductor manufacturers also have CAN FD in the pipeline: Spansion (former Fujitsu) will have the first CAN FD silicon in April for internal review; Infineon and Renesas will ▷

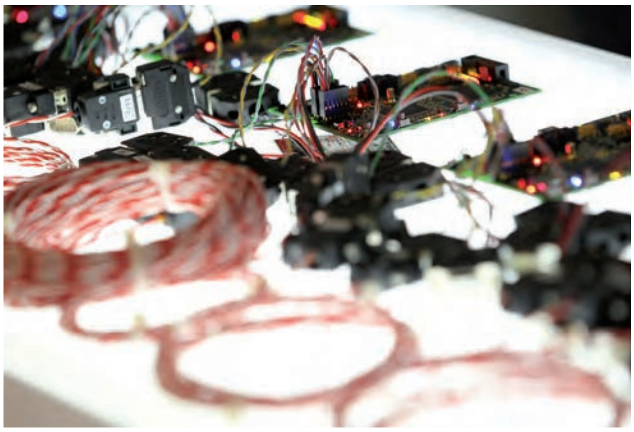


Figure 2: Last year, Bosch presented a CAN FD prototype application with several boards running at 15 Mbit/s at its booth (Photo: Embedded World)

follow. Perhaps Freescale will be the one who presents the first micro-controller prototypes with CAN FD in Nuremberg. We will see.

CAN FD: not the only hot topic

But there are other interesting topics: 3S Smart Software Solutions introduced its Codesys software for Raspberry Pi modules. The IEC 61131-3 compliant development and runtime system supporting CANopen is used, for example, in embedded controllers for mobile machines and for building automation. The open-source hardware platform is used increasingly in this kind of application. The trade-off is that Raspberry Pi requires an add-on module for the CAN interface, which is why some CiA members are evaluating the development of an open-source hardware platform for CAN applications. “Besides the academic and hobbyist markets, we are addressing the professional developers,” said Thilo Schumann from CAN in Automation (CiA). “The project under the codename CANware is also interesting for prototyping.”

CiA
Booth no. 608
Hall 1

Gateways linking CAN and Ethernet are another hot topic. EMS Dr. Wuensche launches, for example, the EtherCAN CI-ARM9 gateway. It comprises a 454-MHz processor, 2-GiB of flash memory, and a 128-MiB DDR memory, which makes the product suitable even for sophisticated gateway applications. The product features a USB 2.0 interface, which allows adapting wireless connections, e.g. Bluetooth or WLAN. For the two-CAN channels gateway with an SD slot, the supplier developed a Profinet-to-CANopen software. For simple tunneling of CAN messages via Ethernet, the company already offers the EtherCAN CI-ARM7 module.

Companies focused on industrial automation have expanded their portfolios and are looking for customers at the Embedded World. Wago, for example, will show the PFC200 controller, which is based on the Linux real-time operating system. It features two Ethernet interfaces as well as one CAN port (optionally with CANopen software). The controller can be connected via CANopen to the company’s broad range of I/O modules. Those products are in competition to those of companies coming from embedded systems now offering also Codesys or other PLC software. A typical example is the Hipecs family by Frenzel + Berg, which comprises host controllers as well as I/O modules. Another provider of CANopen PLC cores and I/O modules for embedded control systems is Systec. The company offers IEC 61131-3 programmable board-level products, which come with CANopen Manager software.

Of course, the halls will be stuffed with CAN products. More than 250 of the 832 exhibitors will show CAN-related products. Most of them are not new; nevertheless visitors have a good chance to find all kinds of CAN products (hardware and software) for embedded systems. ◄

CANopen preserves food

For obvious reasons the food industry places high demands on their machines: Hygienic design with corresponding materials and ease of cleaning are especially important in this sector.

Author
Tarak Viol
Technical Sales Consultant
Wago Kontakttechnik
GmbH & Co. KG
Hansastr. 27
DE-32423 Minden
Tel.: +49-571-8870
Fax: +49-571-887169
info@wago.com

Links
www.wago.com
www.guenther-foodtech.de

Pickling is a method that has been in use since ancient times to preserve meats and vegetables. A nitrite salting mix prevents the proliferation of microorganisms that would otherwise quickly spoil the goods. In classic pickling methods, completing the process takes a few weeks. This process happens significantly faster when the pickling salt is injected directly into the meat in the form of liquid brine.

Brine injectors and tumblers

This injection method demands machines of the type that Günther Maschinenbau, located in Dieburg, Hesse, has developed and manufactures. When the conveyor belt carries the pieces of meat through the injectors, they pass under a so-called needle bar. There are up to 850 injection needles mounted on this bar, and during operation the needles are pressed through the bar and into the meat to inject the brine. The cycle time of the machines is continuously variable and allows up to 80 strokes per minute. The stroke height can also be continuously adjusted so that pieces with differing thicknesses can be easily processed.

The machines have their own pumping circuit to supply the brine and, depending on the version, are provided with a fully automated rotary filter unit. The entire pump circuit is thus completely separated from all electromechanical components. This hygienic design is of particular importance for machines used in the food industry. The plastic parts are made of Polyoxymethylene (POM) and the metal parts of stainless steel. The conveyor belt and the needle bar can easily be disassembled and cleaned.

“The demands placed on machines used in the food industry are very, very high.
Jörg Schwebel

High requirements

“The demands placed on machines used in the food industry are very, very high,” explains Jörg Schwebel, who is head of electrical engineering at Günther Maschinenbau. His colleague, Andreas Jäckel adds, “The mechanical robustness is especially important.” Cleaning with high-pressure steam cleaners is obviously a daily occurrence in this sector. For this reason, all electrical components that are mounted outside the machines must fulfill the high requirements of protection type IP69K. This includes the pluggable connectors for the power supply, as well as the touch panel used to operate the machine. All other electrical components are located in a control cabinet that is doubly sealed and integrated into the machine. All operator inputs happen via the touch panel, which is run by a Codesys soft PLC using Windows CE. Communication with the drive's frequency converter and the machine sensors and actuators takes place using the CANopen protocol. At Günther, they rely on 750-337 CANopen Fieldbus Couplers from Wago, which can be augmented by I/O modules from the Wago-I/O-System 750 product range.

“The high flexibility of the I/O system is one of the reasons we rely on Wago,” explains Torsten Haupenthal, who is responsible for the electronics in the machines at Günther. Digital and analog I/O modules, Pt100 resistance sensors, and DMS cards for integrated weighing technology are integrated into almost all machines as standard components. Even for special cases, they often find suitable modules in the company’s catalog. Jäckel recalls, “In order to realize a cable-free connection to a supply unit, we installed a Bluetooth module”. Almost all sensors and actuators are directly connected using the I/O system. 788 Series Coupler Relays are additionally used for components with high power requirements. These are necessary for the controllers for hydraulic or pneumatic valves.

Safe power supply for the controllers

In order to supply the components in the control cabinet with the necessary 24 V_{DC}, the developers at Günther rely on Epsitron Switched-Mode Power Supplies. Wago’s 787 Series ▷

Figure 1: Pickling injectors, as well as brine mixing machines and tumblers, form the two main product (Source: Günther Maschinenbau GmbH

Power Supplies are available in different outputs, so that a suitable device is available for the different types of machines. In addition to the power supply units, Epsitron Uninterruptible Power Supplies (UPS) ensure that the controller can still be operated during electrical failure. This is especially important for the so-called tumblers, which Günther also offers. The pieces of meat are mechanically tumbled in these machines, which accelerates the pickling process after the brine injection. "The tumblers often operate at night, when there are no operators on site," explains Torsten Haupenthal. "The UPS ensures that the controller has the machine continue at the same point in the process after an electrical interruption."

If the electricity goes out for a longer period, or if there is a fault at the machine, a service person has to be notified. In this case, the Wago To-Pass Compact Telecontrol Module steps in, as it can send an error message using text messaging, for example. The module can be parameterized, for example, different texts can be sent depending on the type of error. The text message can even be sent to different numbers.

Günther Maschinenbau chose Wago due to their experience with the CANopen network protocol. They settled on the Wago-I/O-System, which offers I/O modules in addition to a CANopen Fieldbus Coupler. In order to clearly identify all of the electrical components in the control cabinet, employees in the electrical shop use Wago labeling units. Andreas Jäckel explains an additional reason for choosing Wago: "As a mid-size company, we feel like we are in good hands and our concerns are taken seriously." At Wago, companies generally have direct access to a contact person. Haupenthal confirms, "Whenever we have questions, we always get an answer very quickly and a solution to our problem." Last, but not least, the increased use of Wago products means that Günther Maschinenbau was able to reduce the number of suppliers for their electrical components. ◀

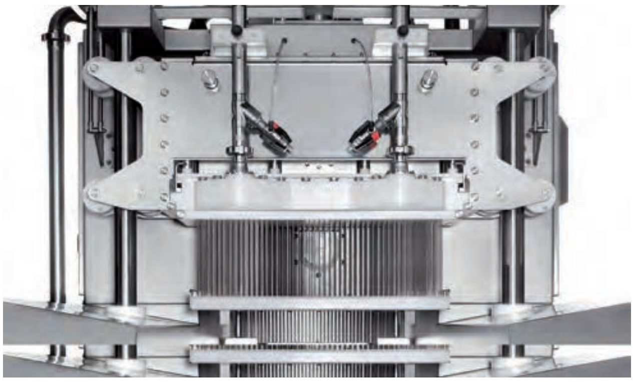


Figure 2: Up to 354 needles inject the brine into the meat (Source: Günther Maschinenbau GmbH)

Figure 3: A CANopen Fieldbus Coupler and various I/O modules from the Wago-I/O-System ensure communication with the sensors and actuators in the control cabinet (Source: Marc Fippel Fotografie/vor-ort-foto.de)

To the light tower

A tailor-made telematics CAN solution for mobile lighting towers combines different CAN components. With these, floodlights can be remote controlled and monitored via the Internet.

Company
Proemion GmbH
Donaustr. 14
DE-36043 Fulda
Tel.: +49-661-9490-600
Fax: +49-661-9490-666
info@proemion.com

Links
www.proemion.com

Proemion's telematics system for the remote control of mobile lighting systems increases the uptime of mobile lighting systems by minimizing the effort required for operating the units. The company developed the solution in conjunction with U.S. mobile floodlight manufacturer Allmand Bros. Inc. By interfacing Proemion's web portal into Allmand floodlight masts, control and monitoring of the floodlight systems can be performed from a virtual console located apart from the physical floodlights, giving users operating advantages and upside economics by minimizing downtime and emergency maintenance. The monitoring and controlling of the mobile floodlight system, which was demonstrated at the Bauma 2013 in Munich, was operated from the Proemion premises located in Fulda, 400 km away.

Allmand's Night-Lite PRO V-Series is often used under harsh conditions. The reliable function of these mobile light poles is critical to operating in difficult work environments typically found at public events, night construction sites, emergency operations, mining and industrial plants. Rarely is staff available that can take proper care of the floodlights and ensure their correct operation.

In a bid to ease operations, Allmand's project management approached Proemion to develop a new control system. The goal was to simplify as many basic functions, control measures and system monitoring as possible. Allmand came to Proemion with initial specifications of functional and non-functional requirements. The team of computer scientists and software specialists solved four tasks with the new control system that can be implemented in any location worldwide:

- Monitoring and reporting of the operating conditions of the mobile floodlighting engine, mast and fittings;
- Remote control of the functions of the motor, mast and lights;
- A web-based data connection to perform monitoring and control functions for three user groups: the operator, who often rents the units; the owner, Allmand's customer; and Allmand, the manufacturer;
- Data evaluation based on each user group's concerns.

On the hardware side, three components were combined into a CAN solution and integrated into the floodlight masts. The CAN-link UMTS 5302 transmits all operating and diagnostic data between the CAN network system and the server at high transmission rates, which are almost in real time.

The CANsense I/O unit monitors and controls the lights, mast and fittings. It is optimized for switching and digital power output queries in mobile applications. Thanks to this module not only are the lights controlled but also the hydraulic pump for the extension and retraction of the mast. In addition CANsense I/O also monitors the end position of the mast. Necessary interlocks, for example, turn off the hydraulic when the mast is fully extended. It also transmits the relevant data between the CAN network system of the monitored system and the server.

The CANsense ECU monitors and controls the diesel engine, the preheating time, operation of the control pedal, engine starts and stops as well as hours of operation, coolant temperature and oil pressure. The server collects all data sent via a web portal making maps and statistics functioning available.

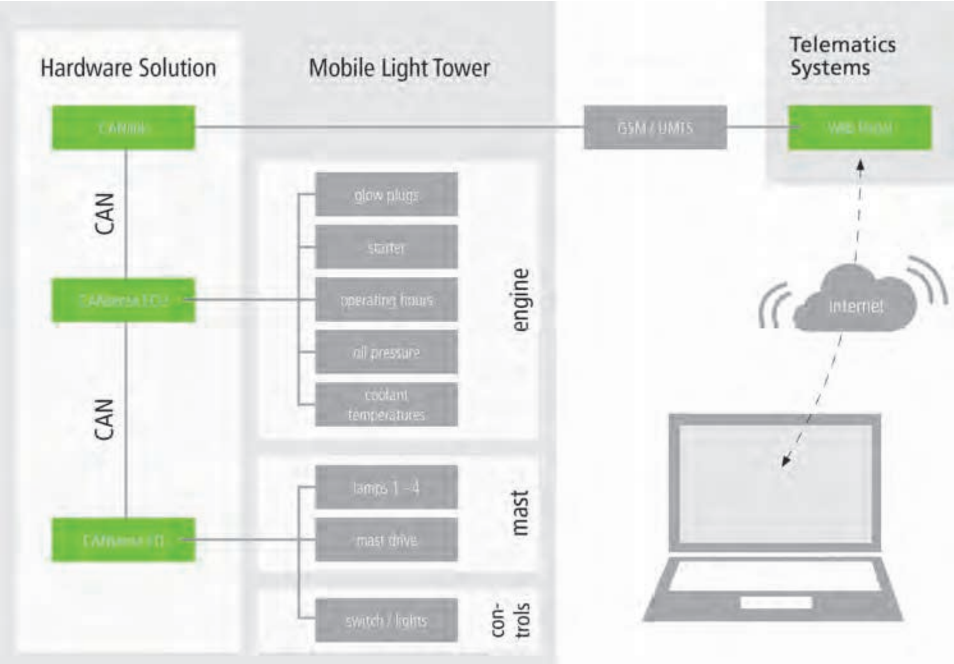


Figure 1: The system operator can retrieve the usage and maintenance information on the web portal and operate the system remotely; operation is equally possible via PC, laptop and smartphone

a web-based console operation, causing a significant reduction in operating expenses.

Thus, far greater functionality and efficiency have been achieved. For telematics specialists the light poles project is a prime example of a web-based remote monitoring and control system that can be transferred to other devices and equipment for other tasks and constraints. The core of the task was always the central operation and monitoring done simultaneously at widely dispersed and mobile work places. The web-based operation can account for all distance limits, while the web portal can be aligned to individual evaluation concerns. ◀

The web portal was created as a controller for the various user groups and programmed according to each user's requirements. A range of control functions, audit and alarms, notification, statistics and display functions are available.

Fuel gauge on smartphones

All transmitted CAN data are collected and treated on the company owned server. The Proemion web portal facilitates each user group in their monitoring and control of the floodlights according to their own business reasons. The users can access their associated data and controls from any PC, laptop or smartphone from anywhere.

The operator, who is often the lessee of the system, can control one or several light poles via their user interface on the web portal.

They can check the fuel level, start the engine, extend the mast, turn the lights on or turn off in a few seconds.

They can check the coolant temperature and oil pressure, the operating time of the engine and bulbs, or turn off lights individually. These routine operations, grouping of multiple systems, and common control functions are possible remotely.

The owner can monitor their entire fleet of systems, and especially note the operating time of the motors and lights to ensure compliance with contractual agreements.

