March 2023

CAN Newsletter

Hardware + Software + Tools + Engineering

CAN XL ecosystem and product availability

CAN SIC XL proof-of-concept transceiver

SIC or SIC XL – this is not the question

Physical layer

www.can-newsletter.org

Product Line: PCAN-MicroMod FD

I/O Modules with CAN FD & CANopen FD

The PCAN-MicroMod FD is a plug-in board that provides a CAN FD interface and I/O functionality for the integration into your hardware. An evaluation board facilitates developing your custom solution. The modules are configured with a Windows software via CAN and then operate independently.

Ready-to-Use Motherboards

The PCAN-MicroMod FD is available with motherboards providing peripherals for specific applications.

Common Features:

- Board with plugged on PCAN-MicroMod FD
- CAN FD connection with switchable CAN termination
- 2 frequency outputs (Low-side switches, adjustable range)
- Analog input for voltage monitoring up to 30 V (12 bit)
- Aluminum casing with spring terminal connectors
- Extended operating temperature range from -40 to +85 °C
- Operating voltage 8 to 30 V

PCAN-MicroMod FD Analog 1:

- 8 analog inputs (16 bit, adjustable range)
- 4 analog inputs (12 bit, 0 to 10 V)
- 4 analog outputs (12 bit, adjustable range)
- 4 digital inputs (pull-up or pull-down)

PCAN-MicroMod FD Digital 1 / Digital 2:

- 8 digital inputs (pull-up or pull-down)
- 3 analog inputs (12 bit, 0 to 10 V)
- Digital 1: 8 digital outputs with Low-side switches
- Digital 2: 8 digital outputs with High-side switches

CANopen & CANopen FD Solutions

The PCAN-MicroMod FD DR CANopen Digital 1 is an I/O module for operation in CANopen (FD)® networks.

Main Features:

- CANopen® and CANopen FD® connection
  - Communication profiles according to CiA® 301 version 4.2.0 and CiA® 1301 version 1.0.0
  - Device profile according to CiA® 401 version 3.0.0
  - Certified CANopen® and CANopen FD® conformity
- 8 digital inputs, comply with the IEC 61131-2 standard
- 8 digital outputs with High-side switches
- Plastic casing (width: 22.5 mm) for mounting on a DIN rail

All PCAN-MicroMod FD products can alternatively be operated with CANopen® and CANopen FD® firmware from our partner Embedded Systems Academy.

embeddedworld2023
Exhibition&Conference
... it's a smarter world

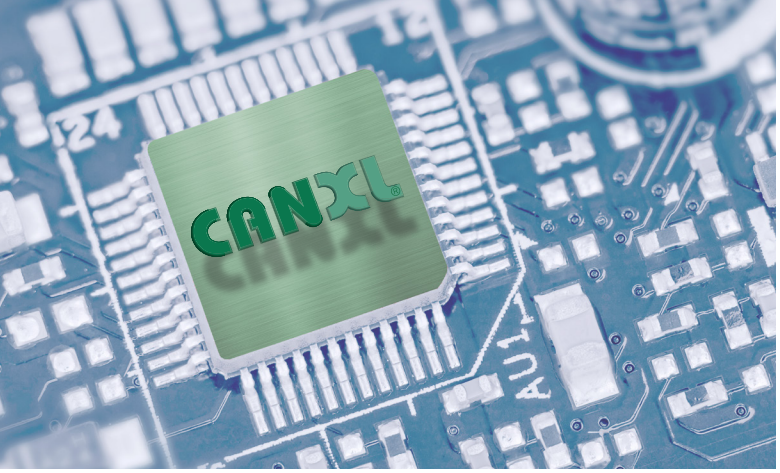
Meet us in hall **1**, booth **304**

PEAK-System Technik GmbH

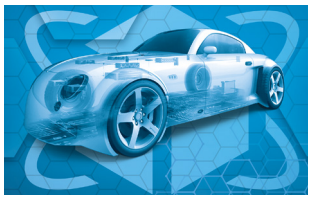
Otto-Roehm-Str. 69, 64293 Darmstadt, Germany
Phone: +49 6151 8173-20 - Fax: +49 6151 8173-29
E-mail: info@peak-system.com

www.peak-system.com

PEAK System



CAN XL



Tools

Gateways

Brief news

Newly released CiA documents

End of 2022 and beginning of 2023, CiA has updated some documents and renamed some. The former CiA 303-2 technical report (TR) recommending representation of SI units and prefixes for CANopen profile specifications has been substituted by CiA 890. The CiA 890 applies to all CiA specifications and is no longer limited to CANopen.

CAN in Automation has released the CiA 406 encoder device profile series as draft specification proposal (DSP). The CiA 406-B version 1.0.0 specifies the functional behavior as well as application parameters for different types of linear and rotary encoders. It is the successor of the CiA 406 monolithic specification. The CiA 406-C and CiA 406-F documents specify the CANopen respectively CANopen FD PDO communication and mapping parameters for encoders compliant with CiA 406-B. The updated CiA 406-J version 1.2.0 refers now to the CiA 406-B specification. It specifies the mapping of process data into J1939 parameter groups (PGs). This includes the specification of PGs and the configuration by means of CAM11 and CAM21 parameter groups as defined in CiA 510.

CiA has updated the CANopen profile for SIIS level-2 devices (CiA 443) specifying interfaces for subsea measurement systems including redundant controllers, different sensors, actuators, valves, etc. For instance, the off-shore platforms for oil production are linked to such underwater measurement equipment.

CiA has also updated the CiA 319 CANopen implementation and configuration guideline for safety-related devices. This includes the functional-safe configuration procedure of parameters and authentication proof of the configuration, which is not covered by EN 50325-5 (functional-safety communication for CANopen networks).

Imprint

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

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

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

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

Layout
Nickel Plankermann

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

Downloads December issue
(retrieved February 26, 2023)
4440 full magazine

Table of contents

CAN XL ecosystem and product availability

(Source: Adobe Stock)

Since 2018, the CiA special interest group (SIG) CAN XL is specifying the CAN XL ecosystem. In the meantime, the SIG CAN XL has established four task forces (TF): TF CAN XL physical layer, TF CAN XL higher layer, TF CAN XL security, and TF simulation. The related CiA meetings are participated by more than 30 attendees working with auto-makers (OEMs), Tier-1 suppliers, semiconductor manufacturers as well as tool vendors and service providers.

There are three CAN protocol (data link layer) generations, which have been specified internationally.

- 1993: ISO 11898 standard (1st generation), also known as Classical CAN protocol;
- 2015: ISO 11898-1 standard (2nd generation), includes the CAN FD protocol option;
- 2021: CiA 610-1 specification (3rd generation), also known as CAN XL protocol, XL stands for “extended data field length”, and the ISO 11898-1 is under review to include CAN XL in the next edition.

Today there are different transceiver technologies (physical layer) that are used in CAN networks. Figure 1 shows the evolution of the most used CAN transceiver type, and the newly developed transceiver types. In principle, the compatibility between the used transceiver types in one network is guaranteed. But you should be aware of the configuration possibilities, as to enable/disable error signaling and transceiver mode switching (fast Tx/Rx mode or SIC mode).

Editor´s note: For more details about the physical layer options, you can find another two articles from Infineon and NXP in this CAN Newsletter issue.

HS CAN transceiver

- Up to 1 Mbit/s
- ISO 11898-2:2016

CAN FD transceiver

- Higher than 1 Mbit/s
- Up to 5 Mbit/s
- ISO 11898-2:2016

CAN SIC transceiver

- Up to 8 Mbit/s
- Signal improvement capability
- CiA 601-4
- *ISO 11898-2:2023 (under revision)*

CAN SIC XL transceiver

- Up to 20 Mbit/s
- Signal improvement capability
- Transceiver mode switching configurable
- CiA 610-3
- *ISO 11898-2:2023 (under revision)*

Figure 1: Properties of the specified CAN transceiver technologies (Source: CAN in Automation)

Specifications and other documents

Inside the SIC CAN XL and the TFs, the ecosystem of CAN XL is developed. Table 1 shows the CAN XL related specifications and documents. The SIG CAN XL has already released the CiA 610-1 CAN XL data link layer requirements, the CiA 610-3 CAN XL physical layer requirements, and the CiA 611-1 SDU (service data unit) types for the CAN XL higher-layer services.

The CiA 120 document will specify test and measurement methods for EMC evaluation of CAN SIC transceiver ICs and CAN SIC XL transceiver ICs under network conditions. It should be compliant with IEC 62228-3:2019. It defines test configurations, test conditions, test signals, failure criteria, test procedures, test setups, and test boards. It covers the emission of RF disturbances, the immunity against RF disturbances, the immunity against impulses, and the immunity against electrostatic discharges (ESD). The aim is to submit this specification to IEC for international standardization.

The CiA 610 series provides requirement specifications and conformance test plans for the CAN XL data link layer and physical layer. It is intended for chip implementers of e.g. CAN XL protocol controllers as well as CAN SIC XL transceivers. Optionally, the CAN XL protocol controller provides the PWM encoding to be linked to a CAN SIC XL transceiver, which provides the PWM decoding. The CAN XL specifications and test plans series comprises five parts as shown in Table 1. CiA 610-5 is the interoperability test plan for heterogeneous networks comprising nodes with transceiver ICs from different suppliers. It recommends interoperability test set-ups using dedicated PMA implementations. The interoperability test plan completes the CiA 610-4 PMA conformance test plan.

The CiA 611 series specify additional services and protocols, which can be mapped to the CAN XL data link layer as specified in CiA 610-1. This includes OSI (open system interconnect) higher layer communication and OSI layer management functionality. The service data unit (SDU) type field indicates the used next higher OSI layer protocol data unit (PDU). The SDU type defines how management information such as addressing, virtualization, or data size are mapped on dedicated LLC (logical link control) frame fields or how they are mapped into the CAN XL LLC data. SIG CAN XL has released the CiA 611-1 version 1.0.0 as Draft Specification Proposal (DSP) in ▷

Table 1: CAN XL ecosystem specifications and documents

Document number	Document title	Actual status
CiA 120	EMC evaluation of CAN SIC transceivers and CAN SIC XL transceivers	WD
CiA 610-1	CAN XL specifications and test plans – Part 1: Data link layer and physical coding sub-layer requirements	DS version 1.0.0 released
CiA 610-2	CAN XL specifications and test plans – Part 2: Data link layer and physical coding sub-layer conformance test plan	WD
CiA 610-3	CAN XL specifications and test plans – Part 3: Physical medium attachment (PMA) sub-layer requirements	DS version 1.0.0 released
CiA 610-4	CAN XL specifications and test plans – Part 4: Physical medium attachment sub-layer test plan	WD
CiA 610-5	CAN XL specifications and test plans – Part 5: Additional interoperability tests for physical medium attachment	WD (will be released as TR)
CiA 611-1	CAN XL higher-layer services – Part 1: SDU types	DSP version 1.0.0 released
CiA 611-2	CAN XL higher-layer services – Part 2: Multi-PDU	WD
CiA 612-1	CAN XL guidelines and application notes – Part 1: System design recommendations	WD
CiA 612-2	CAN XL guidelines and application notes – Part 2: PWM coding guideline	WD
CiA 613-1	CAN XL add-on services – Part 1: Simple/extended content (SEC) indication	WD
CiA 613-2	CAN XL add-on services – Part 2: Security	WD
CiA 613-3	CAN XL add-on services – Part 3: LLC frame fragmentation	WD
CiA 910-1	CAN simulation model – Part 1: General terms and use cases	WD
CiA 910-2	CAN simulation model – Part 2: PMA simulation model requirements	WD
CiA 910-3	CAN simulation model – Part 3: PMD simulation model requirements	WD
CiA 910-4	CAN simulation model – Part 4: Recommendations between PMA sub-layer and PCS	WD

DS Draft Specification
DSP Draft Specification Proposal
WD Work Draft
TR Technical Report

November 2022. Implementation of the CiA 611-1 enables "tunneling" of Classical CAN, CAN FD, and Ethernet frames via CAN XL networks. Directly after, Autosar has integrated CiA 611-1 in its November 2022 release. With Ethernet “tunneling” (Ethernet frame mapping), CAN XL can bring IP communication to any ECU (electronic control unit). By this, CAN XL qualifies itself as cost-efficient and flexible enabler of future E/E architectures.

CiA 612 series provides recommendations for the system design such as CAN clock recommendation, bit timing setting rules, and physical layer design recommendation. Following these, a robust communication with higher bit rate could be achieved easier.

In order to activate the required higher data phase performance in the CAN XL physical layer, CAN XL introduces an optional PWM (pulse-width modulation) encoding and decoding sub-layer at the AUI (attachment unit interface). This sub-layer is used to optionally convert the transmitted NRZ-coded TXD data between PCS (physical coding sub-layer) and PMA (physical media attachment) into a PWM-coded TXD data during the CAN XL data phase within the PCS on demand. The PMA uses the received PWM coded TXD data as an indicator to switch from the known “dominant/recessive” level towards the new “Level_0/Level_1” on the bus wires while decoding the PWM symbols back to NRZ format on the bus lines. The PWM coding acts like a “hidden control signal” towards the PMA switching between the two behaviors of the PMA. Since the PCS resides within the CAN XL protocol controller, the PWM encoding specification can be found in CiA 610-1. The corresponding PWM decoding is done within the PMA and is specified within CiA 610-3. The CiA 612-2 document gives guidelines how to configure the PWM coding and how to configure the node, if the "transceiver mode switching" is supported.

The CiA 613 series specifies the CAN XL add-ons services. They can be added transparently and concatenated independently. Planed add-on services include security functions (in CiA 613-2), and LLC frame fragmentation (in CiA 613-3). The SEC (simple/extended content) bit as specified in CiA 613-1 can signal add-on functions applied to the CAN XL data link layer. The CiA 613-2 document specifies the security protocol (CANsec), which aims to protect the integrity, freshness, authenticity of origin, and confidentiality of data in CAN-based networks using CAN XL communication. The CiA 613-3 document specifies the LLC (logic link control) frame fragmentation, which guarantees latency constraints of the system in a transparent manner. CAN XL allows to transmit frames with a maximum of 2048 bytes in the data field. A CAN XL frame at 10 Mbit/s with 2048 byte occupies the network for approximately 2 ms. For applications that require to transmit high-priority control information, a latency of 2 ms is perhaps too long. Therefore, a service is required that allows to interrupt an ongoing transmission.

The CiA 910 series specifies simulation models for CAN XL networks. Such models can support tool vendors to provide a CAN SIC (XL) system integrator with necessary tools to approve its network designs with confidence and furthermore allow the specific analysis of network design issues arising in the development phases. They will comprise the physical layer model (e.g., transceivers and cables) requirements and recommendations for models between transceivers and protocol controllers.

CAN XL availability

The availability of CAN XL building blocks is important for engineers to adapt their applications to CAN XL. With the availability of the CAN XL IPs (intellectual properties), the ecosystem around CAN XL is quickly expanding. Hardware and software from different manufacturers are already available or will follow, soon.

CAN XL IPs:

- Bosch released the new protocol controller IP module X_CAN. It can be implemented in a SoC and supports Classical CAN, CAN FD, and CAN XL.
- Fraunhofer IPMS provides the CAN XL IP, which is purchased via CAST.
- NXP and Vector have also developed CAN XL IPs, which are only used for their own MCUs respectively tools.

MCUs with CAN XL on chip:

- Infineon has announced the Aurix TC4xx MCU family.
- NXP is developing new processors S32Z2 and S32E2 with respectively two CAN XL channels. The processors are currently in preproduction and samples are available.
- Renesas is developing the RH850/U2x MCU series, which will support CAN XL.
- STMicroelectronics has unveiled the MCUs Stellar P6 for EV (electric vehicle) platform system integration. The automotive MCUs are qualifiable components for 2024-model-year vehicles that incorporate the CAN XL on-board communication. Samples are available.

CAN SIC XL transceiver:

- Bosch's CAN SIC XL (proof of concept) transceiver and the Power Management ICs with CAN SIC XL transceiver are under development. Samples of the concept transceivers are available.
- NXP is developing the CAN SIC XL (proof of concept) transceiver. Samples are available.
- Texas Instruments' CAN SIC XL transceivers are under development.

Tooling/software:

- Keysight, LeCroy, and Rohde & Schwarz are developing CAN XL protocol signal decoders.
- Vector's new CANoe tool version will support CAN XL.

CAN XL plugfest

To test interoperability of the available transceivers and protocol controllers from different sources in network environments, CiA is organizing the so-called CAN XL plugfests.

The first plugfest was held on July 2021 in Nuremberg, Germany. The IP cores from Bosch, Fraunhofer ▷

Documents submitted for ISO standardization

In 2022, CiA has submitted the CiA 610-3 and CiA 601-4 documents for integration into the next edition of ISO 11898-2. The related DIS (draft international standard) has been balloted positively with some technical comments. As already discussed within CiA, new parameters need to be specified. They are already part of the DIS comments.

The CiA 610-1 and CiA 604-1 (CAN FD Light) documents are also submitted to ISO to be integrated into the ISO 11898-1 standard.

The aim of the ISO working group (TC22 SC31 WG3) is to prepare the release of new ISO 11898-1 and ISO 11898-2 versions in 2023. In the meantime, the working group is also considering the review of the conformance test plan for the data link layer and physical layer, i.e., ISO 16845-1 respectively ISO 16845-2.

