June 2016

CAN Newsletter

Hardware + Software + Tools + Engineering

The world's smallest motion controller

Positioning made easy

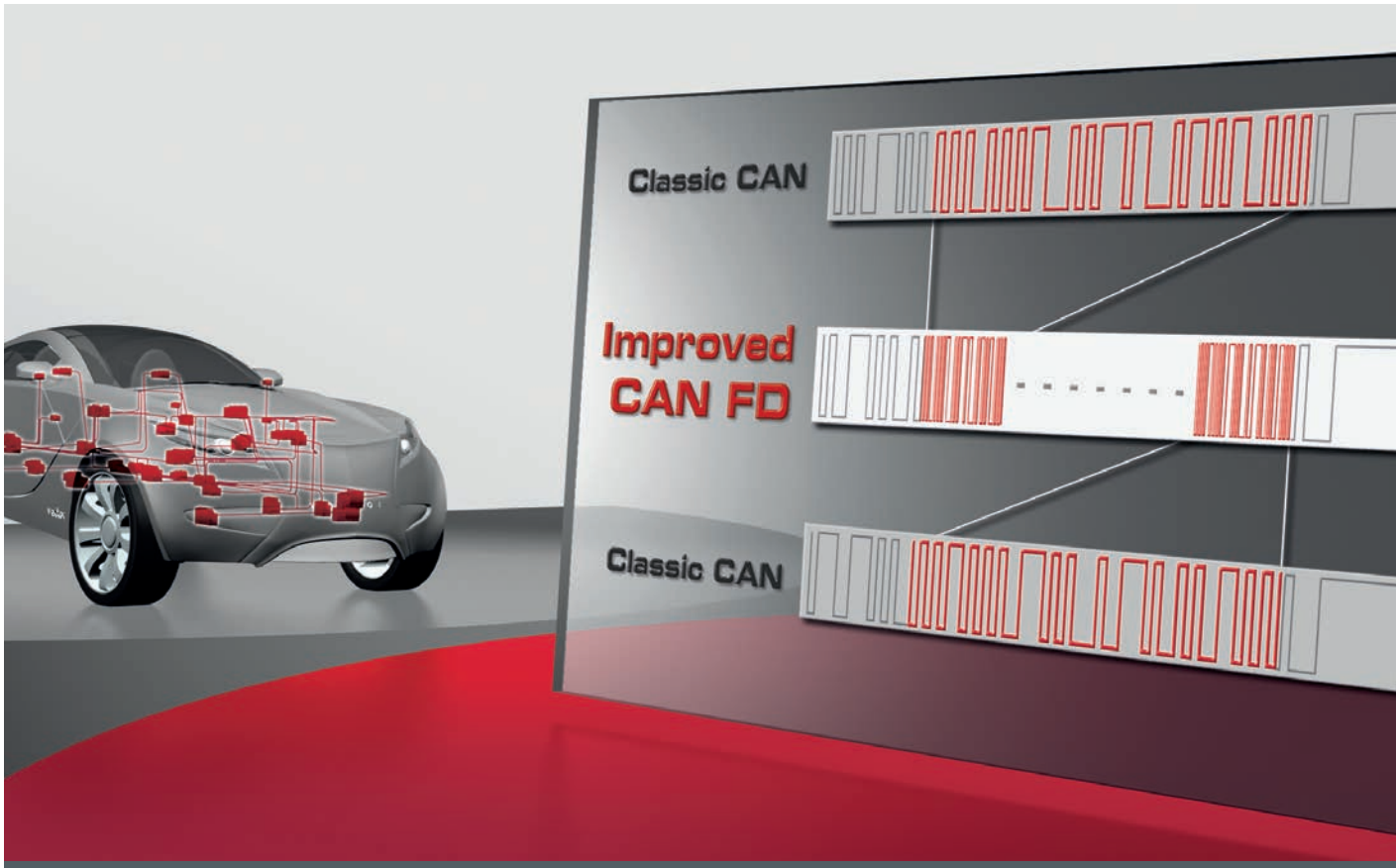
Using CANopen instead of analog signals

Good to know: PDO re-mapping procedure

CANopen

www.can-newsletter.org

VECTOR



First class solutions
for your CAN and CAN FD based projects

Complete and universal tool chain

Increase the efficiency of your projects with the use of the complete tool chain from Vector:

- Tools for testing, flashing and calibrating ECUs
- Flexible bus network interfaces
- High performance Scope for bit accurate signal analysis
- Easy to configure AUTOSAR basic software
- Worldwide engineering services and trainings

Information and downloads: **www.can-solutions.com**

More CAN power: benefit from over 25 years of networking experience.

CAN/CAN FD Poster
now order for free:
www.vector.com/canfd_poster

Vector Informatik GmbH | Germany · USA · Brazil · France · UK · Italy · Austria · Sweden · Japan · Korea · India · China | www.vector.com/contact

CANopen

Imprint

Publisher
CAN in Automation GmbH
Kontumazgarten 3
DE-90429 Nuremberg

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

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

CEO Holger Zeltwanger
AG Nürnberg 24338

Downloads last issue:
11 000 full magazine

Editors
pr@can-cia.org

Annegret Emerich
Cindy Weissmueller
Holger Zeltwanger
(responsible according
to the press law)

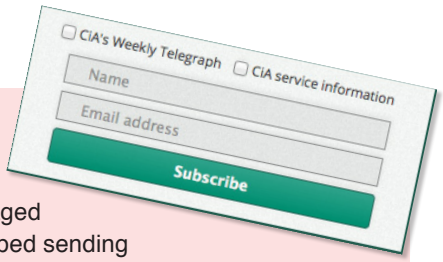
Layout
Nickel Plankermann

Media consultants
Gisela Scheib
(responsible according
to the press law)
Meng Xie-Buchert

Distribution manager
Meng Xie-Buchert

CAN FD

CAN meets IT



CiA SignUp

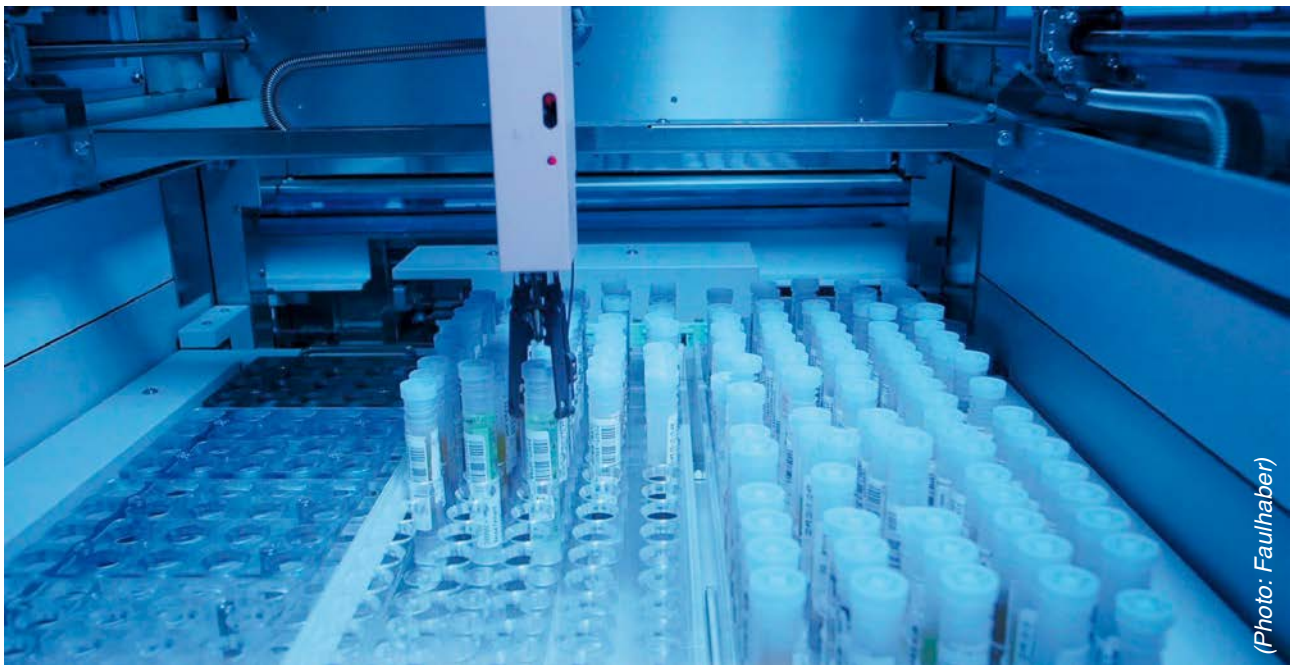
If you are reading this, you have obviously managed to find our magazine, even though we have stopped sending an announcement email to our subscribers. Surprisingly, the number of downloads has gone way up (from around 2000 to 11000) since we decided to cancel that email.

Even without the announcement email, there is another way to never miss a new edition of the CAN Newsletter magazine: if you subscribe to CiA's Weekly Telegraph you not only get a weekly overview of all articles published in the CAN Newsletter Online, you also get the link to each new edition of the CAN Newsletter magazine. If weekly emails seem too many, you can put an alert in your calendar and come back to the online newsletter every third month to simply download the pdf there.

Table of contents

The world's smallest motion controller

Faulhaber has launched a 22-mm DC-micromotor with integrated CANopen motion controller. The motor complies with the CiA 402 profile for drives and motion controllers.



The Faulhaber Group specializes in the development, production, and deployment of high-precision miniaturized and miniature drive systems, servo components, and drive electronics with up to 200 W of output power. This includes putting into effect customer-specific packaged solutions as well as an extensive range of standard products, such as brushless motors, DC-micromotors, stepper motors, encoders, precision gearheads, and speed/motion controllers. The company comes with 1700 staff members and its trademarks are recognized worldwide in complex and demanding application areas – in medical technology, automatic placement machine, precision optics, telecommunications, aviation and aerospace, and robotics, for example. From microdrives with 1,9 mm diameter up to the powerful 44-mm brushless motor that can be combined with various precision transmissions, the company offers dependable system solutions for a multitude of applications.

From the DC motor with a continuous torque of 200 mNm to the filigree Microdrive with an outer diameter of 1,9 mm, the Faulhaber standard range can be combined in more than 25 million different ways to create the optimum drive system for a particular application. At the same time, this "construction kit" is the basis for modifications, which allows the user to configure special versions. The company's integrated motion controllers combine high performance single axis motion controllers with the benefits of brushless DC servomotors to provide a large portfolio of integrated motor controllers, whether configured as stand-alone single axis positioning drives or integrated into a multi-axis CANopen network. It offers products ranging from 22 mm to 35 mm, a nominal voltage of 24 V, an a continuous output from 18 mNm to 96 mNm. The brushless drive with 22-mm housing provides the smallest integrated CANopen motion controller of the world. It fully supports CiA 402 – the CANopen device profile for drives and motion control. Any number of axes can be driven synchronously. Besides CANopen, the motion controllers ▷

Figure 1: The latest generation of motion controllers in its housing with four plug connections (Photo: Faulhaber)

offer EIA-232. Operation of higher-level controllers such as PLCs and easy networking via dynamic PDO mapping is favored in particular for networked applications in factory automation and industrial machinery. The standardized protocol with corresponding device profiles enables the synchronous control of several axes in a convenient and reliable manner. The drives on the field bus level, meaning the motion controllers and the motors connected to them, can be configured as before with the Software Motion Manager by Faulhaber.

Drive technology in a networked industry

Pressure to reduce costs, the requirement for short start-up and stop times of machinery, and a heterogeneous training level for machine operators mean that electrical drive systems need to be extremely user-friendly. Users expect easy operation and flexible interfaces in order to ensure that communication in the automation network is problem-free, and the possibility of synchronizing several axes in a practice-orientated way. The motion controllers for a new generation by Faulhaber meet these requirements and therefore pave the way for intelligent drive systems in the direction of networked industry.

Drive technology plays an important role within the context of networked industry; after all, automation is not possible without a driving force. For motors and drive electronics, the new approach has far reaching consequences: decentralized intelligence and the capacity for real-time communication with higher level process control technology via field bus systems such as CANopen and flexibility in usage applications are today's requirements for cutting-edge drive systems.

Like the existing products and the products that continue to be available, generation V 3.0 is coordinated to DC-micromotors from the company's own portfolio but not limited to them. New devices can be integrated into varied environments via interfaces such as CANopen, EIA-232, USB, or Ethercat. For start-up a user software is available; the electrical connection is made easier by a consistent plug concept and a full set of accessory lines. There is a more powerful programming environment for the applications and autarkic usage areas without higher level controller that dominate the market to date. Furthermore, hardware and software offer further possibilities when necessary and can also be adapted as before to customer specifications.

As the tasks and operation environments of micromotors and the associated controllers are very complex and varied three different device customizations are available: the MC 5005, MC 5010, and MC 5004 motion controllers. The MC 5005 and MC 5010 with housing and plug connectors are designed for use in switch cabinets or in devices. In addition, the products can be mounted both directly as well as using installation aids such as top-hat rail adapters, for convenient installation. The MC 5004 motion controller is designed for use in existing housing as an open plug-in card. An optionally ▷

Figure 2: Three device variants for different applications are available (Photo: Faulhaber)

Figure 3: Motion control system with integrated motor and controller (Photo: Faulhaber)

available motherboard makes it possbile to get started in multi-axis applications.

All three versions use the same technology basis, offer the same interfaces options, the same operating philosophy, and the same functionality. Thus, there is a suitable solution for many applications and users from completely different areas can profit from the connection options, operating modes, and control options. Motion control systems as servomotors with integrated motion controller are already pre-configured and make use directly in the automation environment possible. They are connected via round connectors as per industry standards. A modular system makes it possible to integrate diverse brushless DC servomotors into standardized housing.

Automated operating procedures

The Motion Manager version 6 is presented with a new look and can be downloaded from the company's website for free. Functions such as the graphical analysis of internal signals have been further developed. A software oscilloscope for processes directly in the controller, as well as other functions via graphical dialogues, is now also directly available. Initial start-up is completed within five minutes because of the assistant functions for connection establishment, motor selection, and controller configuration. Further graphical dialogs support the user with the fine-tuning of the application and when testing the different operating modes. Diagnostic functions make continuous monitoring of the drive possible. The connection to the motion controller and the motion control system is possible via CANopen, USB, or EIA-232. Operating procedures such as for start-up or for periodic tests can be automated via Visual Basic. Project administration is also new, which combines the settings and data of a new drive into one project file and thus simplifies versioning and maintenance.

The functions integrated into the controllers make it easier for the user to handle the technology and create flexible potential applications. The respective motor type can be adjusted on the MC 5010, MC 5005, and MC 5004 motion controllers. The user can therefore freely select whether a DC-micromotor, a brushless DC-servomotor, or a linear DC-servomotor should be actuated. The corresponding motor on the other hand is already preconfigured at the factory for the integrated servo drive of the motion control system series. Either position, speed, or current (torque or power) can then be controlled. The CSP (cyclic synchronized position), CSV (cyclic synchronized velocity), and CST (cyclic synchronized torque) modes that are normally used for synchronized operation of multiple axes are also supported when doing this.

Alternative point-to-point movements to the dynamics of the application can be adjusted via the integrated profile generator, so even complex profiles are feasible. However, position, speed, or current can also be controlled via analog specifications independent from the field bus. Diverse variants for reference drives are available via the reference and limit switch. For the first time, referencing on a mechanical stop is integrated as a standard as well. Furthermore, the dynamics are increased compared to previous products due to a new control structure. Thermal models provide motor winding and power electronics particularly in high-dynamic operation to protect the motors and the electronics.

Figure 4: The Software Motion Manager 6 enables access to the settings and parameters of the connected controller (Photo: Faulhaber)

Two encoder interfaces are now available as standard with the motor interface and can be connected to the optical and incremental encoder, absolute encoder (12-bit AES/BiSS, 12-bit SSI) or the digital and analog Hall sensors in the motor. The resolution of the Hall sensors is 4096 increments per revolution, i.e. also 12 bits. In addition, analog or PWM signals can also be used as position and speed feedback. Two sensors can also be used to detect the speed and position separately.

The motion controllers of generation Version 3.0 offer three to eight digital inputs as standard; two flexible analog inputs, and two digital outputs can be used which can also directly control an optionally connected holding brake. Another ▷

ifm electronic

Look what we have for you!