Operations such as fuel level checks, engine starts, mast extends and light turn offs are done in a few seconds, even with several mobile floodlights. The system triggers an alarm or notification at low levels or approaching inspection dates to perform maintenance in a targeted manner, and it is even possible to track the device location - in case of theft a helpful aid. The manufacturer has access to important statistical evaluations. They can view the history of their products, which may include all maintenance data that can be used to improve manufacturing or determine improper use. The project management predicts future time-saving benefits for the operator through saving them long walks and working hours and allowing an arbitrarily positioned control center machine control:

"Some other smart features that we have planned as an option and add-on to protect all parties from harm and inconvenience are:

Light sensors that automatically turn off when daylight increases, which saves fuel, bulbs and wear; movement and wind sensors that cause the automatic retraction of the telescopic mast to prevent damage during strong-winds; and programming of specific functions for defined periods of time. "

Proemion has extended the operating concept of the floodlight equipment to

Figure 2: Light towers are often used under harsh conditions (Source: Allmand)


ifm electronic
Visit us at
HannoverMesse 2014
▶ hall 9 · stand D36
Look what we have for you!
Faster 32-bit-SafetyController for mobile machines.
TÜV certified safety controller to EN 13849 Pl d and EN 62061 SIL cl2, multifunctional inputs and outputs,
CAN interfaces with CANopen, CANsafety and SAE J 1939 protocols.
www.ifm.com/gb/32bit

The physical layer in the CAN FD world

With CAN FD data-rates can be raised up to 2 Mbit/s in multi-drop networks and up to 5 Mbit/s in point-to-point communication. Let's take a look at the impact that this development has on the physical layer.

Author

Magnus-Maria Hell
Infineon Technologies
Am Campeon 1-12
DE-85579 Neubiberg

Links
www.infineon.com

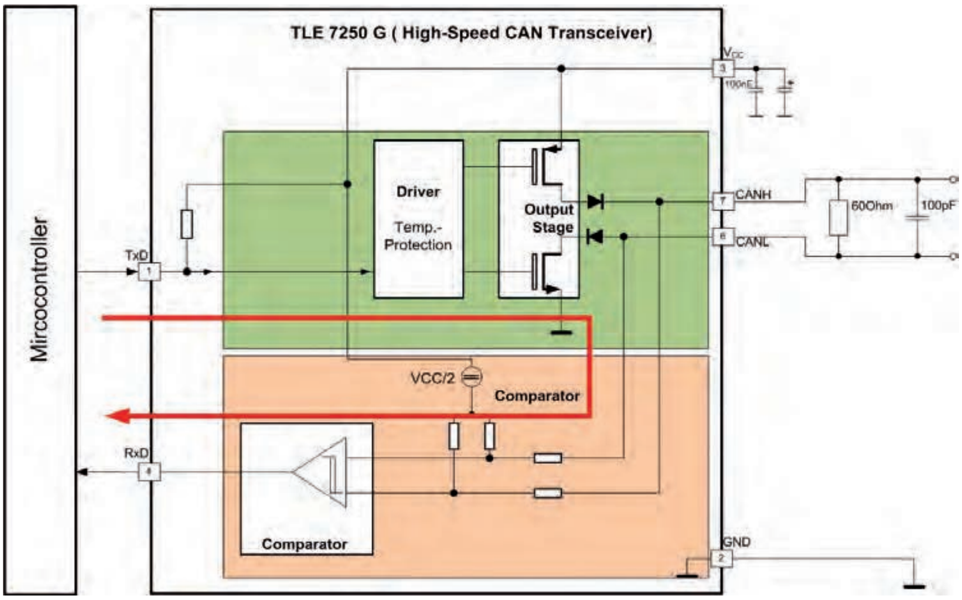


Figure 1: TxD-to-RxD transceiver propagation delay specification

In automotive applications CAN bit-rates of 125 kbit/s, 250 kbit/s, and 500 kbit/s are well approved. In the industrial area lower bit-rates down to 50 kbit/s and higher bit-rates up to 1 Mbit/s have been used for years. The ISO standards 11898-2, -5, and -6 are relevant for the development of so-called CAN high-speed transceivers. With the CAN FD protocol, the data-rate can be increased in the data-phase. At the moment, the automotive industry is discussing 2 Mbit/s in multi-drop networks and up to 5 Mbit/s in point-to-point communication. The impact on the physical layer, which includes the transceiver, the network, and the interface between microcontroller and transceiver, will be discussed in this article. In ISO 11898-2, -5, and -6, a lot of static parameters are specified, e.g. the recessive and the dominant voltage level. But for higher bit-rates dynamic parameters are even more important. The only dynamic parameter for the physical layer is the TxD-to-RxD propagation delay (loop-delay) with a maximum value of 280 ns in the current ISO 11898-2, and 255 ns in the current ISO 11898-5 standards. The ISO 11898-6 based on the ISO 11898-5 and the propagation delay specification is the same. This propagation delay is specified for the transceiver with a defined load, but in real applications ▷

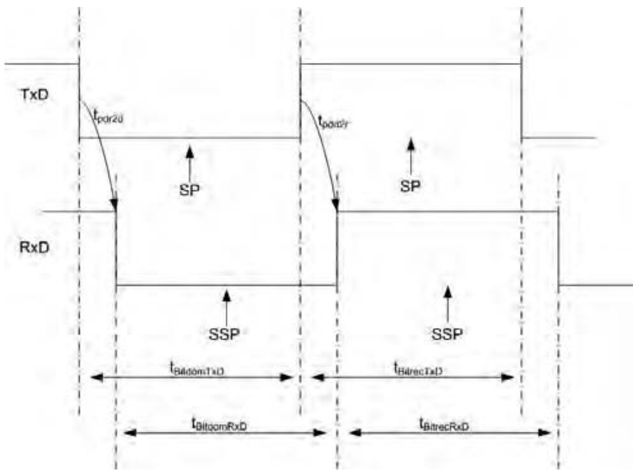


Figure 2: Transceiver with a perfect symmetric TxD-to-RxD propagation delay

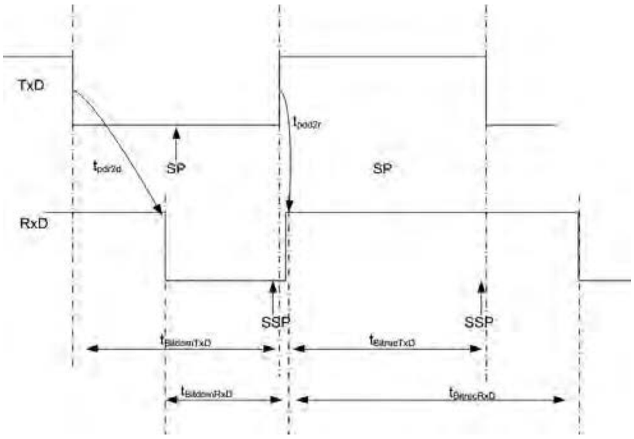


Figure 3: Transceiver with a very asymmetric TxD-to-RxD propagation delay

additional delays have to be taken into account, for example:

- Delay between micro-controller and transceiver;
- Delay of components improving the ESD and EMC robustness;
- Ringing, especially at the end of the dominant to recessive edge.

The TxD-to-RxD loop-delay is valid for the recessive-to-dominant transition and for the dominant-to-recessive transition.

The parameter is specified for a busload of 60 Ω and 100 pF. The disadvantage of this specification is that it allows a very asymmetric propagation delay for both transitions. This can shorten or expand the bit length of the recessive or dominant bits and limits the maximum possible bit-rate in the data phase of the CAN FD telegrams.

Propagation delay symmetry

Figure 2 shows a very symmetric TxD-to-RxD propagation delay performance. The RxD bit-time of the dominant bits is the same as the bit-time of the TxD bits. In Figure 3 a very asymmetric behavior is shown. The dominant bit of RxD is extremely shortened and the recessive bit of RxD is expanded. Such an extreme asymmetry limits the minimum possible bit-time and the maximum possible bit-rate. To optimize the transceiver behavior for CAN FD applications, the propagation delay symmetry needs to be specified. During analyses of several CAN transceivers on the market, we found out that the number of dominant bits in a row has an impact on the transceiver's behavior.

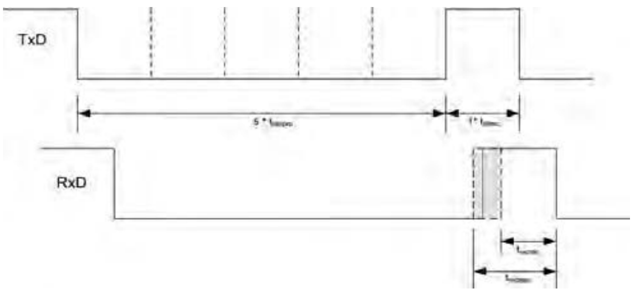


Figure 4: Propagation delay specification for CAN FD transceivers

To cover this observation in the specification, the bit-time of the recessive bit after five dominant bits in a row needs to be specified. Normally, lower bit-rates have no impact on this performance. This specification can be used for lower bit-rates, too. Two different bit-rates for the data-phase are in discussion at the moment: 2 Mbit/s for communication in complex networks and 5 Mbit/s for point-to-point communication. For higher bit-rates, a higher precision is needed. That is the reason why different limits are possible for 2 Mbit/s and for 5 Mbit/s. To cover this specification with one kind of transceiver the temperature range and the 5-V supply (V_{CC}) range are tailored.

The advantage of this proposal is that it can be used for lower bit-rates, too. This parameter shows that for all lower bit-rates the recessive bits will be shortened by up to 100 ns and can be expand by up to 50 ns. These values can now be used for the network design and the sample-point calculation in the arbitration-phase.

Another reason for asymmetric delay is the physical behavior of the network itself. CAN transceivers have open-drain output stages (see Figure 1) and no push-pull power stages like, for example, Flexray transceivers. This open-drain concept allows controlling the dominant level on the bus only and the recessive-to-dominant slew-rate to optimize the emission. For the dominant-to-recessive transition the maximum slew-rate will be controlled by the output stages, but the minimum possible slew-rate is dominated by the bus. In case of a high capacitive load, resulting from a high number of nodes and/or of additional external ESD or EMC components, the dominant-to-recessive transition time can be increased and reduces the bit-time of a recessive bit. Figure 5 shows the impact of two different capacitive loads. In the upper part of Figure 5, the bus differential voltage behavior with a capacitive load of 220 pF is shown and on the bottom the same curve is shown for a capacitive load of 1,5 nF. Both edges have a smaller slew-rate, but the dominant bit is expanded. The length of the dominant bit-time depends on the threshold levels of the receiver like Figure 6 implies. A receiver with a high threshold (900 mV) detects a smaller dominant bit-time as a receiver with the minimum possible threshold.

Further reasons for variation

Further reason for the asymmetry of the propagation delay is the temperature. Depending on the technology and the driver concept, the temperature coefficient can be positive or negative. Another reason for the variation of the asymmetry is the dominant differential voltage (V_{CAN_H}-V_{CAN_L}) level. If the dominant voltage level is high, for example close to the maximum level of 3 V, the switch-off time becomes longer, until the differential voltage level is below the minimum receiver threshold level of 500 mV. The dominant differential voltage level depends on the fabrication variation of the Ron of CAN_H and CAN_L, the temperature, and the ▷

Table 1: Specification for the TxD-to-RxD propagation delay symmetry

Recessive bit time	t_{recmin}	t_{recmax}
2 Mbit/sec 4,75 V< V_{CC} <5.25 V -40 °C ≤ T_j ≤ 150 °C	400 ns	550 ns
5 Mbit/sec 4,85 V< V_{CC} <5.15 V -40 °C ≤ T_j ≤ 105 °C	120 ns	220 ns

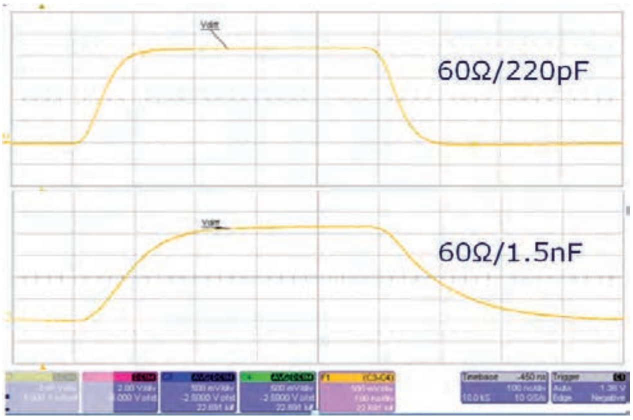


Figure 5: The impact of different capacitive load on the dominant bit-time

5-V power supply variation. For higher bit-rates the V_{CC} range and the temperature range are tightened to achieve a stable communication for higher bit-rates, too.

TxD output driver of the micro-controller and the slew-rate symmetry of the transceiver RxD output driver also has an impact on the symmetry. The capacitive load on the board as well as the capacitive input load

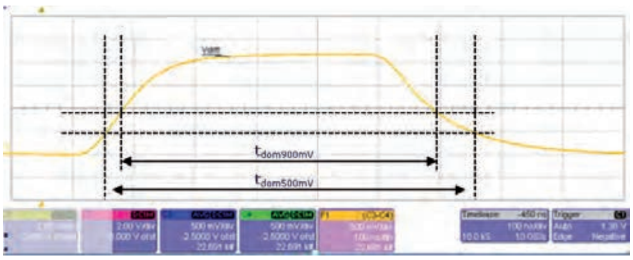


Figure 6: The maximum and minimum receiver threshold levels are marked

MCU-to-transceiver interface

The interface between micro-controller and transceiver can also be a reason for asymmetric delay. The slew-rate symmetry of the of the transceiver TxD input or the micro-controller RxD input can modify the symmetry. Especially, the input concept of the transceivers TxD input buffer like CMOS level input or TTL level input threshold can lead to additional asymmetry. The CMOS level input has less impact on the symmetry if the slew-rates of the output driver are perfectly matched. The asymmetry is dominated by the symmetry performance of the driver. If the transceiver TxD input has TTL input levels these thresholds add an additional asymmetry created by the thresholds itself.

Figure 7 shows an example with a very low input threshold and a very small hysteresis. The slew-rates of the driver are very symmetric, but the dominant bit-time is shortened by the TTL input stage. This asymmetry can be helpful, because it expands the recessive bit while normally the bus reduces the recessive bit-time. In point-to-point networks with a termination at both ends, this limits the bit-rate, too.

In Figure 8 the impact of asymmetric signals on the transceiver TxD input is shown. Asymmetric signals especially at high capacitive loads modify the bit-time of the recessive and dominant bits, as well. Therefore, the receiver and the micro-controller output drivers have to be symmetrical, especially for high capacitive loads.

In galvanically isolated applications with an optocoupler as interface between micro-controllers and transceiver, the propagation delay of the optocoupler has to be taken into account. Optocoupler have an open drain output stage. The high-to-low edge (recessive to dominant) is driven by the output transistor. The dominant-to-recessive edge depends on the external RC circuitry.

Furthermore a reason for asymmetry is the ringing at the dominant-to-recessive transition. As a reminder: this is the uncontrolled transition. Terminated wires and star topologies are not the reason for ringing at this transition. Additionally, this ringing shortens the recessive bit. The recessive-to-dominant transition is less critical, because the transceiver controls this transition with its output stages. If a ringing is present it is damped by the powerful output stages.