IPMS, and Vector were under test. NXP and Infineon provided their CAN SIC (XL) transceiver implementations. In May 2022, the companies attended the second plugfest. On both plugfests, the compatibility of CAN XL IPs and CAN SIC XL transceivers have been tested. The experts have also built different topologies to prove the robustness. Currently, the CiA is organizing the third CAN XL plugfest on April 25, 2023, in Detroit area (USA). Interested parties are welcome to contact CiA at secretary@can-cia.org.

Author

Yao Yao
CAN in Automation
pr@can-cia.org
www.can-cia.org

Kickstarting CAN XL evaluation: CAN SIC XL proof-of-concept transceiver

After CAN SIC overcame the limitations of CAN FD, CAN XL will take the next step by introducing data rates up to 20 Mbit/s and 2048-byte payloads. NXP's CAN SIC XL prototype transceivers facilitate the start of CAN XL technology and data path evaluation (on ECU and vehicle level), establishing expertise on the protocol, transceiver, and application.

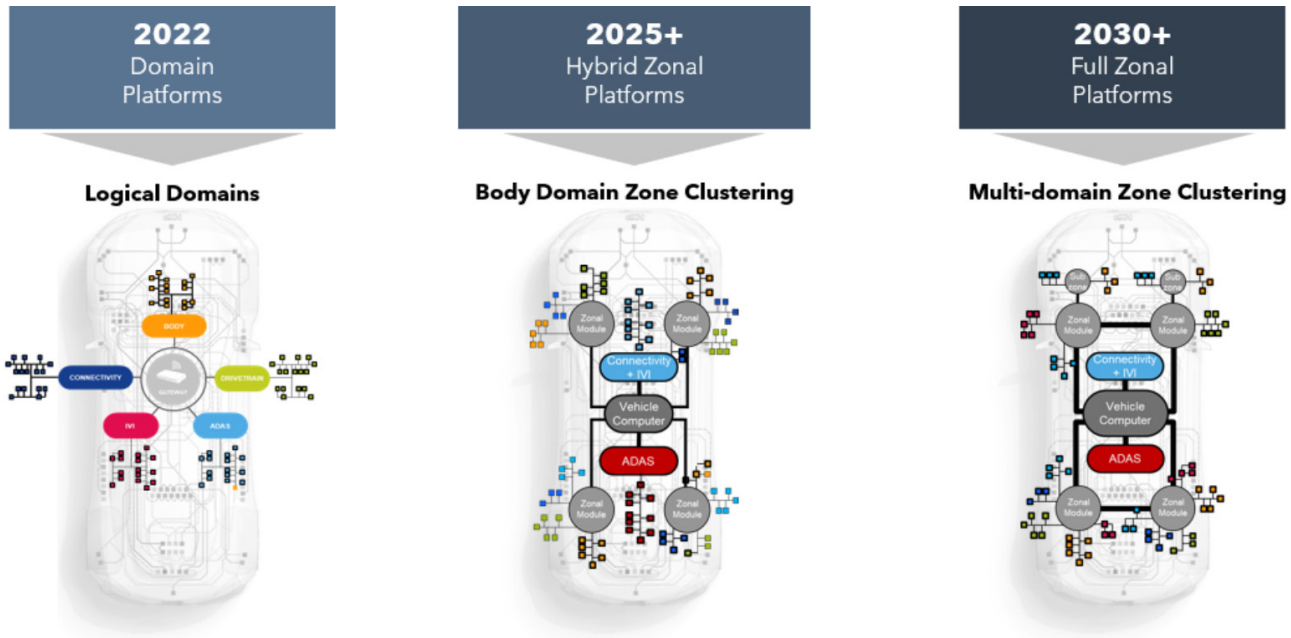


Figure 1: Architectural trend of automotive vehicle networks; from domain-based to zonal-based networks (Source: NXP)

With major automotive trends like electrification and autonomous driving, in-vehicle networks are expanding rapidly to integrate new functionality and applications. The resulting network complexity and required bandwidth are growing too, redefining the role of CAN in in-vehicle network architectures.

To support these major trends, vehicle networks are moving from domain-based platforms towards zonal network architectures (see Figure 1). The backbone connections between multiple vehicle computers or zonal gateways are generally served with Automotive Ethernet, while CAN communication is pushed toward dedicated domains and edges of the network, interfacing between the edge nodes and the Ethernet backbone, or as backup and wake-up network.

CAN SIC overcomes limitations of CAN FD

The introduction of CAN FD (flexible data-rate) enabled bit rates up to 5 Mbit/s, supporting the industry with more bandwidth beyond Classical CAN networks. In reality however, the achievable bit rate is a trade-off between signal ringing and topology. As a result, CAN FD networks are generally limited to a bit rate of 2 Mbit/s in small and linear networks. To extend the performance potential of CAN FD, NXP developed an implementation of the Signal Improvement Capability (SIC) technology, first introduced in the TJA146x CAN SIC transceiver family compliant with the CiA 601-4 specification. CAN SIC actively improves the CAN signal allowing network designers to implement more complex topologies and extend the achievable data rate up to 8 Mbit/s. Consequently, CAN SIC enables more effective CAN FD networks, allowing more efficient cabling and thus saving weight and cost.

CAN XL: the future of CAN

CAN XL was created to provide additional functionality to CAN, fitting to the changes of the vehicle network architecture, while fixing the limitations of CAN FD. It allows for increased bit rates and larger payloads, while offering all the benefits of CAN, such as large multi-drop networks, (bit rate) scalability, quality of service, and EMC (electro-magnetic compatibility) robustness. Due to its flexibility, CAN XL ▷

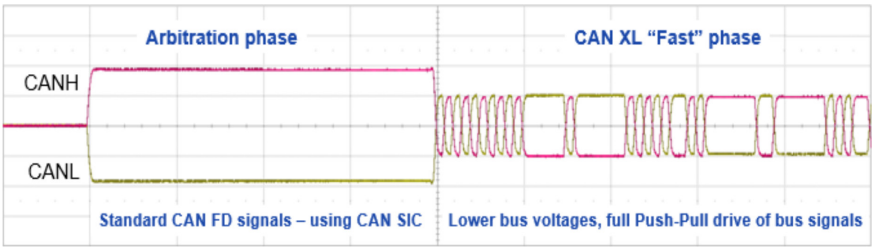


Figure 2: Two physical level schemes of CAN XL – normal CAN FD signal when using CAN SIC (left) and new CAN XL "fast mode" level scheme (right) to enable data rates up to 20 Mbit/s (Source: NXP)

is not bound to zones, but can also create low-latency inter-zonal connections or serve as an efficient implementation of domain networks. In short: CAN XL makes CAN technology ready for seamless integration into the next-generation networks while maintaining the key properties of CAN.

Basics of CAN SIC XL

The benefits of CAN XL are based in both a data link layer protocol extension and an improved physical medium attachment sub-layer implementable in transceivers. The CAN XL protocol itself extends CAN FD with a data payload of up to 2048 byte. CAN XL also enables a transition to a secondary physical level scheme during the data phase, called CAN XL "fast mode". CAN SIC XL transceivers are an extension of CAN SIC, being backwards compatible to CAN FD and utilizing the technology in the non-fast phase of CAN XL. Additionally, it supports a secondary, optimized physical level scheme during the "fast mode", which enables CAN SIC XL transceivers to achieve data rates of up to 20 Mbit/s during that fast phase. This has been first showcased by NXP with its CAN SIC XL proof-of-concept transceiver, called "Albi" during various CiA plugfest events from 2021 to 2023.

Due to the new level scheme and backwards compatibility, the CAN SIC XL transceivers can act in two modes (see Figure 2):

- *SIC mode:* Working according to the original CAN (FD) level scheme in combination with SIC, with a maximum data rate of 8 Mbit/s and the benefits of signal improvement on topology freedom.
- *CAN XL "fast mode":* Enabling the new level scheme and up to 20 Mbit/s data rate capabilities. The different communication styles are initiated by the CAN XL protocol controller.

Use cases for CAN SIC and CAN SIC XL – mixing controllers and transceivers

CAN XL is backwards compatible to CAN FD, meaning controllers and transceivers can be mixed to create ▷

Transceiver	CAN FD	CAN SIC	CAN SIC	CAN SIC XL
Controller	CAN FD	CAN FD	CAN XL	CAN XL
Data rate (up to)	5 Mbit/s	8 Mbit/s	8 Mbit/s	20 Mbit/s
Payload	64 bytes	64 bytes	2048 bytes	2048 bytes
Topology	Small and linear	Large and complex	Large and complex	Large and complex
Signal Improvement	X	✓	✓	✓
CAN XL "Fast Mode"	X	X	X	✓
Standardization	ISO11898-2:2023			
		CiA601-4		
			CiA610-3	

Figure 3: Use cases for CAN SIC and CAN XL – benefits of mixing transceivers and controllers (Source: NXP)

heterogenous networks and manage adoption of the new technology over time. Four use cases are outlined in Figure 3 and below, each providing their benefits to mix and matching transceivers and controllers.

- *CAN FD controller + CAN FD transceiver:* Enables CAN FD communication up to 5 Mbit/s, but is generally limited to 2 Mbit/s in smaller and more linear networks due to the effects of signal ringing.
- *CAN FD controller + CAN SIC transceivers:* NXP's CAN SIC transceivers are fully backwards compatible to legacy CAN-HS (high-speed) and CAN FD transceivers, enabling an easy and hassle-free upgrade of a CAN FD module by a simple replacement of the transceiver to benefit from the boosted network performances for any CAN FD network. This results in higher achievable data rates in more complex networks.
- *CAN XL controller + CAN SIC transceivers:* This scenario brings two benefits with respect to the previous. By using a CAN XL controller, all benefits of the CAN XL protocol (e.g. 2048 bytes payload) can be utilized up to a bit rate of 8 Mbit/s. This is further extending the capabilities of CAN SIC, while it allows for additional flexibility and a single solution approach for multiple use-cases. Furthermore, NXP is planning to have identical pinning for CAN SIC and CAN SIC XL transceivers, meaning this scenario enables an easy upgrade towards full CAN XL networks.
- *CAN XL controller + CAN SIC XL transceivers:* Getting the maximum performance out of the CAN network by combining the power of both the CAN XL controller as well as the CAN SIC XL transceiver to reach data rates up to 20 Mbit/s. By increasing both the maximum data rate and the payload, CAN XL enables more complex topologies at higher data rates, Ethernet frame tunneling and backwards compatibility with CAN FD. This makes it a very attractive technology for future networks.

System level implementation: why the proof-of-concept silicon is relevant

NXP was the first to launch a CAN SIC XL proof-of-concept silicon ("Albi") capable of demonstrating 20 Mbit/s in CAN XL network, raising the bar for CAN XL and doubling its previous 10 Mbit/s performance target. During the CiA plugfest 2022, C&S has showcased an Ethernet "tunneling" demo over CAN XL using NXP's CAN SIC XL silicon.

Albi has been introduced as a prototype transceiver to proof the extended capabilities of CAN XL up to 20 Mbit/s and allow the market to start early evaluation. Albi is capable of running full 20 Mbit/s communication in real topologies with already proven EMC performance, establishing the starting point for prototype development boards, CAN XL data path and topology evaluation and vehicle-level network tests with CAN XL.

Together with industry partners, C&S and Bosch, a full CAN XL evaluation suite is offered, providing interested adopters access to evaluate the potential of CAN XL as a technology. Multiple parties have started network validation to build up knowledge and expertise in assessing CAN XL for future networks. NXP is also providing CAN SIC XL transceiver simulation models to perform network topology assessments, enabling simple and accessible first-hand experience with CAN XL.

With CAN XL controller IPs available from multiple vendors, the ecosystem around CAN XL is quickly expanding. NXP is currently sampling its first MCUs with integrated CAN XL controllers (S32Z2/E2), enabling easy deployment of CAN XL and supporting customers in building their first CAN XL applications.

Conclusions and product outlook

Besides CAN FD and CAN SIC, there is a clear need to move beyond the available capabilities of CAN both in terms of payload and achievable data rate to support new trends in the vehicle network, while maintaining all the benefits that CAN has to offer.

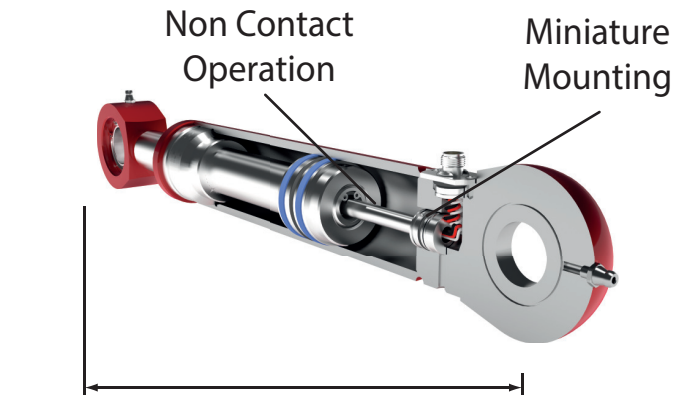
CAN SIC has been facilitating increased topology and data rate flexibility, optimizing networks for cabling and cost and offering network owners an increased freedom to define their network. CAN SIC XL delivers CAN networks with more performance, enabling network consolidation, simplified domains and a sustainable way towards full zonalization. NXP's CAN SIC XL proof-of-concept silicon "Albi" is allowing OEMs and other industry partners to start capability studies and early evaluation, facilitating a headstart on CAN XL and preparing their networks and applications for future deployment. NXP plans to develop CAN SIC XL transceivers with relevant specifications to serve the networking trends of tomorrow. ◀

Author

Teun Hulman
NXP
teun.hulman@nxp.com
www.nxp.com

COFFEE or TEA?

You also have a choice for hydraulic cylinder positioning



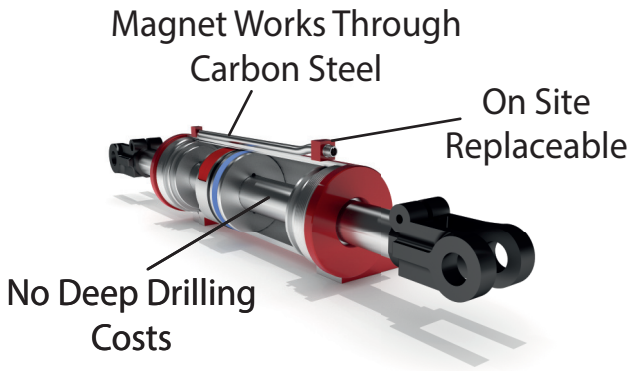
Inside the cylinder?

Compact, robust design

Maintains ASAE pin dimensions

20g RMS Vibration Rating

UN ECE R10 Automotive Approval



Or Outside the cylinder?

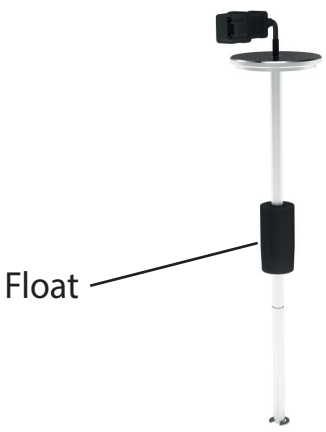
Easily field replaceable for maximum machine uptime

Ideal for steering cylinders

Ideal for long cylinders

Our Hall Effect Transducers Give You A Choice

Also from Rota



Tank Level Transducers

3 in 1 - Capable of

- Position
- Velocity
- Temperature

Up to 6 metres

High Accuracy

Independantly Mounted Transducers

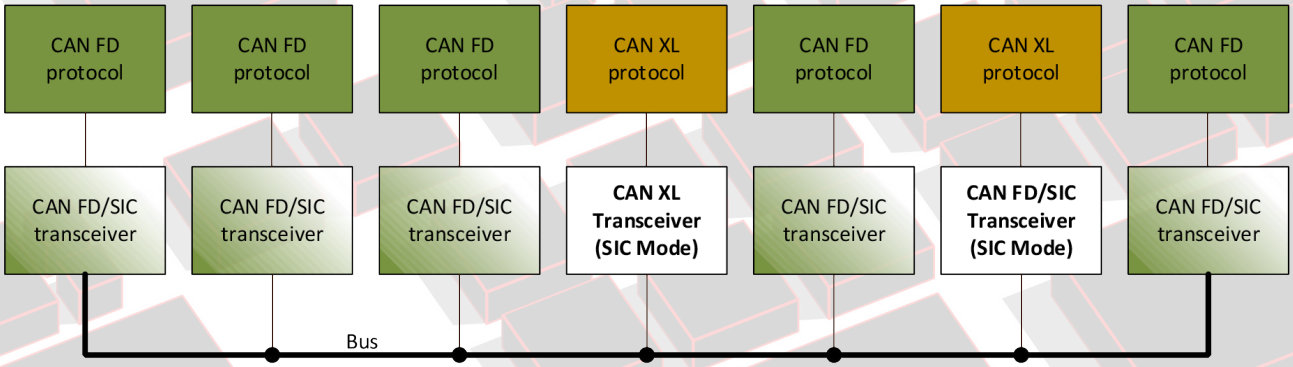
- Light Duty
- Mounts with cylinder
- Ideal for high volume, low cost OEM applications

rota ©

Rota Engineering

Manchester, UK
www.rota-eng.com
info@rota-eng.com

SIC or SIC XL – this is not the question



(Source: Infineon/Adobe Stock)

In the beginning, there was the high-speed (HS) CAN transceiver supporting bit rates up to 1 Mbit/s. In 2016, it has been improved for higher speeds (2 Mbit/s and 5 Mbit/s). With the introduction of SIC (signal improvement capability) technology, CAN FD networks are able to go to 8 Mbit/s. CAN SIC XL transceiver can achieve in FAST mode up to 20 Mbit/s. This article describes the differences and the possible combinations of CAN protocol generations and CAN transceiver technologies.