An absolute must-have!

ecomat*mobile* BasicController*relay*: modular mini controller with powerful relay outputs with diagnostic capabilities for mobile applications. Direct connection of sensors and actuators without further external wiring, powerful CAN interfaces, programmable to IEC 61131-3 with CODESYS.
Can be extended with other components, such as the BasicDisplay. With E1 type approval of course.

www.ifm.com/gb/ecomatmobile_basic

Phone: +49 0800 16 16 16 4

reference encoder for positioning settings (gearing mode) can also be connected via the inputs or a pulse/dir signal for setting the position. Alternatively, the movement of the drive can be synchronized to an ongoing movement via the reference encoder and the touch-probe input. Configuring the set point is possible via CANopen, USB interface, discrete inputs/outputs, or sequential programs. Thereby, up to eight sequential programs written in Basic can be saved in the motion controllers; one of which can be selected as an auto-start option.

CANopen networked

The series offers a total of four interfaces for different tasks. For example, configuration occurs via the USB interface. CANopen and EIA-232 are provided as default connection to the automation technology. The following applies: All functions and operating modes are available via all interfaces and the configuration is based on the CiA 402 profile. However, the Ethercat interface is not integrated into the microdrive's 22-mm enclosure. It requires a larger footprint and consumes some more energy compared to the CANopen variant.

The motion controllers are designed for industrial use. The housing versions fulfill the requirements of protection class IP40, the motion control systems fulfill the requirements of protection class IP54. The housed controllers are designed for a motor supply of 0 V to 50 V; the voltage supply for the electronics is between 12 V and 50 V. The continuous current is specified at 5 A and 10 A, whereby peak currents of 15 A and 30 A are possible. The controllers are suitable for a speed range of 0 revolutions per minute to 30 000 revolutions per minute (motors with sinus commutation) and 0 revolutions per minute to 60 000 revolutions per minute (motors with block commutation). Thus, intelligent drive systems are available for diverse applications, which can be integrated into modern automation landscapes and are easy to operate. ◀

Figure 5: With only 22 mm in diameter, Faulhaber presents a complete system made of brushless DC servomotors and the CANopen motion controller (Photo: Faulhaber)

Author

Cindy Weissmueller
CAN in Automation
www.can-cia.org
pr@can-cia.org

Connecting Devices™

Anybus® www.anybus.com

IXXAT® www.ixxat.com

netbiter® www.netbiter.com

All you need for CAN

HMS offers one of the largest portfolios of products and services for CAN

Anybus

CompactCom™

Multi-network connectivity for your device – as chip, brick or module

- Integrate Anybus CompactCom into your device to make it communicate with CANopen or any other network

Anybus

X-gateway™

- Connect any two industrial networks. More than 250 network combinations for fieldbus and Ethernet
- Easy configuration - no programming!

IXXAT

CM CANopen

CANopen PLC extension

- Extend your SIMATIC® S7-1200 to communicate with CANopen-based devices
- Proprietary protocols supported by additional transparent CAN 2.0A mode

Anybus

Communicator™

Your external businterface

- Connect a CAN-based device to any fieldbus or industrial Ethernet network – no changes to your hardware required and no programming!

IXXAT

PC/CAN Interfaces

- Eays connection of CAN or CAN FD systems to your computer – for control, analysis and configuration
- All common PC interface standards supported

IXXAT

CAN Repeaters and Bridges

- Increase the system reliability, implement line protection and save costs due to simple wiring
- Perform large distance bridging via Bluetooth/Ethernet

IXXAT

Protocol Software

- Use proven and tested IXXAT software stacks to run applications on CANopen, DeviceNet and SAE J1939
- Highly flexible protocol implementation for various microcontrollers/compilers

IXXAT

Controllers – Econ Series

Stand-alone embedded PC with multi-protocol support

- Control your system or setup gateways by using a platform providing a unique number of interfaces – analog/digital IO, fieldbus, industrial Ethernet
- Easy programming via Soft-PLC or Application Development Kits

Netbiter

- Remotely monitor and control your CAN-based field equipment – anytime, anyplace!

Service makes the difference

Our solution centers in Halmstad (Sweden) and Ravensburg (Germany) adapt our products to meet you requirements and deliver ready-to-go OEM solutions.

HMS Industrial Networks
info@hms-networks.com

Tel.: +49 721 989777-000 (Germany)
Tel.: +46 35 172900 (Head office, Sweden)

www.hms-networks.com

Positioning made easy

The Epos4 positioning controller with CANopen connectivity supports the CiA 402 device profile. It is one of the latest products developed by Maxon Motor based on the existing Epos series.

Epos is a modular, digital positioning controller by Maxon Motor, which has been quite successful in the marketplace. It is suitable for permanent magnet-activated motors plus encoders with a range of 1 W to 1500 W output power. Its range of operating modes, as well as various command interfaces, makes it suitable for use in many different drive systems in the fields of automation technology and mechatronics. Since its launch in 2005, more than 100 000 units have come in use worldwide. To build upon this success, the Swiss drive specialist has launched the Epos4 as the next generation of positioning controllers. The first product in this line is the high-performance Epos4 module with detachable pin headers and two different power ratings. With a connector board, the modules can be combined into a ready-to-install compact solution. The positioning controllers are suitable for efficient and dynamic control of brushed DC motors and brushless BLDC motors (EC motors) with Hall sensors and encoders up to 750 W continuous power and 1500 W peak power. The units support various feedback options, such as Hall sensors, incremental encoders, as well as absolute sensors in a multitude of drive applications. The controllers are specially designed to be commanded and controlled as an NMT slave node in a CANopen network. In addition, the units can be operated via any USB or EIA-232 communication port of a Windows or Linux workstation. An Ethercat extension card will follow in 2017.

Additional performance

The drive specialists at Maxon Motor have equipped the CANopen positioning controllers with more power, better control performance, and additional functionalities. All these features are based on the principle of the company's positioning system. The combination of a range of operating modes and control characteristics like field oriented control (FOC) with multiple analog and digital I/Os along with various command options enables applications in a large number of fields from medical technology to robotics. Maxon relies on integrated protective devices like the safe torque off (STO) functionality.

The Epos4 range of functions will grow by updates. In a next release, the positioning control units will implement cyclic-synchronous modes for velocity and position control (as specified in IEC 61800-7-201/301:2008) as well as interpolated position mode. They already feature cyclic synchronous torque, profile velocity, profile position and homing mode. The digital I/O functionality includes touch probe, reference switch, limit switch, quick stop, and drive enable. The configurable digital outputs comprise position compare, holding brake, and ready/fault. The CANopen interface is capable to run up to 1 Mbit/s. In the future it will comply with CiA 305 supporting the layer setting services (LSS). This means that the node-ID can be assigned by the LSS master via the CAN network. The smallest family member so far measures 59,5 mm x 46,0 mm x 14,1mm and can be operated from -30 °C to +45 °C under full load, with derating even up to + 77° C. There will be further versions soon to form a complete EPOS4 product line in the future.

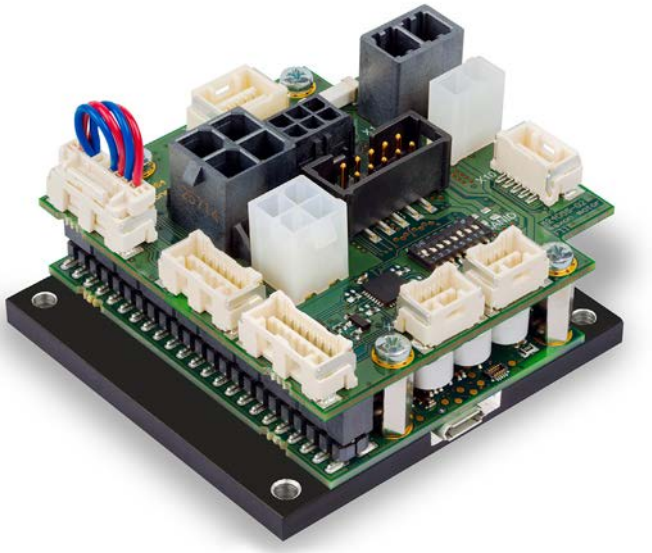


Figure 1: Ready solution for connection, consisting of the Epos4 module 50/15 and the matching connector board (Photo: Maxon Motor)

The product comes with a Windows DLL and software support for PC interface boards from HMS, Kvaser, National Instruments and Vector. An IEC 61131-3 library for Beckhoff as well as support for NI's Soft Motion environment will follow. Start-up and parameterization are performed with

Figure 2: Epos2 in the Cobot robot arm, which gives employees in industry a hand (Photo RB3D)

an advanced graphical user interface called Epos Studio and menu-controlled wizards. An automatic process for controller tuning has also been part of the package for years. Customers are thus free to fully dedicate themselves to their real task: developing their devices. Together with the three freely available libraries and programming examples, this enables the integration in a variety of systems. All these characteristics are combined with an input voltage range of up to 50 V_{DC}, high power density, and up to 98 % efficiency, says Maxon.

The Epos2 series is already used in a range of application areas. One example is the Cobot of the French company RB3D. It gives workers in the industry a hand, literally. The robot arm is attached to a wall and comes with seven axes and an operating range of more than two meters. At the lower end of the arm, a heavy tool such as a grinding machine can be attached. Thus, workers do not have to hold the device themself but only lead it while Cobot does the lifting work. The DC motors of the RE-line in combination with matching planetary gear heads, encoders, and the Epos positioning controllers are used in the robot arm.

Another application example was already reported in a separate article of the CAN Newsletter a while ago. Tumor treatment with a CANopen motor: a new technology that 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. Viewray collaborated with Maxon for a few important components.

Figure 3: In the MRT, the soft tissue of the body gets recorded and analyzed in real-time during radiation therapy (Photo: Viewray)

The team chose the Epos2 module 36-2 digital positioning controller. The motors are also constructed for operating as slave nodes in a CANopen network. ◀

Author

Cindy Weissmueller
CAN in Automation
www.can-cia.org
pr@can-cia.org

Flexible diagnosis for CAN FD

Going deep into a CAN FD network is possible with a handeld device. It can handle diagnosis on the data link layer and the physical layer.

In many cases, CAN diagnosis cannot be done in a laboratory environment where appropriate but stationary hardware is available. A handheld device which is specialized in CAN – and also the new CAN FD standard with its higher data bit-rates – helps to fulfill this task flexibly but still in a comprehensive manner.

The general CAN communication is based on the lower two layers of the OSI model (Open Systems Interconnection Model). The CAN FD protocol as defined in ISO 11898-1 refers to layer 2, the data link layer. This communication is managed by CAN controllers. If the CAN communication fails in new CAN FD environments with heterogeneous nodes and there is no way to get status outputs of the CAN controllers, it is time to take a look at the physical layer (layer 1) of the CAN network. The interesting thing to know is what actually happens on the CAN_H and CAN_L lines of the high-speed CAN (ISO 11898-2). The handheld device PCAN-Diag FD includes an oscilloscope function, specialized in the work with CAN FD communication.

The pure signal course of the two CAN lines already helps to detect basic cabling errors. For example, the assumed development environment is susceptible to mixed up CAN lines. This is reflected by the scope channels amplitudes pointing to wrong directions.

CAN frame decoding

More interesting is the analysis of the physical signal course for CAN and CAN FD frames. The scope function of the PCAN-Diag FD is able to decode a CAN frame from the signal on the lines and show information about the frame

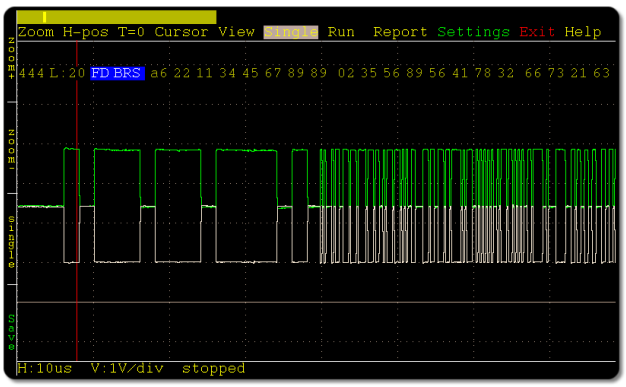


Figure 1: A CAN FD frame on the scope including frame information decoded from the CAN transceiver's data stream (Photo: Peak-System)

Figure 2: Handheld device PCAN-Diag FD for diagnosis of a CAN FD network (Photo: Peak-System)

and its logical sections. This also works for broken CAN frames because the detection is independent of the CAN controller. Going into CAN FD peculiarities, there are two incompatible flavors of the protocol. The initial one and the one with improved CRC handling, which is now part of ISO 11898-1. If a non-ISO frame is decoded, but the CAN FD network should work only in ISO mode and other FD nodes already do, the situation is clear.

With higher bit-rates for the data part of the CAN FD frame and the resulting short bit times, timing issues are pushed to the foreground. The Report function shows the actual nominal bit-rate (for the arbitration) and data bit-rate. Both are calculated from the measured duration of the corresponding CAN frame parts. A CAN FD node may be configured with a wrong data bit-rate, e.g. 2,5 Mbit/s instead of 2,0 Mbit/s. As the CAN-ID of the faulty frame is also determined, the misconfigured CAN node is easily detected.

Figure 3: The upper curve displays the data stream from the CAN transceiver; the marked position exemplarily shows that the transceivers threshold is not reached by the analog signal (Photo: Peak-System)

Not only the analog signal course can be used to assess the signal quality. Important is what the CAN transceiver can pull out of a disturbed signal from the CAN network lines. As it uses the difference between CAN_H and CAN_L to interpret the signal course, it is good to take a look at this – on both sides of the CAN transceiver. The scope function has options to display the calculated differential signal and also the RxD channel as it is delivered by the CAN transceiver. The question is if all slopes on the physical lines are correctly converted into changes between 1 and 0.

This inspection should be done at different taps of the CAN network in order to see where state changes may not be detected properly anymore. This could happen if the amplitudes of the CAN signals are becoming low due to very long CAN lines or an improper termination with too many resistors or with wrong resistance values.

Layer-combined diagnosis

The PCAN-Diag FD acts as a regular CAN FD node. For example, it is able to initiate communication with other nodes that rely on specific CAN message sequences, e.g. control units. Transmit lists of CAN messages can be set up on the PCAN-Diag FD, even with defined pauses between single messages. As the trigger of the scope function can be set to a specific CAN-ID, the expected response can be observed on the scope. The dual-layer diagnosis is complemented by measuring functions for CAN termination and bus load during communication as well as tracing and playback of CAN traffic. Many aspects of the inspection can be handled by means of projects, i.e. CAN communication parameters, scope settings, and even a customized splash screen for a better distinction for the user. Projects are saved on the PCAN-Diag FD in order to handle different use cases without further need of configuring.

Author

Mark Gerber
Peak-System Technik GmbH
www.peak-sytem.com
info@peak-system.com

Related articles

- Mark Gerber (Peak-System): CAN frames through IP networks
- Holger Zeltwanger (CiA): Hand-held CANopen diagnostic tool

The new dynamic parameters of CAN FD

ISO 11898-2:2016 will be released soon; the CiA 601-1 specification helps to understand the CAN FD high-speed transmission. Let us take a look at the dynamic parameters.

In the past, three standards specified the CAN high-speed physical layer: ISO 11898-2, ISO 11898-5 (low-power mode), and ISO 11898-6 (selective wake-up). These three standards will be merged into one standard, published as ISO 11898-2:2016. The norm also specifies the additional dynamic parameters for bit-rates above 1 Mbit/s. Some of the existing parameters have been modified and adjusted.
During the arbitration phase, when two or more nodes are in competition to win the arbitration, the maximum bit-rate is limited by the network and transceiver propagation delays as well as reflections on the bus-lines. In the data-phase, the propagation delay between nodes is not important anymore, but the bit-width variations, caused by the network behavior and the transceiver performance, are now relevant. The most critical parts in a physical network are:

- Interface between micro-controller and transceiver,
- Transceiver,
- Network (reflection, damping).

The transceiver has three different kinds of propagation delays:

- Loop delay TxD-to-RxD,
- Transceiver Tx (transmitter) delay,
- Transceiver Rx (receiver) delay.