Sampling-point

Why is symmetry of the physical layer so important? The asymmetry of the physical layer reduces the possible range for the sampling-point. If we have a look at the latest possible sampling-point time then two different scenarios have to be checked. Scenario 1 is the maximum possible distance between two recessive to dominant edges, which can be synchronized again. That time is 10 bit-times. To calculate the latest possible sampling point the oscilla- ▷

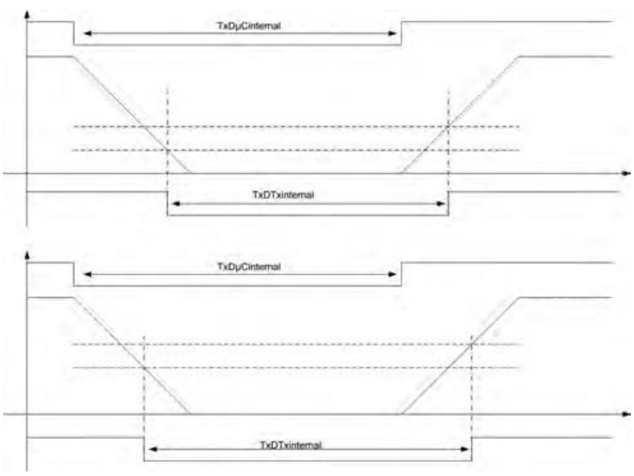


Figure 7: Comparison of TTL and CMOS transceiver TxD input concept

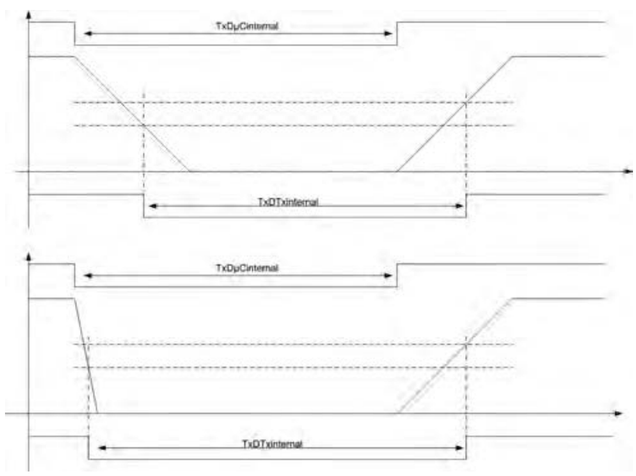


Figure 8: The impact of the transceiver internal bit-time depends on the slew rate

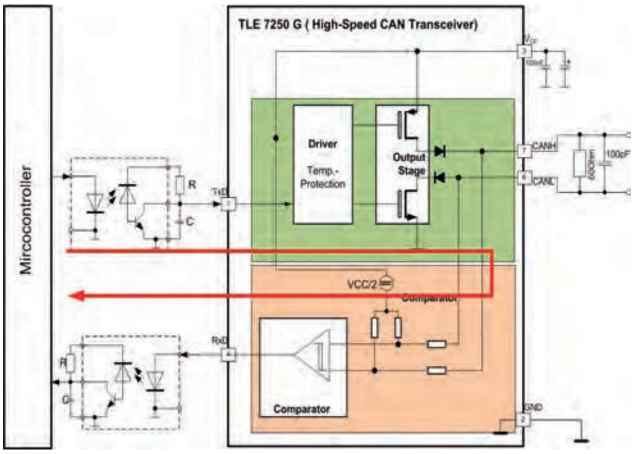


Figure 9: Optocoupler as an interface for isolation

tor tolerance of sender and receiver, the re-synchronization jump-width, and the asymmetry of the interface between micro-controller and transceiver have to be taken into account.

Scenario 2 is the 5-bit case with the maximum number of dominant bits in a row. In this scenario, the above-mentioned points have to be considered as well as the transceiver asymmetry (50 ns for 2 Mbit/s and 20 ns for 5 Mbit/s). For the earliest possible sampling-time, the recessive bit after five dominant bits is the most critical situation. In this scenario, the transceiver asymmetry (100 ns for 2 Mbit/s or 80 ns for 5 Mbit/s), the network ringing, and the bus-load have to be taken into account, besides the other points.

To get a successful and stable communication in a CAN FD network running at higher bit-rates (2 Mbit/s and more), special CAN FD transceivers should be used. Additionally, it is recommended to use a linear network topology with short stubs. The capacitive bus-load should be low as well as the capacitive loads on the ECU board. An intensive analysis of the sampling-point is necessary. The new parameter for transceivers will be helpful for classical CAN networks and for CAN FD networks. For classical CAN networks, these parameters help calculate the sampling-point more easily or more reliable. No values must be evaluated or estimated by the user, because they will be given in future datasheets. Standardization will start at the beginning of 2014. The ISO 11898-2, -5, and-6 parts will be harmonized and the new parameter will be added. Infineon will start the investigation on existing CAN transceivers and add this new parameter to the datasheets. ◀

Sending digital audio data via CAN

Authors

Ulrich Bschorer

Gabriele Cappelli

Mixed Mode
Lochhamer Schlag 17
DE-82166 Gräfelfing
Tel.: +49-89-89868-200
Fax: +49-89-89868-222
sales@mixed-mode.de

Links
www.mixed-mode.de

References

[1] Mahesh Mahajan, Monoj Baruah, Srinivas T., Suresh Sureddi: VoiceOverCAN. iCC 2003

[2] www.st.com (Discovery Evaluation Board)

[3] www.speex.org

[4] www.opus-codec.org

In mobile communication as well as the Internet, the digital transmission of speech and music has long been a standard. Audio codecs can also improve audio data transmission via CAN.

Audio codecs play a major role in ensuring efficient transmission rates by reducing the bit-rate of the audio signal. For that reason it is worthwhile assessing their usefulness in systems with low transmission capacities. Our goal was to find out how audio codecs can improve audio data transmission via the CAN network.

The main advantage of the CAN network is its real-time capacity, which qualifies the network in particular for time critical jobs. On the other hand, the transmission capacity of the CAN network is lower than that of e.g Ethernet. The CAN network is therefore widely used in industrial automation, aeronautics as well as in cars and rail vehicles. The CAN network can also be used for digital audio and speech transmission [1], but the quality of music data is poor unless transmitted over short distances. By using modern audio codecs, we tried to improve the transmission performance and lower the bit-rate. Our aim was to enable the CAN network to transmit audio data, in particular music data, over longer distances than previously possible. In the following, the capabilities of the CAN network using audio codecs will be demonstrated by means of a simple breadboarding and three test scenarios.

Our breadboarding consists of easy to get components. The STM32F4 Discovery Board (STMicroelectronics) has an integrated microphone and an audio output for headphones or loudspeakers. The CAN transceiver is realized by the microchip MCP2551. The workload of the CAN network was measured by a CAN adapter from Ixxat.

Figure 1 shows the schematic diagram for the breadboarding. Two STM32F4 Discovery Boards are connected to the CAN ▷

Table 1: Calculated workload on the CAN network dependent on the diverse audio codecs; the blue columns show the test scenarios dependent on the network length, the right columns the audio codecs sorted by descending required bit-rate

Test scenario	Bus length	PCM	G.711	G.726	SPEEX	OPUS
Voice unidirectional, 8 KHz, 8 Bit, mono	100 m	21,60 %	10,80 %	5,40 %	8,44 %	3,71 %
Voice full duplex, 8 KHz, 8 Bit, mono	100 m	43,20 %	21,60 %	10,80 %	16,87 %	7,42 %
Audio CD unidirectional, 44 KHz, 16 Bit, stereo	100 m	-	-	-	-	21,60 %
Voice unidirectional, 8 KHz, 8 Bit, mono	500 m	86,40 %	43,20 %	21,60 %	33,75 %	14,85 %
Voice full duplex, 8 KHz, 8 Bit, mono	500 m	-	86,40 %	43,20 %	67,50	29,70 %
Audio CD unidirectional, 44 KHz, 16 Bit, stereo	500 m	-	-	-	-	86,40 %

Table 2: The transmission capacity of the CAN network decreases as the distance increases

Bitrate (kbit/s)	Bus length (m)
1000	25
800	50
500	100
250	250
125	500
50	1000
20	2500

network. On the boards the test application digitizes the audio signal received by the microphone and sends it to the receiver on the remote board via CAN. The remote board plays the audio data via headphones. Using this construction we simulated a public address system and a communication system with two participants. On transmitting audio data the workload was measured using analysis software together with the CAN adapter. To assess the quality of the transmitted audio (music) signal we did tests by talking and listening to ourselves, but the incorruptible ears of colleagues, who were not involved with the project itself, but were attracted by the unexpected music sounds in the laboratory, were of paramount importance for testing the sound quality. If the audio system were ever used in public areas (e.g. a public address system used at railway stations, evacuation systems etc.), speech perception would of course be tested by Stipa standard specification (Speech Transmission Index for Public Address Systems [2]). Within the scope of our breadboarding, however, Stipa measurements would have been too much and were thus not made.

Practical experience shows that the use of microphones requires elimination of ambient noise as far as possible as there are sources of interference such as engines, fans and ventilators as well as other ambient loudspeakers. In case of full duplex communication, loudspeakers can cause acoustic feedback and recoupling. We could effectively eliminate disturbances caused by these sources using echo cancellation and noise reduction filters. In our breadboarding we eliminated acoustic feedback by dispensing with loudspeakers and using only headphones. If the audio (music) data is to be played by several loudspeakers connected to diverse consoles, the sounds may be reproduced with phase shift. When designing an audio system this eventuality should be kept in mind.

The following test scenarios are typical audio transmission use cases: voice streaming, bidirectional speech transmission and music streaming. We calculated the theoretically required bit-rate for the test scenarios and measured the workload of the CAN network in our laboratory.

The frequency bandwidth of human speech is small when compared to the bandwidth of music. To reduce the required bit-rate for speech transmission, only speech relevant frequencies are encoded. Thus voice streaming is one of the audio transmission use cases with the lowest bit-rate. A well-known example for voice streaming is public address systems at railway stations or on trains. In this use case, speech is unidirectionally transmitted, which means from the speaker to the listener only. Another example is a text-to-speech-system, e.g. reading texts from the computer screen to people with reduced eyesight. Unidirectional speech transmission requires one voice channel only, thus this kind of audio transmission is called half duplex transmission. ▷

The audio codecs

We used only public licensed audio codecs and moreover only lossy audio codecs because they have better compression rates with nearly constant quality.

Pulse code modulation (PCM): The uncompressed digital representation of an audio signal.

MP3: Known as a popular music format and available as public license library. Despite good compression capabilities, this codec is not qualified for our test scenarios, because the relatively long processing time leads to noticeable delay in communication.

G.711: Widely used in telephony. It lowers the bit-rate by confining the bandwidth of the voice (speech) signal. Only the frequencies from 80 Hz to 12 kHz are encoded because these are relevant for perceptibility of human speech. Codec G.711 is not designed for music signal transmission.

G.726: Also called Adaptive Differential Pulse Code Modulation (ADPCM), this codec was developed from G.711. It also uses only speech relevant frequencies. In addition, G.726 reaches double compression rates compared to G.711 by encoding only the difference between two scanning spots.

Speex: Purpose-made for voice signal compression. The compression technique is based on pattern recognition. As an example the long vowel "a" as in "land" is learnt as a new pattern and at the next occurrence, as soon as it is detected, it is anticipated as long as the voice signal does not change drastically. This means that the anticipated voice signal (here the long vowel "a") is described by the pattern specific parameters and replaces the real voice signal until a new speech pattern begins; in our example this is the sound "n". On decoding the compressed voice signal the onset of known voice patterns is used to generate a similar, but not completely identical voice signal. The pattern based generated voice signal is well suitable for speech transmission but it is not ideal for music transmission.
However, with some tolerable cut back expectations, Speex could theoretically also be applied for music transmission. Because of the especially low latency of Speex, this codec is widely used in telephony and voice over IT [3].

Opus: Partially based upon Speex and both suitable for voice (speech) and music compression. Therefore, this codec is qualified for all shown use cases. Opus also shows low latency and is used in telephony [4].

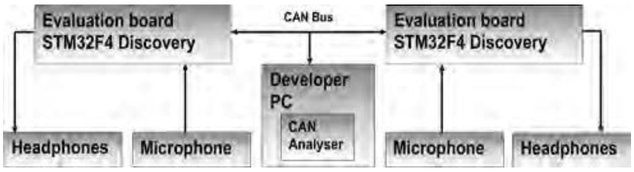


Figure 1: Two evaluation boards STM32F4 Discovery are connected to the CAN network together with the CAN analyzer; there is one headphone set and one microphone on every board

Bidirectional speech transmission (full duplex) uses two voice channels, which leads to a doubling of the required bit-rate. Voice over IP and telephony are well-known examples for full duplex transmission systems. In order to achieve fluent communication, latency between sending an audio signal and reception at the remote receiver should be as low as possible.

In contrast to the cited use cases above, audio transmission in CD quality is a very challenging task with respect to the required bit-rates. A piece of music can include all audible frequencies, which rules out the possibility of excluding certain frequency ranges from the audio signal. Thus high quality music transmission leads to much higher bit-rates compared to pure speech transmission. On the other hand the latency constraints need not be as strict as music playback delay will hardly be noticed.

Table 2 shows the possible bit-rates of the CAN network in kbit/s dependent on the network length in meter. Data is transferred by the CAN frame, which includes the identifier segment and the data field. The identifier segment contains information belonging to the application layer protocol. It is used to address the network participants and to code the message type. If the application layer protocol of an existing application is extended for audio transmission the available space

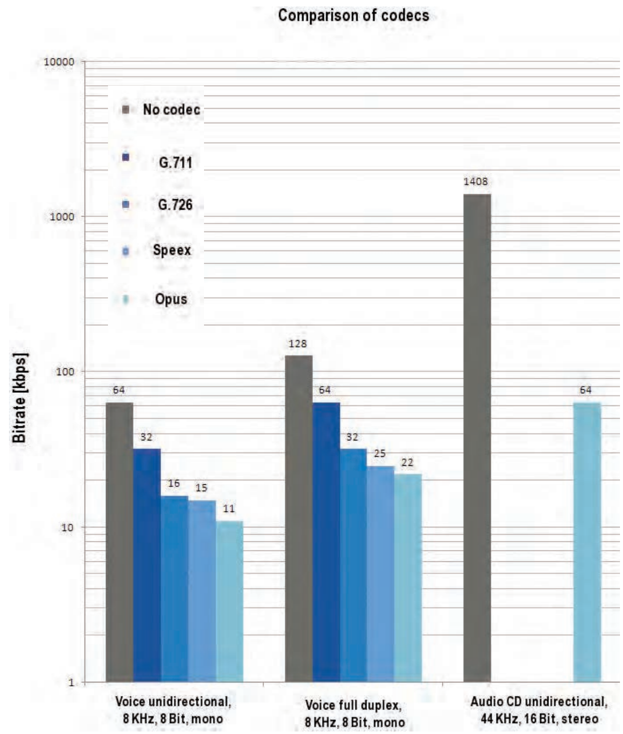


Figure 2: Comparison of the compression rate of the audio codecs assessed in our test scenarios: the x-axis displays the three test scenarios divided into groups, the logarithmic y-axis shows the required bitrate in kbit/s

in the identifier segment may become insufficient. In this case the protocol information is situated in the data field. As an example let us take a protocol overhead of 2 byte per CAN frame: In this case we could achieve 75 % of the maximum possible CAN performance shown in Table 1 for audio transmission.

The following formula calculates the bit-rate of an audio signal:

> bit-rate = number of channels (mono = 1, stereo = 2) * number of bytes of sampling depth * sampling rate * 8

An uncompressed voice stream in half duplex operation mode with a sampling depth of 8 kHz, 8 bit, mono thus needs 64 kbit/s. Bidirectional voice (speech) transmission in full duplex operation mode needs twice as much, i.e. 128 kbit/s. Music streaming with a sampling rate of 44 kHz, 16 bit, stereo requires 1408 kbit/s. Figure 3 shows the required bit-rates for codecs depending on the transmission use case.

Table 1 shows the calculated workload of the CAN network for the diverse audio codecs. The following test scenarios are displayed: voice streaming (voice, half duplex, 8 kHz, 8 bit, mono), bidirectional voice (speech) transmission (voice, full duplex, 8 kHz, 8 bit, mono) and music streaming (audio CD, half duplex, 44 kHz, 16 bit, stereo). These test scenarios are variegated with transmission lengths of 100 m and 500 m. The columns of Table 1 show the audio codecs listed downward according to required bit-rates. Empty cells signal that the corresponding test scenario exceeds the capabilities of the CAN network. Using codec Speex makes full duplex operation mode possible up to 500 m with 67,5 % workload on the CAN network. Codec Opus can even reduce the workload for voice (speech) transmission over 500 m to 29,7 % and for audio streaming in CD quality to 86,4 %.