At the moment three variants of the CAN protocol are available: Classical CAN with 11-bit and 29-bit identifier fields, an 8-byte data field, and one bit rate; CAN FD with 11-bit and 29-bit identifier fields, a 64-byte data field, and two bit rates (arbitration phase and data phase); CAN XL with an 11-bit priority identifier and a separate 32-bit acceptance field, and two bit rates (similar to CAN FD).

As more bytes in the data field are given as longer the time to transmit a data frame is. Additional types of transceivers are needed to increase the bit rate and to reduce the time to transmit a data frame. In the last years, three new CAN transceiver types have been developed.

CAN FD transceiver

The first step to improve bit rate was an improvement of the performance of the CAN HS transceivers. For higher bit rates the specification of the symmetry parameter for the transmitter and the receiver were added and tailored compared to the established CAN transceivers. Transceivers do not care about the protocol. They are only acting as a level shifter and a more precise driver performance allows to increase the bit rate in a network. The basic concept of the transceiver was not changed. With this new concept up to 5 Mbit/s in linear topologies are possible. In star topologies the transmitter concept generates ringing after the dominant-to-recessive transition and this ringing reduces the possible maximum bit rate.

CAN SIC transceiver

The second improvement step of CAN transceiver is the adding of signal improvement capability (SIC). There are two SIC transceiver concepts:

- the transmitter-based approach;
- the receiver-based approach.

In the transmitter-based approach, the transmitter controls the dominant-to-recessive transition and drives the network lines actively to a 0-V differential signal for a certain time (called SIC time). The impedance of the transmitter during the SIC time is 100 Ohm like a typical CAN wire impedance. This reduces the ringing to a minimum and allows higher bit rates. The advantage of this concept is that the recessive bit time can be shorter than the SIC time. The transmitter directly switches from SIC mode to dominant if a dominant signal is transmitted. Bit rates up to 8 Mbit/s are possible with this approach.
The disadvantage is that the ringing is reduced on the transmitting node only. But the transmitting node is the source of the ringing and reduces this ringing very effectively.

The receiver-based approach activates an additional transceiver-internal termination resistor after the dominant-to-recessive transition is detected by the receiver. The advantage is that this additional resistor is activated on all nodes in a network. The disadvantage is that for each bit rate own transceiver implementations are needed. In addition, a shorter bit time leads to a shorter SIC time. For high bit rates the impact is low and 8 Mbit/s cannot be supported.

With CAN SIC transceivers, a 64-byte CAN FD data frame running at 5 Mbit/s in the data phase becomes shorter than an 8-byte Classical CAN frame transmitted with 500 kbit/s. But for CAN XL data frames with payloads up to 2048 byte, a data-phase bit rate of 5 Mbit/s is to slow. A calculation example:

- 8-byte Classical CAN data frame at 500 kbit/s: ~260 µs
- 64-byte CAN FD data frame at 500 kbit/5 Mbit/s: ~200 µs
- 2048-byte CAN XL data frame at 500 kbit/5 Mbit/s: ~3,7 ms

CAN SIC XL transceiver

To increase the bit rate further, the CAN SIC XL transceiver supports two transmitter modes:

- The *SIC mode* is used in the arbitration phase of the CAN XL protocol. It is also possible to use this mode in the data phase. In this mode, the CAN SIC XL transceiver acts as an CAN SIC transceiver. With this mode up to 8 Mbit/s in the data phase are possible.
- In the *FAST mode*, the transceiver controls both levels on the network lines like a Flexray transceiver. The symmetric alternating differential bus signal and the transmitter impedance of 100 Ohm (like a typical CAN wire impedance) allow higher bit rates in the data phase of the CAN XL protocol.

The mode change from SIC mode to FAST mode is controlled by the CAN XL controller (often embedded in a host controller) via the TxD pin. During arbitration phase, the TxD signals are the same as for all other kind of transceivers. TxD high controls recessive level on the network lines and TxD low controls the dominant level. During the FAST mode phase, the CAN XL controller transmits PWM symbols to the transceiver. The length of the PWM symbols can vary between 50 ns and 200 ns. If a transceiver detects this PWM symbol, it changes the mode from SIC to FAST and if no symbols are detected anymore the transceiver switches back to SIC mode. The duty cycle of the PWM symbol represents the level, which is transmitted. If the duty cycle is less than 50 %, this represents a logical 0 and level 0 (positive differential signal). If the duty cycle is above 50 %, this ▷

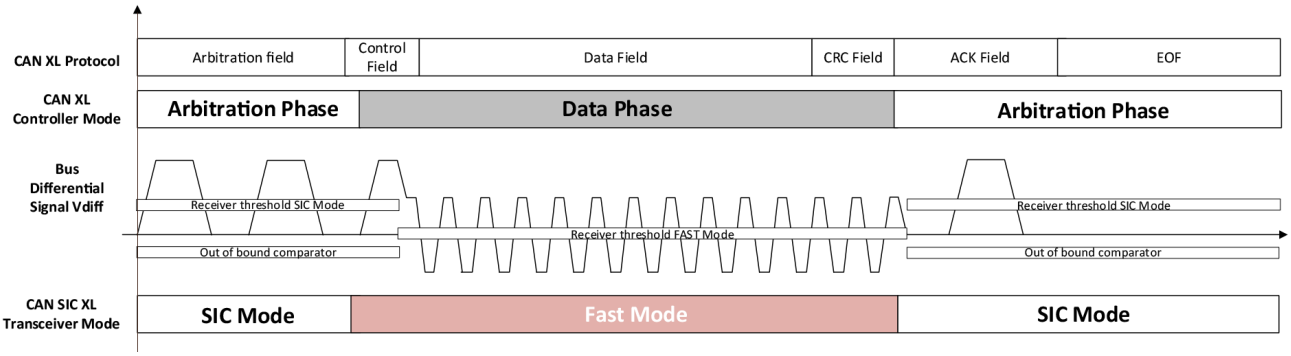


Figure 1: Differential bus signal and receiver thresholds in CAN SIC XL transceiver communication (Source: Infineon)

Table 1: Combination options for CAN SIC XL transceivers and CAN protocol controllers

CAN protocol	Supported CAN SIC XL transceiver mode		Max. possible bit rate
	SIC mode	SIC and FAST mode	
Classical CAN	X	-	1 Mbit/s
CAN FD	X	-	up to 8 Mbit/s
CAN XL SIC mode only used	X	-	up to 8 Mbit/s
CAN XL SIC and FAST mode used	-	X	up to 20 Mbit/s

Table 2: Combination options for all CAN transceiver types

CAN protocol type	CAN transceiver type			Max possible bit rate
	HS transceiver	CAN FD transceiver	SIC (XL) transceiver	
Classical CAN	X	X	X	1 Mbit/s
CAN FD	X	-	-	1 Mbit/s
	-	X	-	up to 5 Mbit/s (point to point)
	-	-	X	up to 8 Mbit/s

represents a logical 1 and level 1 (negative differential signal).

Not only transmitting transceivers are controlled during the data phase with PWM signals. Also receiving transceivers evaluate the PWM signal to switch the receiver into FAST mode. In FAST mode, the receiver thresholds are set to 0 V instead of 700 mV in SIC mode. For more details, you should consult the CiA 612-2 document.

The CAN SIC XL concept guarantees that the CAN protocol controllers and the transceivers are always in the same mode. There is no mismatch due to errors possible.

CAN SIC XL transceiver and CAN protocol variants

The CAN SIC XL transceivers can be used with all CAN protocol generations: Classical CAN, CAN FD, and CAN XL. The CAN XL protocol handler according to CiA 610-1 (in the near future ISO 11898-1) supports all variants of CAN protocols:

- Classical CAN with 11-bit and 29-bit identifier
- CAN FD protocol with 11-bit and 29-bit identifier
- CAN FD light with 11-bit identifier
- CAN XL with 11-bit priority identifier.

CAN Newsletter Online

CAN Newsletter magazine

The new dynamic parameters of CAN SIC

The CiA 601-4 specification for CAN SIC transceivers is released and will be hand over to the updated ISO 11898-2 soon; the CiA 601-1 specification helps to understand the CAN FD high-speed transmission.

Read on

CiA marketing group

Promoting CAN XL

CAN in Automation (CiA) has established the Marketing Group (MG) CAN XL. It organizes joint marketing activities in order to promote the CAN XL protocol as well as related specifications and recommendations.

Read on

CAN technology trends

Back to the roots and closer to the front end

In 2023, the CAN XL ecosystem is going to be completed, CAN FD is increasingly adapted in non-automotive applications, and Classical CAN is applied in deeply embedded networks substituting traditional serial communication links.

Read on

CAN Newsletter magazine

Interviews with providers: CAN SIC transceivers

CAN SIC (signal improvement capability) transceivers can be used in Classical CAN, CAN FD, and CAN XL networks, reduce signal ringing, improve achievable bit rates, and provide more design flexibility regarding topology.

Read on

MCUs with CAN XL

Ready for automotive cybersecurity management certification

Infineon announced that Aurix TC4xx is the first micro-controller unit (MCU) family to be certified according to ISO/SAE 21434 standard for automotive cybersecurity management systems.

Read on

CAN Newsletter magazine

30 years of CiA: Celebration and feedback

On June 1 and 2, CiA and its members celebrated the 30th birthday of CAN in Automation in a nice location in Nuremberg in the midst of the city park. The CAN Newsletter magazine reported about the celebration and CiA members answered some questions in an interview.

Read on

The new CAN SIC XL transceiver supports

- SIC mode (like SIC transceivers according to CiA 601-4 and ISO 11898-2:2023)
- FAST mode (for high bit rates in the CAN XL data phase)

This flexibility allows the combinations of CAN SIC XL transceivers and CAN protocol controllers shown in the Table 1.

The maximum bit rate, given in these tables, depends on the network topology and can be lower. The maximal possible bit rate can be achieved in a point-to-point network (just two nodes) with termination resistors on both ends.

The CAN FD protocol and the CAN XL protocol allows a mixed communication in one network. If a CAN FD protocol handler detects a CAN XL data frame, the protocol handler stops frame detection after FDF bit and changes into the reintegration mode and is waiting to the end of the CAN XL data frame. The CAN XL controller is able to support both data frame types. But for both protocols configuration is needed.

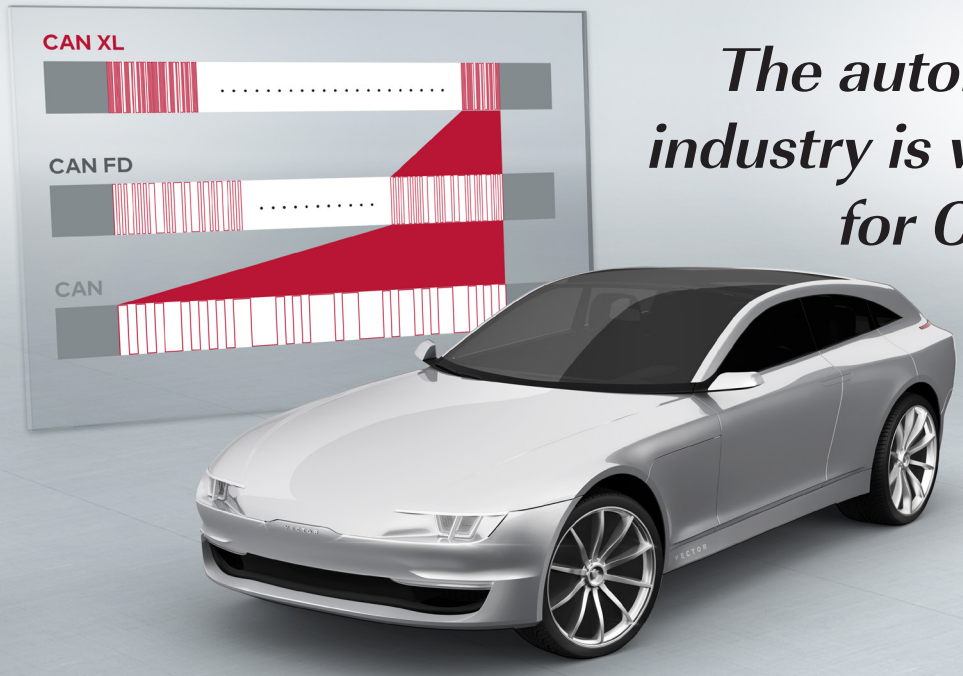
On the physical layer side, it is possible that in FAST mode the differential bus levels can be below the receiver thresholds of CAN FD and CAN SIC transceiver. This has the consequence that from the physical layer point of view a reliable mixed protocol communication is only possible, if all nodes are using CAN FD or SIC mode only. The transceiver with the lowest possible bit rate determines the bit rate.

An example: Some nodes in the network using CAN FD controller and CAN FD or CAN SIC transceiver and other nodes using CAN XL controller and CAN SIC XL transceiver. The communication is working, if the CAN SIC XL transceiver is working in SIC mode only (in arbitration and data phase). This can be configured in the CAN XL controller. In such a network, CAN SIC transceivers allow up to 8 Mbit/s and the maximum possible bit rate in this network can be maximum 8 Mbit/s for CAN FD and CAN XL communication. The maximum bit rate can be reduces depending on the network topology. Have in mind that reflection and ringing on the network lines can reduce the bit rate dramatically. The maximum possible bit rate for each network should be verified via simulation.

The CAN XL protocol handler combined with a CAN SIC XL transceiver allows to support Classical CAN, CAN FD, and CAN XL communication without hardware modification. Only different configurations are needed. Also mixed CAN FD and CAN XL communication in one network is possible.

Author

Magnus-Maria Hell
Infineon Technologies
info@infineon.com
www.infineon.com



The automotive industry is waiting for CAN XL

CAN XL contains many new impressive features, supports both signal-based and service-oriented communication, and is ideally tailored to future requirements. Numerous experts from the CAN industry met to exchange ideas on this topic at the Vector CAN Technology Symposium in Stuttgart at the end of October 2022.

(Source: Vector Informatik)

After many online events recently, the symposium organized by Vector (the CAN Newsletter Online reported) as a face-to-face event offered international participants a welcome platform for direct exchange and intensive networking (Figure 1 and Figure 2). The thematic focus was on CAN XL, the third CAN generation that will play a significant role in shaping the E/E architectures of future vehicles. The program included a broad spectrum of presentations given by Bosch, CAN in Automation, Infineon, NXP, Renesas, STMicroelectronics, VW/Cariad, and Vector – as well as an accompanying exhibition. This article summarizes selected topics of the presentations.

Our mobility is currently undergoing fundamental changes, with electronic systems in motor vehicles gaining considerable importance. The trend favors centralization with high-performance computers (HPC) and zone controllers. ECUs (electronic control unit) and networks are no longer functionally divided into domains such as powertrain, chassis control, infotainment, and so on; instead, the focus is on zone architectures with subordinate networks (Figure 3). With up to 200 ECUs in a vehicle, the automotive industry must keep the costs for cabling, hardware, and software manageable. For this purpose, the Volkswagen group has founded the affiliated software company Cariad.

CAN XL increased to 20 Mbit/s

One of the main motivations for CAN XL is to bridge the bit rate gap between Classical CAN/CAN FD and Ethernet 100BASE-T1. On the other hand, even modern E/E architectures cannot do without fast signal-based communication, for example in real-time control circuits within zones. In this bit rate range, the 10-Mbit Ethernet version 10BASE-T1S is also available as a networking option.

With CAN XL, a sophisticated networking solution has been created, combining all essential requirements in one system. Thanks to a transfer rate of up to 20 Mbit/s, CAN XL easily meets the original requirement of ≥ 10 Mbit/s. It is (cost)-effective, robust, and real-time capable like the previous versions and, as a special feature, is also able to transmit external protocol information via tunneling. The latter primarily aims at enabling a service-oriented architecture for XL nodes as well. Ethernet tunneling also allows them to receive and transmit Ethernet frames – in addition to CAN XL messages, of course.

CAN XL: Technical details

Thanks to the features mentioned above, CAN XL is ideally suited for future automotive applications. On the one hand it is flexible, and on the other hand it provides important additions and innovations with regard to the protocol to implement the mentioned functionality. The CAN XL data field may now have lengths between 1 and 2048 bytes. This large user data length is required to tunnel Ethernet frames. In contrast to Classical CAN and CAN FD with identifiers of either 11 bits or 29 bits, CAN XL only uses 11-bit identifiers. This is fully sufficient, because – as will be shown below – CAN XL has quite a few new fields that provide more clarity and thus simplify handling. The restriction to the 11-bit identifier also increases robustness.