The symmetry requirements of these delays have now been added to ISO 11898-2. In ISO 11898-2, two bit-rates for the CAN FD data phase are specified in detail including the dynamic symmetry requirements: 2 Mbit/s and 5 Mbit/s. Normally, the symmetry of the transceiver is independent from data bit-rates. A 5-Mbit/s transceiver can also be used for lower bit-rates like 2 Mbit/s or 500 kbit/s. The permanent TxD dominant timeout limits the minimum bit-rate. This feature is implemented to block the bus communication in

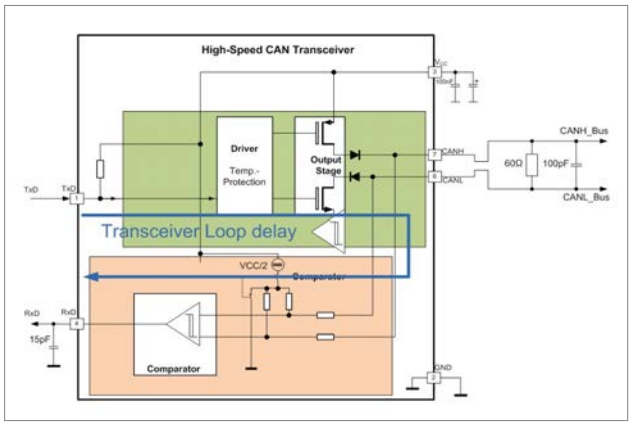


Figure 1: Transceiver loop-delay elements (Photo: Infineon)

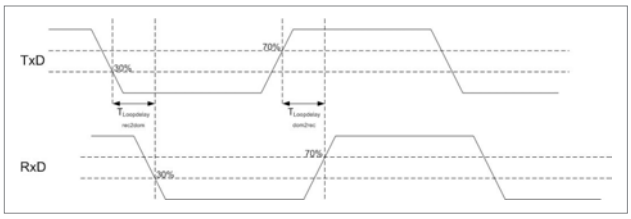


Figure 2: Transceiver loop-delay specification (Photo: Infineon)

case the TxD pin of a transceiver is permanently clamped to ground. With the parameter values given in ISO 11898-2, a minimum bit-rate of 50 kbit/s can be realized.

Loop-delay symmetry

The loop-delay is the time between the TxD input signal and the RxD output signal of a transmitting transceiver. Figure 1 illustrates the transceiver loop-delay. In the "old" ISO 11898-5 this propagation delay is specified with maximum 255 ns. In the "new" ISO 11898-2 the condition for how to test and to guarantee has been added and the maximum allowed delay is unchanged. Figure 2 illustrates how the loop-delay is specified. The delay of the recessive-to-dominant transition (falling edge in TxD) starts at 30 % of the TxD voltage swing and stops at 30 % of the RxD output level.

The dominant-to-recessive transition (rising edge) starts at 70 % of the TxD level and stops at 70 % of its RxD level. The loop-delay is an important parameter for a transmitting CAN FD node. The transceiver loop-delay is part of the transmitter loop-delay, which can be ▷

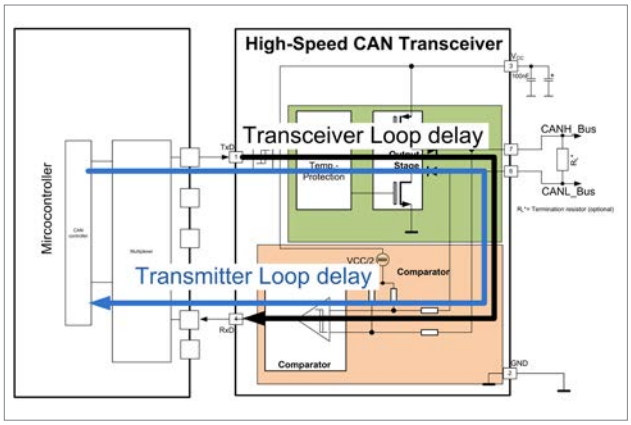


Figure 3: Difference between transmitter and transceiver loop-delay (Photo: Infineon)

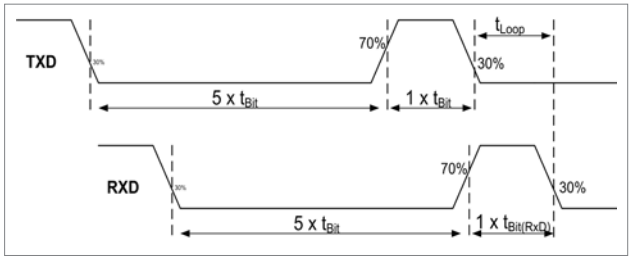


Figure 4: Transceiver loop-delay symmetry specification (Photo: Infineon)

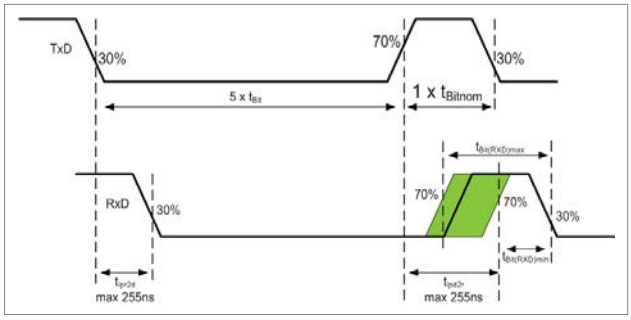


Figure 5: Variation on RxD recessive bit-length (Photo: Infineon)

compensated by the transmitter delay compensation unit (TDC) in the CAN FD controller. The transmitter loop-delay starts at the output of the CAN FD controller as a part of the micro-controller and ends on the receiver input of the CAN FD controller. For high bit-rates the nominal bit-time may be shorter than the propagation delay. The TDC in the CAN FD controller compensates the transmitter delay. For high bit-rates a high resolution of this unit is recommended. The symmetry of the recessive-to-dominant and dominant-to-recessive transition is very important for the transmitting node and may be different. To check this dynamic performance of the transceiver, the recessive bit-width on the RxD pin ($t_{Bit(RXD)}$) after five consecutive dominant bits (see Figure 4) is defined in the "new" ISO 11898-2. Table 1 shows the RxD recessive bit-width specification.

Depending on the asymmetry, the recessive bit-width is shortened or extended. The limits of this parameter are asymmetric to the nominal bit-rate. Figure 5 shows the impact on the recessive bit-width. The recessive signal has a wide range of variation and the sample point should be set as late as possible. The maximum propagation delay TxD-to-RxD for both edges is below 255 ns. In general, the asymmetric behavior is caused by the busload (resistive and capacitive), the maximum differential voltage of the dominant bit, and the temperature dependency of the transceiver internal delays.

Table 1: The RxD recessive bit-width (transceiver loop-delay symmetry)

Data-phase bit-rate	2 Mbit/s	5 Mbit/s
$t_{Bit(RxD)}$ min	400 ns	120 ns
$t_{Bit(RxD)}$ max	550 ns	220 ns
$t_{Bit(RxD)}$ nom	500 ns	200 ns
$t_{(loop)}$	<255 ns	<255 ns
Bus-load	60 Ω ‖ 100 pF	60 Ω ‖ 100 pF

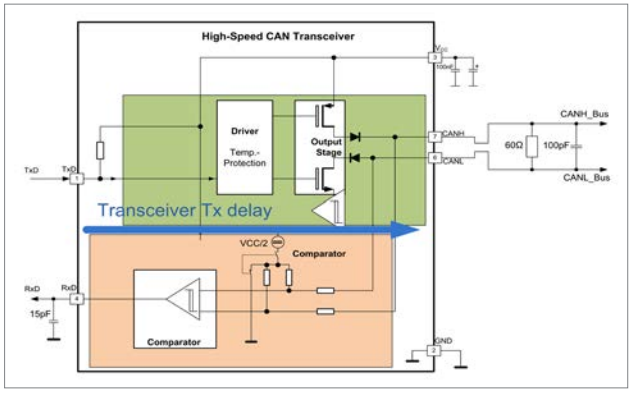


Figure 6: Transceiver Tx delay (Photo: Infineon)

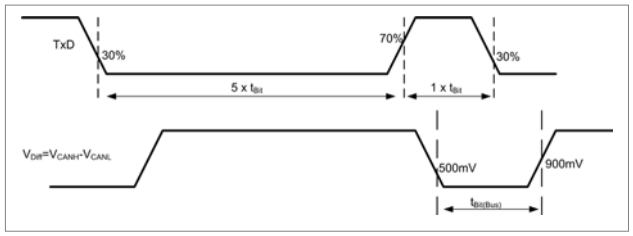


Figure 7: Specification of the recessive bit-width (Photo: Infineon)

Transceiver Tx delay symmetry

The transceiver Tx delay is the time between the TxD input signal and the differential bus output signal as shown in Figure 6. The symmetry is the difference between the recessive-to-dominant delay and the dominant-to-recessive delay. The symmetry is specified like it is for the loop-delay. The recessive bit-length is the distance between 500 mV of the falling edge to 900 mV of the rising edge (see Figure 7). Table 2 shows the new $t_{Bit(Bus)}$ parameter values. The variation of the symmetry is smaller than for the loop-delay ($t_{Bit(RxD)}$). This parameter is valid for the defined busload. For higher busloads the variation may be different.

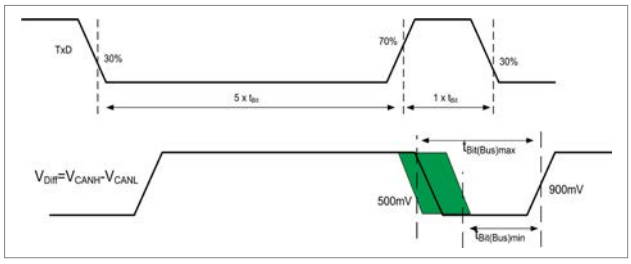


Figure 8: Variation of the bus recessive bit-length (Photo: Infineon)

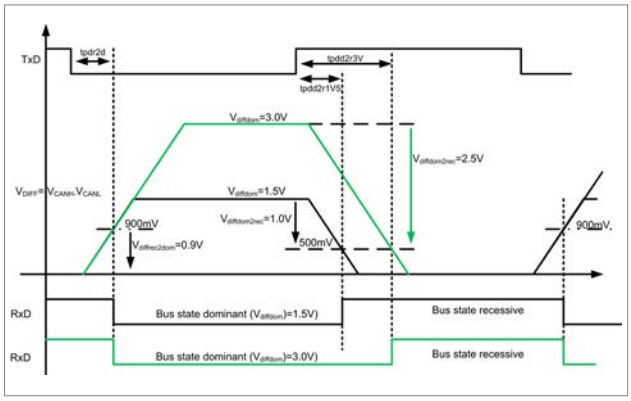


Figure 9: Impact of the dominant voltage level on the recessive bit-width (Photo: Infineon)

Figure 8 illustrates the impact of the recessive bus-width. The recessive to dominant edge is controlled by the transceiver, but the dominant to recessive edge is dominated by the bus load. One reason for the asymmetry is the internal delay from TxD pin to the output stages. The second reason is the differential voltage level of the dominant signal. This dominant voltage level depends on the transmitter supply voltage (V_{CC}), the physical busload, and the transceiver temperature. To reduce the emission of transmitting signals, the slew-rates are controlled and as slow as possible for high bit-rates. The voltage difference between the recessive level and the dominant differential threshold level are always 900 mV ($V_{diffrec2dom}$) (see Figure 9). The slew-rate defines the delay time.

The voltage difference ($V_{diffdom2rec}$) between dominant voltage level and the recessive threshold may differ from 1 V (1,5 V dominant level minus 500 mV recessive threshold) up to 2,5 V (3 V dominant level minus 500 mV recessive threshold). Due to the constant slew-rate, the dominant-to-recessive delay-time depends on the voltage level of the dominant signal. Figure 9 illustrates these two scenarios. The higher the dominant voltage level on the bus, the longer will the dominant bit-width be, or the smaller will the receive bit-width on the RxD pin be. In this scenario the impact of the bus load is ignored. To reduce the variation of the recessive bit-width, a small range of the transceiver supply (V_{CC}) is recommended.

Transceiver Rx delay symmetry

The transceiver Rx delay is the propagation time between the differential bus signal and the RxD output signal. This symmetry depends on:

- Production dispersion,
- Temperature variation,
- Receiver thresholds,
- Supply voltage variation,
- Bus differential voltage(V_{diff}) slew-rate.

Δt_{Rec} is a calculated value:

$$\Delta t_{Rec} = t_{Bit(RxD)} - t_{Bit(Bus)}$$

The parameter of the RxD symmetry is also specified in ISO 11898-2 (see Table 3).

Table 2: Bus recessive bit-width (transmitter loop-delay symmetry)

Data-phase bit-rate	2 Mbit/s	5 Mbit/s
$t_{Bit(RxD)}$ min	435 ns	155 ns
$t_{Bit(RxD)}$ max	530 ns	210 ns
$t_{Bit(RxD)}$ nom	500 ns	200 ns
Bus-load	60 Ω ‖ 100 pF	60 Ω ‖ 100 pF

Table 3: Tolerance of the receiver

Data-phase bit-rate	2 Mbit/s	5 Mbit/s
$t_{Bit(Bus)}$ min	-65 ns	-45 ns
$t_{Bit(Bus)}$ max	+40 ns	+15 ns
Load on RxD	15 pF	15 pF

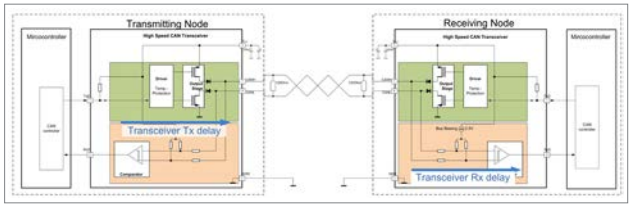


Figure 10: Typical communication path in CAN (Photo: Infineon)

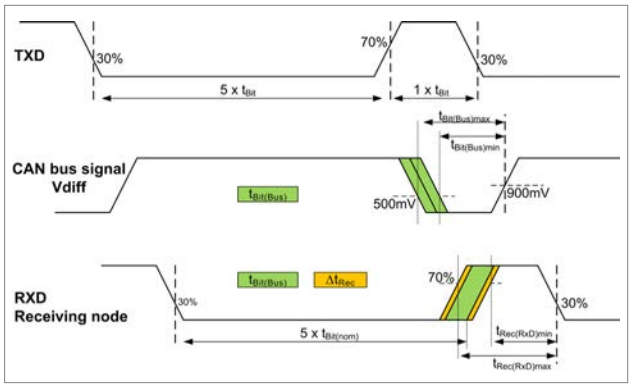


Figure 11: Illustration of the recessive bit width on a receiving node (Photo: Infineon)

Bit-timing symmetry in a CAN FD network

Figure 10 shows a typical communication path from a transmitting node to a receiving node in a network. The transmitter Tx delay, the network, and the asymmetry of the receiver modify the bit-width. In a worst-case scenario, the variation of the RxD recessive bit time on a receiving node is the sum of the transceiver Tx delay symmetry and the transceiver Rx delay symmetry (see Figure 11).

Table 4 provides the possible variations of the recessive bit-width on a receiving node with a 60 Ω ‖ 100 pF busload. This calculated value is the sum of the transceiver Tx delay symmetry and the transceiver Rx symmetry. The impact of the network is excluded in this calculation. The rising edges may jitter. The falling edges are stable, as this is the edge on which a CAN node synchronizes and the transmitter drives actively the dominant bus-level.