Figure 2 compares the compression rates of the audio codecs for the three test scenarios. The logarithmic y-axis shows the bit-rate in kbit/s. On the x-axis the test scenarios are divided into groups. Without any codec the bit-rate is highest (PCM) and reduces with the increasing compression rates of the audio codecs. For the test scenario music streaming (audio CD, unidirectional, 44 kHz, 16 bit, stereo) only PCM and codec Opus are displayed, because all the other codecs that we assessed are not qualified for music transmission.

Our test scenarios show evidence for considerable enhancement of CAN network capabilities using audio codecs. Without any codec, bidirectional voice transmission is possible over 100 m at most. Using the codecs Speex and Opus, this limit could be extended fivefold up to 500 m. With respect to quality we were able to show that with codec Opus it is possible to enhance audio quality up to a CD-like level by at the same time keeping the required bit-rate on a comparatively low rate. This means that the CAN network is not operated at its limits for long terms which is similar to voice streaming without codec. Hence, it is possible to use the CAN network for voice streaming, bidirectional voice (speech) as well as music transmission when audio codecs are employed. By this method not only the transmission distance capacity of the CAN network can be considerably enhanced but also - as we deduced from the red-glowing but yet incorruptible test ears of our colleagues - the quality of music transmission can be drastically improved. ◀

Making networks more secure

Automobiles today feature a high level of interconnected technologies and they link personal data with vehicle functions. "Trust anchors" can help securing networks against unauthorized access and manipulation.

Author

Dirk Besenbruch
NXP Semiconductors
High Tech Campus 60
NL-5656 AG Eindhoven

Link
www.nxp.com

Almost 25 years have passed since the development and introduction of the CAN network in the automotive industry. During this time, the E/E architecture of a vehicle has been shaped by an increasing number of interconnected electronic control units (ECUs) that constantly exchange data during operation. The reliability of the network has been a key focus of the development of CAN from the outset. Further requirements for the network include high flexibility, the use of sound communication standards, and secured interoperability. This is particularly important in order to provide vehicle manufacturers with the opportunity to offer various series and alternative extras for a vehicle, as well as applying individual modules and ECUs in various platforms across different models (maximum reuse).

In addition to the CAN network, other network systems have also been developed in recent decades, which are used in modern vehicles. Depending on the area of application, these systems can offer advantages in terms of bandwidth and real-time capability. However, the primary requirements are reliability and high availability, with protection against potential manipulation barely considered during development.

Following the various stages of expansion (there can easily be up to 70 control units and processor modules used in a car), and the combined use of different network systems, we end up with a system architecture that is sub-divided into sub-network systems, which come together in a central ECU, a gateway. Figure 1 shows an example of a typical network topology.

Another trend that should be noted is the modern vehicle's provision of a range of interfaces that can connect external services and consumer devices, such as web services via WLAN or Bluetooth for the connection of cellular phones. Vehicle-related applications downloadable from the internet are also being developed or are already available, while telematics and emergency call modules provide additional external interfaces that connect to the in-vehicle network.

Until now, little focus has been placed on securing the vehicle network from unauthorized manipulation. Moreover, the measures outlined regarding compatibility and reliability also make the process of establishing and implementing an appropriate security architecture more complicated. As such, ▷

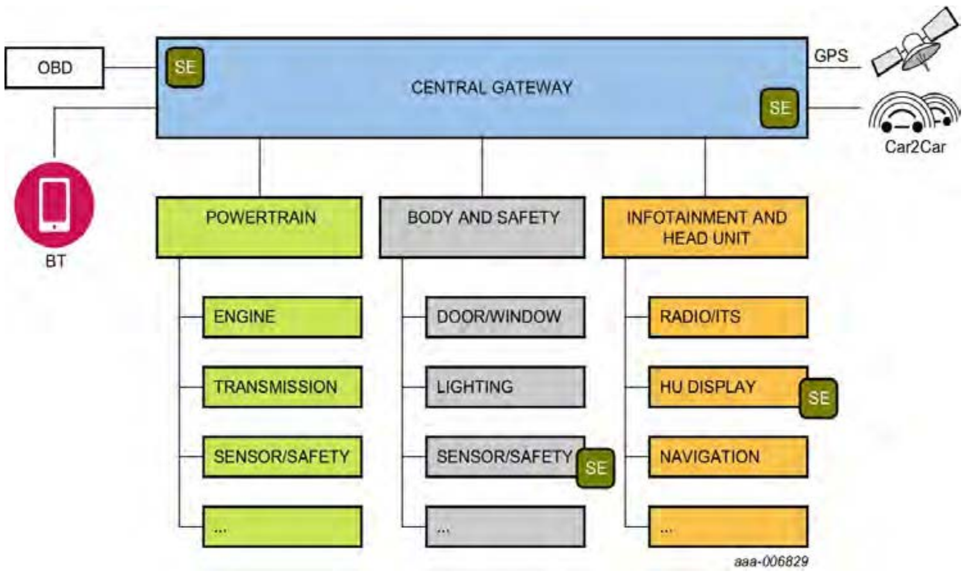


Figure 1: Example of a typical network topology

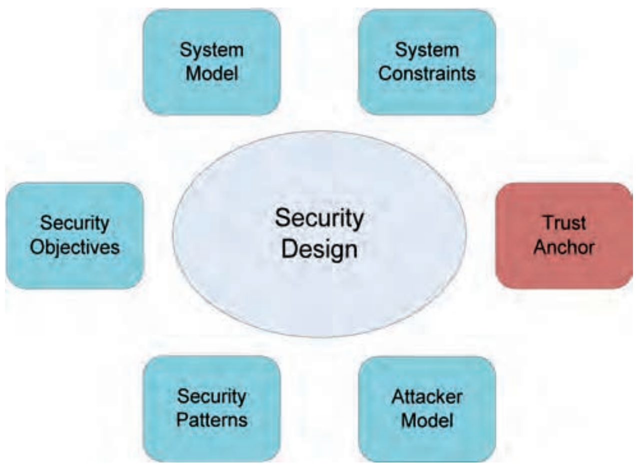


Figure 2: Security design aspects

integrating security into the architecture definition of the in-vehicle network should be carried out at an early stage of development.

Attack scenarios

In the last two years, a number of hacking attacks targeting the vulnerabilities of the networked architecture have been publicized. It was shown how certain functions within the vehicle can be enabled or disabled through external interfaces. For example, we learned about attacks and manipulations that modified the mileage and service entries in the vehicle, made use of TPMS modules for unauthorized geolocating of specific vehicles, installed Trojan horses in the infotainment system by means of infected CDs, listened to telephone conversations via Bluetooth, and caused chip tuning through the manipulation of electronic control unit software.

Some of the attack methods employed included:

- Eavesdropping: Listening in on internal vehicle communications in order to try to identify potential weaknesses in the system.
- Replay attacks: Interception of messages from the data bus in order to play these back at a later time, causing the ECUs to carry out the function in question.
- Man-in-the-middle attacks: Here, the original message is intercepted and modified before it is passed on.
- Modification of individual ECUs and changes to non-volatile memory: The ECU software is manipulated and reinstalled via the JTAG diagnosis interfaces.

In many cases, the OBD interface was used for cable-based physical access to the vehicle.

Increased system security and integrity

It seems obvious that we need to increase security against manipulation of the vehicle network to guarantee data integrity. Yet at the same time, we need to ensure that network reliability and performance will not be affected.

For instance, the use of encryption technology should not impair any safety-related system, such as the brakes or airbags. The flexibility that the various types of equipment in the vehicle provide should also not be compromised.

The right solution should be compatible with the existing architecture and systems. Current hardware platforms and software components should be modified as little as possible.

The idea: integration of a trust anchor

One possible way to secure existing and future systems is to integrate a secure memory area that can only ▷

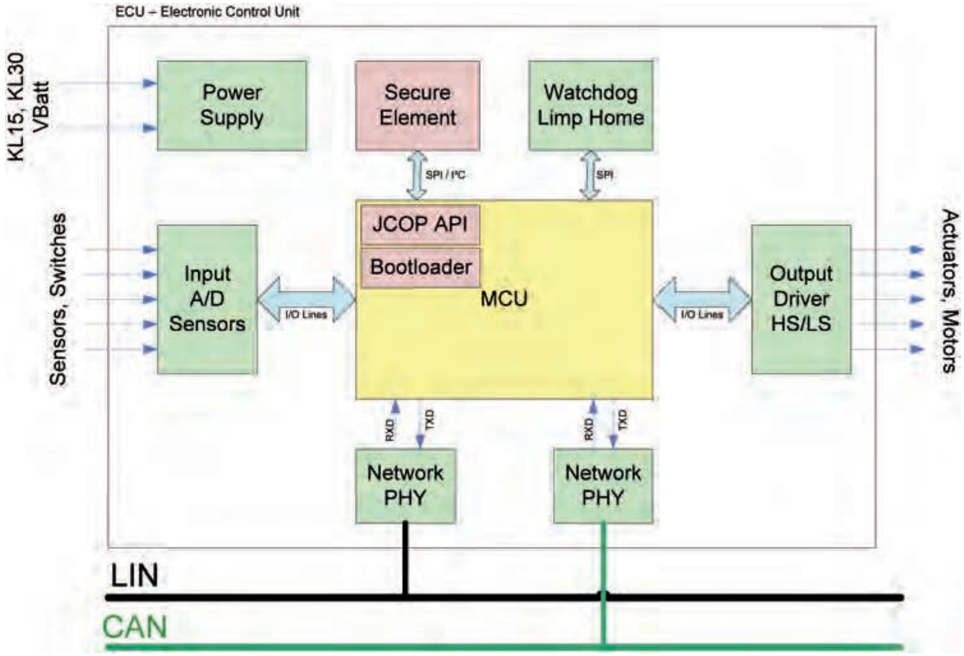


Figure 3: Secure element in ECU architecture

be written to and read with authorized access. By integrating a trustworthy element - a trust anchor - into security-related ECUs, the security of data can be improved. Trust anchors, in the form of a security microcontroller, appear in many security-related systems, including credit cards and telephone SIM cards. This additional microcontroller is considered in relation to other aspects within the entire system, as listed in Figure 2.

A trust anchor within the electronics of a vehicle

The trust anchor can be implemented by means of a secure element. A secure element consolidates security-related functions into a dedicated unit. A security processor can thus be provided for an ECU, supporting the following functionalities:

- A secure memory area that can only be read or written on by authorized parties within the system;
- Cryptographic co-processors for symmetric and asymmetric communication encryption;
- Management of certificates and private keys;
- Generation of public keys and checksums.

The NXP secure element, based on the A700x product group combined with an existing microcontroller, is suitable for the implementation of security-related features, including:

- Firewall applications for securing the gateway: for this purpose, communications can be authenticated before they are passed on to the relevant sub-network;
- Secure storage applications, such as error logs or mileages, which can only be written on by means of authentication;
- Secure boot; which ensures that the software of individual ECUs has not been compromised;
- Certification of (electronic) replacement parts: only authorized ECUs can be introduced into the vehicle network;
- Registration with external services through protected connections. The secure element provides the access data for VPN and HTTPS connections.

A700x – system integration

Within the automotive field, we deploy secure elements, for example, to protect data and access to the telematics module in NXP ATOP (Automotive Telematics On-Board Unit Platform). Another example of a standalone secure element in the automotive domain is the "payment key," using a credit card as the vehicle's key. This function requires a secure element certified in accordance with Common Criteria Level 5+. The A700x secure element is also currently being used successfully in many security-related applications outside of the automotive industry.

Secure element for securing an ECU

If the functions and applications that have to be protected against attacks from hackers are defined, then the corresponding ECUs that need to be equipped with a trust anchor in the form of a secure element can be identified in the network architecture. This can involve functions that should be protected locally, such as "saving," "calling," or "authenticating" data used by the ECU's main microcontroller, or securing a connection with additional ECUs.

A secure boot algorithm that prevents manipulation of the software should be implemented in all cases.

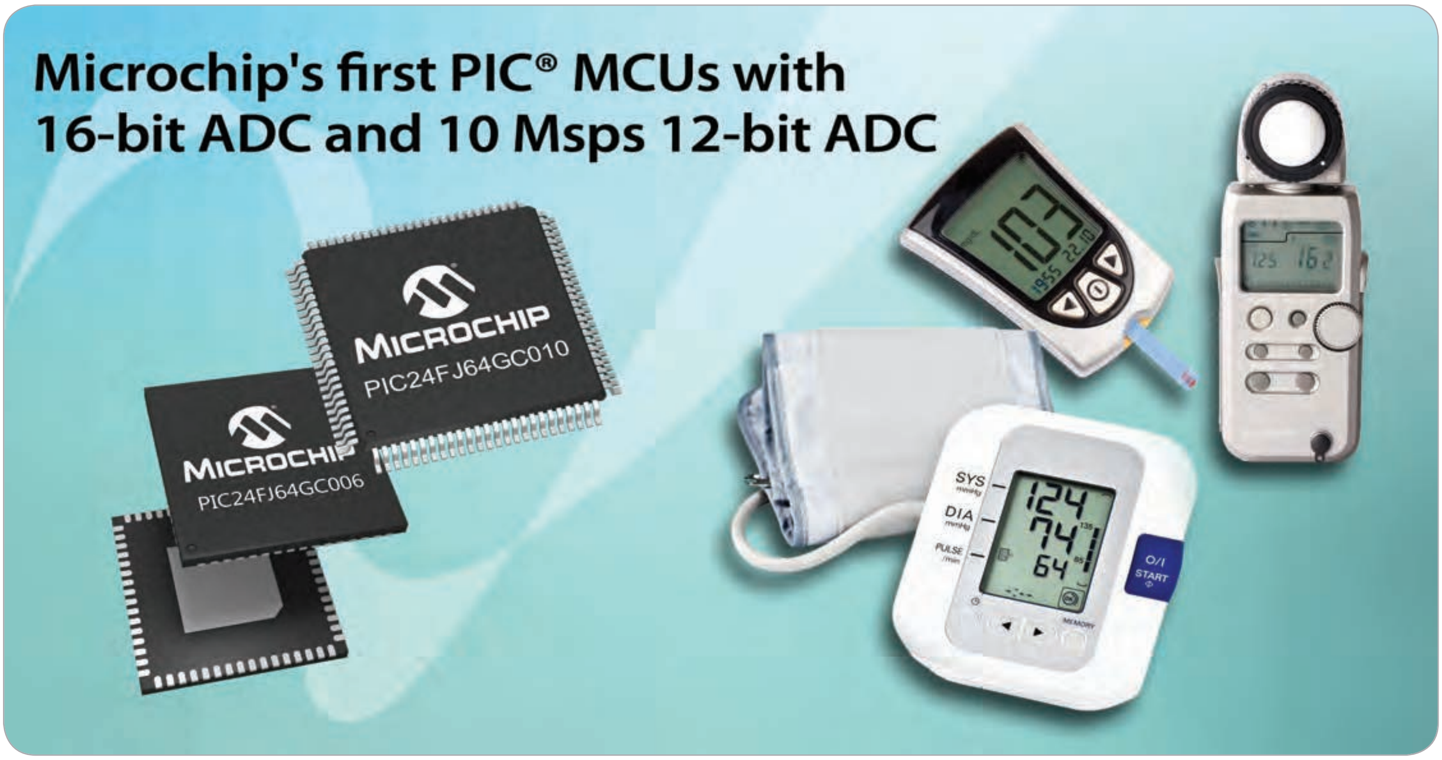
The secure element can be connected to the ECU's microcontroller via an SPI or I2C interface.

A non-volatile memory area of up to 80 KiB can be used to create independent applications, and securely store certificates and private keys. Application-dependent security functions can be implemented and executed on the embedded 80C51 core-based security CPU within the secure element. Some examples are the secure boot of the microcontroller, generation of public keys, session keys, or security certificates for the authentication of communications from the on-board network, and secure storage of microcontroller parameters and calculations or information from the on-board network, e.g. secure tachograph data or special parameters.