No changes have been made to the network access method; the CSMA/CR method (Carrier Sense Multiple Access/Collision Resolution) is still used. It provides a clear priority concept that allows the more important frame to be transmitted with no delays. The identifiers of Classical CAN and CAN FD include some important information such as priority, frame type, and source and destination addresses. ▷

Figure 1 + 2: 150 experts with international backgrounds welcomed the Vector Symposium in Stuttgart as a platform for information exchange and intensive networking (Source: Vector Informatik, photographer: Marc Feix Photography, Stuttgart)

This is a hindrance for large networks and high dynamics. Therefore, CAN XL defines a clear separation and introduces some new fields and new functions. The Arbitration field, for example, now contains only the priority.

The new fields and functions include the Acceptance Field, VCAN ID, SDU Type, Bit Stuffing, CRC (PCRC 13 bit and FCRC 32 bit), and Transceiver Mode Switching. While the SDT Field (Service-Data-Unit-Type) specifies the information in the Data Field (Figure 4), the SEC bit signals whether further layer-2 functions are applied, for example QoS or Security. The VCID Field allows the assignment of virtual CAN IDs. Up to 256 virtual networks can be defined within a single CAN XL network segment. They can be used to build up logical structures depending on how they are useful to make work easier. The AF (Acceptance Field) has a width of 32 bits and can be used for addressing. Source and destination addresses and also 29-bit identifiers can be stored.

CAN XL uses fixed stuff-bits, which are used in the data phase. As with Flexray, there are now two cascaded CRCs (cyclic redundancy checking) instead of just one for the detection of transmission errors. This provides very high transmission reliability with a Hamming distance of 6. The reliability of CAN XL frames has been independently verified by the Special Interest Group (SIG) CAN XL of Stuttgart and Kassel Universities. During the CAN Technology Symposium event, a video with the chairman of the Special Interest Group CAN XL at CAN in Automation, Mr. Dr. Arthur Mutter (Bosch), was recorded about CAN XL called "CAN XL - The next step in CAN evolution".

New physical-layer technologies

The symposium participants were given interesting insights into the processes on the physical layer, which is no longer a matter of bits and bytes, but of analog voltage characteristics. The transceivers are always responsible for generating the bus voltages. A fundamental requirement for transceivers is to be highly resistant against interference of all kinds, for example electrostatic discharge (ESD), and to emit little interference themselves. The performance of the transceiver type determines the bit rates a network can achieve. Therefore, CAN versions with increased or very high bit rates require better transceivers. Two new technologies are dominating current discussions on signal enhancement in this context: CAN SIC and CAN SIC XL. CAN allows complex topologies consisting of mixed line and star networks including long stubs, which naturally leads to reflections on the bus. Since ringing caused by reflections limits bit rates, this is where the improvements through SIC and SIC XL technologies must come into play.

With CAN SIC up to 8 Mbit/s

CAN SIC has been specified in the CiA 601-4 document by CAN in Automation (CiA). The goal is to actively dampen the ringing during transition from dominant to recessive. This allows the signal to reach a steady state more quickly, and it can be sampled correctly. Bit rates of up to 8 Mbit/s are possible even in networks with sophisticated topologies.

CAN SIC XL for 20 Mbit/s

For CAN XL transmission rates up to 20 Mbit/s, SIC XL transceivers are required. They also provide a special Fast mode in the data phase. While SIC XL uses SIC technology in the arbitration phase, a push-pull concept with alternating differential signal of ±1 V is used in Fast mode. Due to the lower differential voltage and the active driving of both levels, bit rates of 20 Mbit/s are possible.

Even experts are often unaware that there is no rigid link between the protocol and the type of transceiver. For CAN XL communication, all types of transceivers can be used. If a CAN FD transceiver is used for CAN XL, only the bit rate is limited to approx. 5 Mbit/s. Micro-controllers with CAN XL IP can handle automatically the Classical CAN, CAN FD, and CAN XL protocols. The controller just needs to be configured in the software. The resulting flexibility makes it much easier to switch from Classical CAN or CAN FD to CAN XL. The bit rate can be configured in the same flexible way. The usual speeds of 2 Mbit/s, 5 Mbit/s, 8 Mbit/s are merely limits. If any difficulties should arise with a network originally designed for 8 Mbit/s, the bit rate can easily be reduced, for example to 7,5 Mbit/s.

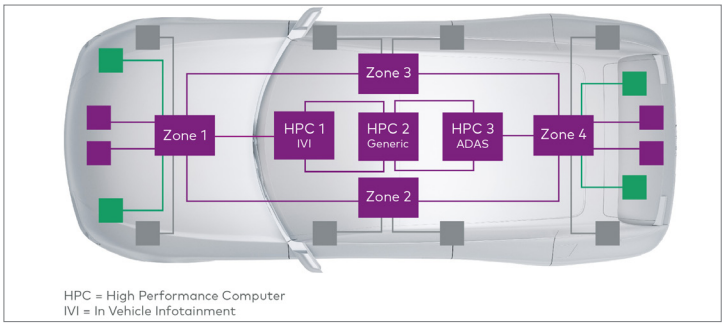
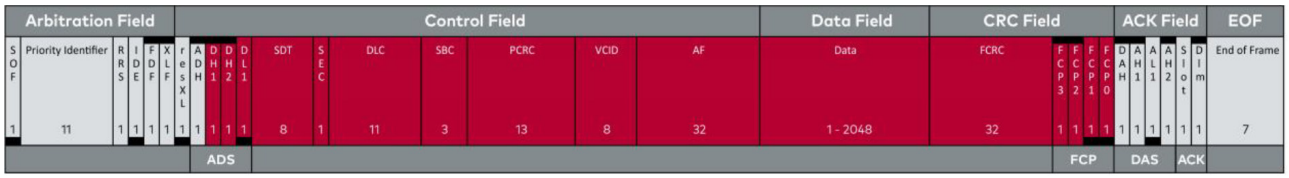


Figure 3: Possible future zone architecture in vehicles (Source: Vector Informatik)



SOF	Start of Frame
PID	Priority Identifier
RRS	Remote Request Substitution
IDE	Identifier Extension
FDF	FD Format
XLF	XL Format
resXL	reserved bit XL format
ADS	Arbitration-to-Dataphase Switch
SDT	Service Data Unit Type
SEC	Simple Extended Content
DLC	Data Length Code

SBC	Stuff Bit Count
PCRC	Preface CRC
VCID	Virtual CAN Identifier
AF	Acceptance Field
Data	Data Field
FCRC	Frame CRC
FCP	Format Check Pattern
DAS	Dataphase-to-Arbitration Switch
ACK	Acknowledge
EOF	End of Frame

Figure 4 + Table 1: Detailed description of CAN XL frame (Source: Vector Informatik)

CAN XL meets Autosar

How do CAN XL and Autosar fit together? What are the main changes in Autosar? What effort is necessary to upgrade ECUs for CAN XL? As expected, concrete changes to the Autosar documents can mainly be found in the specifications for CAN transceivers, CAN drivers, and CAN interfaces, but also in the Ethernet interface specifications. CAN XL must now be definable as a physical medium for the Ethernet stack. For this, new configuration parameters have been defined. It must be possible to describe the CAN XL controllers in the ECU configuration. Existing value ranges such as bit rates, for example, must be adjusted. For this, these two new documents will be added: AUTOSAR_SWS_CANXLDriver and AUTOSAR_SWS_CANXLTransceiverDriver.

Modifications to the Autosar system template are required for the system description of the CAN XL-specific controller configuration. Frame triggering has been adapted for CAN XL frames and the new XL fields have been integrated. Fortunately, there is no need to change the description of signals and PDUs. For Ethernet frame tunneling, however, somewhat major changes must be made to the system template. Among other things, the responsible Autosar Concept Group has decided to introduce the Ethernet interface as a further upper layer for CAN XL. This allows access to the IP stack and service-oriented communication (SOME/IP, SOME/IP-SD). Consequently, IP communication via complex CAN topologies is now possible.

For a project update of a pure CAN ECU to CAN XL with unchanged communication description, adjustments are mainly necessary to the CAN interface and the driver layers. A more complex process, however, is the migration of an Ethernet ECU to a CAN XL ECU. New modules are added, especially because the ECU now needs a CAN interface and a CAN state manager even with pure Ethernet tunneling. However, this provides the advantage of using CAN and Ethernet communication on the same network. The CAN XL Autosar concept was approved in November 2022. A CAN XL product solution for the Autosar workflow is expected from Vector around mid 2023.

CANsec: Hardware-implementable security protocol

Another key requirement for future mobility is security. The new CANsec security protocol adds integrity, authenticity, and confidentiality to ECU communication. Without appropriate measures, it is basically quite easy to attack CAN. Since every CAN participant listens to all frames, it is sufficient to compromise a node to gain access to the communication. Attacks such as spoofing, sniffing, and message replay make the operation of engine controls, braking systems, and so on directly vulnerable. Autosar already has the SecOC security protocol, but this is at the top end of the protocol stack and places high demands on CPU performance.

The CANsec protocol provides the solution. Preferably implemented in hardware, it works efficiently and fast. Both sender and receiver have secret keys that must be transferred to the devices beforehand in a secured way. The AES (advanced encryption standard) generator on the CANsec controller encrypts the frame to be sent and provides it with the Integrity Check Value (ICV) and verification information. If the receiver calculates the same ICV value during decryption, data transmission was done correctly. CANsec allows secure zones to be formed from several participants. Their communication can now no longer be interpreted by other participants on the same network segment. CANsec is fully implementable in hardware and software to enable smooth migration to the next vehicle platforms.

Small and smart: CAN FD Light

CAN FD Light is a simple but efficient networking system derived from CAN FD. Unlike all other CAN versions, the commander-responder principle is used here, similar to ▷

LIN. Since only a limited number of nodes are to be controlled, 11-bit identifiers are sufficient. There is no bi-trate switching, the data rate always corresponds to the arbitration data rate. CAN FD Light uses exclusively CAN FD frames because they offer clear advantages over Classical CAN with their user data length of 64 byte. CAN FD transceivers according to standard ISO 11898-2 are provided for the bus structure.

CAN FD Light protocol controllers for responder nodes are housed in a single monolithic IC. On the responder side, no more software is required. The responders' memory addresses are accessed directly. In addition to addressing individual participants, many responders can be addressed simultaneously via multicast and broadcast frames. On the commander side, a conventional CAN FD controller is used. CAN FD Light thus offers a cost-effective solution for query sensors and controlling many small actuators.

Existing CAN FD know-how, analysis tools, and interfaces can be reused almost unchanged for CAN FD Light. The SIG of CiA is responsible for standardization, design recommendations, and conformance testing. The CAN FD Light specification on the part of CiA has been completed; ISO standardization as a normative annex for ISO 11898-1 is in progress.

Summary and perspectives

CAN XL, which has been further developed on the basis of Classical CAN and CAN FD, scores with several innovations and is ideally tailored to the requirements of future E/E zone architectures. New fields in the protocol provide more clarity and facilitate software development. On the physical layer, the new CAN SIC and CAN SIC XL technologies significantly increase transmission speed up to 20 Mbit/s.

One of CAN XL's outstanding features is the tunneling of Ethernet frames. This allows both signal-based real-time communication and service-oriented communication via the same network. Consequently, CAN networks with complex technologies are also available for IP communication. Multi-drop architectures connect multiple participants without switches and save costs on cable harnesses. On the software stack side, any CAN XL ECU can be turned into an Ethernet endpoint and allow service-oriented communication there as well. CAN XL thus also offers good prerequisites for the migration of various higher protocols. The first controller prototypes are expected to be distributed to OEMs (original equipment manufacturers) by semiconductor manufacturers in mid 2023, so the first CAN XL controllers could be freely available by mid 2024.

Author

Peter Decker
Vector Informatik
info@vector.com
www.vector.com

CAN XL as backbone for body application

CAN XL, the third CAN generation, provides high-layer protocol management functionality. This allows running multiple applications using different higher-layer protocols on a single CAN XL backbone network. A typical application is commercial vehicle backbone network for body applications.

Some commercial road vehicles, trucks, and trailers, provide a gateway device for body builders. The gateway is connected to the in-vehicle networks often based on Classical CAN J1939 networks and provides on the other side a Classical CAN port to be connected to body applications. Body applications include tail-lifts, truck-mounted cranes, tippers, refrigerators, etc. There are also complex body applications with more than one control unit. Especially, refuse-collecting trucks and fire-fighting vehicles implement even several CAN body application networks. Most of the CAN interfaces for the body builder provide J1939 parameter groups (PG); an exception is Iveco offering a CANopen-based interface. In order to backbone multiple body application units with optional deeply embedded CAN networks, the DIN 4630 standard has been developed. The first edition was published in May 2022. It is based on Classical CAN using J1939 or CANopen as higher-layer protocol.

CAN XL possibilities

In 2018, CiA members started to develop the third CAN generation, also known as CAN XL. The CAN XL protocol (CiA 610-1) separates the ID functionality represented by two independent protocol fields: the 11-bit Priority ID field and the 32-bit Acceptance field. The data field has a length of 1 byte to 2048 byte. The CAN XL SIC physical medium attachment specification (CiA 610-3) uses optionally a PWM (pulse-width modulation) coding enabling dataphase bit rates of above 10 Mbit/s. Applying linear topologies, up to 20 Mbit/s have been achieved. CiA has already submitted its CAN XL lower layer specifications (CiA 610-1 and CiA 610-3) to ISO for international standardization.

The CAN XL data link layer protocol features embedded OSI layer configuration as specified in ISO 7498-4 (Information processing systems – Open Systems Interconnection – Basic Reference Model – Part 4: Management framework). This includes the PCS (traditional non-return to zero (NRZ)) coding or the optional PWM coding, the data link layer (Classical CAN, CAN FD, or CAN XL frame formats), and the higher layers. The higher-layer configuration possibility by means of the SDT (Service Data Unit Type) field is new. It allows the transmitter to indicate in the CAN XL data frame, which higher-layer protocol is used. This enables the network designer to run different higher-layer protocols on the same cable. The usage of the 8-bit SDT field is specified in the CiA 611-1 document. The receiver of a CAN XL data frame knows from the SDT value, how to interpret the CAN XL data field.

Additionally, the CAN XL protocol provides the VCID (Virtual CAN Network ID) field. This 8-bit field indicates to which virtual network the received data frame belongs to. With this approach, the system designer can implement several network applications on one network cable, if such a backbone network provides sufficient bandwidth. Combined with the SDT field one can run even multiple instances of the same higher-layer protocol on such a backbone network.

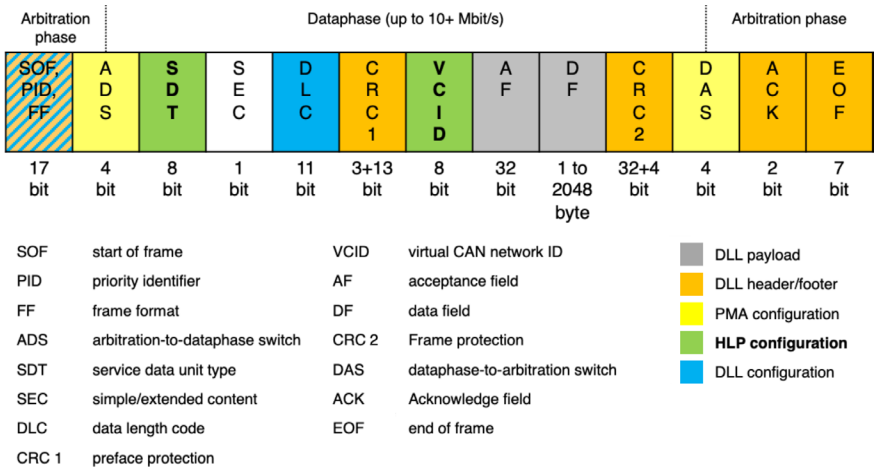


Figure 1: The CAN XL frame embeds higher-layer protocol (HLP) management information: the SDT and the VCID fields enable to run multiple instances of different HLPs on the same network segment (Source: CAN in Automation)

Example: Fire-fighting body application units

Fire-fighting trucks are equipped with body application units (BAUs). Some of these BAUs need to communicate with the in-vehicle networks provided by the truck or chassis manufacturer by means of an IGU (in-vehicle network gateway unit). Optionally, there are additional units connected to this body builder network such as a TGU (telematic gateway unit) or an FMU (fleet management unit). Each BAU may also comprise a deeply embedded ▷

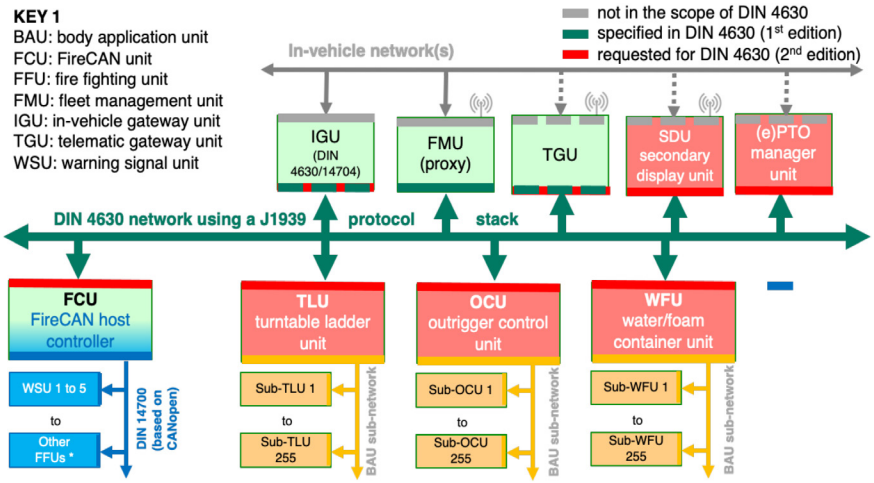


Figure 2: Example of the body application of a fire-fighting truck using Classical CAN networks (Source: CAN in Automation)

network. Typically, all these networks are based on Classical CAN. Most truck OEMs (original equipment manufacturers) provide a J1939-based IGU, to which the fire-fighting truck suppliers connect their BAUs.