Table 4: Variation of the recessive bit-width on a receiving RxD

Data-phase bit-rate	1 Mbit/s	2 Mbit/s	5 Mbit/s
$t_{Bit(RxDrec)}$ **min**	n. a.	370 ns	110 ns
$t_{Bit(RxDrec)}$ **max**	n. a.	570 ns	225 ns
$t_{Bit(Bus)}$ **nom**	1 µs	500 ns	200 ns

Table 5: Deviation of a 2-Mbit/s transceiver to the nominal bit time

Parameter	**Bit-width**		**Nominal bit-time deviation**	
	min	**max**	**min**	**max**
Loop-delay symmetry	400 ns	550 ns	-100 ns	50 ns
Transceiver Tx delay symmetry	435 ns	530 ns	-65 ns	30 ns
Transceiver Rx delay symmetry	-65 ns	40 ns	-65 ns	40 ns

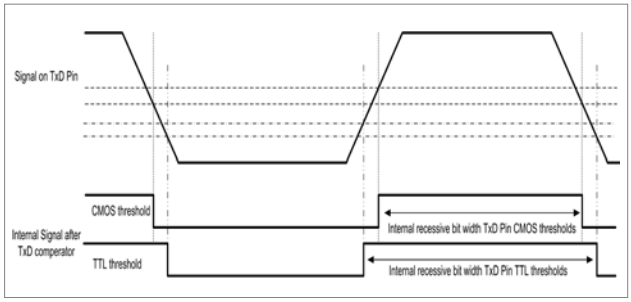


Figure 12: Transceiver internal bit-width modification caused by TxD input thresholds

Table 6: Calculated bit-width variation of a 2-Mbit/s transceiver used in a 1-Mbit/s network

Parameter	Calculated bit-width		Nominal bit-time deviation	
	min	max	min	max
Loop-delay symmetry	900 ns	1050 ns	-100 ns	50 ns
Transceiver Tx delay symmetry	935 ns	1030 ns	-65 ns	30 ns
Transceiver Rx delay symmetry	-65 ns	40 ns	-65 ns	40 ns

Table 7: Deviation of a 5-Mbit/s transceiver compared with the nominal bit-time

Parameter	Calculated bit-width		Nominal bit-time deviation	
	min	max	min	max
Loop-delay symmetry	170 ns	270 ns	-80 ns	20 ns
Transceiver Tx delay symmetry	205 ns	260 ns	-45 ns	10 ns
Transceiver Rx delay symmetry	-45 ns	15 ns	-45 ns	15 ns

Table 8: Calculated bit-width variation of a 5-Mbit/s transceiver used in a 4-Mbit/s network

Parameter	Calculated bit-width		Nominal bit-time deviation	
	min	max	min	max
Loop-delay symmetry	170 ns	270 ns	-80 ns	20 ns
Transceiver Tx delay symmetry	205 ns	260 ns	-45 ns	10 ns
Transceiver Rx delay symmetry	-45 ns	15 ns	-45 ns	15 ns

Table 9: Calculated bit-width variation of a 5-Mbit/s transceiver used in a 2-Mbit/s application

Parameter	Calculated bit-width		Nominal bit-time deviation	
	min	max	min	max
Loop-delay symmetry	420 ns	520 ns	-80 ns	20 ns
Transceiver Tx delay symmetry	455 ns	510 ns	-45 ns	10 ns
Transceiver Rx delay symmetry	-45 ns	15 ns	-45 ns	15 ns

The range marked in green is the variation of the transmitter and the range marked in yellow is the variation of the receiver. To analyze the worst-case scenario, both parameters must be added. For 2 Mbit/s and 5 Mbit/s, the scenarios are described in the following chapters.

Symmetry for networks up to 2 Mbit/s

For data phase bit-rates between 1 Mbit/s and 2 Mbit/s, a transceiver specified for 2 Mbit/s should be chosen. The jitter at the RxD pin at the receiving node for bit-rates below 2 Mbit/s can be calculated.

The maximum and minimum recessive bit-length $t_{Rec(RxD)}$ seen by the receiving node can be calculated by the following formulas (t_{Bit} nom = 500 ns):

$t_{Rec(RxD)}$ max = $t_{Bit(Bus)}$ nom + ($t_{Bit(Bus)}$ max - $t_{nom(2Mbit/s)}$) + Δt_{Rec} max

$t_{Rec(RxD)}$ min = $t_{Bit(Bus)}$ nom + ($t_{Bit(Bus)}$ min - $t_{nom(2Mbit/s)}$) + Δt_{Rec} min

In Table 5 the deviation of the symmetry parameter to the nominal bit-time is calculated. These deviations of a transceiver are bit-rate independent. A transceiver has no information about bit-rate and protocol. A transceiver transmits the level on the TxD pin on the bus-pins up to the maximal specified bit-rate. Based on this experience the deviation for 1 Mbit/s using a 2-Mbit/s transceiver can be calculated (see Table 6).

Symmetry for networks up to 5 Mbit/s

For bit-rates up to 5 Mbit/s, a transceiver specified for 5 Mbit/s should be chosen. The jitter at the RxD-pin can be calculated. The maximum and minimum recessive bit length $t_{Rec(RxD)}$ seen by the receiving node is calculated with the following formulas:

$t_{Rec(RxD)}$ max = nominal bit time + max TX delay sym. deviation + max value of Δ_{tRec}

$t_{Rec(RxD)}$ min = nominal bit time + min TX delay sym. deviation + min value of Δt_{Rec}

These values consider only the influence of the transceiver. Additional effects like clock tolerance and the phase shift of the network are not considered.

Note that the deviations given in Table 7 are bit-rate independent. A transceiver has no information on bit-rate and protocol but transmits the level on the TxD pin on the bus-pins up to the maximum specified bit-rate. Based on this experience the deviation for 4 Mbit/s with a 5-Mbit/s transceiver can be calculated (see Table 8). The calculated deviation for 4 Mbit/s are shown in Table 8.

In a real network, a lot of ringing can be found at the end of a dominant-to-recessive transition. This causes a reduction of the recessive bit-time or limits the network topology. Using a 5-Mbit/s transceiver in a 2-Mbit/s network gives a little bit more margin for the network topology. Table 9 provides the calculated figures of the variation of a 5-Mbit/s transceiver in a 2-Mbit/s network. As shown, the spread is smaller and especially the recessive bit-width variance on the RxD-pin of a receiving node is much smaller compared to a 2-Mbit/s transceiver using the same network topology (see Table 10).

Table 10: Comparison of the recessive bit-width on a receiving node

CAN FD transceiver	5-Mbit/s transceiver	2-Mbit/s transceiver
$t_{Bit(RxD)}$ **min**	410 ns	370 ns
$t_{Bit(RxD)}$ **max**	525 ns	570 ns
$t_{Bit(RxD)}$ **nom**	500 ns	500 ns
Bus-load	60 Ω ‖ 100 pF	60 Ω ‖ 100 pF

The difference is 40 ns. This margin makes the network more reliable against noise and EMC jitter. When designing the physical CAN FD network, the PLL jitter, the propagation delay, and the symmetry need to be considered. The interface between micro-controller and transceiver has to be taken into account, too.

Interface between micro-controller and transceiver

Depending on the micro-controller port, which is used for TxD and the length of the board wire, the propagation delay can be up to 50 ns. Due to the high capacitive load in case of a long wire on the ECU board, the slew-rates are slow, too. To get no additional asymmetry, the TxD-input thresholds should be symmetric (CMOS level) to the transceiver I/O supply.

A TTL-level based TxD input threshold causes an internal modification of the bit-width depending on the slew-rate of the TxD input signal. Figure 12 illustrated such a bit-width modification. The symmetry of the slew-rates must be taken into account too. The higher the bit-rate, the higher is the need for a symmetric slew-rate of the micro-controller's TxD signal and the transceiver RxD signal. ◀

Author

Magnus-Maria Hell
Infineon Technologies AG
magnus-maria.hell@infineon.com
www.infineon.com

Magnus-Maria Hell started his career as a designer for automotive smart power ICs. For more than 20 years, he has been working as a transceiver designer and system engineer for automotive in-vehicle networks.

Related articles

- Magnus-Maria Hell (Infineon): The physical layer in the CAN FD world
- Tobias Islinger, Yasuhiro Mori (Denso): Ringing suppression in CAN FD networks
- Holger Zeltwanger (CiA): 15th iCC: Focus on CAN FD
- Tony Adamson (NXP): Hybrid CAN and CAN FD networks

CAN FD plugfest: Testing the robustness

Plugfests are a kind of interoperability test. The devices under test (DUT) have to proof themselves in a system. In Detroit, participants tested the robustness of CAN FD implementations.

CAN FD as standardized in ISO 11898-1:2015 has been implemented by several parties. To proof the interoperability of these implementations, CiA organizes so-called plugfests. The last CAN FD plugfest took place in Detroit in April. About 20 different parties participated. The attendees tested among other things the robustness of their implementations.

The robustness in CAN FD networks is mainly determined by the oscillator tolerance and the "phase margin". Dr. Arthur Mutter from Bosch has described this in detail in one of his iCC papers (Robustness of a CAN FD bus system – about oscillator tolerance and edge deviations). One important measurement is the tolerance against edge shifts. In the test in Detroit, a linear bus-line topology with short stubs was used. The termination resistors were located at both ends of the cabling. The bit-rates were set to 500 kbit/s in the arbitration phase and 2 Mbit/s in the data phase, as this is the bit-rate combination which is targeted by most users. In Detroit, pattern generators were used to send the manipulated CAN FD frames. About 10 different robustness tests were performed. These covered edge shifts at various positions of the frame, bit flips of reserved bits, glitches, and oscillator tolerance. Here a few exemplary results are sketched.

The edge shift test in the data phase: A dominant-to-recessive edge (being the more sensitive one) was shifted back and forth. All parties could correctly receive the frames with an edge shift of -125 ns up to +300 ns. These values are close to the theoretical limits with an ideal physical layer. In general, the rising edges (dominant-to-recessive) are more likely to jitter; the falling edges (recessive-to-dominant) are more stable as the bus line is actively driven by the transceivers in the dominant state.

The oscillator tolerance test: In this test regular CAN frames were transmitted. The transmitted bits were scaled in length to emulate a transmitter with high oscillator tolerance. All parties could correctly receive the frames when the transmitter had an oscillator frequency in the range f_{nom}*(1 - 1,5 %) … f_{nom}*(1 + 2,5 %). The values exceeded the theoretical limits of the oscillator tolerance by far, because here regular CAN frames were used instead of worst-case bit patterns.

The glitch test: In this test glitches were introduced in the res-bit. All CAN FD controllers ignored them as specified in ISO 11898-1:2015. This will be part of the conformance testing as standardized in ISO 16845-1, which has not been published yet. Publication is expected in the next months. Also, the shorting of the res-bit (just 1,85 µs instead of 2 µs, meaning the BRS-bit started earlier) was successfully tested.

On the second day of the CAN FD plugfest, the wiring harnesses provided by Ford and General Motors (GM) were tested. Both were linear topology networks with non-terminated stubs. Individual stub lengths were less than 1,7 m. All edge-shifting tests were successful at a data phase bit-rate of 2 Mbit/s, even if there was some ringing on the bus line. To reduce the ringing in case of the GM cabling, the RSC (ringing suppression circuit) from Denso (see March issue of CAN Newsletter 2016) was used at the longest stub. Figure 1 shows bits in the data phase with and without ringing suppression. It was the first time that the RSC – originally invented to reduce ringing in star and hybrid topologies – proofed its functionality in quasi-linear networks.

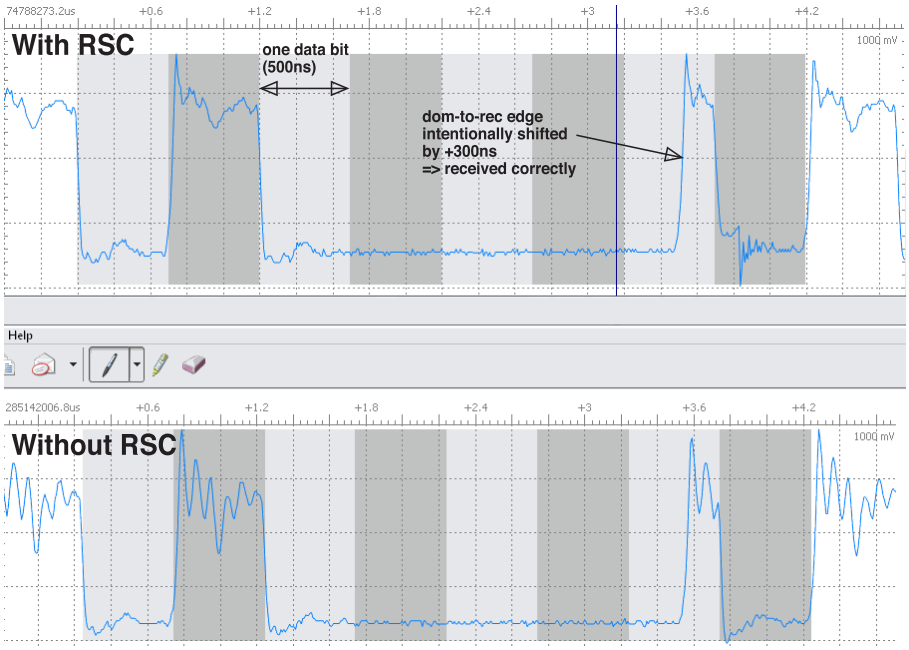


Figure 1: GM wiring harness at 2 Mbit/s in the data phase – with (top) and without (bottom) RSC-capable transceiver at longest stub

The plugfest demonstrated the robustness of linear CAN FD networks for data phase bit-rates of 2 Mbit/s. The provided wiring harnesses also worked at higher bit-rates. With optimized device and network designs even higher bit-rates will be robust enough for automotive and industrial application requirements. Nevertheless, additional robustness tests should proof this.

The next CAN FD plugfest takes place on June 2 and 3, 2016 in Nuremberg. If CiA members and OEMs request additional plugfests, CiA schedules them. CiA also organizes plugfests for other purposes: regularly plugfests proof the interoperability of CANopen Lift devices compliant to CiA 417 and from time-to-time also for CANopen subsea devices compliant to CiA 443. Other plugfests can be scheduled if a sufficient number of CiA members ask for them.

Author

Holger Zeltwanger
CAN in Automation
headquarters@can-cia.org
www.can-cia.org

CAN Newsletter Online

The CAN Newsletter Online sister publication provides brief product-related information. For more details please visit www.can-newsletter.org.

CAN FD plugfest
Robust operation of controller IP Core
The CAN FD controller IP Core by Cast met or exceeded bit-rate and error handling tests in its second CAN FD plugfest. It ran in representative automotive networks from Ford and General Motors.

Read on

CAN FD plugfest
Proof of robustness for CAN FD
Happy faces, some minor issues, and two days full of experience: The second CAN FD plugfest in Detroit saw about 40 participants from 20 parties. To the organizers, the plugfest proofed the robustness of the CAN FD technology.

Read on

CAN FD
Plugfest in Detroit
CiA has organized a CAN FD plugfest in close cooperation with General Motors (GM). About 14 companies tested their products for interoperability.

Read on

Plugfest
CAN FD ringing suppression
CiA has organized a CAN FD plugfest in Nuremberg. Several companies tested their products on interoperability using different network topologies.

Read on

Using CANopen instead of analog signals

Analog signal paths are still widely used in new installations. Does that really make sense anymore? Analog signaling is outdated when it comes to accuracy, dependability, diagnostics, and manageability.

The required dependability of communication increases rapidly when higher control performance is required. The adoption of telemetry, remote monitoring, and controls also requires a higher communication dependability, because no human operators exist as local backups. Especially IoT (Internet of Things) applications need to receive accurate and correct information. If the information is incorrect or inaccurate, it is not just useless and wastes analytics services, it is also, most probably, misleading for future decisions.

Traditional instrumentation based on analog signaling is outdated in many areas. Thanks to the fact that it is the traditional approach, there is a lot of reliable information available. Reliability also applies to the system assembly and service, wherever increasing efficiency requirements expect faster throughput and better quality. Efficiency means not only automated actions, but also smaller numbers of corrections as an integral part of the assembly and service work.

Sensing accuracy

A detailed analysis of the sensing accuracy difference between analog sensors and CANopen sensors has already been published [1]. The provided accuracy numbers apply only for the best-case conditions, where the analog signal path is in perfect condition. Typical low-cost pressure transmitters provide a digital linearization. After this, the additional DA (digital-analog) and AD (analog-digital) conversions in the analog instrumentation introduce additional inaccuracies caused by a quantization noise [2]. However, the weakest point in the analog instrumentation is the signal path from the sensor, over the cabling with connectors into a consuming device.

Analog transmitters require a supply voltage (VS) within a special range. Transgressions of this range are only visible by a deviated output signal. A constrained supply voltage range often requires the use of a dedicated sensor supply voltage instead of the main supply voltage. In some cases, the static inaccuracy (caused e.g. by the signal path or deviations in the input impedance of the consuming device) may be compensated by field calibration, which is time-consuming and sensitive to human mistakes. Deviations caused by dynamic conditions, such as voltage drops (caused e.g. by cranking of a diesel engine or by large variations in power consumption of other electrics), cannot be compensated.