In addition to the programmable security CPU inside the secure element, cryptographic co-processors are also available to the user. A public key cryptography co-processor supports techniques including RSA (up to 2048 bit), Diffie-Hellman and elliptic curves with key lengths of up to 320 bit. For symmetric encryption with AES co-processors, the operating mode Electronic Cypher Codebook (ECB) is supported for data packets of up to 128 bit, while Cypher Block Chaining (CBC) is supported for larger data quantities. To form hash sums and thus examine memory areas for manipulation, co-processors are available for SHA1, SHA224, and SHA256, as well as SEED algorithms and MD5. A certified genuine random number generator (TRNG), which complies with AIS-31, has also been included. ▷

Looking to speed your analog development time?

PIC® MCUs with Intelligent Analog make designs easier



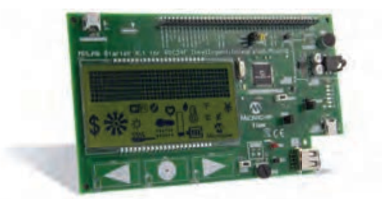
With a powerful combination of rich analog integration and low power consumption, the PIC24FJ128GC010 family enables a significant cost reduction over a multi-chip design as well as enabling lower noise, faster throughput, smaller PCB size and a faster time to market.

In addition to Microchip's first 16-bit ADC and a 10 Msps 12-bit ADC, the PIC24FJ128GC010 integrates a DAC and dual op amps to simplify precision analog design. The on-chip LCD driver provides the ability to drive displays with up to 472 segments for information-rich user displays; whilst mTouch™ capacitive touch sensing adds advanced touch capabilities.

The PIC24FJ128GC010 family helps to reduce noise to deliver more consistent analog performance in a very small form factor. Simply add sensors to the low-cost starter kit for easy prototyping.

GET STARTED IN 3 EASY STEPS:

1. Begin with the low-cost PIC24F Starter Kit for Intelligent Analog (DM240015)
2. Add custom sensors to the clean analog header to create a prototype
3. Re-use and modify the demo code to speed development



PIC24F Starter Kit for Intelligent Analog (DM240015)

For more information, go to: www.microchip.com/get/euGC010

MICROCHIP

Microcontrollers • Digital Signal Controllers • Analog • Memory • Wireless

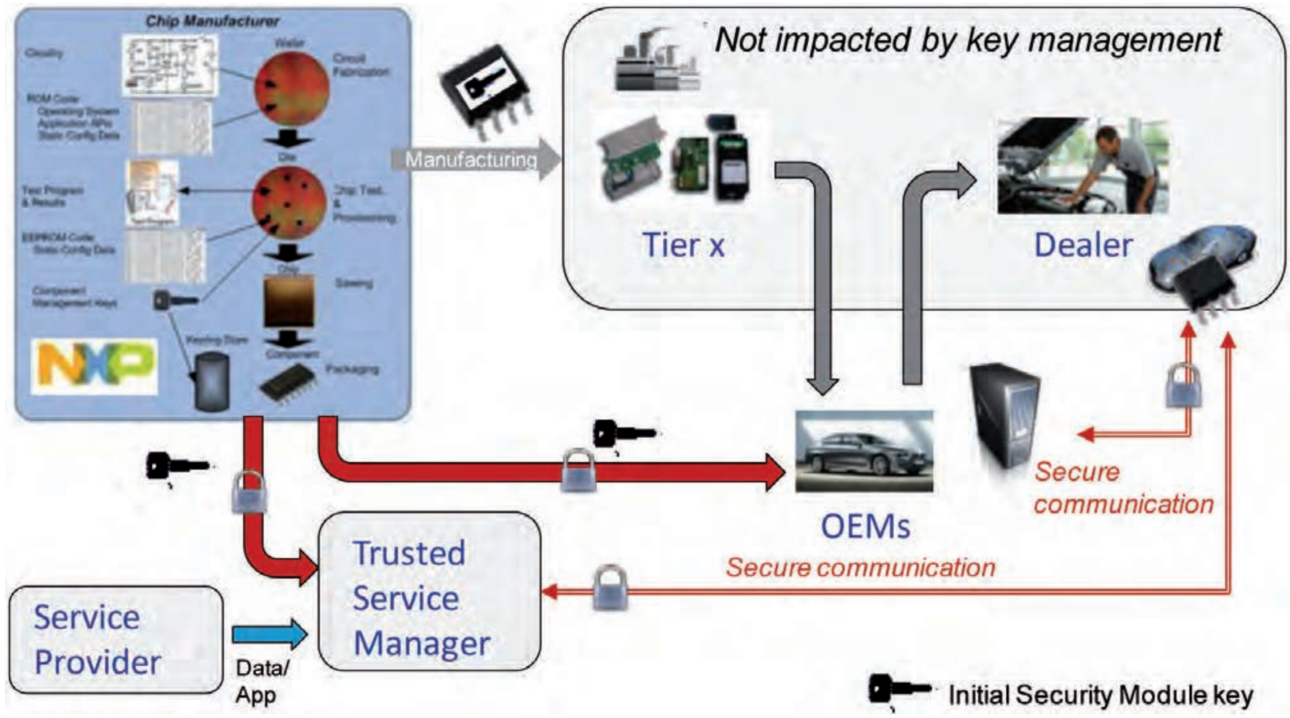


Figure 4: Trust provisioning schema

The hardware is protected against physical attacks at a high security level. Side-channel and reverse engineering attacks are prevented by means of effective countermeasures. It is possible to carry out certification based on Common Criteria or FIPS in the case of a closed system, such as a payment function.

JCOP operating system

The secure element contains an independent Java-based operating system that is compliant with Java Card and provides the user with routines and functions for using the cryptographic routines and co-processors.

The JCOP operating system manages the individual applications and provides an interface for controlling GPIO. The user can develop their own applications using a Java-enabled development environment (e.g. Eclipse), which are then written into secure memory. The user of the secure element has the option to develop their own customized applications, fulfilling an ECU-specific function. Examples of this include secure boot of external microcontrollers, enabling of protected ECU parameters, and secure data log management. If required, an application can generate temporary certificates and public keys. In this case, the required secret key is never accessible outside of the secure element, and thus not visible to hackers. The applications are launched externally by means of a corresponding call from the MCU. Another example of use includes the authentication of network communications by the secure element. Here the secret key for the hash- or checksum calculation also remains in the protected memory area; the calculations are performed within the secure element and are not visible externally.

JCOP operating system functions and application calls within the secure element are carried out by a host controller API (Application Programmer Interface) which is executed on the main microcontroller of the ECU. The API consists of two significant parts, the host driver itself and an authentication library. The host driver is called by the main program in the microcontroller and forms the interface to the application on the secure element. The authentication library is used to verify the identity of the host by the secure element.

Trust provisioning for production and delivery

Another aspect that should be taken into account when defining the system is the management and transfer of keys and secrets onto the installed ECUs during the module production. The vehicle manufacturer must specify which partners are to install the secure element in the value chain, who installs the keys in the ECUs, and how the allocation is managed at each step in the distribution chain.

Proven procedures from bank and credit card supply chains can be used here and adapted for use in automotive production. Figure 4 shows a procedure where the ECU is personalized by the vehicle manufacturer. Up to final assembly in the vehicle, module manufacturers (Tier 1) and semiconductor suppliers work with pre-agreed transport keys. These are also installed during the procurement of replacement parts. The transport keys are written to the memory area of the secure element in a secure production environment during semiconductor production. This ensures that the installed components can only be used by the dedicated module suppliers.

Once the module has been delivered by the Tier1 supplier, the vehicle manufacturer then verifies the transport keys using the application-specific data keys designed for the individual vehicle and synchronizes this data with its back-end database entry for the specific vehicle. A dedicated application can be pre-installed in the secure element (either by the Tier1 or Semi supplier), providing the connection data (for a VPN tunnel, for example) to the back-end system and thus enabling "end-to-end" encryption. This procedure ▷

could be used in the case of an exchange of the ECU in the field, for instance.

Summary

Securing electronic systems in the vehicle is becoming increasingly important. There are three main reasons for this:

1. The extensive interconnectedness of electronic control units within a vehicle means that they need to be secured against unauthorized changes in their functionality and against (often dangerous) manipulation.
2. A growing number of interfaces to (mobile) devices in the vehicle and connection to external services (app stores/internet) means that a security solution is needed.
3. Car-to-X communication and the use of emergency call modules (eCall) must be secured to protect personal data and safely prevent remote-controlled manipulation of the vehicle.

The resulting security demands can be resolved with the aid of a secure element. Guidelines relating to special systems, lifecycle and reliability should be taken into consideration. The secure element provides a "root of trust," a trustworthy place in the system. Securing the system against unauthorized manipulation should happen at an early stage of the definition and design process. In doing so, functional security must not be impaired. However, these requirements can be conflicting in practice.

In addition to its use in the network, a secure element can also be used to secure individual operations, such as manipulation-proof implementation of vehicle error logs or mileage and service data. In the case of eCall, telematics, and general back-end services, the secure element can be used as a trust anchor to create secure connections to the vehicle manufacturer's servers via a VPN tunnel or HTTPS. The secure saving of user-related data in telematics applications should also be enabled.

Outlook

Security against manipulation needs to be increased for vehicles. Vehicle manufacturers need to assess the security of their entire systems and also consider an examination of potential hacking scenarios and the data that needs to be protected.

The following will be important in the future:

- Flexible solutions that protect individual functions and entire systems;
- Standards by which a system can be classified as secure;
- Test scenarios that can be carried out across an entire system.

Ultimately, secure internal vehicle networks are a prerequisite for future car-to-X communication. ◀

The dragon awakes in the year of the horse

The number of CiA members headquartered in China is growing. The map shows the current Chinese CiA members (22) and briefly introduces their business activities.

Last year, the number of locally manufactured CANopen products increased. At the IAS exhibition in Shanghai, local brands (such as Delta, Estun, Kinco, and Softlink) presented industrial control equipment with CANopen connectivity. Leadshine exhibited its CANopen servo drives for the first time.

The main challenge is posed by system integration. Most of the European CANopen suppliers provide system design services. This leads to the strange situation that device makers employ more system engineers than their customers, which means that OEMs and machine builders are loosing their system design knowledge. That is going to change. In the past, Chinese money was invested mainly into treasury bonds. Now, the state-owned companies go on shopping tours in Europe and America, where they buy technology. As early as 2008, Zoomlion acquired Cifa, the Italian concrete pump maker. In the following years, other leading Chinese construction machine builders, XCMG and Sany, bought the German companies Schwing respectively Putzmeister, also technology-leaders in concrete pumps. This enables the Chinese company to offer complete infrastructure projects in emerging countries. But there is also an emerging trend to strengthen the system design business of European companies in China. For example, Schneider Electric, Lenze, and Festo increasingly provide CANopen solutions tailored for Chinese machine builders. The economy of China may slow down, but it is still one of the most growing industries in the world. In ▷

CSR Nanjing Puzhen Rolling Stock
Member since 2008
The system designer of metros and light rail vehicles uses CANopen as an internal network in its products.
www.csrpz.com

Nanjing Kangni Electronic
Member since 2008
Their rail vehicle doors come optionally with CAN/CANopen connectivity.
www.kn-nanjing.com

Nanjing Lektec Engineering
Member since 2013
The company provides CAN-connectable GPS modules, inclinometers, and encoders.
www.lixuegps.com

Xi'an Advantech Software
Member since 2007
The enterprise has developed CANopen interfaces for several of its products. This includes a CiA-certified CANopen master board. www.advantech.com.cn

Xi'an Precise Measurement
Member since 2013
The company manufactures sensors including a CANopen-compliant inclinometer.
www.siliconmems.com

Guangzhou Zhiyuan
Member since 2009
Besides a broad range of CAN interface products, the company also offers CAN tools from bus-analyzer to CAN oscilloscope as well as CAN evaluation boards. www.zlg.cn

Jari Institute
Member since 2013
The state-owned institute establishes CAN and CANopen system integration and research services.
www.jari.cn

Taian Technology
Member since 2013
The company provides frequency inverters and other low-voltage gear-switch products.
www.taian-technology.com

China Leadshine Technology
Member since 2011
The servo motor company demonstrated its integrated CANopen motion controller at the end of 2013.
www.leisai.com

Kinco Electric Shenzhen
Member since 2008
The company develops and produces a broad range of CANopen automation device. This includes PLCs, HMIs, I/Os, and motion controllers.
www.kinco.cn

Sino Medical-Device Technology
Member since 2013
The enterprise developing healthcare equipment has developed different medical devices using embedded CAN networks. www.sinomdt.com

Softlink Automation System
Member since 2012
Besides a CANopen PLC family, the company also offers I/O modules with CANopen interfaces.
www.softlink.cn

2013, the growth was about 7,6 percent, and for 2014 the government predicts another 7,5 percent.

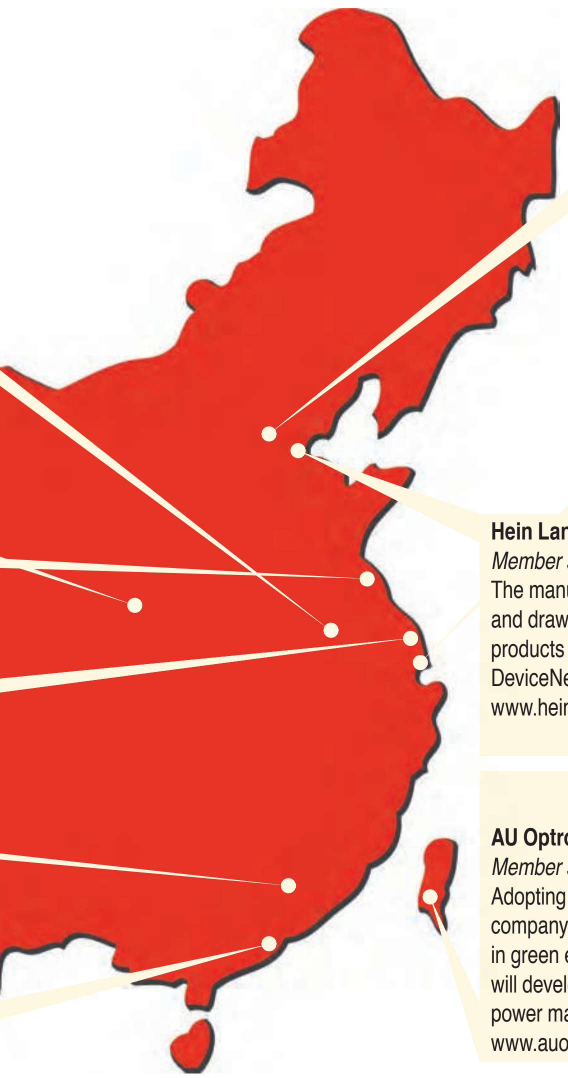
Many construction machines use embedded control systems based on CANopen. During the last years, this industry suffered a decrease in business, but the business in emerging countries is going to increase. Chinese companies such as Sany and Zoomlion seem to be prepared. They offer a very broad range of products including machines dedicated for the markets in Africa, South America, and Southeast Asia.

CANopen control systems designed for mobile machines come mainly from Europe, in particular from Germany and North Europe and CANopen sensors such as encoders and inclinometers are made in Europe.

Many Chinese OEMs use them in their machines. However, the first Chinese companies already offer CANopen products for mobile machines and wind power. System design services for these markets are not only offered by European companies: For many years, CiA member Pal-Fin (Shanghai) has successfully integrated CANopen systems for mobile machines using devices from different European suppliers. Also, the state-owned Jiangsu Automation Research Institute (JARI) has started to provide CANopen system integration services for the Chinese mobile machine industry. In other CANopen-committed industries, local heroes are emerging too. Sino MDT has launched a digital mammography system, developed and produced in Shenzhen. In the beginning the company developed injection/infusion devices. Today, the CiA member is competing against GE Healthcare, Philips Healthcare, and Siemens Healthcare. CANopen devices for this market are also available from Chinese brands, one of them CiA member Kinco. Another CANopen-minded market in China is maritime electronics. The first CANopen implementation in ships was not for fisher-boats. Network redundancy as specified in the CiA 302 series was one of the key elements in adapting CANopen for marine applications.