The body builder network for commercial vehicles is standardized in DIN 4630 (Road vehicles – Data parameter specification for body application units in commercial vehicles) in English language. It specifies a generic IGU, the TGU, the FMU, and several BAUs. The first edition of this document does not standardize specific BAUs for fire-fighting vehicles.

Depending on the fire-fighting vehicle's functionality, there are different proprietary BAUs connected to the body application network. Normally, fire-fighting trucks are produced in low quantities. They provide more or less a unique functionality. This is not cost effective. Each vehicle needs to be equipped individually. This is why the fire-fighting industry (vehicle OEMs and suppliers) developed the DIN 14700 series standardizing fire-fighting devices such as battery chargers, frequency inverters, pumps, signal warning units, etc. This approach is also known as FireCAN. The specified communication interface for the devices is based on CANopen, but not compliant to the above-mentioned standards and specifications. To overcome this weakness, the DIN 14700 series is currently in review. One objective is to harmonize the communication optionally with the CiA 301 CANopen application layer and communication profile. The DIN 14700 parts will be integrated into a single standard also published in English language. The DIN 14700 host controller manages the communication with the fire-fighting units (FFU). These FFUs are virtual entities. This means a real device can host one or more FFUs. They are directly connected to ▷

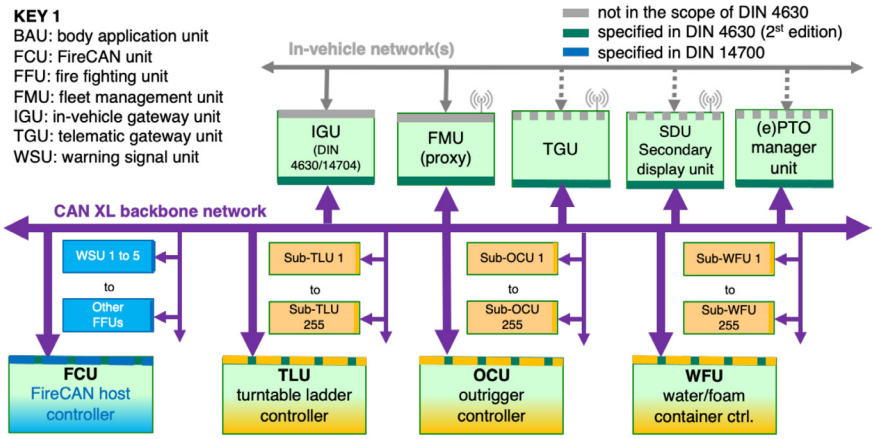


Figure 3: Example of a fire-fighting truck body application with a CAN XL backbone network (Source: CAN in Automation)

the body application network. The host controller acts as a gateway communicating with the IGU, TGU, and FMU by means of the body builder network (in the future based on DIN 4630). In order to standardize the IGU specifically for fire-fighting trucks, DIN has developed a special document. The DIN 14704 (Fire-fighting and fire protection – Fire-fighting-specific parameters for in-vehicle gateway units) standard is based on DIN 4630 using a J1939 mapping of parameters. It specifies the mandatory and optional suspect parameters (SP) and the parameter groups (PG).

But there are still several not standardized interfaces for fire-fighting BAUs. This includes the FireCAN unit (FCU) interface, the water/foam container unit (CU), the outrigger control unit (OCU), the turn-table ladder unit (TLU), the aerial working platform unit (AWPU), etc. For e-vehicles, additional equipment such as power battery units (PBU) and an energy management unit (EMU) is required. There is also a desire to use the vehicle's second dashboard for body application purposes.

Implementing multiple Classical CAN networks leads to complex wiring harnesses and additional hardware for bridges, routers, and gateways. The effort to tailor the body application functionality is high. Even with standardized units the integration of fire-fighting equipment is somehow challenging. When implementing a single backbone network, the integration task would be much easier.

CAN XL provides suitable features

CAN XL is a candidate for such body application backbone networks. It provides sufficient bandwidth to substitute multiple Classical CAN networks. Additionally, it features the necessary functionality to migrate from a multiple Classical CAN approach to a single backbone network approach. The protocol-embedded higher-layer protocol configuration function, the SDT field, allows to indicate the used higher-layer protocol (e.g. CANopen, J1939, or proprietary ones). This enables running CANopen and J1939 applications on the same network. In combination with the VCID field indicating a dedicated virtual network, one can even run multiple CANopen or multiple J1939 networks on the same network cable. In total, one can assign 255 virtual network IDs.

Applying virtual networks and virtual functional units allows implementing multiple virtual communication interfaces on a single CAN XL hardware port. Implementing multiple functional units is already supported by classical CANopen: up to eight logical devices can share one node-ID. If more functional units need to be realized, multiple CANopen nodes with different node-IDs can be implemented. Another option is the implementation of an application profile. CANopen application profiles enable the implementation of virtual devices as the J1939 application profiles are doing. But the mixing of CANopen devices and J1939 devices in a single Classical CAN network is only possible in theory. The limited bandwidth is one practical challenge. Another one is that J1939 allows proprietary use of data frames in CBFF (CAN base frame format). This could lead to double-use of 11-bit identifiers. CANopen supports optionally the use of data frames in CEFF (CAN extended frame format), which could lead to conflicts with J1939 parameter groups. If multiple proprietary higher-layer protocols need to be integrated, a single Classical CAN network with a harmonized network layer is required.

Conclusions

Body builder networks based on CAN XL overcome all described limitations and challenges. Especially, the above-mentioned higher-layer management options (SDT and VCID) embedded in the CAN XL data frame enable the integration of heterogeneous higher-layer protocol approaches. The separation of arbitration and addressing functions in the CAN XL protocol is another important feature to enable the integration of heterogenous higher-layer protocols, which can be instanced, too.

The data-phase bit rate of more than 10 Mbit/s allows the straight-forward integrations of multiple Classical CAN network segments without communication optimization. However, this high bit-rate requires the use of so-called SIC XL transceivers, which limit the arbitration bit rate. But this is not a real limitation, because the required network length limits the nominal bit-rate to 500 kbit/s (125 m) or even lower to 250 kbit/s (250 m).

Adapting an MPDU (multiple process data unit) concept mapping several application layer PDUs in a single CAN XL data frame can optimize the communication, because the data link layer (DLL) header/footer is shorter and the DLL payload is longer (up to 2048 byte). Of course, such an MPDU concept requires an additional header/footer in the communication middleware mapped to the application layer payload. But this protocol overhead is mapped into the CAN XL data field, which is transmitted with the configured data-phase bit rate.

Coming back to the example of the fire-fighting vehicle: The legacy body application integration network (legacy backbone) can be integrated with the BAU-specific embedded networks (e.g. DIN 14700). The legacy hardware gateways become virtual gateways folded on a single CAN XL port. This allows to use a single wiring harness optimized to the vehicle's constructions and to pre-install connectors at places, where generic electronic control units (ECU) with CAN XL connectivity can be placed. The ECU functionality is software-configurable as well as gateway functionality. This reduces the effort for the wiring harness as well as number of CAN XL ports.

The described fire-fighting vehicle example is applicable to other complex vehicle body applications ("machines on wheels"). This includes, for example, refuse collecting trucks and trucks with multiple BAU functions (e.g. refrigerator and tail-lift or truck-mounted crane and tipper). The presented backbone approach integrating several legacy networks is also suitable for other commercial off-highway and off-road vehicles as well as agriculture, forestry, mining, and earth-moving machinery. Container-handling equipment, forklifts, and road pavers are other examples. ◀

Author

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

Virtual commissioning for industrial machines

Simulation of a robot plant in automotive manufacturing (Source: Adobe Stock, Machineering)

The Iphysics tool from Machineering enables virtual simulation of a machine on the physical and software levels. For example, CANopen-based communication between integrated drives and higher-level control can be simulated as well. Especially in the planning and development phase, this helps to save costs and time.

A lot of medium-sized companies either do not or only occasionally use virtual commissioning in engineering, the reason being that it is difficult to quantify the benefits of these technologies. On closer inspection, it becomes apparent that cost and time savings are possible in different project-phase areas.

Iphysics from Machineering provides users a tool for implementing virtual commissioning. Especially the connection of devices such as controllers, drives (also implementing CANopen interfaces) as well as various kinematics from different manufacturers make the system implementation more intuitive, safe, and fast. Using virtual commissioning, problems and possible improvements can be identified early in the development process and can thus often be avoided. Expensive repairs of the actual machine and subsequent customer complaints are therefore reduced. Engineers have more time for their actual tasks if they do not have to deal with time-consuming amendments, sometimes at the customer's site.

What is virtual commissioning

Virtual commissioning is part of a modern machine development process. It includes testing and changing of construction data, planning data, and control software in advance using a virtual system. After a successful virtual commissioning, and once changes and optimizations are carried out virtually, the transfer to a real machine can begin. Therefore, errors are recognized and can be eliminated in the early development phases. This happens before the errors could lead to additional expenditure in terms of costs and time.

A physics-based 3D simulation serves as the basis for virtual commissioning, which simulates the real behavior of the machine as a virtual model, ideally in real time. In this way, the entire system, individual machines, or certain machine elements can be presented. This enables to visualize, in particular, the interplay between the individual machines and more complex collaborations with, for example, robots or material flows.

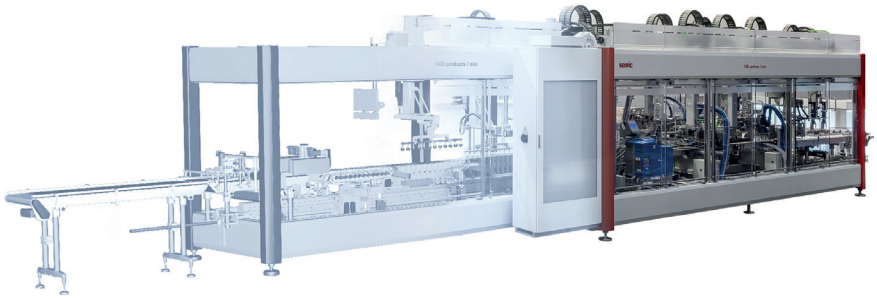


Figure 1: Simulation model of a complete packaging machine (Source: Somic Verpackungsmaschinen, Machineering)

From today's perspective, virtual commissioning considers all the challenges that arise during the development, such as changing customer requirements or changes in construction. Even technologies that are not yet fully developed, supplier bottlenecks or the lack of communication between those involved in the development, can be recognized and avoided at an early stage. This eliminates time-consuming changes at the end of the development process. Problems on the real machine that could not have been foreseen beforehand, can be avoided. Furthermore, projects that cannot be implemented can be stopped early and then adapted according to given possibilities.

The software component of machines is steadily increasing these days. With the help of virtual commissioning, it is possible to represent the interaction of mechanics, electronics, and software at any point in the development process. Thus, companies can counteract the increasing cost pressure, reduce material waste during machine start-up, and avoid production interruptions due to inadequately tested software.

Commissioning through simulation

Virtual commissioning can be carried out with the help of simulation. The simulation software should be at the center of the development as a cross-departmental platform to verify the current state of development at all times and check for feasibility with other areas. Hereby, the mechanical, electrical, and software departments use the same models simultaneously, which they work on in their native development environment, furthering the development together and immediately able to test the interaction using the simulation. This way, the current state of development in mechatronics development is tested in an interdisciplinary and continuous manner during the earliest phases of the process.

To use the simulation software as a cross-departmental platform, it is necessary that the simulation has a stable bi-directional interface to the inventor. This is implemented in the simulation software Iphysics whereby changes on the simulated model are also immediately available in the CAD (computer-aided design) system, thus eliminating the need to change the model redundantly. By connecting

Figure 2: Coboworx pelletizing cell and panel with the digital twin of the plant (Source: Coboworx, Machineering)

various control devices, drives, and robot kinematics, these can already be tested during virtual commissioning under real conditions and, if necessary, adapted.

CiA 402 drive operation modes available in library

The Iphysics tool supports software libraries for simulation of drives' real-time behavior inside of machines in the design phase. Recently, Machineering has extended the library with drive functionalities according to the CANopen device profile for drives and motion control (CiA 402). CiA 402 (IEC 61800-7-201/-301) specifies several operation modes and according application parameters for frequency inverters, servo-controllers, and stepper motors. The tool supports the common operation modes for positioning, velocity control, homing, as well as the cyclic synchronous position mode. The implemented homing mode includes homing methods with limit and homing switches. Thus, simulation of a pre-defined CANopen-based communication between drives (moving machine parts) and higher-level control is possible. In the future, it is planned to implement further operation modes such as the touch-probe functionality.

Potential of virtual commissioning

Practice has proved that using of virtual commissioning can have positive effects on productivity, quality, and the time-saving factors. It can also help to reduce invisible waste in the processes. With regard to productivity, early safeguarding of machine concepts and machine behavior reduce the risk for both human and machine. Due to improved communication and early knowledge, the coordination effort and the effort for troubleshooting can be reduced. As different program variants can be run, the optimal program can be developed early in the process. Productivity is also increased because of greater employee satisfaction, as they can focus on their actual tasks. With the help of virtual commissioning and the digital twin that is being created in parallel with the development, training for customers is possible on the virtual machine. Conversion to new products can also be tested in advance and implemented quickly during operation.

Companies can also benefit from a reduction in quality costs, as machine elements with the software to be installed have already been tested at an early stage. Thus, the company is able to deliver sophisticated machines to the customer. The customer will not have to deal with subsequent rework, corrections, and modifications. During the developmental phase, individual steps can be coordinated with the customer and approvals as well as identified problems can be discussed using the digital twin. Solutions that were virtually tested in advance can thus be transferred to the actual machine.

A shortening of the overall development time as well as the associated adherence to delivery dates speak to the use of virtual commissioning. Due to the parallel engineering in particular, the PLC (programmable logic controller) programming, for example, is adequately adapted, which results in the throughput time being shortened by 70 %. The time for troubleshooting and rectification of potential errors is also significantly reduced. Employees are able to spend less time at the customer's site, as many issues can be clarified in advance. Thus, they are able to focus on new projects sooner.

Practical example

In a practical example, an inventory was carried out at an exemplary machine manufacturer. Process indicators such as throughput times, complaint and error rates, KPIs (key performance indicators) for ongoing projects, and personnel costs were determined. A customer-specific concept with a set of rules for the use of simulations was then developed, showing how virtual commissioning can be optimally anchored and implemented within the company.

One year after the project start, these key figures were determined once again and the savings achieved were quantified. Around two-thirds of these savings can be

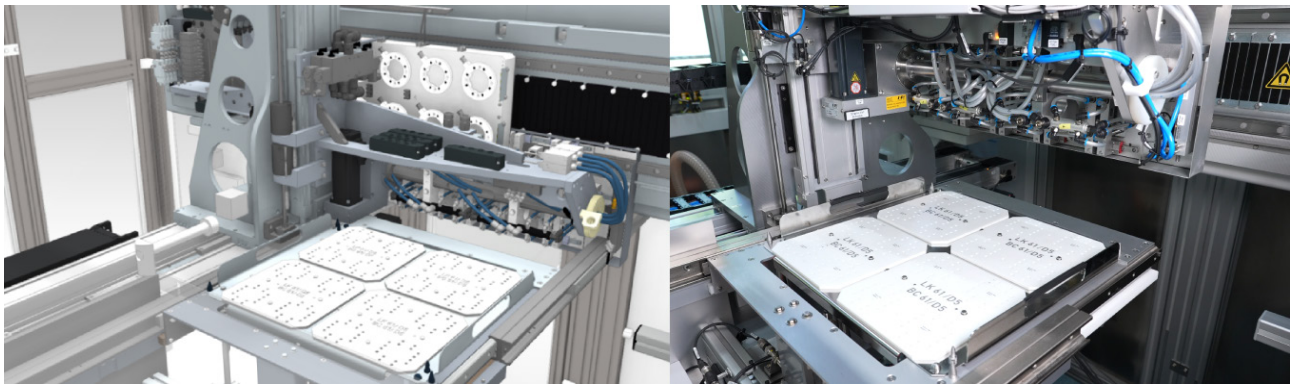


Figure 3: Plastic injection molding machine for pharmaceutical disposables and its digital twin (Source: MI Micro, Otto Männer, Machineering)

Figure 4: AR (augmented reality) application from Iphysics for hall planning (Source: Adobe Stock, Machineering)

attributed to the increase in employee productivity, mainly generated by the early validation of concepts and the avoidance of unnecessary activities such as trouble shooting. 26% of the savings were achieved by improving quality and measuring the reduction in quality costs through the decrease in customer complaints and error messages. 8% were due to the savings based on the increased adherence to delivery dates and the reduction of contractual penalties. The practice has also shown that the potential of virtual commissioning can only be fully exploited if it is deeply implemented in the processes. ◀

Author

Beate Freyer
Machineering
sales@machineering.com
www.machineering.com

Standards and specifications

(Source: Adobe Stock)

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

Does it matter, if something is required, commanded, confirmed, or indicated?