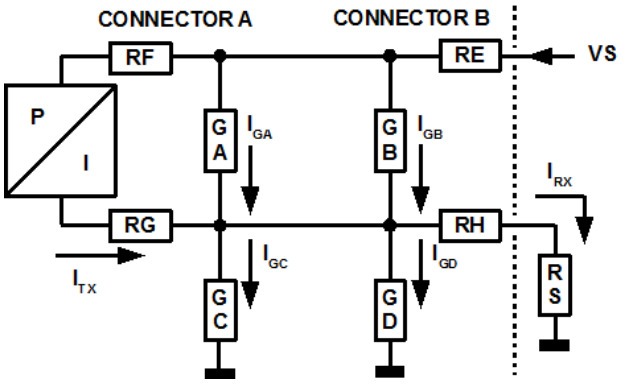


Figure 1: Practical analog sensor connection with standard fault modes included [10], where ITX is signal sent by the sensor and IRX signal received by the consuming device

In the example depicted in Figure 1, it can be seen that under error conditions the sensor signal ITX may be affected by a random set of conductances and resistances caused by typical connection failures. Conductances and resistances randomly result from various problems in the connections, as the latter are exposed to varying environmental conditions. It is obvious in Equation 1 that as long as only the shunt resistance (RS) exists in the signal line, it works as designed. If an additional series resistance occurs (e.g. due to corroded contacts, worn or deformed connectors), the available supply voltage is not sufficient to provide the required voltage difference over the sensor (U_{PI}). Only the required U_{PI} would enable the transmitter to drive the full current (I_{RX_MAX}).

$$VS = U_{PI} + I_{RX\_MAX} * (RE + RF + RG + RH + RS) \quad (1)$$

CANopen transmitters typically operate in a wide supply voltage range. There is no correlation between the supply voltage changes and measurement accuracy. Furthermore, any problem in the transmission line may lead to a delayed or blocked delivery of the signal value, but not to a degradation of the accuracy.

Dependability

The CAN message structure provides numerous safeguards: CRC, fixed fields, fields affecting the message length, and continuous monitoring of the transmitted bits [3]. CANopen adds more safeguards, including application level monitoring of the message length, update of the ▷

deadline, and signal plausibility supported by the configuration management process [4]. The CAN (and also CANopen) fault confinement mechanism provides an additional safeguard against error bursts. The availability of several nodes in a network improves the MTTFd (mean time to failure) further, due to the continuous monitoring of the network by all connected nodes [5]. This leads to a minimal probability of random residual transmission errors caused by external disturbances. The effect of such errors is minimal, because either the next update provides the correct result or a timeout will be detected. Layered MTTFd computation models for CAN communication with CANopen application layer services has proved that the probability of getting two consecutive failed and undetected messages through the network is extremely rare [6].

In an analog sensor, all signal paths are sensitive to the cable length, cable failures, connection mistakes, and various connector failures (e.g. corrosion, leaked liquids, dirt inside connectors) as depicted in Figure 1. Due to a missing packet coding, the only diagnostics feature in analog signals is the out-of-range detection. Before it makes sense to check the signal validity, validating the sensor should be possible. Typical analog sensors can provide only the primary signal (ITX) to the consuming device, but no information about the sensor's identity. Thus, the consuming device has no possibility to validate whether the producing device has the correct identity and the correct measurement range or not. Thus, a scenario is possible where all redundant sensors are replaced by those with a wider range, leading to accidentally increased safety thresholds, without any possibility for consistency checking by the control system itself. Under certain conditions, even a missing transmitter may not be detected in a single-channel system.

Analyzing failure distributions in mechatronic systems shows that various wiring, cabling, and connector failures dominate [7]. As actually required by the functional safety standards, such conditions must be seriously considered. It is clearly written that in addition to the inputs, logics, and outputs, also the "interconnection means" must be analyzed [8]. Residual error characteristics of analog signaling and CANopen communication have been compared. The results show that in this area the standard CANopen communication is better than the analog connection by several magnitudes.

Diagnostics

Diagnostics capabilities may be analyzed based on Figure 1, too. It is obvious in Equation 2 that there cannot be a systematic way to determine the signal line condition by measuring the IRX only. Adding of a sensor-specific supply with current sensing does not help either, because a random set of conductances (GA, GB, GC, GD) might exist in parallel with the sensor connection. Such conductances represent commonly existing and well-known error scenarios, mainly caused by the moisture in the connectors. Any external diagnostics tool might introduce deviations in the signaling, which potentially leads to inaccuracies and potentially erroneous results.

$$I_{RX} = I_{TX} + I_{GA} + I_{GB} - I_{GC} - I_{GD} \qquad (2)$$

Extreme cases appear when an analog transmitter tries to signal a failure condition by sending either a current less than 4 mA or higher than 20 mA. Properly transmitted fault condition may be transformed to a totally valid look-a-like received process value. Furthermore, it cannot be guaranteed that such a value cannot be close enough to the actual process value indicated by the optional additional parallel channels (redundant measurement), typically used in old-fashioned safety controls. The sensor may also be missing and other typical connection failures may exist in the cabling, resulting in a totally look-a-like "valid" process value.

In CANopen systems, a standardized start-up mechanism exists that enables a detailed verification of the system structure before starting the full operation. After start-up, persistence of the verified structure may be simply monitored based on the heartbeat (HB) protocol. Another parallel mechanism for signal validity verification is the monitoring of signal updates via RPDO (receive process data object) timeout monitoring. The HB provides the rough operational state information of the producing node. The RPDO monitoring supplements the HB by providing timeliness information of the last signal update. Each combination of boot-up, HB, and RPDO failures provides an indication of potential error source, as summarized in Table 1. More detailed information may be retrieved from the object dictionaries of both (local and remote) nodes.

In order to increase runtime operation monitoring, CANopen provides a couple of state machines at the top of the dependable network communication. The NMT state machine provides a managed device start-up with consistency checks. Device profiles for electric and hydraulic drives provide a supplemental device state machine, which enables redundant and parallel control of the actual drive operation [9]. For I/O-oriented profiles a simpler error state machine exists, providing local error reaction capabilities for the cases where communication to the host has failed. Each CANopen network can be analyzed using an appropriate tool and medium attachment.

Manageability

The advantages of a standardized design process have been described in some publications [13]. It is clearly evident that the following systematic design approach results in a significant efficiency boost in the design. In addition, such an approach enables a streamlined assembly and service activities by error input for such actions. Standardized information access interfaces – CANopen design files, tool integration, and device configuration management mechanisms – are the key factors enabling error-free assembly and service activities.

After the managed assembly and service actions, each CANopen system start-up provides a regular and accurate consistency check. A standardized CANopen network start-up process may consist of the system structure checking i.e. which kind of devices are installed in which position. In the simplest case, only the appropriate device profiles match and the most accurate configuration leads to checks of the full identity, including serial number of each individual device. Thus, CANopen control systems can provide intrinsic consistency checks for the entire system structure, which only need to be used in the relevant control systems.

Reusability and maintainability

Reusability and maintainability are important factors in the industrial way of working. Using the standardized CANopen device profiles and the device classes within the profiles, CANopen enables intrinsic second sourcing among standard devices and replacing obsolete devices with new ones without any changes in the application software. A standardized design process provides required support for managing such replacements and upgrades. Device profiles also supplement the start-up process in the flexible part support – when only the device type is checked, any compliant device from any vendor may be installed. This provides easy logistics without changes in the control software and without risk of accidentally changing the system behavior. Usage of standard device connectors and cables enables fast and reliable physical layer assemblies.

One significant advantage of the CANopen device profiles is that they provide standardized mechanisms for managing signal units and scaling [12]. Especially in sensor device profiles (e.g. CiA 404), there are typically SI units used by default. Thus, the CANopen interface forms a harmonized interface and the whole scaling and calibration process is performed by each sensor. Such an approach enables more extreme changes in systems, e.g. replacing a

Table 1: Simplified node state decoding based on boot, HB and RPDO status

Boot-up	Heartbeat (HB)	RPDO	Indication
No			The node does not exist in the network. Any HB or RPDO from this node-ID is faulty.
Yes	No	No	The node existed, but may have been lost after start-up and state "unknown", or after a configuration error.
Yes	Yes		The node existed, but may have been lost after start-up or a misconfigured HB. An invalid node may produce the RPDO.
Yes	Yes	No	The node exists, but may not be operational or may have a PDO configuration problem.
Yes	Yes	Yes	The node exists, its state is known and signals received from it are up-to-date.

250-bar pressure transmitter by a 400-bar version, when a higher pressure-peak-tolerance is required. No changes are required in such a case, as long as the device profile specific signaling with SI units is used. A further advantage of such standardized signal interfaces is that calibration has been included into the sensor itself. The main consequence is that the vendor calibrates the sensors and the field calibration is no longer required. This makes the sensors more cost-efficient in use.

Analog signals are often connected wire-by-wire in the field, in order to virtually save material costs. Actually, this increases the labor costs and decreases the manageability by increasing the connection work effort and the number of potential mistakes, when compared with the use of CANopen systems [11]. Due to the large number of connectors (caused by point-to-point connections), a risk for wrong connections on the connector level remains anyway. The use of analog signals leads to the use of electrical units in the signal path, instead of SI units according to the process. This introduces a significant increase in the system-instance-specific calibration and scaling actions, decreasing the efficiency of the assembly and service and increasing the number of mistakes.

Discussion

The difference in accuracy is significant, mostly due to the packet coding provided by CANopen communication. Dependability is another key factor. Unlike analog signaling, the typical behavior of CANopen communication is fail-silent. In case of a fatal transmission-line problem, potentially invalid process values are not updated and a good basis for reliable error handling exists. Furthermore, the dependability of CANopen communication increases when the number of nodes in a network increases. It is possible to differentiate between sensor failures and transmission line failures in a single-channel CANopen system. With analog signaling, getting comparable accuracy and confidence requires 3-way redundant analog sensors.

Analog instrumentation is still popular, because it looks cheap at first glance, but this is only based on the bill of materials for the main components and by forgetting the higher assembly labor costs and the costs of additional components. While the CANopen-networked sensing approach consists only of sensors and network cables, the analog sensing approach consists of sensors, I/O devices, and cables from each individual sensor to the I/O devices as well as the uplink connecting the devices to the application-processing platform.

Analog sensing is also commonly regarded as easy-to-diagnose, which is actually not true. For example, adding external measurements to the current loop requires a special adapter and multimeter to be added in between each signal line. This leads to an interruption of the measurement, unlike adding a CAN analyzer to the service connector of a network. Even in the case of a single-channel measurement, a significant difference exists. In analog signaling, a significant risk exists to disturb the entire measurement by ▷

References

[1] Bildstein M., Heusel S., Digital transmission in pressure sensors, Wika Alexander Wiegand SE & Co. KG, CAN-Newsletter, 1/2015, CAN in Automation, pp. 24-27

[2] Razavi B., Data Conversion System Design, IEEE Press, New York, USA, 1995, ISBN 0-7803-1093-4, p. 256

[3] Unruh J., Mathony H.-J., Kaiser K.-H., Error Detection Analysis of Automotive Communication Protocols, SAE technical paper 900699, SAE, p. 10

[4] Saha H., CANopen safeguards, CAN Newsletter, 1/2015, CAN in Automation, 2015, pp. 36-39

[5] Unruh J., Mathony H.-J., Kaiser K.-H., Eror Detection analysis of Automotive Communication Protocols, SAE technical paper 900699, SAE, p. 10

[6] Saha H., Huikkola M., Analysis of residual errors and their consequences in CANopen systems, Proceedings of the 14th iCC, CAN in Automation, 2013, p. 7

[7] Hänninen S., Järvenpää J., Reunanen M., Suominen J., The failure of mechatronic components and devices, Technical note 15/90, The central of Finnish metal, machinery and electrical industries, 1990, ISBN 951-817-479-2 (in Finnish)

[8] Hietikko M., Malm T., Saha H., Comparing performance level estimation of safety functions in three distributed structures, Journal of Reliability Engineering and System Safety, Issue 134, Elsevier, 2014, pp. 218-229

[9] Saha H., CANopen safeguards, CAN Newsletter 1/2015, CAN in Automation, 2015, pp. 36-39

[10] Safety of machinery – Safety-related parts of control systems – Part 2: Validation, ISO 13849-2

[11] M12 - Pin assignments for I/O boxes and sensors/valves, DESINA, 2003

[12] Saha H., SI-Unit and scaling management in CANopen, CAN-Newsletter 3/2013, CAN in Automation, 2013, pp. 30-34

[13] Saha H., Improved management of CANopen-based distributed control-systems, Proceedings of the 2nd MMC, CAN in Automation, 2015, p. 8

additionally connected stuff. There exists also a significant difference in the signal visualization – analog measurement is typically done in mA, which must be transformed into SI units specific to the measurements. A multimeter enables a single measurement only without the possibility to save it into a log file. A networked sensing system typically transfers signals already converted into the SI units, and scaling and representation can be automatically performed during the measurement set-up, into communication description (DBC) file in the case of CANopen. All values in a network can be measured and optionally saved in a log file with a single tool connection.

CANopen implementations in the field have been strange. Standard control systems are mainly based on the signal transfer (PDO: process data object) with an optional device monitoring (HB). The so-called safety systems have been mainly implemented with the safety-relevant signal transfer (SRDO: safety-relevant data object). Standard services with RPDO monitoring may provide a nice intermediate approach, but with much less complexity and bandwidth. Human mistakes during assembly and maintenance are more common than just the MTTFd of the communication and devices. Each known case with accidentally increased MTTFd of the communication was caused by human mistakes. Main reasons are the use of improper cabling components or an improper network structure.

Conclusions

Analog signaling was compared with CANopen communication in four main areas: accuracy, dependability, diagnostics, and manageability. It is obvious that analog signaling is outdated in all areas. The most significant area where CANopen has significantly better characteristics is dependability. Together with diagnostics, dependability acts as a background variable for safety performance, which often drives the control system development. Despite these hard facts, it is amazing how often the old and unreliable approach is used. Dependability of the latest remotely operated systems must be much higher, because there are no human operators as backup anymore.

In addition to a more reliable communication, CANopen enables a more efficient design process. Moving from a manual to a computer-aided design process is also strongly recommended by the safety standards. In this area, CANopen provides excellent support by means of standardized design information storage and exchange file formats as well as design process. The main open question is in how many applications the standard CANopen communication with its built-in safeguards could be used? Becoming able to use a simple standard communication could open easy upgrades of outdated analog implementations. ◀

Author

Dr. Heikki Saha
TK Engineering
heikki.saha@tke.fi
www.tke.fi

FAULHABER

FAULHABER Motion Control

Feel the Power

NEW

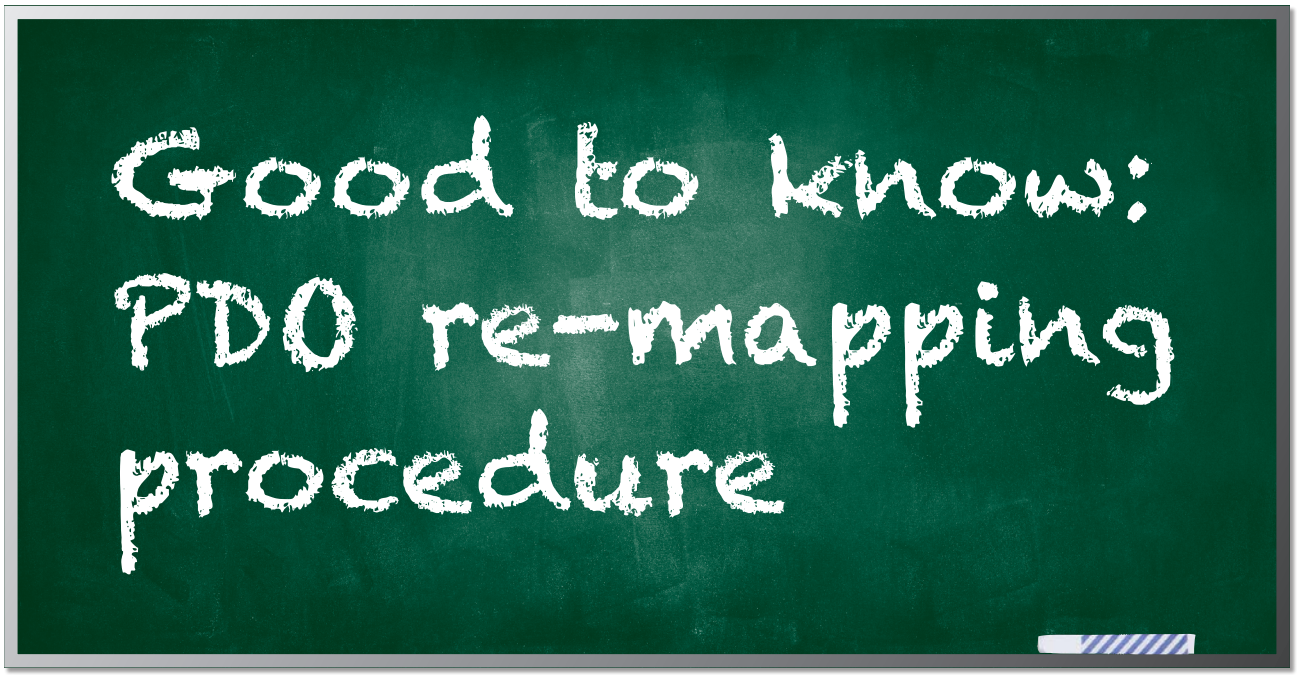
WE CREATE MOTION

FAULHABER Motion Controller Series MC 5004 / 5005 / 5010

Decentralised intelligence promotes maximum performance: our new motion controllers are optimised for the FAULHABER drive program and extract the maximum from any motor – whether DC-micromotors, brushless motors or linear DC-servomotors. And, equipped with USB, RS232, EtherCAT and CANopen interfaces, they secure future connections. Ready for networked industry? It's in your hands with FAULHABER.

www.faulhaber.com/mc/en

Easy commissioning with the new Motion Manager 6



PDO mapping is one of the essential features of CANopen: it describes which individual process variables in the data field of a PDO are transmitted. CiA 301 requires a dedicated re-mapping procedure.