Chinese carmakers also use CAN-based in-vehicle networks. While the leading automotive suppliers develop most of the CAN-connectable ECUs abroad, nevertheless, the market for local ECU developers is increasing. High-end CAN interface boards for development and test purposes are still made in Europe or USA. Apparently, even if price matters, performance and quality is required nonetheless. That is why ESD, Kvaser, and others are successful in China.

The current 5-year plan has started an innovation offensive in machine building industries. The government plans on expanding the business, in particular in the state-of the-art markets, which is supported by governmental research projects. For local mass transportation such as metros and commuter trains, CANopen is one of the candidates to be accepted as coach network. CiA members CSR and Kangni are already using CANopen networks for this purpose. ◀



Beijing Itekon Technology
Member since 2013
The CAN interface products and gateways of this company provide CANopen and J1939 interfaces as well as CAN layer-2 ports.
www.itek.net.cn

Shanghai Pal-Fin
Member since 2007
The company provides system integration, especially for mobile machines.
www.pal-fin.com

Shanghai Gemple M & E
Member since 2009
The sensor maker provides CANopen encoders for different application fields.
www.gemple.cn

Sibotech Automation
Member since 2011
The gateway specialist offers CANopen and DeviceNet to Profibus-DP or Modbus products.
www.sibotech.net

Hein Lanz (Tianjin)
Member since 2013
The manufacturer of encoders and draw-wire sensors offers products with CANopen and DeviceNet connectivity.
www.heinlanz.com

Joint Peer Systec
Member since 2010
The company produces multi-axis servo controllers featuring optionally CANopen interfaces.
www.jps.com.tw

TD Hitech Energy
Member since 2013
Focused on batteries for LEVs, the company participates actively in the development of the CiA 454 specification.
www.htenergy.com.tw

AU Optronics
Member since 2014
Adopting “Benq Solar”, the company has started to invest in green energy. In the future, it will develop CAN-connectable power management systems.
www.auo.com

Chieftek Precision
Member since 2013
Following the trend of miniaturized linear motion controllers, the company will offer also products with CAN connectivity.
www.chieftek.com

Fatek Automation
Member since 2010
The PLC maker provides a CANopen interface board and a related CANopen development tool.
www.fatek.com

Optional structures in CANopen projects

CANopen systems with alternative devices can be designed and maintained with existing system tools and in compliance with standard process and file formats.

Author

Dr. Heikki Saha
TK Engineering
P.O. Box 810
FI-65101 Vaasa
Tel.: +358-6-35763-00
Fax: +358-6-35763-20
info@tke.fi

Links
www.tke.fi

References

Ever increasing requirements for control performance, dependability and serviceability have lead to an increasing use of digital communication instead of analog instrumentation. One of the most significant advantages of modern serial bus systems, such as CANopen, is a support for standardized system configuration management.The old analog systems do not support device identification and systematic configuration management, which has erroneously led people to consider such technology simple. However, device specific configuration principles and the lack of identification capabilities have introduced noticeable inefficiencies in assembly and service.

In addition to extremely dependable communication services [2] [10], CANopen provides standardized processes for managing system structures, storing device configurations [12], and linking development tools [13]. It has been proved that following the standard process and using appropriate tools can improve time-to-market and the resulting quality. Maintenance of the projects with current tools is not as efficient, because the tools do not support the use of alternative devices for each position of target systems.

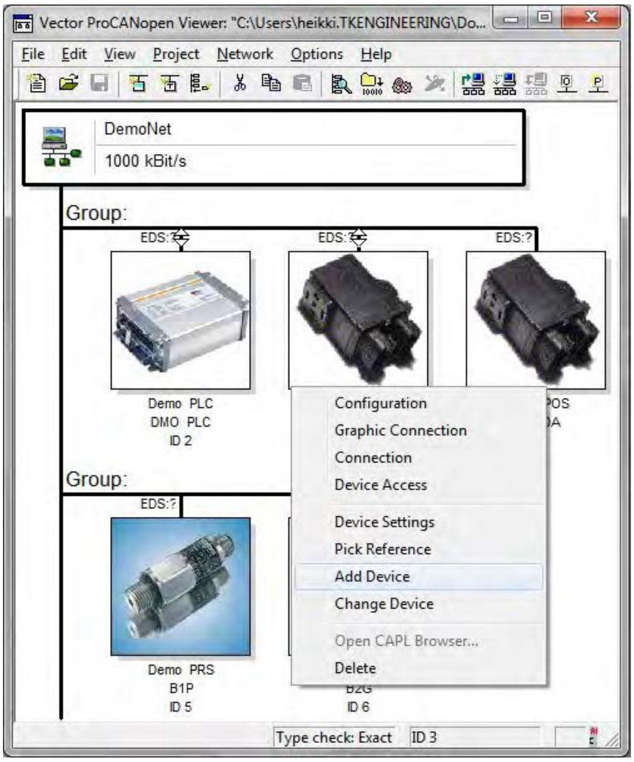


Figure 1: Original CANopen project

Typical use-cases

The most typical use-cases leading to a need for alternative devices can be divided into three groups. The most common use-case is the management of multiple, fully compatible devices, which are typically either second sources for primary ones or new models replacing the current ones. This use-case is very easy to realize by using devices following device profiles corresponding to the system functions. Additionally, using mainly the mandatory default part of the device profile specific interface by the control system minimizes possibility of compatibility problems [1]. As a result, only the device type, signal objects and parameter objects accessed by e.g. master controllers need to be equal in all alternative devices. If optional features are required by the application, it is required to determine the feature generally supported by the devices on the market. In case of application-programmable devices, e.g. PLCs, it is well known how to improve the efficiency of software development and maintenance by CANopen processes and tools [3] [4].

There may also be differences in the other disciplines having an effect on the control system's components. Different system models may use linear or rotary encoders or encoders with different measurement accuracies, depending on the mechanical structure of target system. Pressure levels may vary from system to system, which may ▷

lead into the use of multiple pressure ranges by pressure transmitters. Hydraulic valves in different systems may need specific hydraulic options, which are identified by their own product codes. Valves may also be used in different modes in the systems. When single coil valve drivers are used, each coil connector type needs a dedicated driver variant, also identified by unique product codes. The device model and version may be same, but different target systems may require e.g. different parameter values. Regardless of the reason, at least the device type, used signals and remotely accessible parameters must be equal in all alternative devices.

Also, the master device may need various configurations to fulfill all scalability requirements. The master device may either be an NMT-master functionality embedded as part of another device profile functionality or an application programmable device including NMT-master [1]. If there are options requiring different sets of devices in the system, corresponding configurations are needed for NMT-master. Due to the various membership and condition monitoring possibilities of CANopen systems [3] [4] [8], application specific parameters may need different configurations to adjust the monitoring services accordingly. Otherwise there may be unwanted exceptions caused e.g. by signals missing from devices, which do not belong to the current configuration.

Extending CANopen projects

A CANopen project consists of a DCF file of each device and a nodelist.cpj file listing the DCF files of the project [12] [13]. It is also assumed that there is a central device library, where EDS files of the library component are located after they have passed acceptance tests. In addition to the communication and device parameters, EDS and DCF files may contain device specific tool commands. An extension for alternative devices is based on the properties of EDS and DCF files and a CANopen system design tool. System design tool capabilities are extended by an external application program, which is called from the system tool and uses the standard interfaces to access the CANopen project. Listed use-cases can be covered by two functions, adding a new device and changing to another, already included device. An example project opened in an example system tool is shown in Figure 1.

When the user needs a new variant for a device, one can just call up the device specific tool command "Add Device". Figure 1 shows how it may be performed with an exemplary system tool for a negative direction valve driver. During the start, the extension application reads the system integration interface settings from the DCF file of the selected device. Then the tool searches all compatible devices in the device library and lists them for selection. The first criterion for the listed devices is the same device profile as the original device. Second, all signals which are mapped in the current project, must be supported as well as enough PDOs and PDO mapping entries. Third, all objects that are indicated as remotely accessible must be supported.

One may notice that if there are only signals which are defined as mandatory default by the corresponding device profile problems cannot occur when finding alternative devices. The same applies for remotely accessible parameters [1]. The tool uses DCF files of the projects and EDS files of the library components,

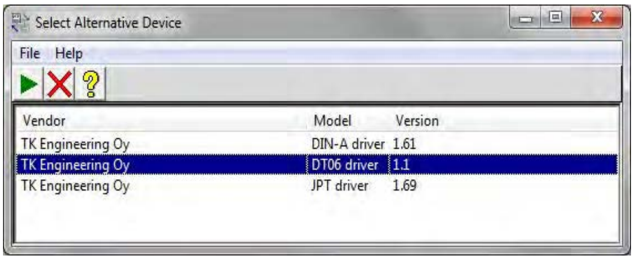


Figure 2: List of defined alternative devices for current position

but shows the vendor, device, and version information to users in order to enable them to concentrate on the system design, instead of technology specific details. A list of devices compatible with the example target position is shown in Figure 2 and an updated example project with a recently selected device variant in Figure 3. After getting the new device variant, the device parameters need to be adjusted accordingly, because only position specific communication settings are written automatically. The device parameters may be set or imported manually or with a device editor [11]. Signal object names of the new device must also be updated according to the system to ensure that correct names appear in the communication database (DBC).

Selecting another alternative device works similarly, but with the command "Change Device". Now the tool searches the current project of devices which have the same network-ID and node-ID. Of course the primary assumption is that the interfaces of the new devices were verified when they were added. There are some common minor deviations in the devices and this approach enables coping with those anomalies by enabling manual addition of such alternative devices. There is no sense in adding each device-specific strange compatibility issue into the search function.

Post-processing

The communication database (DBC) does not change, because there are no changes in the process signals and PDOs with any set of alternative devices. The system tool always includes all system positions into the communication database, regardless of the active product variant. This is because the variant is identified only by the NMT-master configuration, not by adding and removing devices. The emergency error code (EEC) collection may be performed for the whole project folder, which provides a uniform decoding function for the whole project, including all alternative devices [6]. The only additional constraint is that there must not exist overlapping error codes within any position. Transfer to assembly and production may also be performed for the whole project folder and thus it is as easy as usually to prepare the project for assembly and service [5].

The generation of IEC 61131-3 communication abstraction layer [3] with signal units and scaling [9] works as it did before. The export type is determined from the identity of the target PLC. Support for the corresponding output format shall be one approval criterion of a new PLC. Calls to the device editors are included in EDS and DCF files and they automatically follow the device changes [11]. The only prerequisite is that the calls must be inserted and verified as part of device acceptance tests.

Results and difficulties

The main purpose of any design tool is to increase the efficiency of the work and to let software perform repetitive routines. With a device library containing 90 EDS files, together over 9 MiB, the search for compatible devices takes approximately 25 s. It is impossible to get even a single file checked manually during that time. Furthermore, the manual check is prone to errors and it decreases productivity further by moving focus from important design decisions into raw file accesses.

Although the presented approach works well with all CANopen devices, some challenges were found in the device profiles. I/O-devices may be so flexible that there is a high probability for compatibility problems without thorough market research, especially with run-time adjustable parameters [14]. Pressure transmitters are well replaceable as long as only temperature signals are used, but it is impossible to distinguish between temperature and pressure transmitters without a detailed object dictionary analysis [15] [9]. Encoders are compatible from a device profile point of view, but automated compatibility checking is challenging due to e.g. the use of either single- or multi-sensor output objects [16]. Also, output objects of rotary and linear encoders are not fully compatible. The hydraulic drive profile itself is well defined, but variable type objects are used instead of array objects in some implementations, making automated compatibility checking challenging [17]. Inclinometers are easy to handle because major options are indicated by the device type [18].

The presented approach was successfully tested with an example system design tool. The approach can also be used with relatively old versions without problems. But, like many tools on the market, proprietary projects and node list files are used by the example tool. That ▷

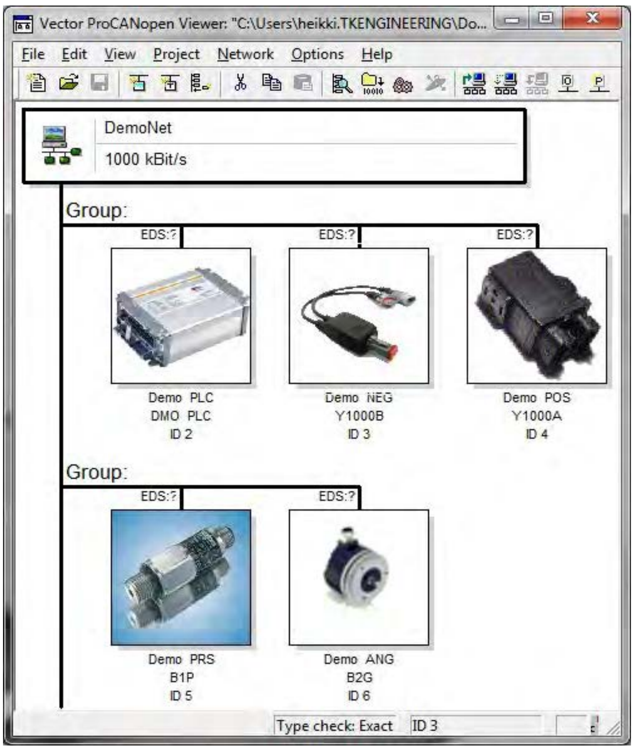


Figure 3: Example CANopen project after selection of an alternative device

anomaly was coped with by implementing some additional functions, with which an alternative device manager stores the required information to those proprietary files in addition to the DCF files and the standard nodelist.cpj file. The writes are conditional; if tool specific project files exist they are updated. It must be emphasized that tool specific files increased development effort, but not significantly.

Though the concept works fine, there are still some topics for future research and development. Measurement and control accuracies and response times are not included into EDS files, which may cause faulty selections. It should be investigated whether such information should be added into EDS and DCF files, or if a multi-disciplinary and machine-understandable datasheet or comparable concept would work better [7]. The main focus should be put on finding a standardized description principle, which in best case is already in use.

Another open issue is object naming. It is defined that application specific object names may be added to the "Denotation" attribute or simply overwrite the "Parameter Name" attribute [12]. From a generic tool point of view it is challenging to determine unambiguously which way should be used. "Denotation" could be missing, because it is not used or also because it has not been defined yet.

An approach to expanding the capabilities of CANopen projects was developed without need for changes in corresponding standards, tools and off-the-shelf devices. Such compatibility enables utilization of the whole CANopen ecosystem for both devices and system tools. A new compatible device can be found at least 100 times faster than manually, without considering the effect of human errors that typically happen in the manual search. The developed approach enables flexible editing of projects with current tools, improving management of various optional structures and alternative devices. The new approach is fully compatible with the earlier developed tools.

Standardized information storage formats enabled information management. Example system tools also use proprietary project files, but it was easy to cope with them because the information content was the same. There are also some devices on the market, which are more difficult to handle because the implementations slightly differ from the device profiles. One significant outcome is that the closer standards are followed, the easier it is to hide the underlying technology and present only the design task related information to the designer. Another important outcome was that information's content is much more important than file format. CANopen fulfills current requirements by providing not only dependable communication, but also dependable design information management, especially when compared with analog instrumentation. ◀

Inclinometer survey

This survey collects information about CANopen tilt sensors compliant to the CiA 410 profile. These products are available in many variations. The suppliers also provide application-specific versions not listed in the table.

CiA members develop standardized CANopen profiles, in order to improve the interoperability and exchangeability of devices. For inclinometers the CiA 410 profile has been available since 2000. This profile specification includes a default TPDO mapping for measured inclination. The publically available version specifies that in the first TPDO, the x-inclination and optionally the y-inclination are transmitted as Unsigned16 values (index 6010h resp. 6020h). For applications requiring higher resolutions, the second TPDO contains Unsigned32 values (index 6110h resp. 6120h) by default. CiA has tested the products from C.O.B.O. on CANopen conformity successfully.