Parameter specifications in SAE J1939 documents and also in ISO standards referencing the SAE recommended practices are not always consistent in terminology. This makes them hard to read and to understand. Of course, most of these issues are based on the fact that we have to live with our historical failures. Already the term Suspect Parameter (SP) is today misleading, because not all J1939 parameters provide an embedded error indication, for example some enumeration parameters. Just using the term parameter would be perhaps the better choice. In addition, some J1939-related specifications use the term signal as a synonym of SP. But "signal" seems something related to physics.

ISO 11992-3 is somehow confusing newcomers

If you are a longtime fellow of J1939, you can stop reading. You will not consider the SP descriptions given in the J1939 Digital Annex or one of the ISO standards defining the SPs. Many of them provide ambiguous information and are sometimes not easy to understand – especially for non-native English speakers.

In the last edition of the ISO 11992-3 standard (CAN-based truck/trailer link), many SP descriptions have been reworded. Unfortunately, these texts do not use verbs consistently describing the function of the parameter. It matters, if you define that an SP requests or commands something. We know this quite well from human communication, there is difference to give a command (you are not allowed not oppose) or request something (this is just a wish, but the decision is made by the receiver).

In most cases, the towing or the towed vehicles just send requests and not commands mapped into the Parameter Groups. The corresponding response on the application level is the confirmation by means of SPs containing status information. If, for example, the "Clutch-independent PTO switch" description reads: "This parameter indicates the status of the clutch-independent PTO switch", you can guess if this is a request or command. Or you even may think this is a status.

In order to avoid misunderstandings: The ISO 11992-3 SP specifications are technically correct. The descriptions are in some cases ambiguous and can therefore lead to misunderstandings. This relates mainly to the PTO (power take-off) parameters, the lighting parameters controlling the trailer illumination, and some other functions. ■

DIN 14704 published

Beginning of this year, DIN has published a standard in English language specifying the body builder gateway for fire-fighting trucks. It is based on J1939 and DIN 4630 (published in May 2022). DIN 4630, also written in English language, is a generic standard for commercial vehicle body builders and can be applied on trucks and trailers. DIN 14704 standardizes the mandatory and optional Suspect Parameters (SP) and Parameter Groups (PG) dedicated for fire-fighting trucks. In the next edition, additional functional units (e.g. Telematic Gateway Unit) are intended to be added. ■

Efficient diagnostic simulation on CAN FD

Diagnostic simulation is the proven means when a test counterpart is not yet or no longer available. Whether in test preparation, in regression tests, or in training facilities. The targeted use of such a solution makes it possible to avoid mistakes.

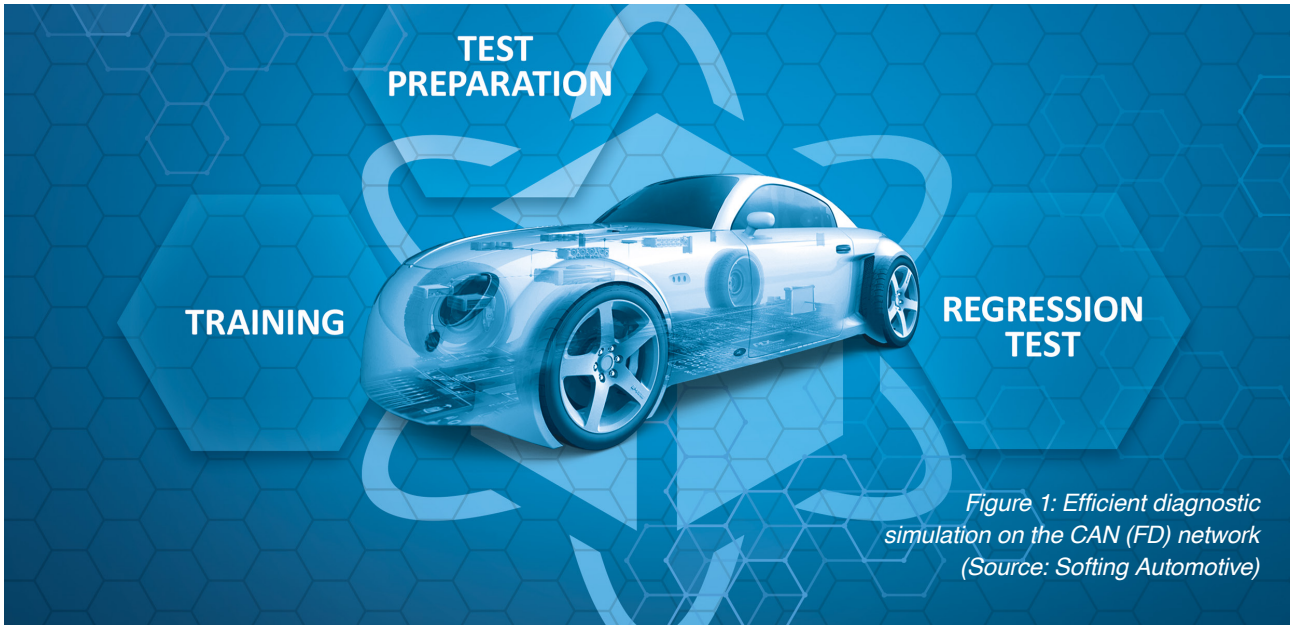


Figure 1: Efficient diagnostic simulation on the CAN (FD) network (Source: Softing Automotive)

The complexity of E/E networking is increasing all the time – and with it the necessary effort involved in testing. This is true both in terms of the validation of functionalities and in terms of ongoing regression tests of the test methods. Modern vehicles all have a large number of variants, which are usually shown by software configurations in combination with varying states of assembly. Different motorizations, for example, are generated both using a range of different engines and via coding. The number of variants also increases over the life cycle, as new software versions with changed behavior enter the field.

In diagnostic testers, this complexity should not be underestimated. After all, the test environment has to be adapted in each case, while ensuring that the existing functionality is not compromised. This has to be proven each time. As far as testing new functionalities is concerned, the question of validating the test environment is also raised on a regular basis. If in doubt, this can be left until the device under test (DuT) arrives. Troubleshooting between the test method, test environment (consisting of computer, vehicle communication interface, and cabling) and the DuT then takes considerable time, time which could well be missing later when it comes to testing.

As different as the two cases may seem, they have something in common: a lack of suitable counterparts. In the case of test preparation, this facilitates the error-free commissioning of the test setup. This means that when the DuT arrives, any error that occurs can be clearly assigned to it. This either results in a reduction of the test time or enables a much greater test depth and range in the same test time. In a regression test, as many installation and software variants as possible must be available to be able to make a valid statement. In practice, this is virtually impossible.

In both cases, a diagnostic simulation results in significant improvements as it offers a reliable, configurable counterpart. In a regression test, this basically means that all variants of all vehicles are available; in test preparation, the test environment can be approved together with the test methodology before the DuT is available. The simulation information is stored in files. The simulation files can be loaded onto the simulation device and started as part of automating the “tester test” in the program sequence. It is also possible to modify communication parameters via the interface and thus to verify the correct behavior of the tester. Such simulation files do not require much storage space and are stored centrally.

Mostly carried out via CAN

Communication between the tester and the diagnostic simulation - even though Ethernet is gaining importance in some applications - is still mostly carried out via CAN. Both, Classical CAN and CAN FD are used. For diagnostics, transmission rates of up to 1 Mbit/s must be supported for Classical CAN and 8 Mbit/s for CAN FD. Softing TCS is a modern diagnostic simulation consisting of the simulation hardware, a configuration application and an API (application programming interface) for integrating the hardware in test automations. The hardware is flexibly tailored to current and upcoming requirements thanks to the Multicore-Linux platform used. It has an ▷

Figure 2: The Softing TCS.device is a configurable diagnostic simulation and can be used as a replacement for real ECUs or vehicles (Source: Softing Automotive)

OBD (on-board diagnose) jack and thus represents a vehicle in entirety as far as diagnostics is concerned. Alternatively, CAN can be accessed in the usual way using a D-SUB jack. Simulation files for different ECUs (electronic control unit) and vehicles are loaded onto the device via a LAN connection or using a USB stick.

The behavior towards the tester is completely configured in simulation files; programming is not necessary. The simulation is generated on the ISO/OSI layer 4 level, i.e. above the CAN network. Communication mechanisms necessary in diagnostics, such as segmenting, flow control, etc., are automatically processed through the protocol stack in the simulation hardware but can be controlled via communication parameters. This is how the timing of a response can be controlled at all times, predefined in the simulation file, but also during runtime via the programming interface. As a minimum response time via the diagnostic CAN, the simulation allows approx. 1 ms. A slower response behavior can be set via the parameterization for checking the tester, even outside the protocol limits.

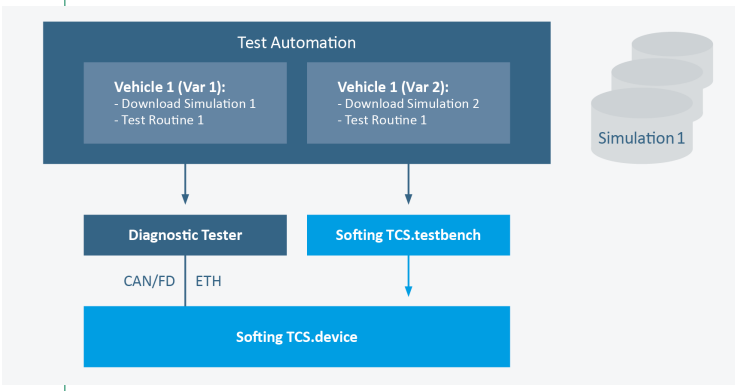


Figure 3: Integration in test automation (Source: Softing Automotive)

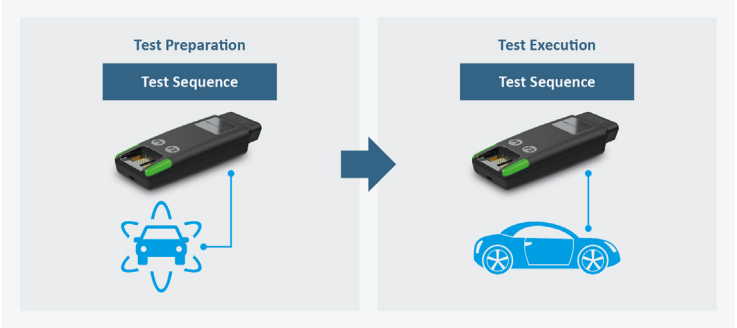


Figure 4: Simulation in test preparation (Source: Softing Automotive)

In the simplest case scenario, a message (request) sent by the tester is compared with exactly one response in the simulation file. A request for a measurement value (e.g. 22_h, 01_h, $2F_h$) is then responded by its corresponding message (e.g. 62_h, 01_h, $2F_h$, 01_hh, 23_h). Wildcards can be used as it is not always desirable to enter all requests specifically in a simulation. Using an 'X', any hex value in the request can lead to a response; a '…' would allow a variable length (e.g., 22_h, 01_h, $2X_h$, ..). Simple chains of effect have also been taken into consideration. This makes it possible to send a different response to a request each time. Changing values can thus be simulated, as can a negative response with the first request and a positive response with the following one.

Using variables is a major simplification. These can be set by a request – this is then marked accordingly in the configuration. Subsequently, the variable value in the response can be entered automatically. Thus, not all combinations have to be edited. Variables can also be used in communication control. A typical diagnostic example is session handling: Specific services can only be used in specific sessions. So, if the relevant service comes from the tester, the variable is set. In the case of relevant critical services, the variable is queried. If the variable is assigned appropriately, a valid response is received; otherwise a negative one.

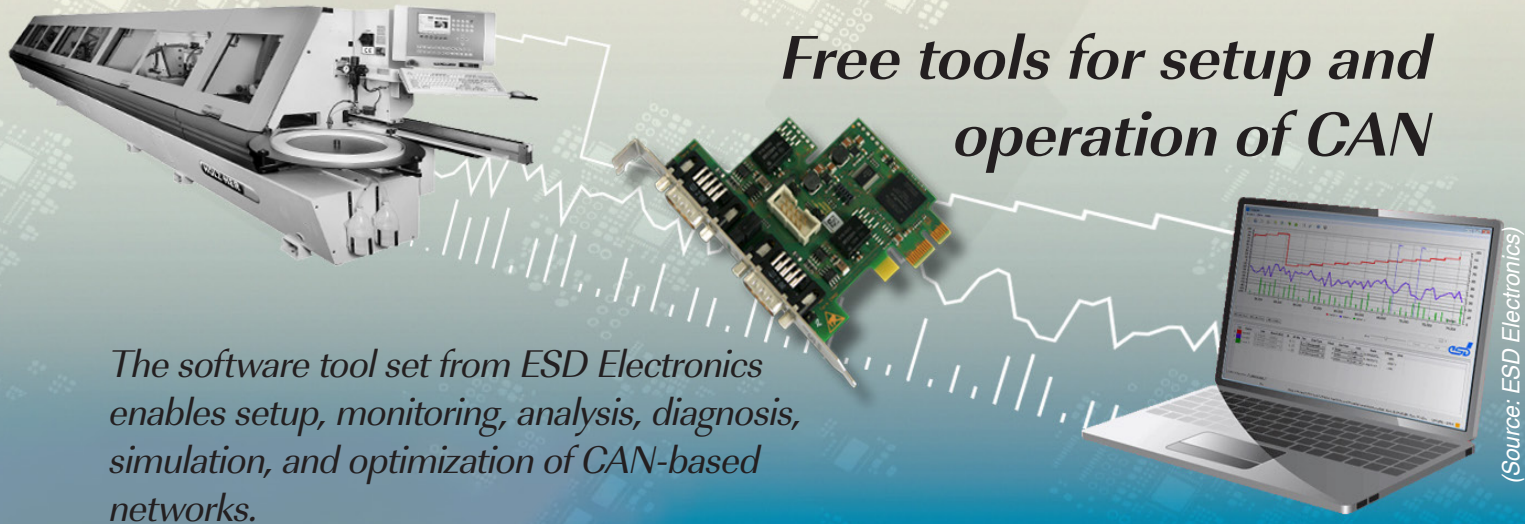
The simulation files are created in different ways. The regular communication between a tester and the ECU or vehicle can be recorded for the regression test. A corresponding simulation file is then generated from the trace file at the push of a button. This works with the usual CAN formats as well as with the PCAP format. In test preparation, the diagnostic specification currently tends to take the form of an ODX file. This can be read in and the simulation can be created using the possible information. This either takes place manually for every service or automatically at the push of a button using definable rules. Both methods can also be used combined. Existing gaps or special cases can then be created manually. Overall, this enables very efficient creation to suit the particular application case.

In summary, diagnostic simulation is the proven means when a test counterpart is not yet or no longer available. Whether in test preparation, in regression tests, or in training facilities. The targeted use of a solution, such as Softing TCS, makes it possible to significantly avoid mistakes. Testing can be more specific and wider-ranging thanks to the time gained by earlier maturity. This means that the simulation not only saves a considerable amount of money, but is also the basis for improving quality.

Author

Markus Steffelbauer
Softing Automotive Electronics
info.automotive@softing.com
automotive.softing.com

Free tools for setup and operation of CAN



(Source: ESD Electronics)

The software tool set from ESD Electronics enables setup, monitoring, analysis, diagnosis, simulation, and optimization of CAN-based networks.

Since the 1980s, CAN has simplified transmission paths to and from analog and digital devices. Today, CAN networks can be found in many industries: from automotive applications to automation technology, medical engineering, and aircraft technology.

Since the early days of CAN, ESD Electronics has concentrated on the development of CAN-connectable components and devices. The product portfolio ranges from CAN interfaces, gateways and bridges, I/O modules, plug-in card systems as well as CPU (central processing unit) boards. To support users while setup and operation of CAN networks based on these components, the company from Hanover (Germany) offers free software tools.

Software tools included

The CAN Software Development Kit (CAN SDK) for the NTCAN API (application programming interface) includes the CAN diagnostic tools CANreal, CANplot, CANrepro, CANscript, and COBview. The system requirement for using these tools is a current Windows operating system as 32-bit or 64-bit version. In addition to the five CAN tools, the CAN SDK includes header files, libraries, sample applications, and documentation. Another tool is the esdACC Error Injection GUI (graphical user interface) tool, which can be used to simulate CAN errors.

The CAN SDK allows developing, debugging, and testing of applications based on CAN hardware. All tools as well as the programming API share the multi-process NTCAN architecture. It supports CAN FD and time-stamped receiving and transmitting of frames including CAN inter-process communication. A virtual CAN driver for developing and testing applications completes the tool-box.

The libraries and samples included in the CAN SDK are available for many programming languages and environments. These include C/C++ (Visual, Borland, MinGW), Visual Basic 6, Delphi, Purebasic, and Python. In addition, the CAN SDK also includes NTCAN.NET class libraries for the Microsoft.NET framework for implementation of applications in C# or VB.NET. In addition, the kit offers function blocks for API functions as well as the function blocks of the CANopen Tiny Manager for use of CAN and CANopen in Labview.