The Process Data Object (PDO) service allows exchanging one or several process variables in one single CAN message. The PDO mapping parameter describes which objects in the CANopen object dictionary are transmitted by the sender. The PDO receiver uses also a PDO mapping parameter, which specifies where to store the received process data in the CANopen object dictionary. The PDO mapping parameter of the transmitter and the sender may use different pointers (16-bit index and 8-bit sub-index) depending on the CANopen profile.

In some simple devices, the user does not have the possibility to configure the PDO mapping parameters. This is called static PDO mapping (take it or leave it). More sophisticated devices provide variable PDO mapping. This means the system designer can re-configure the default PDO mapping or generate new PDOs. Normally, this is done in the NMT pre-operational state, when the PDOs are disabled. Of course, the user can also reconfigure the PDO mapping in the NMT operational state, but then it is necessary to avoid inconsistencies in the PDO mapping on the producer and the consumer side. To avoid this, the PDO must not be produced until the entire reconfiguration is finished.

The CiA 301 application layer specification requires a dedicated re-mapping procedure:

- "Destroy" the TPDO by setting the valid bit to 1_b of sub-index 01_h of the TPDO communication parameter.
- Disable PDO mapping by setting the sub-index 00_h of the PDO mapping parameter to 00_h.
- Modify PDO mapping by changing the values of the corresponding sub-indices of the PDO mapping parameters.
- Enable PDO mapping by setting the sub-index 00_h to the number mapped process data.
- "Create" a TPDO by setting the valid bit to 0_b of sub-index 01_h of the TPDO communication parameter.

If the CANopen device detects that the index and sub-index of the mapped object does not exist or the object cannot be mapped during step 3, the CANopen device responds with the SDO abort transfer service (abort code: 0602 0000_h or 0604 0041_h). If the CANopen device detects that the RPDO mapping is not valid or not possible during step 4, the CANopen device responds with the SDO abort transfer service (abort code: 0602 0000_h or 0604 0042_h). This is tested in the CANopen conformance test.

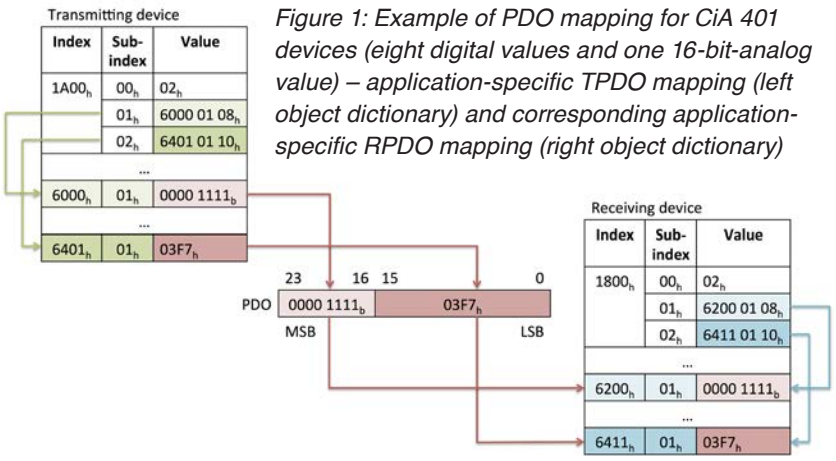


Figure 1: Example of PDO mapping for CiA 401 devices (eight digital values and one 16-bit-analog value) – application-specific TPDO mapping (left object dictionary) and corresponding application-specific RPDO mapping (right object dictionary)

Normally, the corresponding RPDO mappings need to be re-configured too. This should be done before the TPDO is enabled again. At least between step 4 and 5, all related RPDO mappings should be reconfigured, if necessary. Of course, the user can also first re-map all RPDO mappings (either between step 1 and step 2 or between step 2 and step 3).

By the way, the re-mapping in NMT operational state is called dynamic PDO mapping (e.g. in the CANopen feature list of CiA's Product Guide). If the CANopen device is correctly implemented, the RPDO re-mapping follows the same procedure as the TPDO re-mapping: "Destroy" the RPDO, disable the RPDO mapping, modify the RPDO mapping, enable the RPDO mapping, and finally "create" the RPDO. Of course, this should be done for all TPDO-corresponding RPDOs, if the TPDO is sent in multi- or broad-cast.

If the CANopen device receives a PDO that has more data bytes than the number of mapped data bytes (length), then the CANopen device uses the first data bytes up to the length and sends an EMCY message. If a CANopen device receives a PDO with less data bytes than the number of mapped data bytes (length), then the CANopen device sends an EMCY message with the error code 8210_h.

If the TPDO or RPDO re-mapping procedure is not followed, the CANopen device should not change the mapping entries and abort the SDO write service. The device should do this, for example, if the PDO has not been "destroyed" or the mapping has not been disabled. Note: The system designer is responsible for the consistency of the TPDO and the RPDO mapping parameters.

Author

Holger Zeltwanger
CAN in Automation
headquarters@can-cia.org
www.can-cia.org

Related article

- Holger Zeltwanger (CiA): Good to know: Optional is not "don't care"

Mapping of J1939 to CAN FD

CiA members have mapped SAE's J1939 application profile to the CAN FD data link layer. The related CiA 602-2 specification will be released soon.

The J1939-21 application layer specifies how to use the CAN-ID and the protocol that transmits the Parameter Groups (PG). The PGs and the single parameters are described in SAE J1939-71. Traditionally, the J1939 application profile is mapped to the Classical Extended Frame Format (CEFF) data link layer protocol using the 29-bit CAN-ID.

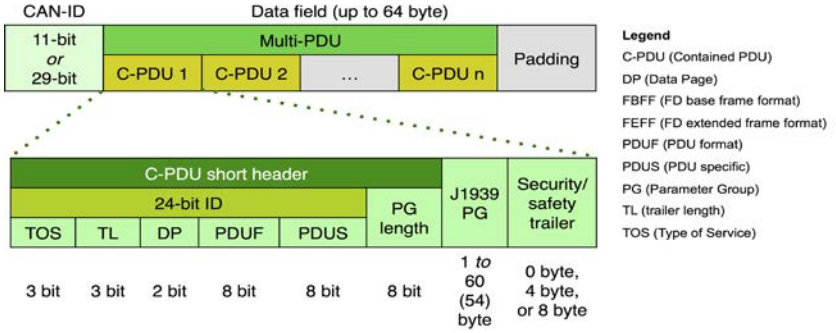


Figure 1: The Multi-PDU as defined in CiA 602-2 can be mapped into 11-bit as well as 29-bit CAN FD messages; the J1939 C-PDU contains one Parameter Group and a 32-bit header compliant with Autosar

Some European OEMs (original equipment manufacturer) of trucks need more bandwidth on their CAN-based in-vehicle networks. Additionally, they require higher throughput when downloading software or uploading diagnostic data. For this reason, some CiA members have started to specify the mapping of J1939 messages to CAN FD. It is intended to run the communication at higher bit-rates (e.g. 2 Mbit/s) and to use the extended payload of up to 64 byte.

Another requirement of the OEMs is the compatibility to Autosar. In order to allow a simple mapping of PGs as defined in J1939-71, a Multi-PDU (process data unit) is used in the CiA 602-2 specification. Such a Multi-PDU can comprise several C-PDUs (Contained PDU). The C-PDU combines a PG and a 4-byte (short) header as described in Autosar. A legacy PG is always 8 byte long. This means you can map in maximum five traditional PGs into one 64-byte CAN FD data frame considering the header. In the future, there may also be shorter and longer PGs, which gives the user more mapping flexibility. Of course this approach is a compromise. It requires some protocol overhead: 4 byte per C-PDU.

FD Base Frame Format (FBFF) as well as FD Extended Frame Format (FEFF) messages are supported. The 11-bit CAN-ID has the benefit that the "slow" arbitration phase is as short as possible. In both approaches, the CAN-ID contains the J1939 source address (SA). The J1939 PDU format and the PDU specific are part of the Autosar PDU short header. Consequently, ECUs (electronic control unit) need to parse all messages. Normally, CAN acceptance hardware filters cannot be used.

Besides the J1939-21 information (PDUF and PDUS), the C-PDU header also comprises a 3-bit Type of Services (TOS) field, a 3-bit information about the optional safety/security "trailer", and an 8-bit PG length indication (necessary, when other than 8-byte PGs are used). With this information, the receiver can interpret the received C-PDU.

The 11-bit CAN-ID provides the 8-bit SA and the 3-bit Protocol Indicator (PI). The PI distinguishes between Multi-PDU container (Autosar compliant), Autosar CAN-NM (network management), SAE address claiming, XCP (extended calibration protocol), J1939 TP connection management (TP.CM), J1939 TP data transfer (TP.DT), and TP extended addressing functional as well as physical (both are defined in ISO 15765-2). The usage of 29-bit CAN-IDs is specified, too. However, this would eat some bandwidth due to the longer arbitration phase (about 20 bit-times not considering stuff-bits). For this approach, CiA needs to request dedicated PDU 1s and PDU 2s from SAE, which is still on the "to do" list.

The usage of a security/safety trailer is indicated by the 3-bit TL (trailer length) sub-field. There may be no trailer, either a security or a safety trailer (32 bit or 64 bit), or a combined security/safety trailer (32 bit + 32 bit). These are placeholders, because the definition of security and safety protocols is not in the scope of CiA 602-2.

The mapping of the BAM or CMDT protocols as specified in J1939-21 into CEFF messages will not be changed, meaning the DLC (data length code) is always 8. The ▷

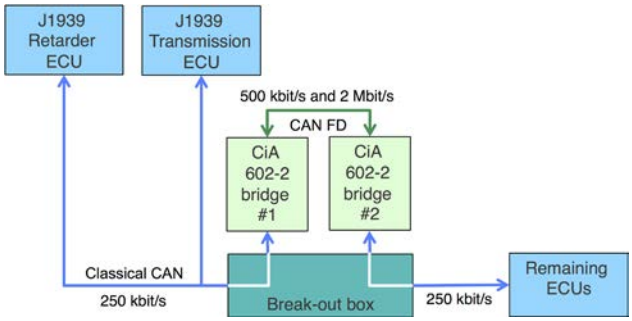


Figure 2: Test set-up for the proof of concept

mapping of these protocols to FBFF and FEFF messages is under development. The idea is to extend the TP.DT frame to 64 byte using 63 byte for the payload and one byte for a sequence counter. The total message size would be 16065 byte (255 x 63 byte).

Proof of concept

The concept of CiA 602-2 has been proofed by Vector and ZF. They simulated a traditional truck communication between ECUs. They opened the simulated J1939 network, introduced a simulated CiA 602-2 network using 500 kbit/s in the arbitration phase and 2 Mbit/s in the data-phase. The two bridges mapped the received J1939 messages into Multi-PDUs and sent them on the CAN FD network and vice versa. The time waiting on J1939 messages was increased in order to optimize the mapping of C-PDUs. This improved the achieved protocol efficiency, because most of the CAN FD messages used the maximum possible payload. On the other hand, when waiting to long, there was some time-outs on the application level.

This straightforward implementation is not really optimized by any means. It is just based on existing J1939 application software. The simulation was compared with the results in a real truck: The J1939 network was opened, two CAN FD bridges introduced, which communicated via a real CAN FD network. The results were the same as the simulated ones. There was a throughput win of about 80 %. The busload decreased from above 50 % to less than 10 %. Of course, not just the data-phase speed was increased to 2 Mbit/s, the arbitration bit-rate was also doubled (from 250 kbit/s to 500 kbit/s). Optimization regarding the periodic transmission, the length of PGs, and the usage of Change-of-State triggering can additionally decrease the busload.

Summary and outlook

The CiA 602-2 specification will be released soon as a Draft Standard Proposal (DSP). It can be used with unchanged J1939 application software, just adding a small bridge program mapping the PGs into Multi-PDUs. Additionally, the CiA 602-2 protocol stack can also accelerate the download of application software and calibration data as well as the uploading of diagnostic information. The CiA 602-2 protocols can also be used for other J1939-based solutions such as Isobus (ISO 11783 series) and NMEA 2000 (IEC 61162-3). In the "CAN 2020" seminars (free-of-charge for CiA members), they are a topic, too. ◀

Author

Holger Zeltwanger
CAN in Automation
headquarters@can-cia.org
www.can-cia.org

Enabling IoT connectivity

An astonishing estimation: in 2020, more than 200 billion devices will be connected to each other. To realize the power of the IoT, the main focus must be on the use of the data that these connected devices provide.

The ability to share data is based on intelligent gateways, which unlock these borders and enable companies to interconnect industrial infrastructure devices and secure data flow between e.g. a CAN network and the cloud. Data can be aggregated, shared, and filtered for analysis purposes – an action field for b-plus and the Gatebox 100.

Connecting a device to the Internet or with a cloud solution is possible with a lot of industrial PCs on the market. But it is not easy to determine which one of this wide variety matches your individual system. To work out the differences between all these industrial PCs is already a question of engineering. Specific interfaces and functions establish the right connection for the needed application. In most existing infrastructures, the basis is a data source and most likely an interface, e.g. analog or digital I/O or a bus interface like CAN.

Most IoT (Internet of Things) gateways offer typical PC interfaces for a simple IoT connectivity. When it comes to more industrial interfaces, the variety of products is smaller and often it is hard to find GPIOs or CAN on these gateways. Thus, most developers have to decide if it makes sense to build a second industrial PC with the required interfaces. The other option is to build and qualify a whole new industrial PC with IoT gateway functionality and at the end to reinvent the wheel to face two applications in one single box.

Knowing this challenge from customers, B-Plus developed an IoT gateway that is a compromise between building a whole new industrial PC and having an extra box for interface connectivity: The Gatebox 100 is a Box PC with flexible I/O shields, called Smart I/O Driver Interface (Siodi). Because of this concept, it is possible to implement additional interfaces without developing something new. It is irrelevant if the customer needs additional analog/digital I/Os, field buses like CAN, audio, or customer specific I/O cards. Predefined options, including scalable CPU Power, are already implemented.

Always up-to-date base unit with CAN options

The base configuration of the Industrial PC with only 150 mm width, 58 mm height, and 95 mm length brings data acquisition and communication together. The standard version with two Gigabit Ethernet interfaces provides two physically separated networks for the setup of firewall applications. Furthermore, the standard box provides two USB 2.0, one HDMI connector, and also two 9-pin Dsub connectors with variable EIA-232/EIA-485/CAN options.