Most of the launched products compliant with CiA 410 follow the defined TPDO default mapping correctly. But some customers request to transmit in these PDOs additional process data (e.g. temperature values). This is why some suppliers have preconfigured or preprogrammed the devices according to the customers' needs. However, they are not compliant with the currently released CiA 410 profile. In order to overcome this situation, the next CiA 410 version will introduce a dedicated bit, in the device type parameter (index 1000h) indicating that the device implements another TPDO mapping than the default one. The latest version of CiA 410 is 1.3.0, which was released in 2010.

> ***"Inclinometers enable sophisticated position control and can be used as an alternative to encoders.***
>
> ***Klaus Matzker (Fraba)***

Table 1 shows CiA 410 compatible tilt sensors. The listed products don't claim completeness. Most

Editors' note:
This survey is based on a questionnaire and Internet browsing. "Not known" means that the supplier did not respond to our questionnaire and we were not able to find this information on the manufacturers website. "Not supported" indicates that this TPDO is not available.

Manufacturer	Product name	Sensing technology	Number of axes
ASM	PTAM2	MEMS	1 or 2
	PTAM5	MEMS	1 or 2
	PTAM27	MEMS	1 or 2
Axiomatic	AX060250	MEMS	1 or 2
	AX060451	MEMS	1 or 2
Baumer	GNAMG.0215P32	not known	2
	GNAMG.0225P32	not known	2
	GNAMG.0235P32	not known	2
	GNAMG.0155P32	not known	1
	GNAMG.0215PA2	not known	2
	GNAMG.0225PA2	not known	2
	GNAMG.0235PA2	not known	2
	GNAMG.0155PA2	not known	1
C.O.B.O.	AMUB 2-Axis	Thick-film	2
	AMUB 0 to 360	Thick-film	1
DPF Sensors	TST20	MEMS	1 or 2
DIS Sensors	QG-series	MEMS	1 or 2
Gemac	IS1BP0 to 360-O-CL	MEMS	1
	IS2BP090-O-CL	MEMS	2
	IS1TK0 to 360-O-CL	MEMS	1
	IS2TK090-O-CL	MEMS	2
	IS1SP0 to 360-O-BL	MEMS	1
	IS2SP090-O-BL	MEMS	2
Intercontrol	4305.18.360	not known	1
	4305.18.0XX	not known	2
ifm	JN2100	MEMS	2
	JN2101	MEMS	2
Kuebler	IS60	MEMS	2
Pepperl + Fuchs	INX0 to 360D-F99-B16-V15	not known	1
Posital/Fraba	Tiltix ACS-080	MEMS	1 or 2
	Tiltix ACS-360	MEMS	1
	Tiltix AGS030	fluid-cell	2
Sensor Systems	DPS-CB	MEMS	1 or 2
Siko	IK360	MEMS	1 or 2
	IK360L	MEMS	1 or 2
TK Engineering	XY-CAN-E	MEMS	1 or 2
Turck	B2N10H-Q42-CNX2-2H1150	MEMS	2
	B2N45H-Q42-CNX2-2H1150	MEMS	2
	B2N60H-Q42-CNX2-2H1150	MEMS	2
	B1N360V-Q42-CNX2-2H1150	MEMS	1
TWK	NBN/C3	MEMS	2 or 3
Vigor Technology	SST20	MEMS	1 or 2
	SST300	MEMS	1 or 2

of them are rated IP67 and higher. Inclinometers are mainly used in mobile machinery. This includes construction machines as well as agriculture and forestry machines. Thousands of them are installed in cranes, working platforms, and concrete pumps, for example.

Inclinometers are used for leveling control, but also for measuring the angle of booms, and for height control of scissor working platforms. In some applications they substitute the classical rotational encoders. They are cheaper and in some cases easier to install. They are simply screwed, adjusted, and connected to the CANopen network. There is no need to fix an axis.

Another application field is sun-trackers in photovoltaic systems. The inclinometer provides via CANopen the angle values to the motor controller. Without an absolute measuring device there is no assurance the solar panel is pointing in the right direction. The software algorithm tells one where to point; the inclinometer ensures of actually pointing there.

Depending on the application, the requested bit-rate is different. Most of the inclinometers support different data-rates as specified in CiA 301 (CANopen application layer). In some cases, additional transmission speeds are provided. The bus access is very often released by means of a 5-pin M12 connector. Of course, measuring range and resolution depends highly on the application. Therefore, some suppliers offer a broad range of variants, in order to serve different requirements.

The inclinometer uses different sensing technologies. Historically, the fluid cell appeared first. Its benefits are high accuracy and high resolutions, if temperature impacts are compensated. Nowadays, the sensor makers prefer MEMS (micro electro-mechanical system). They are cheaper and they measure faster. Additionally, they allow a larger inclination range up to 360°. Sensor elements based on thick-film, so-called heat convection inclinometers, are also in use.

Because some applications require a safe communication for inclinations, the first sensors support the CANopen Safety protocol as specified in EN 50325-5 (before CiA 304). Of course, the controller consuming the inclination value needs to support this protocol, too. TWK was the first supplier developing a safety inclinometer (NBN/S3). This 3-dimensional sensor safely transmits the inclination values by means of SRDOs (safety-related data objects). The next version of the CiA 410 profile will also include the necessary additions for safety-related tilt sensors, e.g. the communication and mapping parameters for SRDOs. ◀

Measurement range [°]	Resolution [°]	TPDO 1 mapping (index of process data)	TPDO 2 mapping (index of process data)	IP rate	Temperature range [°C]	CAN connector(s)	CiA 410 version	CAN bit-rates [kbit/s]
±60 or ±180	0,05	not known	not known	IP67/IP69K	-40 to +85	M12	1.2.0	50, 125, 250, 500, 1000
±60 or ±180	0,05	not known	not known	IP67/IP69K	-40 to +85	M12	1.2.0	50, 125, 250, 500, 1000
±180	0,1	not known	not known	IP67	-40 to +85	M12	1.2.0	50, 125, 250, 500, 1000
±80, 0 to 360	0,05	6010h + 6020h	6110h + 6120h	IP67	-40 to +85	2 x M12	1.2.0	10, 20, 50, 125, 250, 500, 800, 1000
±80, 0 to 360	0,05	6010h + 6020h	6110h + 6120h	IP67	-40 to +85	DT15-4P	1.2.0	10, 20, 50, 125, 250, 500, 800, 1000
±15	0,001 to 1	not known	not known	IP66	-25 to +85	cable gland	not known	not known
±30	0,001 to 1	not known	not known	IP66	-25 to +85	cable gland	not known	not known
±60	0,001 to 1	not known	not known	IP66	-25 to +85	cable gland	not known	not known
0 to 360	0,001 to 1	not known	not known	IP66	-25 to +85	cable gland	not known	not known
±15	0,001 to 1	not known	not known	IP66	-25 to +85	M12	not known	not known
±30	0,001 to 1	not known	not known	IP66	-25 to +85	M12	not known	not known
±60	0,001 to 1	not known	not known	IP66	-25 to +85	M12	not known	not known
0 to 360	0,001 to 1	not known	not known	IP66	-25 to +85	M12	not known	not known
±60	0,1	6010h + 6020h	not supported	IP67	-40 to +80	M12	1.3.0	50, 125, 250, 500, 1000
±180	0,1	6010h	not supported	IP67	-40 to +80	M12	1.3.0	50, 125, 250, 500, 1000
±5, ±10, ±15, ±30, ±45, ±60, ±90, or 0 to 360	0,005 or 0,002	not known	not known	IP69K	-40 to +85	M12	not known	up to 1000
±30, ±90, or 0 to 360	0,01	not known	not known	IP67, or IP67/IP68	-40 to +85	M12, 2 x M12, or cable gland	not known	125, 250, 500, 1000
±0 to 360	0,01	6010h	not supported	IP65/IP67	-40 to +80	2 x M12	1.2.9	10, 20, 50, 62,5, 100, 125, 250, 500, 800, 1000
±90	0,01	6010h + 6020h	not supported	IP65/IP67	-40 to +80	2 x M12	1.2.9	10, 20, 50, 62,5, 100, 125, 250, 500, 800, 1000
±0 to 360	0,01	6010h	not supported	IP65/IP67	-40 to +80	2 x M12	1.2.9	10, 20, 50, 62,5, 100, 125, 250, 500, 800, 1000
±90	0,01	6010h + 6020h	not supported	IP65/IP67	-40 to +80	2 x M12	1.2.9	10, 20, 50, 62,5, 100, 125, 250, 500, 800, 1000
±0 to 360	0,01	6010h	not supported	IP65/IP67	-40 to +80	M8	1.2.9	10, 20, 50, 62,5, 100, 125, 250, 500, 800, 1000
±90	0,01	6010h + 6020h	not supported	IP65/IP67	-40 to +80	M8	1.2.9	10, 20, 50, 62,5, 100, 125, 250, 500, 800, 1000
0 to 360	not known	not known	not known	IP67	-40 to +80	2 x M12	not known	20, 50, 62,5, 100, 125, 250, 500, 800, 1000
±20, ±45, or ±60	not known	not known	not known	IP67	-40 to +80	2 x M12	not known	20, 50, 62,5, 100, 125, 250, 500, 800, 1000
±180	0,05	6010h + 6020h	6110h + 6120h	IP69K	-40 to +80	2 x M12	1.0.0	10, 20, 50, 125, 250, 500, 800, 1000
±45	0,01	6010h + 6020h	6110h + 6120h	IP69K	-40 to +85	M12	1.0.0	10, 20, 50, 125, 250, 500, 800, 1000
±10, ±45, or ±60	0,05	6010h + 6020h + 5000h	not supported	IP68	-40 to +80	M12	not known	10, 20, 50, 125, 250, 500, 800, 1000
0 to 360	0,1	not known	not known	IP68/IP69K	-40 to +85	M12	not known	125, 250, 500, 1000
±80	0,01	6010h + 6020h	6110h + 6120h	IP68/IP69K	-40 to +70 or -40 to +85	M12 or cable gland	1.3.0	20, 50, 100, 125, 250, 500, 800, 1000
0 to 360	0,01	6010h + 6020h	6110h + 6120h	IP68/IP69K	-40 to +70 or -40 to +85	M12 or cable gland	1.3.0	20, 50, 100, 125, 250, 500, 800, 1000
±30	0,001	6010h + 6020h	6110h + 6120h	IP67	-40 to +70 or -40 to +85	M12 or cable gland	1.3.0	20, 50, 100, 125, 250, 500, 800, 1000
±5 to ±60, or 0 to 360	0,01	not known	not known	IP67	-20 to +70	M12	not known	not known
±80, or 0 to 360	0,001	6010h + 6020h	6010h + 6020h	IP69K	-40 to +80	M12	1.3.0	50, 125, 250, 500, 800, 1000
±80, or 0 to 360	0,001	6010h + 6020h	6010h + 6020h	IP69K	-40 to +80	M12	1.3.0	50, 125, 250, 500, 800, 1000
±60	0,04	6010h + 6020h	not supported	IP67	-35 to +70	2 x M12	1.1.0	50, 125, 250, 500, 800, 1000
±10	0,05	6010h + 6020h + 5000h	not supported	IP68/IP69K	-40 to +80	2 x M12	1.2.0	10, 20, 50, 250, 500, 800, 1000
±45	0,1	6010h + 6020h + 5000h	not supported	IP68/IP69K	-40 to +80	2 x M12	1.2.0	10, 20, 50, 250, 500, 800, 1000
±60	0,1	6010h + 6020h + 5000h	not supported	IP68/IP69K	-40 to +80	2 x M12	1.2.0	10, 20, 50, 250, 500, 800, 1000
0 to 360	0,1	6010h + 6020h + 5000h	not supported	IP68/IP69K	-40 to +80	2 x M12	1.2.0	10, 20, 50, 250, 500, 800, 1000
±90	0,01	6010h + 6020h + (6030h)	not supported	IP67/IP69K	-40 to +85	2 x M12	1.2.0	20, 50, 100, 125, 250, 500, 800, 1000
±5, ±10, ±15, ±30, ±45, ±60, ±90, or 0 to 360	0,002 or 0,005	not known	not known	IP69K	-40 to +85	2 x M12	not known	up to 1000
±5, ±10, ±15, ±30, ±45, or ±60	0,0025	not known	not known	IP65/IP67	-40 to +85	not known	not known	up to 1000

Detecting car damages with CAN networks

Minor damages to the car are irritating for the car owner. A research project by the University of Bremen and Hella is building a sensor system that detects damages and evaluates possible sources.

Authors

M.Sc. H. Baumgärtel
Dr. V. Skwarek
Hella Fahrzeugkomponenten GmbH

Dipl.-Ing. S. Gontscharov
Dipl.-Ing. A. Kneifel
Prof. Dr.-Ing. K.-L. Krieger
Item - Elektronische Fahrzeugsysteme
Universität Bremen

Otto-Hahn-Allee
DE-28359 Bremen
Tel.: +49-421-218-62550
Fax: + 49-421-218-9862550

Links
www.item.uni-bremen.de
www.kess.uni-bremen.de
www.hella.com

In the government-funded research project "Kess – Konfigurierbares elektronisches Schadenidentifikationssystem" [1] (German for configurable electronic damage identification system), the international automotive supplier Hella and project partners investigate sensor development to detect minor damages of the vehicle body. In this system, a network of intelligent piezoelectric sensor nodes monitors the vehicle body by analyzing its structure-borne sound. The general idea behind the measurement principle is that every mechanical interaction with the vehicle body emits energy in terms of structure-borne sound. This holds also true for minor damages like scratches and dents. The piezoelectric sensor nodes measure this structure-borne sound and separate it from the general background noise of the car. If these sensors detect an unusual event, which could be a minor damage, they forward the information to a central electronic module. This electronic module then compares the information from all sensor nodes to get an additional plausibility check and to combine the sensor nodes' information with further condition data of the car. Depending on the customer's demands, that condition data could consist of time stamps, GPS data, velocity, engine status (on/off), doors/trunk lock status, seat occupancy, etc. The entire data packet consisting of information on the type of damage, its location on the car, and additional car information is then sent to the fleet management system via a wireless communication system like GPRS. All this information can help fleet managers to reconstruct the cause or process of the damage. For example, if the car was locked and empty the probability is high that someone different than the driver caused the detected damage. On the other hand, if the car speed was 50 km/h when a dent was detected and the customer claims that someone else hit the car with a shopping cart, the fleet manager might challenge the declaration. In the end, the fleet manager can decide whether they want to notify the driver via a smart phone app, the Board Control Unit's (BCU) display, or to forward the damage to the insurance company directly if the costumer wasn't responsible. Furthermore, the fleet manager can also configure the damage detection system of the car by sending data bi-directional over GPRS. This becomes interesting for aligning the sensitivity threshold of the damage detection for certain risk-groups or if the customer has booked an adaptive insurance concept. Figure 1 shows the signal flow in a Car-2-Infratructure (C2I) system, which is being developed in parallel by other Kess project partners.

"Every mechanical interaction with the vehicle body emits energy in terms of structure-borne sound.

Typical minor damages like scratches and dents can occur on every outer part of the vehicle body. Figure 3 shows the sum of all recognized damages of a Ford Fiesta Car-Sharing fleet. These are not the damages of one single car but ▷

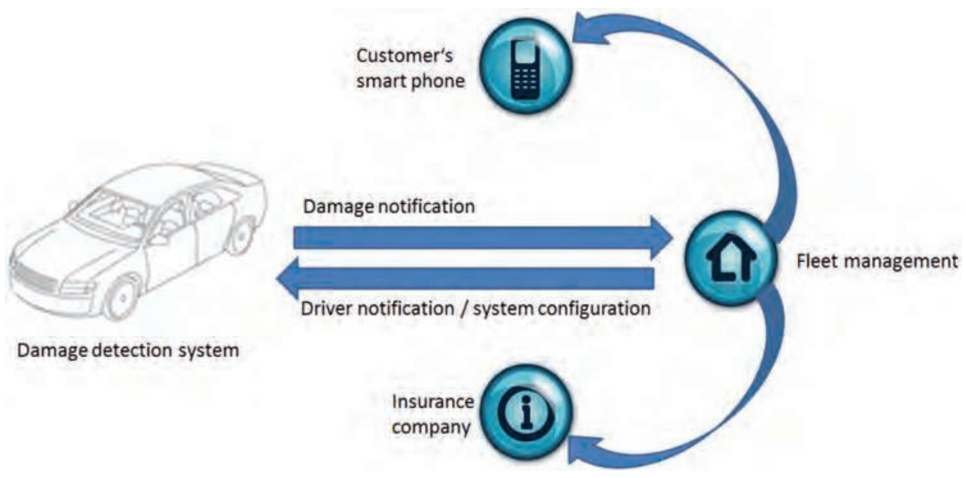


Figure 1: Signal flow of the Car-2-Infrastructure system

The WAGO-I/O-SYSTEM 750 – One System for All Applications!