Third-party software can be used directly with the CAN hardware from ESD through suitable libraries. For example, ESD offers a DLL (dynamic link library) for the CANopen Conformance Test (CCT) from CAN in Automation (CiA) and a corresponding version for the DeviceNet Protocol Conformance Test, a software of the Open DeviceNet Vendors Association (ODVA).

Monitoring and testing of CAN networks

The software tool CANreal is a monitor program for monitoring and analysis. It is also used as a test environment for CAN networks. Thanks to its open plugin interface, both supplied and self-written plugins can be used, such as those for CAN data bases (DBC) or J1939.

With its range of configuration options, the program is also versatile in diagnostics. For example, it is possible to set CAN-Identifier filters for 11-bit and 29-bit CAN-IDs, to log CAN frames and to display parameters decoded with DBC files. Moreover, high-resolution time stamps can be evaluated and CAN error detection as well as a variety of trigger functions can be used. The frames are displayed either as an online list or statically (object mode). The user can configure the columns. The time-stamps of CAN frames can be displayed as absolute values, with or without a date accurate to the microsecond, depending on the settings. An additional column displays the relative value with respect to the previous CAN frame. For CAN hardware supporting IRIG-B time code format, the transmitted time-code can also be set and put out as a time base.

Furthermore, CAN statistics with a calculation of bus loads and with transmit maps for user-defined CAN frames are available for diagnostics. The logging function offers the possibility to split large data sets into several files, or to overwrite them cyclically for data reduction. Files with recorded frames can be converted to CSV files or reloaded into CANreal (offline list) and into such tools as CANplot or CANrepro. The statistics function provides detailed information about the CAN network, the number of CAN data frames, error frames and more.

The single fault diagnosis shows detailed information about faulty CAN frames. A search function with bookmarks allows searching for individual CAN data frames or error frames. An advanced search can be defined individually. Since the tool is based on the ESD CAN driver with the ▷

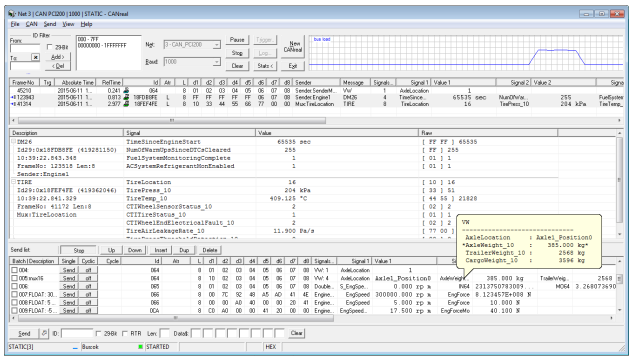


Figure 1: Monitoring program CANreal for control and analysis purposes (Source: ESD Electronics)

multi-process NTCAN architecture, several instances of the CANreal tool can be opened simultaneously to a CAN network. Alternatively, the CAN network used by an application can be directly observed.

Displaying CAN data graphically

Graphics of data not only show values at a glance but also ratios and proportions. CANplot prepares CAN data and displays it graphically on two scalable coordinate axes (online and offline). Thanks to the individual message recognition, criteria such as position in the data field and the data type can be selected and displayed in individual data graphs with color assignment. CAN data can be selected according to the network number, CAN-Identifier, and position in the data field. Several numeric data types are pre-defined for data interpretation. Data formats from Intel and Motorola (big endian/small endian) are supported.

Reproducing CAN frames

For analyzing CAN communication, the CAN frames previously recorded via CANreal can be repeated with CANrepro. This function allows incoming diagnoses or automated test procedures. The original time sequences remain at the reproduced data and the individual CAN-IDs can be selected. Using CANrepro, a realistic simulation of CAN devices is possible and the recorded CAN messages can be reproduced again.

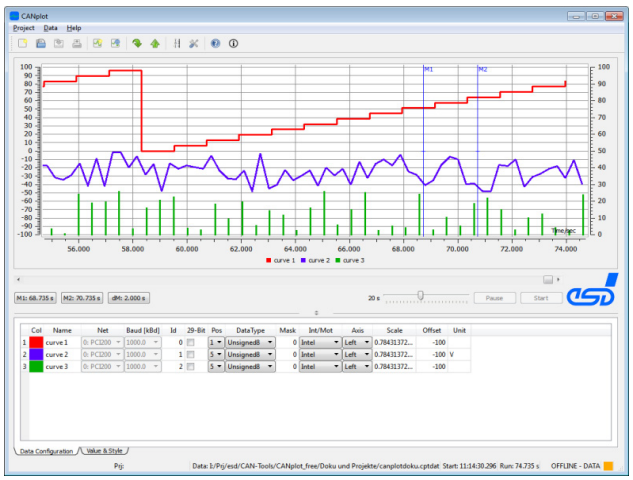


Figure 2: CANplot prepares CAN data and displays them graphically (Source: ESD Electronics)

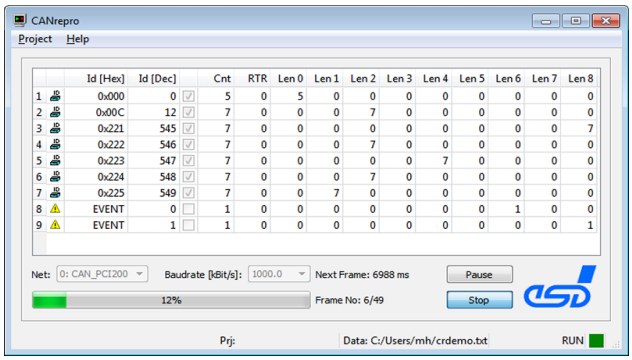


Figure 3: CANrepro for analyzing CAN communication with reproduced messages (Source: ESD Electronics)

Creating Python programs

If executable Python programs (Python scripts) are required, CANscript provides a corresponding GUI frontend allowing execution of PyNTCAN-based scripts for test automation, residual bus simulation, and other applications.

Setting up CANopen nodes

The COBview tool provides the user with a CANopen object overview and enables the modification of device parameters and of the network states for testing purposes as well as for setup of CANopen nodes. In addition, the program helps with the analysis and diagnosis of CANopen nodes and with the search and display of CANopen devices in a CANopen network. The tool offers basic CANopen network management (NMT) functionality (start node, pre-operational, reset, stop) as well as read/write access to the object dictionary. It lists CANopen objects with all sub-indexes and interprets the object data. The objects are read by index and displayed in a list with all sub-indexes. Data interpretation is generic in multiple formats without the need to load EDS (electronic device sheet) files. The network scan function lists all devices on the network.

Simulating CAN errors

The esdACC Error Injection GUI tool provides a free graphical user interface designed for the error injection ▷

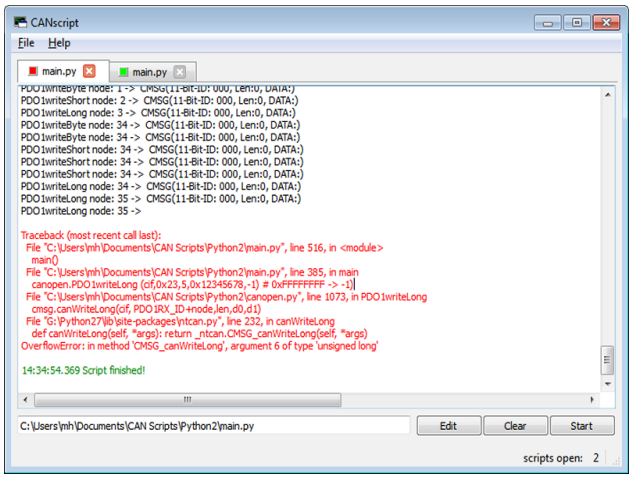


Figure 4: CANscript for test automation of PyNTCAN-based scripts (Source: ESD Electronics)

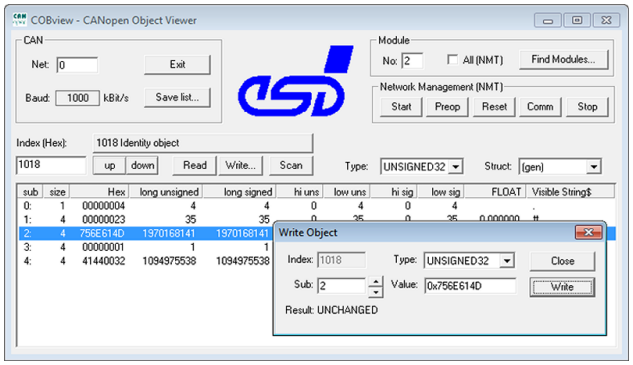
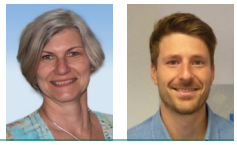


Figure 5: CANview provides CANopen object overview and enables modification of CANopen device parameters (Source: ESD Electronics)

unit integrated into some of manufacturer's CAN interfaces. Conventional CAN controllers available on the market at present, are not able to send faulty CAN frames due to their design. However, the esdACC CAN IP core, supplemented by the error injection unit, can generate or simulate numerous CAN errors. In addition to the GUI tool, error injection can also be configured and used directly via API calls using the NTCAN API. In this way, automated test cases can be realized in complex test scenarios.

Summary

The software support provided in form of different ESD tools enables setup and configuration of CAN networks. Additionally, the tools offer a lot of possibilities for analysis, diagnosis, and optimization of CAN-based communication. Simulations for testing purposes and monitoring, for example in troubleshooting, are given as well.



Authors

Renate Klebe-Klingemann
Hans Kürsten
ESD Electronics
info@esd.eu
www.esd.eu

Implementation requirements for secured gateways

The concept of a security gateway is trivial but the implementation is not: a gateway is not just a functional device that filters CAN data frames, but must operate so that the resulting traffic patterns on the trustworthy CAN network meet all real-time requirements and operate securely at all times. The requirements described in this article are designed to ensure that.

(Source: Adobe Stock)

In road vehicles, there are installed multiple CAN-based in-vehicle network segments for real-time control purposes. Between electronic control units (ECUs) CAN data frames containing sensor and actuator data are exchanged using a publish-subscribe paradigm. Some of the data is sent to – and comes from – inherently untrustworthy devices such as ECUs that are cellularly connected or aftermarket, third party provided.

This is clearly a security issue: these devices cannot in general be trusted and being given direct access to a CAN network would allow all kinds of attacks on the CAN network and hence the vehicle. The approach described here is to create a CAN network for untrustworthy devices separated from internal vehicle communications via a security gateway that forwards traffic between the trusted internal CAN networks and the untrustworthy external CAN network.

Rationale

The National Motor Freight Traffic Association [1] (NMFTA) is a nonprofit motor freight carrier organization in the U.S.A. representing over 500 carriers collectively operating over 200 000 commercial road vehicles. One key focus of the organization is protecting their members' commercial vehicles from the ever-evolving cyber-threat landscape. As such, the organization has been a pioneer in conducting and supporting security research in the transportation domain since 2015.

Because CAN enables robust, low-latency communication among many ECUs at once electronic architectures in commercial vehicles, just as for passenger cars, have utilized CAN as the foundational data link layer protocol for inter-ECU communication. In the commercial vehicle space, application messages have historically been standardized by SAE J1939 to allow 'plug and play' of device suppliers' systems (Figure 1). This has allowed for ultimate configuration and customization to optimize fleet operations, with a diverse supplier industry that has encouraged innovation.

For all its benefits, CAN was never designed with security in mind: communication has relied on each node acting in good faith. A plethora of research has demonstrated CAN is vulnerable to attacks, both at the frame level (such as spoofing fake data frames and eavesdropping on sensitive data) ▷

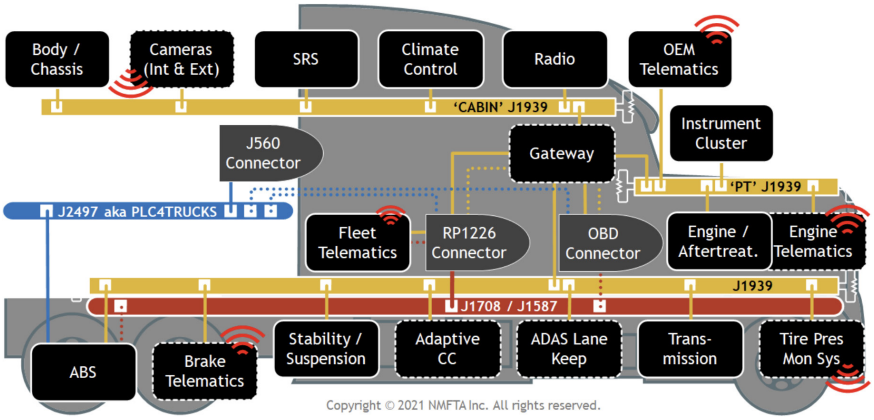


Figure 1: Typical J1939 in-vehicle network architecture (Source: NMFTA)

and at the protocol level itself (such as the Bus Off attack), undermining all three aspects of the Confidentiality/Integrity/Availability (CIA) Triad security objectives. If vehicle electronics were largely isolated and air-gapped systems, these security issues might pose minimal overall security risk. Unfortunately, this is no longer – if it ever was – the case. For one, existing technology such as trailer brake ECUs, which have been a requirement on commercial trailers since the late 1990s, have recently been demonstrated as remote attack vectors [2] and for leaking information via power line communication (PLC) networks. Additionally, third party remote fleet tracking and telematics has proliferated within the industry to track and optimize operations as well as monitor assets for uptime and maintenance. Since 2017, the Federal Motor Carrier Safety Administration (FMCSA) has required connected devices in the form of electronic logging devices (ELDs) to track drivers' hours of service [3].

Clearly, commercial vehicles on the road today have multiple remote vectors that could serve as entry points for an attacker to access and affect the safety critical operations of the vehicle. At the same time, these potential attack vectors provide critical functionality for operators and fleets and cannot be removed entirely. Instead, one method to effectively reduce risk in the case of a remote compromise is to introduce a device to partition any untrusthworthy, connected devices from the safety critical controls of a vehicle: a CAN based security gateway. Gateways have the purpose of physically separating a device with potential risk from the rest of the vehicle system. Messages and data can be defined in a bi-directional manner to ensure no unintended or malicious messages are transported across the gateway boundary.

While CAN-based gateways are already implemented in many vehicle architectures, to date the authors are not aware of public, comprehensive cybersecurity requirements to define such a device. The NMFTA has led a working group to develop such requirements. The main intention of the requirements is for NMFTA member fleets to use as a tool for procurement: to confirm OEM (original equipment manufacturer) vehicles provide protections before purchasing. They could also be used by OEMs and aftermarket suppliers alike as a baseline to develop secure, industry leading gateways.

Top-level requirements

The NMFTA security gateway requirements define two domains: the trustworthy network domain (TND) where the vehicle control systems operate on CAN networks, and the untrustworthy network domain (UND) which inherently cannot be trusted (for example, third-party wirelessly connected devices containing complex software). A security gateway is defined to connect the UND with the TND (normal CAN gateways operating entirely within the TND are not covered by these requirements but obviously nothing prevents a security gateway from being used in that role). There are three top-level requirements for a security gateway connecting the UND with the TND.

1. A security gateway must restrict CAN traffic in each direction to only defined traffic for each operational mode. These modes might include over-the-air downloads taking place and diagnostics sessions (it is not required that modes are mutually exclusive, merely that there is an ability to define what is and is not legal traffic for a given situation). Restricted and defined traffic prevents a compromised, untrustworthy device from both directly spoofing application data frames that originate on TND and tampering with internal diagnostic interfaces.
2. Communication within the TND must not be disrupted by traffic from the UND. This is a less obvious requirement but just as important: the TND forms part of a distributed real-time vehicle control system where the message timing is just as important as message contents. If traffic from the UND exceeds a defined usage there can be serious consequences for the latencies of CAN data frames in the TND, such as timeouts causing false error warnings, buffer overflows and dropped frames and even excessive CPU (central processing unit) load with potential to cause erratic system disruption in receivers.
3. The gateway itself must be secure. Clearly, the security gateway itself needs to be controlled. For example, being instructed to switch between operational modes, or being re-programmed with a new configuration, or even extracting and clearing event logs. This control must be via secure mechanisms to prevent compromising the protections a security gateway seeks to provide.

These top-level requirements are refined into multiple, more specific requirements [4].