Figure 1: Gatebox 100 standard variation

But how can you make sure that the industrial PC includes the perfect balance between computing power and power consumption in your application? With respect to the specific operating conditions or for software reasons, it is important to choose the fitting computing platform. For this reason, the Gatebox 100 is based on Smarc CPU modules which offer various performance classes and architectures. Hence, it can be equipped with Freescale i.MX6 series (ARM) as well as x86 solutions like Intel Quark X1000, Atom E38xx series or DM&P Vortex EX. For the future product life cycle, the next generation of processor modules can be used with the same box.

Variable I/O concept fits any application

To specify your requirements, this industrial PC is equipped with a special interface area where custom interfaces can be added. With the flexible Siodi shields of the Gatebox 100, system designers are able to configure an individual system. With a special system service called Siodi service, the I/O data is made available to the OS. Siodi service is capable of multiple processes, which lets you connect to the Siodi I/O shield with various software processes. For example, you can realize a logging application that runs 24/7 and in parallel a separate maintenance software can grab data from the same source or configure the I/Os. Having the I/O data in the OS, the Siodi API can be included directly in the application and connected to the cloud – without any extra way regarding the shield functions.

One key aspect is the connectivity, because getting available data into the cloud is the main goal of an IoT gateway. The Gatebox 100 has options for wireless connections, like WWAN, WLAN, or LTE to connect to the cloud, and options like CAN or digital I/Os to connect to sensors and the machine.

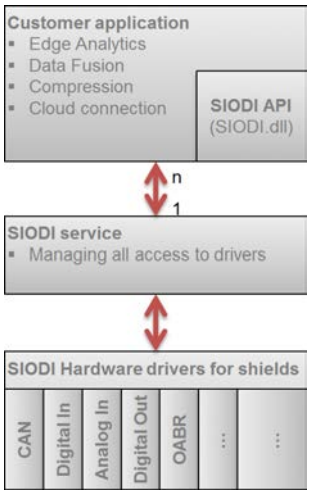


Figure 2: Siodi software architecture

In real time and measurement environments, it is important to get machine or sensor data within temporal correlation between different machines. The gateway offers a CTSS option where the Ethernet port utilizes IEEE1588/802.1AS to synchronize the time within a network. With this time sensitive networking option (TSN), it is possible to acquire sensor data from different data sources, e.g. more gateways, and to send this data to the cloud for analysis.

Robust 24/7 design

A lot of companies are already using industrial PCs for intelligent communication between their machines. Most industrial PCs are developed for installation in air-conditioned cabinets and run 24/7. But what happens with applications in harsh environments? What about all the systems that must endure fluctuating temperatures or voltages, for example outdoor applications?

Especially for these requirements, B-Plus developed the Gatebox 100: it is a robust, small, but powerful industrial PC, which meets the challenges of outdoor operation maintenance-free. It even ensures reliable operation in an operating temperature down to -40 °C, which makes it suitable for the use in outdoor cabinets. In order to meet the requirements of industrial applications, B-Plus has created a 24/7 endurance runner, which is completely maintenance-free. The industrial PC needs no fan, no battery, and also no moving parts. The passive cooling concept, super caps, and industrial 2,5-inch or M.2 SSDs, guarantee reliable operation and reduce service costs.

In some environments, voltage fluctuations can also occur. With standard PC hardware, you will get undefined states or reboots of your PCs. To avoid this, the IoT gateway has a 6,5 V_{DC} to 32 V_{DC} wide range input. To bring existing applications to an IoT infrastructure, it is necessary to find a good spot to mount the gateway. The gateway offers various mounting options, which round up the package enabling operation in the standard desktop version, mounted on the wall or DIN rail.

Maintenance and refitting of Industry 4.0

The complexity of industry systems increases the probability of a system breakdown. With machines that are not connected, the service technician has to do on-site service, even if a reboot of the machine would solve the problem. With an IoT gateway, it is possible to see the status of the machine and remotely do a reboot. Since the gateway itself isn't part of the machine, it stays online and can monitor the reboot. As a consequence, the gateway opens up the use of hidden data for remote diagnostics.

When an industrial machine has broken down, debugging the error can take a long time. This problem doesn't exist with the use of the Gatebox, because it is a stand-alone system which can monitor the health of the whole system. The occurring errors or log files can be analyzed in a laboratory to eliminate further failures. The existing data base of industry PCs together with a corresponding evaluation and analyzing tools make the system complete and support trouble-free function and maintenance of Industry 4.0. ◀

Author

Roland Peindl
B-Plus
www.b-plus.com
services@b-plus.com

CAN Newsletter Online

The CAN Newsletter Online sister publication provides brief product-related information. For more details please visit www.can-newsletter.org.

Box PC

CAN integrated via I/O shields

The Gatebox 100 by B-Plus (Germany) is an embedded, fan-less box PC based on a flexible interface concept. Two optional CAN interfaces are available.

Read on

Control system

Suitable for mobile machines

The increasing complexity of mobile machinery results in growing demands of I/O controllers. In accordance with those market requirements B-Plus (Germany) developed the b-CAN-Cube-Mini.

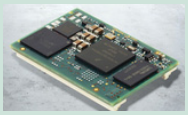
Read on

IoT gateway

Spam filter for IoT

Dell's Edge Gateway 5000 series delivers an IoT gateway with analytic capabilities, I/O options, and the ability to operate in extreme environments. The solution was designed for the rigors of building and factory automation.

Read on



Embedded World 2016

IoT gateway and ARM Cortex modules

At the Embedded World, TQ is showing – in cooperation with Gemalto – a gateway solution to enable "Secure IoT". The company is also planning two mini-modules with ARM Cortex-A7 processor architecture.

Read on

CAN security with hidden key generation

Security is on the agenda; resource-saving solutions are in demand. CANcrypt is one of them: it supports encrypted communication and the implementation of a simplified key management.

Commonly used security methods for authentication and encryption/decryption on the Internet cannot easily be applied to CAN and CANopen. CAN messages can consist of single bytes and need to be processed in real-time by low-performance, low-price micro-controllers usually without any security hardware functionality.

The CANcrypt approach adds different levels of security to CAN. The basic functionality supports the pairing of multiple devices and supports encrypted and authenticated communication between them. The required system resources are not only minimal in comparison to traditional cryptography methods; they can also be scaled towards the application's security requirements. A key hierarchy allows the implementation of a smart, simplified key management that supports manufacturers, system builders/integrators, and owners. CANcrypt is independent from the higher-layer protocol and can be used with CANopen, SAE J1939 or proprietary protocols. Up to 14 devices can participate in the secure communication. A manager/configurator is only required for the generation and exchange of keys, but not during regular operation.

Required resources

Depending on which features are used, the described security solution requires the following resources (ARM Thumb-2 example):

- Memory
  - 1 KiB to 2 KiB for code,
  - 32 byte to 512 byte per key in non-volatile memory,
  - about 100 byte RAM.
- Processor
  - 100 cycles to 150 cycles for encryption/decryption/authentication (vs. thousands of cycles for traditional cypher algorithms),
  - a few 100 cycles for housekeeping (background tasks called once per millisecond).
- Communication
  - one CAN-ID per device for the CANcrypt message,
  - two CAN-IDs for random bit generation,
  - preamble message for each secured CAN frame,
  - two to 16 housekeeping messages per second (dynamic key modification).

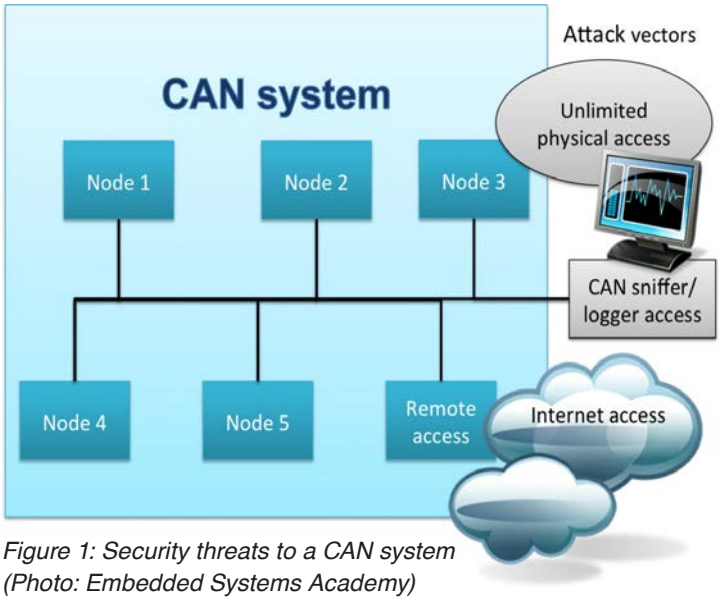


Figure 1: Security threats to a CAN system (Photo: Embedded Systems Academy)

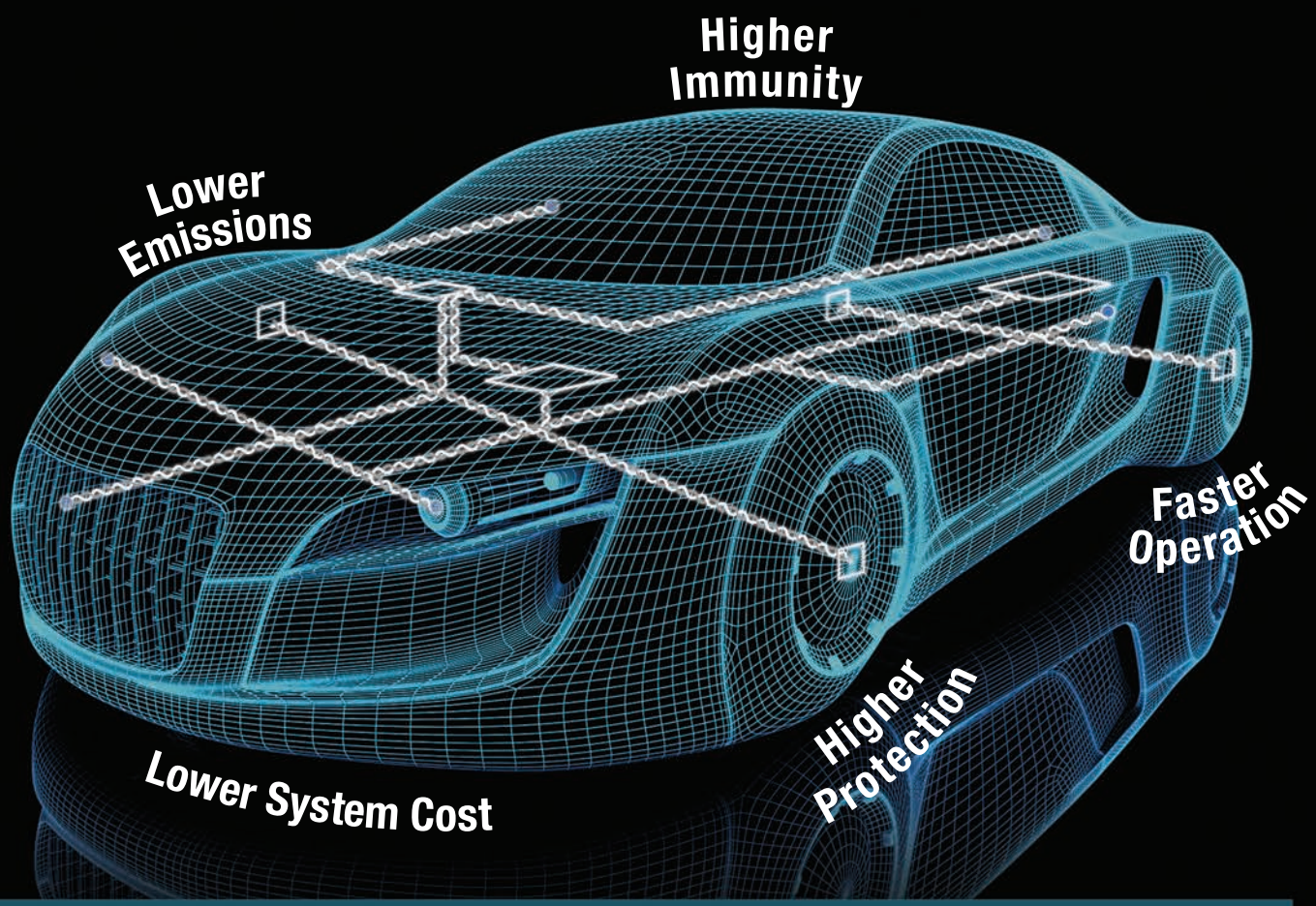
Limitations and levels of security

Looking at CAN/CANopen networks, we can identify three threat levels (unlimited physical access, sniffer access, remote access). These apply to most applications including automotive, industrial, medical, and other machinery. If an intruder has "unlimited physical access to the entire network including device PCBs", then the available security options are very limited. Having potential access to all debug ports of the micro-controllers of a system provides many other attack vectors besides CAN/CANopen. CANcrypt does not cover this aspect. Once intruders have direct access to a CAN/CANopen system (if they have the chance to connect a sniffer device or a laptop with a CAN interface), they have read access to all communication on the network. If they have write access, then "denial of service" style attacks (swamping the bus with messages so that nothing else gets through) are easy and cannot be prevented.

The last attack vector has become more and more popular: remote access through some device that is a gateway to other networks. Remote diagnostics or other kinds of remote access have become common, also increasing the security risk. A manufacturer of a system using CAN/CANopen might not be fully capable of prohibiting a remote access device: a technician or system integrator might add, for example, such a remote access device after delivery and initial installation. ▷

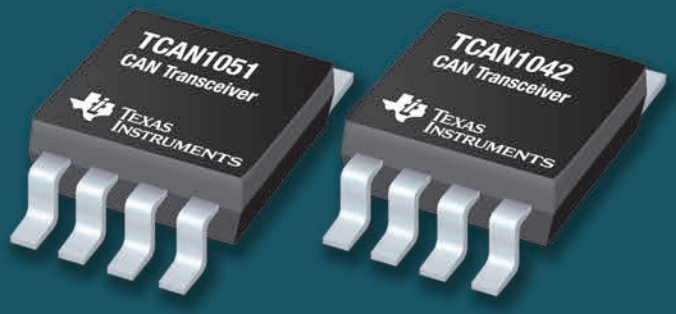
EMC-certified chokeless high-speed CAN transceivers

Texas Instruments



Enabling unrivaled performance and protection

- Superior noise emissions
- High bus-fault protection
- Fast CAN FD speeds
- Shortest loop delay



Visit TI.com/CAN

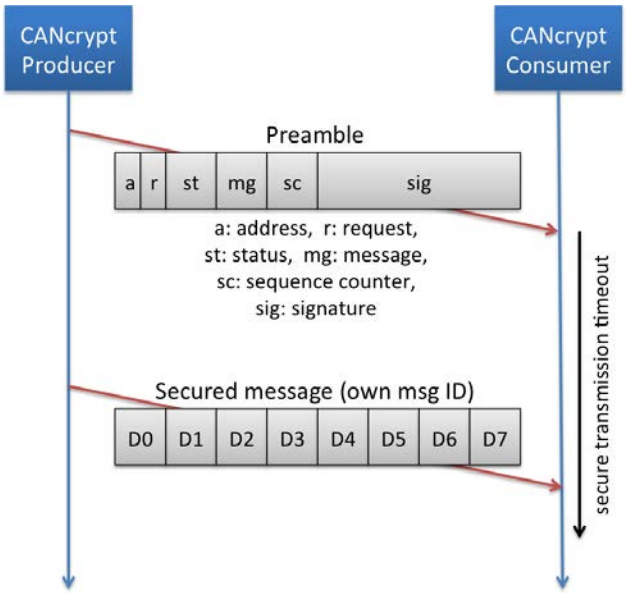


Figure 2: Secure communication using a preamble message (Photo: Embedded Systems Academy)

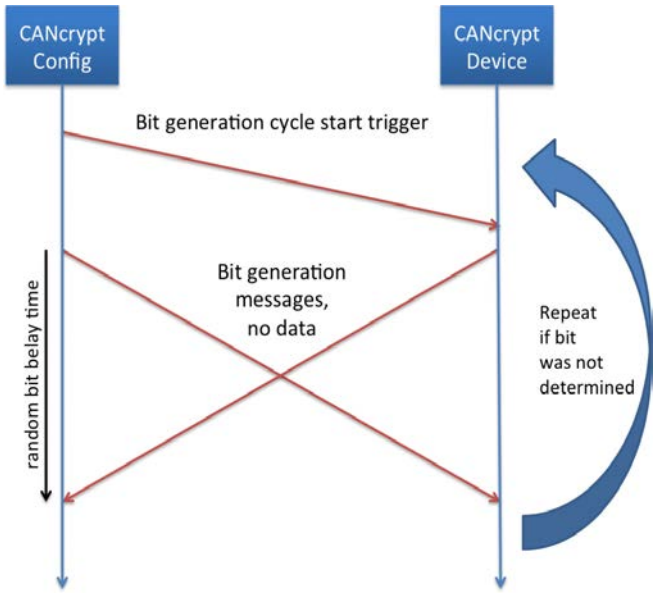


Figure 3: Random secret bit generation (Photo: Embedded Systems Academy)

Core functionality of CANcrypt

All secure communication uses a preamble message announcing the following message. Messages are only accepted (i.e. passed on to the application) if together with the preamble the authentication and decryption is successful. The shared key used is continuously updated and synchronized between the devices. For key generation, CANcrypt uses a CAN feature that allows two devices to exchange a bit not visible to other CAN devices. This allows generating pairing keys that only the two participants know. Note: to some extent this might be visible on signal level, for example on a high-end oscilloscope. However, a possible intruder would need access to that level during key generation AND understand/know how the generated bits are used.