CAN be connected to any fieldbus

CAN


750-337


750-338


750-347


750-348


750-837


767-2501

750-658

NEW

750-658 CAN Gateway:

- Gateway for all CAN protocols
- CAN 2.0A, CAN 2.0B
- Supports all CAN baud rates and autobaud
- Operating modes: sniffer, transparent, mapped I/O

WAGO®

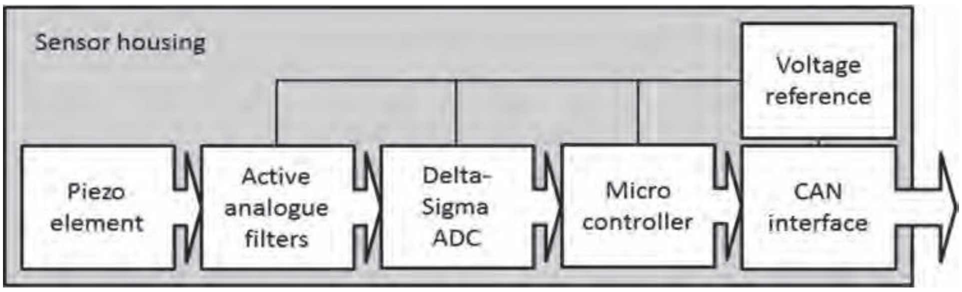


Figure 2: Schematic view of the sensor node

from the entire fleet plotted in one image. It is obvious that there is a higher damage probability distribution in the areas of the fenders than in the rest of the vehicle body, even though every part of the vehicle body is affected by damages [2]. Hence, in order to measure all possible minor damages, it is necessary to monitor all parts of the vehicle body. Recent studies [3,4] show that there is a certain oscillation transfer between body parts, but due to the alleviating behavior of the welded, screwed and glued connections, the structure-borne sound is highly attenuated. Therefore, information gets irretrievably lost on the transfer path. So, for the system setup in the research project, every part of the vehicle body was equipped with at least one piezoelectric sensor. That results in a total of 11 sensor nodes interfaced with the central electronic module and the On-Board-Diagnosis network via CAN. All sensor nodes are mounted on the inside of the vehicle body to be invisible to customers.

The amount of sensors strongly depends on the configuration of the vehicle (e.g. 3 doors / 5 doors) and the requirements regarding the system's sensitivity. For the detection of small scratches it has been found to be obligatory to have a sensor on the affected body part, while heavy impacts overcome the attenuation of the body part connections. Every single sensor node consists of a piezoelectric element to convert the mechanical structure-borne sound signal into a voltage signal, an analog amplification and filter circuit, an A/D converter, as well as a microcontroller unit and an interface to the CAN network.

Figure 3: Distribution of recorded minor damages in a Ford Fiesta Fleet; every dot represents a minor damage (image provided by Cambio Car-Sharing Bremen)

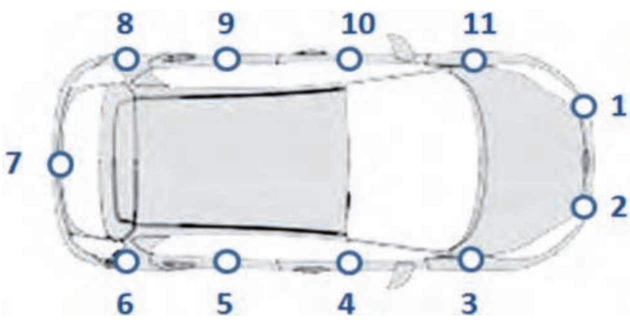


Figure 4: Position of the sensor nodes in a Ford Fiesta (5-door) test car

Every sensor node is connected to the central electronic module via CAN. Furthermore, the central unit is also connected to the OBD II CAN to gather values of the car's status like velocity, revolutions-per-minute (rpm), engine status on/off and door lock sensor information to include those into the minor damage classification. Before a damage message is sent out to the disposition servers of the carsharing company via GPRS, the central electronic module combines all incoming messages from the sensor nodes with the OBD data of the car. Due to this, it is possible to conduct a higher level plausibility check of the event classification. For example, smashing the hood creates a very strong signal in the front bumper that sounds very similar to a damage to the sensor nodes in the front bumpers. But since the other sensor nodes also record vibrations of the impact they send their analysis data to the central unit, too. Having this specific pattern of sensor node information, it is possible to identify the signal correctly. If then, finally, a real damage occurs, the central unit sends out its encrypted GPRS message. The content of the message includes the kind of damage (dent, scratch, 2d scratched surface, unknown damage), a time stamp, an identification number, the position of the damage and a certainty depending on the algorithms output and the latest plausibility check. Optionally, the unit could also send the GPS position, the car's velocity, the gas pedal angle, the engine's rpm, the status of every door and trunk and other useful information to reconstruct the process of damage. This way, if the engine was shut off and the car was locked while a minor damage was created, the carsharing fleet manager can decide if they want to inform the driver via mobile app, SMS or call. ◀

References

[1] http://www.kess.uni-bremen.de, Information on the Kess BMBF research project, Homepage, 2013

[2] S. Gontscharov, Verteilte Intelligenz in einem Sensornetzwerk zur Körperschalldetektion in Fahrzeugen, Universität Bremen, 2013

[3] Becker, M.: Untersuchung und Simulation der Körperschallausbreitung in der Karosserie von Kraftfahrzeugen, University Bremen, Diploma thesis, 2013

[4] Hellbernd, H., Modellbasierte Simulation und Entwicklung eines Sensorsystems zur Detektion von Bagatellschäden in Fahrzeugkarosserien, University of Applied Sciences Bremen, Master thesis, 2012

Tumor treatment with a CANopen motor

A new technology enables the imaging of tumors in real-time during radiation therapy procedures: the soft tissue of the body is protected from damage more than with traditional radiation therapy technologies.

Figure 1: In the MRT the soft tissue of the body gets recorded and analyzed in real-time during radiation therapy (Source: Viewray)

Viewray took on the challenge to design a multileaf collimator (MLC) device that is more accurate than others on the market. They collaborated with Maxon Precision Motors for needed important components. Viewray is a privately held medical device company developing advanced radiation therapy technology for the treatment of cancer. Their system provides continuous soft-tissue imaging during treatment, using MRI-guided radiotherapy. That way doctors are able to see where the actual radiation dose is being delivered and they can adapt to changes in the patient's anatomy. Overall, this system includes five subsystems, which have to work smoothly together for an optimal therapy. The most important sub-systems are: real time MR imaging, treatment planning, forecasting and optimizing of the radiation dose, real time soft-tissue targeting as well as analyzing and confirming it via remote access. The treatment delivery is performed in a split-magnet MRI system. Located in the MRT is a rotating gantry assembly, which helps to position the three shielded Cobalt-60 sources with three multileaf collimators. The imaging in other radiotherapy technologies takes place before or after treatment, not while the beam is on. But this is often a problem for therapies because the radiance cannot be adjusted dynamically.

Through the motion of the soft-tissue, a tumor's position gets often shifted during treatment, which causes soft tissue damage. Viewray solved this problem by using a combination of MR imaging and radiation therapy delivery technologies. With continuous soft-tissue imaging during treatment and with the beam on, the Viewray enclosures can refine the target and re-optimize the dose while the patient is on the treatment table.

Viewray collaborated with Maxon Precision Motors for components including a custom motherboard, DC motors, encoders, gears, and individual motor control modules. According to the engineering team from Viewray, "The MLC motor control system is an important portion of the unit. We knew it would also be one of the more challenging to design because of proximity to the MRI magnet, and volume constraints due to the gantry configuration." The system uses three gamma ray sources, mounted in separate shielded heads. The double-focused MLC is designed to sharpen field edges to produce penumbra ▷

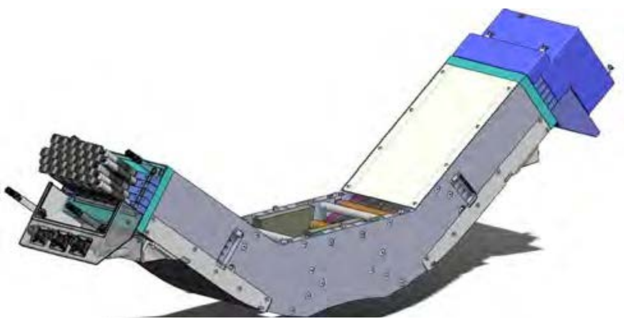


Figure 2: This CAD drawing of one of the collimators shows the motors extending from the left side (Source: Viewray)

Author
Deb Setters
Maxon Precision Motors Inc.
101 Waldron Road
US-02720 Fall River, MA

Viewray Inc.
2 Thermo Fisher Way
US-44146 Oakwood Village, OH

Links
www.maxonmotor.com
www.viewray.com

Figure 3: Developing advanced radiation therapy technology for the treatment of cancer (Source: Viewray)

comparable to conventional accelerators, so the doctors can treat patients with better confidence.

The team chose Maxon's Epos2 Module 36-2 compact digital positioning controllers for their small form factor, which allows packaging 60 channels of motion control for each collimator. Thirty modules can fit on a single custom motherboard, and there are two motherboards per collimator. Each system requires three of these collimators, one for each of the three heads used in the system. These controllers are fully digital, smart motion controllers designed for use as plug-in modules in customer-specific motherboards, and can be used for single axis or multi axis motion control systems. Each Epos module implements a flexible and efficient power stage, and drives a brushed DC motor with a digital encoder. The motors are constructed for operating as slave nodes in a CANopen network.

Each of the collimators contains sixty leaves that are arranged in two opposing banks of thirty. Since there are three collimators, the device uses 180 Epos controllers as well as 180 motor, encoder, and gear assemblies. The MLCs are mounted on the gantry system to provide collimation of the three gamma radiation sources considering the target position. While the gantry is moving into position, each collimator leaf is positioned according to the treatment plan. To position each leaf, the CANopen commands are directed to the associated node. Each node consists of a motor, encoder, gear, and controller. The result is a precisely collimated shape which matches the treatment plan.

The 180 motors used in the system are RE16 brushed DC, 4,5 W motors. Each motor can speed up to 11,000 rpm. The Menc13 hall-effect encoders provide precise motor control while the GP16A gears provide the suited torque for positioning speeds of 1 cm/s. Due to MRI magnetic field effects, the MLC controllers had to be remote from the motors, and housed in a convection cooled chassis. ◀

Subscription

Please use the following classifications for filling in your subscription form:

A **Position in company**
0. Other position
1. Director
2. Technical manager
3. Marketing manager
4. Sales manager
5. System designer
6. Device designer
7. Purchasing manager

B. **Company's CAN business**
0. Other business
1. Semiconductor manufacturer
2. Device manufacturer
3. Software house
4. System integration
5. Service provider
6. End-user
7. Research

C. **CAN application interest**
1. Passenger cars
2. Heavy-duty vehicles
3. Rail vehicles
4. Maritime vehicles
5. Aircraft/Aerospace vehicles
6. Power generation systems
7. Factory automation systems
8. Process automation systems
9. Industrial machine control systems
10. Construction machine control systems
11. Embedded control systems
12. Building automation
13. Door control systems
14. Lift control systems
15. Medical devices and systems
16. Science and research systems

D. **Company size**
1. 1 - 9 employees
2. 10 - 49 employees
3. 50 - 99 employees
4. 100 - 499 employees
5. 500 - 999 employees
6. 1 000 - 4 999 employees
7. 5 000 - 9 999 employees
8. 10 000 - 99 999 employees
9. more than 100 000 employees

CAN Newsletter

I hereby subscribe to the free-of-charge CAN Newsletter for the next four editions (published in March, June, September, and December of every year).

☐ Print version ☐ PDF version

Company

Name

Address

City, ZIP

Phone (Country code - Area code - Number)

Fax (Country code - Area code - Number)

E-mail

URL

Position (see A) Application (see C)

Business (see B) Size (see D)

☐ I like to receive CiA's Weekly Telegraph

Please send your subscription form to CAN in Automation (CiA) GmbH, Kontumazgarten 3, DE-90429 Nuremberg, Germany, or fax it to +49-911-928819-79 or e-mail it to headquarters@can-cia.org. You may also subscribe online at www.can-cia.org.

MICHAELIDES electronics

Record CAN-messages and GPS-data using only one device: CANlogger® GPS provides easy handling and unlimited use.

CANlogger® series

CANlogger® 5001

+ Record CAN messages on SD cards with up to 32 GB
+ Record CAN messages without using a PC
+ Especially suitable for long-term recordings
+ Power management

CANlogger® 5002

+ Record CAN messages on SD cards with up to 32 GB
+ Record CAN messages from 2 CAN-Interfaces without using a PC
+ Especially suitable for long-term recordings
+ Power management
+ Intelligent interface management: 1 each: analog input, digital input and digital output

CANlogger® 5102 (GPS)

+ Record CAN messages on SD cards with up to 32 GB
+ Record CAN messages from 2 CAN-Interfaces without using a PC
+ Especially suitable for long-term recordings
+ Power management
+ Intelligent interface management: 1 each: analog input, digital input and digital output
+ Record position data

DE RM MICHAELIDES SOFTWARE & ELEKTRONIK GMBH
Headquarters | Donaustr. 14 | 36043 Fulda, Germany
Phone +49 661 9490-0 | info@rmcan.com

US RM MICHAELIDES SOFTWARE & ELECTRONIC CORP.
US Subsidiary | 711 E. Monument Ave., Suite 310 | Dayton, Ohio 45402-1490, USA
Toll-Free +1 877 RMCAN-US | Phone +1 937 558-2211 | info@rmcan.com

Find more about our services and products at www.rmcan.com

PCAN-Gateways

Linking CAN busses over IP networks ...

The PCAN-Gateways allow the connection of CAN busses over IP networks. CAN frames are wrapped in TCP or UDP message packets and then forwarded via the IP network from one device to the other.

Different PCAN-Gateway Product Types

PCAN-Ethernet Gateway DR

- CAN to LAN gateway in DIN rail plastic casing
- LAN connection via RJ-45 (10/100 Mbit/s)
- CAN connection via screw-terminal strips (Phoenix)

PCAN-Wireless Gateway DR

- CAN to WLAN gateway in DIN rail plastic casing
- WLAN via external 2.4 GHz dipole antenna (IEEE 802.11 b/g)
- CAN connection via screw-terminal strips (Phoenix)

PCAN-Wireless Gateway

- CAN to WLAN gateway in plastic casing with flange
- WLAN via Internal chip antenna (IEEE 802.11 b/g)
- CAN connection via D-Sub or Tyco automotive connector

General Specifications

- 2 High-speed CAN channels with bit rates up to 1 Mbit/s
- Galvanic isolation of the CAN channels up to 500 V
- Device configuration through a comfortable web interface
- Linux operating system (version 2.6.31)
- Extended operating temperature range from -40 to 85 °C
- Voltage supply from 8 to 30 V

www.peak-system.com

Take a look at our website for the international sales partners.

Scan the QR code on the left to open that page.

embedded world 2014 Exhibition & Conference
... it's a smarter world

Meet us in hall 1, booth 606. The exhibition will take place from 25th to 27th February in Nuremberg, Germany.

PEAK-System Technik GmbH

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

PEAK System