Defining traffic patterns

Traffic definitions for a security gateway define for each operating mode specific frames in one domain (TND or UND) that will be forwarded to the other domain. The traffic patterns define not only CAN IDs but also how the CAN data field is handled. The J1939 application layer defines that for a Parameter Group (PG) with a given PGN (PG number) mapped into the CAN ID field, the payload contains known suspect parameters (SP), sometimes called in laboratory slang *signals*. The J1939 traffic definition may restrict the parameters in a payload on a *need-to-know* basis. For example, if an application in the UND requires access to a CAN data frame for a specific parameter then the other parameters in the CAN data frame ▷

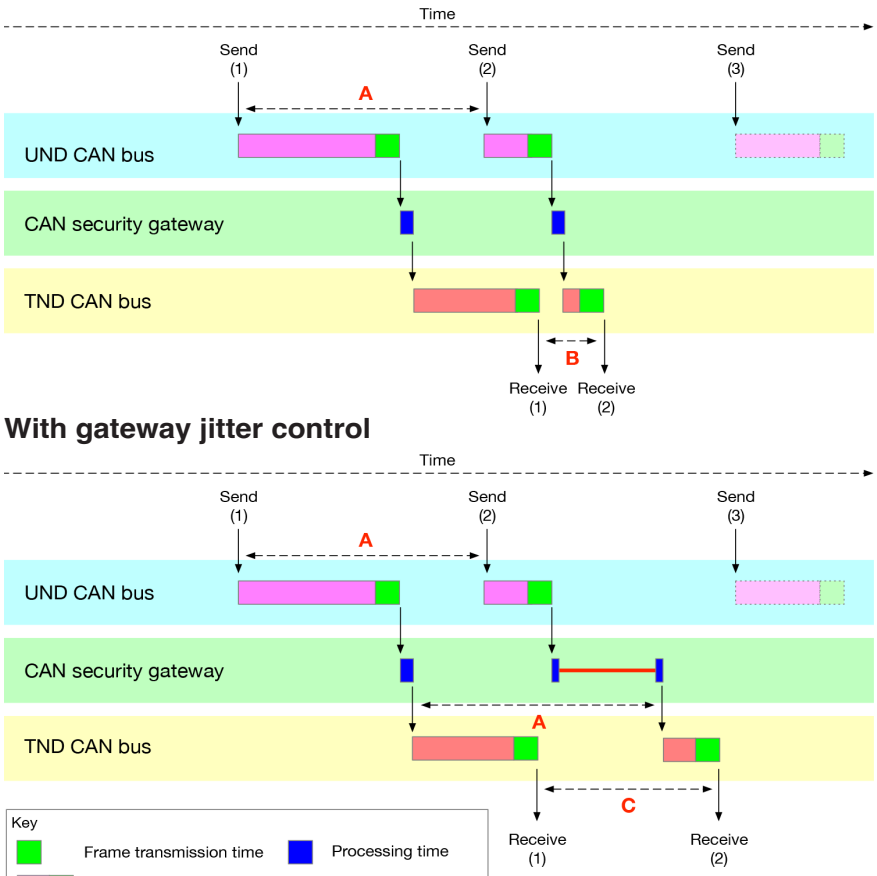


Figure 2: Jitter control in a security gateway (Source: Ken Tindell)

may be zeroed out by the security gateway to avoid inadvertently disclosing proprietary or confidential information.

A traffic definition also specifies a real-time frame rate for each frame to be forwarded so that a CAN data frame is only passed through if that rate is not exceeded. This is the starting point for guaranteeing the timing behavior of the TND: the real-time data frame rates can be used in CAN network schedulability analysis [5] calculations to determine worst-case latencies. This analysis can guarantee all TND CAN data frames will arrive on time no matter how often CAN data frames are sent within the UND. It also allows the buffer space and CPU time dealing with CAN data frames to be bounded and so prevent frame losses and CPU overloads.

CAN frame handling requirements

A crucial requirement for any CAN gateway is that CAN data frames are handled properly: applications built on top of CAN often rely on the network behaving properly (although sometimes unknowingly). For example, multi-frame segments like ISO-TP [6] require frames that form the segment are not dropped and are not transmitted out of order. Another example is with typical cryptographic schemes for CAN networks, like the CryptoCAN [7] scheme of Canis Labs: a chained block cipher mode relies on segments and messages being sent in order. If the security gateway does not handle CAN data frames correctly then the overall system could fail.

One of the key properties of CAN is atomic broadcast/multicast: a CAN data frame that is successfully sent will have been received at all receivers connected to the network. With other protocols like Ethernet, frames that contain errors are just discarded, and atomicity is implemented in software, which is far from easy. Applications using CAN often rely on this property – it's a key feature of the publish/subscribe communications model of CAN – and a security gateway is required to maintain this property. Because the transmission on one side of a gateway has completed before the frame can be sent on the other side, a gateway inherits an obligation (if the frame is legal) to always transmit that frame on the other side. This means that a gateway is required to have sufficient memory for buffers such that no frame will ever be dropped due to a buffer overflowing. Fortunately, it is possible to statically determine the maximum buffer space needed after putting an upper bound on the frame latencies for frames waiting to be sent on the destination CAN network segment.

A security gateway is also required to transmit frames without priority inversion: this is a problem where the latencies of urgent (and hence high priority) activities are normally short but intermittently and unpredictably become very large. This can induce further problems (such as triggering timeouts leading to spurious fault handling) and must be avoided. Priority inversion can occur in any system scheduled by priorities and most famously occurred during NASA's Mars Pathfinder Mission [8]. It can nearly always be avoided by writing CAN driver software correctly so that there is a priority-ordered (i.e. ordered by CAN ID) queue of frames to be transmitted, where the driver software ensures that the highest priority CAN data frame is always entered into CAN arbitration whenever it starts.

There is a requirement for a gateway to transmit CAN data frames in order (for example, so that ISO-TP segments are not corrupted). This at first sight may appear to conflict with the requirement for no priority inversion – in effect it is mandating FIFO frame transmission. But this is not so: the requirement is that FIFO order is required for multiple frames of the same sequence with respect to each other. This cannot be left to the hardware: with most CAN controller hardware, if two frames with same ID are sent at the same time then the hardware will arbitrarily pick a frame to send first, which would violate the requirement to transmit frames in order. So, a typical way to meet this frame ordering requirement is to put related frames (typically those with the same ID) into their own FIFO, and for this FIFO to feed the priority-ordered frame queue.

Another requirement for frame handling is to control the jitter of a CAN data frame: frames can be queued on a CAN network with a precisely regular periodicity (matching the defined rate of the frame) but there will be variations in latency and so the relative arrival time of the frame will vary. If the frame were immediately placed into an outgoing CAN controller then the ▷

frame would inherit jitter in the queueing time, and by the time it was transmitted on the network the variability would be even larger, potentially so large that two CAN data frames with the same CAN ID could arrive back-to-back, and this could cause a receiver to overwrite one frame with another before the first frame could be handled – effectively dropping a frame and violating the requirement not to drop frames. A security gateway is required to limit this jitter: if a CAN data frame arrives on one CAN network sooner than its defined period [9] since the previous arrival time then it must be held back and only queued on the outgoing CAN network segment when this elapsed time has reached its period (Figure 2).

This requirement does mean that the average latency through a security gateway is increased, but average case for real-time control systems is not very important: it is the worst-case latency that matters. This jitter control means that CAN schedulability analysis on a TND can take place without knowledge of the timing properties of the UND and therefore the UND cannot disrupt the timing behavior of the TND.

Secure gateway control

A security gateway itself needs to be secure. Aside from normal protections common to most embedded systems (like firmware secure boot), the control of the gateway must be secure. Control includes programming a configuration, setting operational modes, and clearing event logs. There is a requirement that gateway control must be authenticated. This could be done by cryptographically secure communications. For example, a cryptographically secure message between a driver's touch screen display and the security gateway. An alternative is to use a physical interlock switch that prevents changes until a human has turned a key or flipped a switch.

For cryptographically secure messaging, a security gateway must store keys securely (so that not even software in the gateway can read them) and then execute cryptographic operations with these keys. This can be done by using a hardware security module (HSM) and the automotive industry has defined its own Secure Hardware Extensions (SHE) standard for HSMs. A secure challenge-response protocol using HSM operations can provide mutual authentication between a control tool and a security gateway.

Discussion

There are several ways to instantiate the NMFTA security gateway requirements. One is by using dedicated firmware on a regular microcontroller with multiple CAN controllers (either within an existing ECU with the necessary CAN connections or in a dedicated security ECU). Another is by using a Hardware Security Gateway Module (HGM): dedicated silicon IP (intellectual property) cores (like an HSM) that implements a complete security gateway (including CAN controllers) in silicon, deployed as a stand-alone chip or within a System-on-Chip (SoC) package and designed into an ECU.

The security gateway functionality may be provided by an OEM to protect certain safety critical systems or provided by a dedicated third-party interface for aftermarket installation of telematics services, ELDs, etc. This might be implemented as a dedicated security ECU or by augmenting the functionality of an existing ECU design. A dedicated security gateway may also be provided as a third-party aftermarket option to retrofit into existing vehicles that are not equipped with an OEM-provided security gateway.

The NMFTA security gateway requirements described here are necessary but not necessarily sufficient. It is recognized that there are additional security requirements needed to make a comprehensive set of requirements for a security gateway and the NMFTA will be tackling these in the Truck Matrix security requirements work [10]; Furthermore, they are primarily intended as tool for procurement by fleets – but they may not be sufficient for all product security applications of a security gateway. For example, there may be frames in the TND that use cryptographic authentication and payload encryption to prevent physical access spoofing and snooping attacks, and a security gateway may need to encrypt, decrypt (and potentially re-encrypt) messages to and from this domain. In these cases, the NMFTA security gateway requirements should be seen as a starting point for a more comprehensive functional specification – one perhaps contributing to a wider industry standardization process. Such a standard could offer not just easier procurement but also cost savings by creating a market for standardized security gateway implementations and interoperable tools. ◀

References

[1] More about NMFTA cybersecurity is available at https://nmfta.org/cybersecurity
[2] CVE-2022-25922 and CVE-2022-26131
[3] https://eld.fmcsa.dot.gov
[4] https://nmfta-repo.github.io/vcr-experiment/vcr-experiment/01_gateways.html
[5] Using schedulability analysis on CAN network was pioneered by Volvo in the 1990s. Today, it is used by many manufacturers as part of a design-for-correctness engineering approach to CAN networking
[6] ISO 15765-2
[7] CAN Newsletter issue 4/2022
[8] Blog post at https://kentindell.github.io/2020/06/29/can-priority-inversion
[9] Period is the inverse of rate, so a 100-Hz frame has a period of 10 ms
[10] See the draft here: https://github.com/nmfta-repo/nmfta-vehicle_cybersecurity_requirements



Authors

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

Ben Gardiner, NMFTA
Ben.Gardiner@nmfta.org
www.nmfta.org

John Maag, Cummins
john.maag@cummins.com
www.cummins.com

Telematics gateway: Choosing criteria and usage

(Source: Iwave)

This article explains the functionality, discusses the choosing criteria, and describes the use cases of a telematics gateway on an example telematics device from Iwave.

With cars becoming more connected, OEMs (original equipment manufacturers) need telematics solutions that facilitate seamless communication within and outside the vehicle. The device should be cloud-enabled, connectable to servers for real-time computation and analysis, and offer an intuitive user interface that allows users to interact and control various operations.

Telematics gateway choosing criteria

When choosing a telematics gateway, various factors should be considered. These include the type and nature of clients, geographical conditions, the average distance to cover, and the vehicle type. The following considerations should be taken in account:

- *Connectivity options:* Reliable connectivity solutions are critical for the connected mobility data transformation. The telematics gateway should be able to scale up and down communication standards based on the connectivity infrastructure required for a vehicle. Depending on the end application, a telematics gateway should be able to support multiple wireless communication infrastructures such as Wi-Fi, Bluethooth, LTE, DSRC (dedicated short range communication), and so on.
- *Type of data to be collected:* The increasing number of vehicle makers, models, and options necessitate a telematics gateway with a modular architecture capable of supporting multiple interfaces to the in-vehicle networks such as CAN (e.g. using CANopen or J1939 higher-layer protocols), Ethernet, EIA-232, EIA-485, and others.
- *Software flexibility:* A scalable software is a must for the simultaneous tracking of diverse assets and vehicles. The software stacks supported on the gateway should ensure interoperability among different vehicles and mobility infrastructures as well as reduce the development time of customized applications.

Available functionality

The telematics gateway from Iwave offers car manufacturers a modular computing platform, which allows data exchange between multiple electronic control units (ECUs) and servers. It provides a secured execution environment and prevents unauthorized access to the device while maintaining data integrity.

Figure 1: Features of the telematics gateway (Source: Iwave)

The device integrates a range of interfaces to collect data from vehicles and to provide it to users for further actions. Wireless communication possibilities include 4G/LTE (long term evolution) cellular network connectivity for M2M/IoT (machine-to-machine/Internet of things) applications. Other options include Wi-Fi, Bluetooth 5.0, and UWB (ultra-wideband) wireless transceiver, enabling data transfer from vehicle to the cloud. Provided wired interfaces such as CAN FD, EIA-232, EIA-485, Automotive Ethernet, and analog inputs enable interconnection with ADAS (advanced driver assistant systems), within self-driving cars, vehicle-to-everything connectivity, and more. For real-time vehicle monitoring five CAN-FD ports supporting data bit-rates up to 5 Mbit/s are provided. The gateway implements protocol stacks for such higher-layer protocols and applications as ISO 15765-4 (diagnostic communication over CAN), SAE J1939, CANopen, and CiA 447 (CANopen application profile for special-purpose car add-on devices). Thus, the device is suitable for deployment in heavy-duty trucks, off-road vehicles, special-purpose and emergency vehicles as well as further transportation and mobility infrastructures.

The gateway is based on the i.MX 8 DXL CPU (central processing unit) by NXP with 64-bit ARMv8 architecture. Processing power scaling with ARM Cortex A35 and ARM Cortex M4 processors and an internal memory of 2 GiB is possible. The device supports advanced fleet management, configurations, and remote management. For uninterrupted vehicle location, a high-precision GNSS (global navigation satellite system) module is integrated in the telematics unit. GPS (global positioning system), Glonass, Beidou, and Galileo satellite-based systems are supported. The telematics device also includes a three-axis gyroscope, accelerometer, and magnetometer for continuous real-time motion monitoring, driver behavior analysis, and auto-calibration.

Regarding security, the device offers an eSIM (embedded subscriber identity module) data encryption, multiple IMSI (international mobile subscriber identity), and a multiple-profile UICC (universal integrated circuit card) SIM technology remote file/applet management. The protection functions of the implemented Hardware Secure Element (NCJ38A) restrict unauthorized installation of applications on the gateway. Thus, only trusted applications and devices can access the telematics device. The provider also offers a security suite that includes a secure boot, secure storage, and Wi-Fi security functions.

The telematics gateway is FCC, CE, and ISED certified. The company also supports country-specific certifications such as Kominfo and E-Mark. To shorten the pre-programming cycle, available user-friendly APIs (application programming interfaces) eliminate the effort with complicated embedded scripting and proprietary device management tools. Based on the requirement, the manufacturer also provides customization options on hardware features, type of enclosure, and branding for the telematics gateway.

Telematics gateway use cases

For example, a telematics gateway can be deployed in the following use cases:

Figure 2: Telematics gateway use cases (Source: Iwave)

- *Predictive maintenance in electric vehicles:* Drivers of electric vehicles must be aware of their battery health, the charge level, and the nearest charging station to plan the trip appropriately. Telematics gateways with various on-board features and wired as well as wireless interfaces can provide valuable data needed to improve the vehicle algorithm.
- *Control and track farm equipment:* Manufacturers of farm equipment strive to improve farmer operations by securely sharing information about their daily operations. Telematics gateways installed in tractors, vehicles, and other farm equipment enable tracking of vehicle movement, location, driver status, gasoline usage, and more.
- *Fleet management:* Failures in fleet management, such as vehicle recalls resulting in service interruption, can be very costly. A telematics device reduces this risk with built-in interfaces such as CAN, EIA-232, and EIA-485 to collect and securely share fleet information with owners. As a result, it enhances fleet productivity and reduces costly failures.
- *Heavy-duty and off-road vehicles:* Forklifts, cranes, and heavy-duty trucks are often used in extreme conditions for long hours, making them vulnerable to frequent breakdowns. Via the integrated J1939 interface, the telematics gateway is able to retrieve diagnostic information and real-time data from the in-vehicle ECUs, which ensures vehicle uptime and predictive maintenance.

Author

Tawfeeq Ahmad
Iwave Systems
tawfeeq.ahmad@iwavesystems.com
www.iwavesystems.com

CAN in Automation

April 26, 2023
Detroit area (MI, USA)

CAN XL technology day

This CiA technology day focuses on CAN XL. During this onsite event the speakers discuss all relevant CAN XL topics such as technical details, implementations, availability, and addressed markets. Additionally, they provide an outlook to the usage of CAN XL as embedded backbone network. The event is accompanied by an exhibition of CAN XL demonstrators, provided by companies offering CAN XL-based solutions.

Agenda*

08:30 to 09:00	Registration	12.00 to 13.30	Lunch break
09:00 to 09:15	Welcome (Holger Zeltwanger, CiA)	13.30 to 14:00	Cybersecurity and CAN XL (Wes Mir, Aptiv)
09:15 to 09:45	Excurse CAN FD Light (Fred Renning, ST)	14:00 to 14:30	CAN XL and Autosar (Peter Decker, Vector)
09:45 to 10:15	General introduction to CAN XL technology (Arthur Mutter, Bosch)	14:30 to 15:00	CANsec implementation (CAST)
10:15 to 10:45	Coffee break	15:00 to 15:30	Coffee break
10:45 to 11:15	CAN XL physical layer implementations (Teun Hulman, NXP)	15:30 to 16:00	CAN XL conformance and interoperability testing (Maen Mohammad, C&S)
11:15 to 11:45	CAN XL physical layer network design (Magnus-Maria Hell, Infineon)	16.00 to 16.30	Discussion (Q & A)
11:45 to 12:00	Availability of CAN XL solutions (Holger Zeltwanger, CiA)		

* Agenda may change without notice.

For more details please contact
CiA office at events(at)can-cia.org

www.can-cia.org