When monitoring CAN messages, one cannot determine the device that sent an individual message because on the lowest level any device can transmit any message. As an example, let us allow two devices (named dominant device and recessive device) to transmit messages with the CAN-IDs 0010_h and 0011_h (and data length zero) within a "bit select time window". Each node shall randomly send one of the two messages at a random time within the time window.

At the end of the bit select time window a trace recording will show one of the following scenarios:

a) one or two messages of CAN-ID 0010_h,
b) one each of CAN-ID 0010_h and 0011_h,
c) one or two messages of CAN-ID 0011_h.

Let us have a closer look at case b) - one each. If these are transmitted randomly within the bit response time window, then an observer has no clue as to which device sent which message. However, the devices themselves know it and derive a bit from it. Unfortunately we cannot use case a) and c), so if those happen, both nodes need to recognize it and retry (use another next bit select time window).

Note: A variation of this scheme is to not use a random delay, but instead ensure that both devices directly transmit their message after the trigger message. Then both messages arbitrate the bus at the same time and we will always see 0010_h followed by 0011_h.

Choosing cipher algorithms

Even the simplest "cipher algorithm" like a single XOR is considered unbreakable (literally safer than anything commonly used today), if the key is as big as the data and only used once. This is referred to as the one-time pad cipher. If we can generate a single one-time 32-bit key, combined with a single XOR, for a transferred 32-bit value, then we already have an encryption stronger than any other cryptography method in use today.

To a certain extent (depending on how much secure communication overhead is used and how often) the

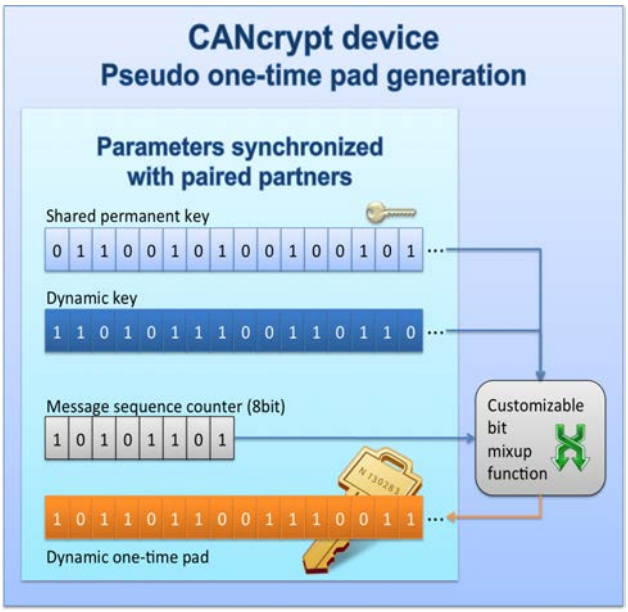


Figure 4: The CANcrypt key hierarchy (Photo: Embedded Systems Academy)

TTControl
HYDAC INTERNATIONAL

Powerful Control Units for High-Safety Applications: HY-TTC 500 Family

Flexibility & Usability

- Single controller for whole vehicle for centralized architectures
- Extensive I/O set with multiple software configuration options per pin
- Open programming environments C, CODESYS® V3.x and CODESYS® V3.x Safety SIL 2

Safety

- TÜV-certified according to IEC 61508 (SIL 2) and EN ISO 13849 (PL d)
- ISO 25119 AgPL d certifiable
- CODESYS® Safety SIL 2 including support for CANopen® Safety Master and easy separation of safe / non-safe code
- Safety mechanisms in hardware to minimize CPU load
- Up to 3 output groups for selective shut-off in case of safety relevant fault
- Safety companion and safety mechanism in hardware

Connectivity

- Up to 7 CAN interfaces
- Automatic baudrate detection and configurable termination for CAN
- Ethernet for fast download and debugging purpose

Performance

- 32 bit / 180 MHz TI TMS570 dual core lockstep processor (ARM architecture)
- Up to 2.3 MB RAM / 11 MB Flash
- Floating-point-unit

Robustness

- Automotive style housing suited for very rough operating conditions
- Total current up to 60 A

www.ttcontrol.com/HY-TTC-500-Family


Safety Certified ECUs


General Purpose ECUs


I/O Modules


Safe I/O Modules


Operator Interfaces

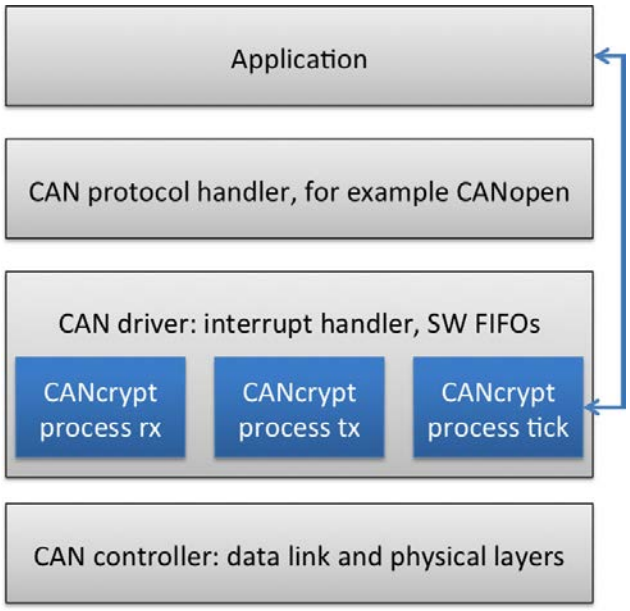


Figure 6: CANcrypt integration on driver level (Photo: Embedded Systems Academy)

CANcrypt methods would allow providing an individual key for each transfer. However, "the best protection available" is hardly required for CAN communication, so even if the same or an only slightly different key is used a few times, the protection is still strong. Per default, CANcrypt uses a dynamic 64-bit key to cover the longest possible secure data block, 8 byte. The pseudo one-time pad generated from it changes after every use. It depends on the CANcrypt configuration how often new random bits are introduced into this key modification.

Secured embedded systems require some sort of a key management system. When keys are installed, who installs which keys and how much "authority" does each have? With CANcrypt the suggested method is to keep the number of key copies required outside the system to a minimum. At some point a pairing process is started generating keys – and these are only stored locally. If devices need to be added or exchanged, a next higher authorized key is used to erase the existing pairing information and start a new pairing process.

Code integration

The CANcrypt functionality is mostly integrated into the "driver" level like the CAN receive interrupt and the software transmit mechanism (typically some FIFO). During initialization, the application passes a list of CAN message IDs that require protection. The CANcrypt driver then "catches" all these messages coming in or out and applies the configured security features. The messages are only passed on to other layers of the communication protocol if the device is securely paired with its communication partners and the configured ciphering and authentication mechanisms have been applied. This ensures that any software "above" the driver level does not need to be aware of CANcrypt. It processes CAN messages just as it used to do, which simplifies the integration into existing systems. ◀

The book: Implementing scalable CAN security with CANcrypt

Written by Olaf Pfeiffer, "Implementing scalable CAN security with CANcrypt" introduces the freely available CANcrypt protocol and software. After an introduction into CAN and CANopen technology as well as security, the author focuses on the description of the precautions and the functionality of CANcrypt. Common parameters and secure message tables are introduced as well as the security error counter. The author also provides some examples (secure push button) and explains customizable security functions including checksum generation. The book addresses not just security experts, but also newcomers and beginners. The reader gets not just an overview, but also details documenting the freely available code examples.

Review of possible attack vectors

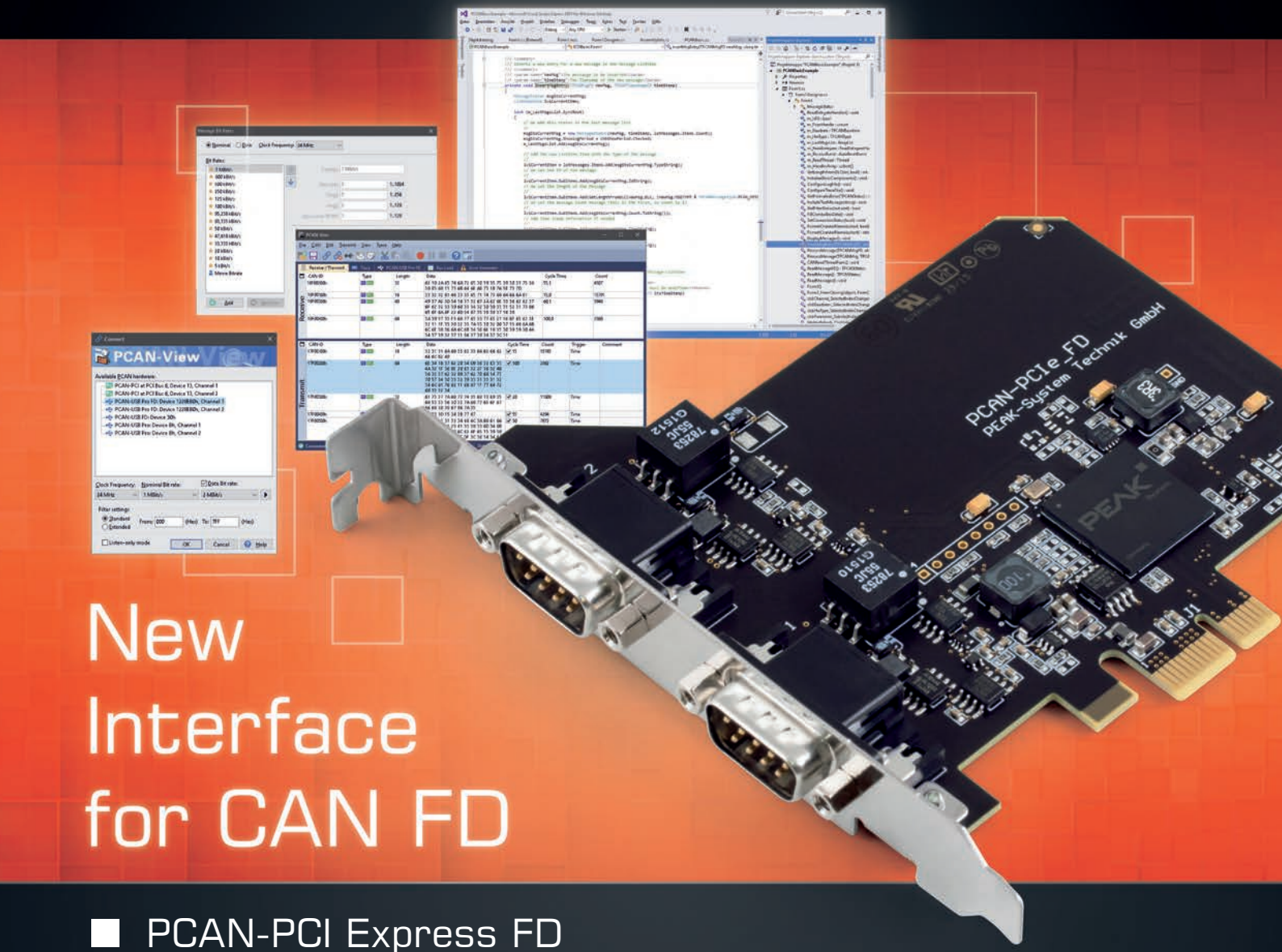
1. Randomness: Wherever random numbers are used, a typical attack vector is to assume that the numbers are not random and to determine a pattern. It must be ensured that the random numbers used by the paired devices are "reasonably good", which means they must differ with every power cycle.
2. Read/write access to CAN/CANopen network (remote access, sniffer): In CAN networks, a typical attack involves recording messages and replaying them. If the messages that are exchanged after power up are always the same, an attacker could fake initial messages by replaying them. However, due to the dynamic and random key changes, a hacker would probably look at alternate methods first.
3. Ability to physically remove/replace devices (or re-flash a device with new code): If one of the paired devices is removed and replaced with a tampered device, then it will not be able to identify itself correctly, unless it has a copy of the key hierarchy.
4. Signal level access to CAN/CANopen network and PCBs: If an attacker has that kind of access, other methods (JTAG interfaces or bootloaders of microcontrollers) might be more promising then deciphering CANcrypt.

Summary:

At this point we are not aware of any promising attack vectors on the CAN/CANopen level. That includes any remote access (for example through a hacked gateway) as well as direct access with a CAN sniffer utility.

Author

Olaf Pfeiffer
Embedded Systems Academy
opfeiffer@esacademy.de
www.esacademy.com



New Interface for CAN FD

PCAN-PCI Express FD

CAN FD Interface for PCI Express

With the new PCAN-PCI Express FD we expand our product range of CAN FD interfaces by a plug-in card (PCIe-x1) for the PCI Express slot.

- 1 or 2 High-speed CAN channels (ISO 11898-2)
- Complies with CAN specifications 2.0 A/B and FD
- CAN FD support for ISO and Non-ISO standards switchable
- CAN FD bit rates for the data field up to 12 Mbit/s
- CAN bit rates from 25 kbit/s up to 1 Mbit/s
- CAN bus connection via D-Sub, 9-pin (in accordance with CiA® 102)
- Galvanic isolation on the CAN connection up to 500 V, separate for each CAN channel
- CAN termination and 5-Volt supply at the CAN connection can be activated through solder jumpers, separately for each CAN channel
- PCIe data transfer via bus master DMA
- DMA memory access operations with 32- and 64-bit addresses
- Extended operating temperature range from -40 to 85 °C
- Measurement of bus load including error frames and overload frames on the physical bus
- Induced error generation for incoming and outgoing CAN messages

Driver, Software, and Programming Interfaces

Every PC interface from PEAK-System is delivered with a wide range of drivers, software, and programming interfaces. The scope of supply includes:

- CAN FD interface drivers for Windows 10, 8.1, 7 and **Linux**
- **PCAN-View**: Windows software for monitoring CAN and CAN FD busses
- **PCAN-Basic API** for developing applications with CAN and CAN FD connection for Windows (32/64 bit)
- **PCAN-PassThru** for using applications that are based on Pass-Thru (SAE J2534) with interfaces from PEAK-System
- Programming interfaces for standardized protocols from the automotive sector like:
  - **PCAN-CCP API** for the communication with ECUs according to the CAN Calibration Protocol
  - **PCAN-XCP API** for communication with ECUs according to the Universal Measurement and Calibration Protocol (CAN FD support since version 2)
  - **PCAN-ISO-TP API** for the transfer of data packages according to ISO-TP (ISO 15765-2)
  - **PCAN-UDS API** for the communication with ECUs according to UDS (ISO 14229-1)
  - **PCAN-OBD-2 API** for vehicle diagnostics according to OBD-2 (ISO 15765-4)

www.peak-system.com

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

PEAK-System Technik GmbH

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

PEAK System

CAN in Automation

CANopen conformance test center

- Conformance testing of your CANopen implementation
- Interoperability testing in a multi-vendor test stand
- Test your devices together with other engineers at a plug fest

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

www.can-cia.org