December 2019

CAN Newsletter

Hardware + Software + Tools + Engineering

CANopen birthday: review and outlook

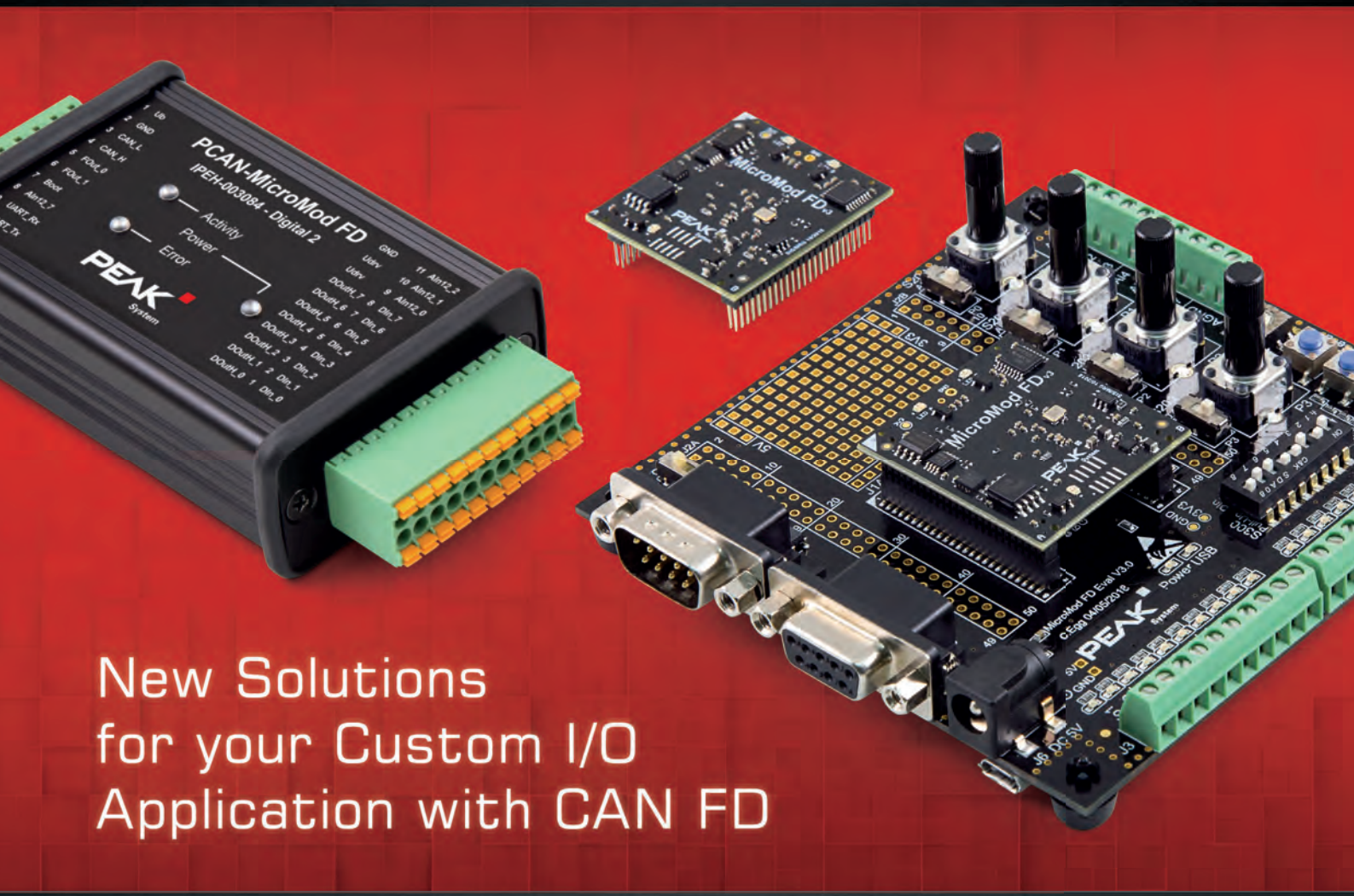
SAE J1939: 25th anniversary

Charging communication in Chinese

CiA 601-4: CAN signal improvement

Specifications

www.can-newsletter.org



New Solutions for your Custom I/O Application with CAN FD

PCAN-MicroMod FD

Universal I/O module with CAN FD interface

The PCAN-MicroMod FD is a small plug-in board which provides a CAN FD connection and enhanced I/O functionality for the integration into your hardware. An evaluation board facilitates the development of your custom solution. The module is configured with a Windows software via the CAN bus and then operates independently.

Features:

- NXP LPC54618 microcontroller
- 1 High-speed CAN connection
  - Complies with CAN specifications 2.0 A/B and FD
  - CAN bit rates from 20 kbit/s up to 1 Mbit/s
  - CAN FD bit rates from 20 kbit/s up to 10 Mbit/s
  - Microchip MCP2558FD CAN transceiver
- 8 digital inputs and 8 digital outputs
- 2 frequency outputs
- 8 analog inputs
  - Measuring range unipolar 0 to 3 V
  - Resolution 12 bit, sample rate 1 kHz
- Configuration via the CAN bus with a Windows software
- Selective configuration of up to 16 devices in a CAN bus
- Extended operating temperature range from -40 to 85 °C
- Dimensions: 33 x 36 mm
- Voltage supply 3.3 V

Ready-to-use motherboards

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

Common Features:

- Board with plugged on PCAN-MicroMod FD
- CAN 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 - 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 - 10 V)
- Digital 1: 8 digital outputs with Low-side switches
- Digital 2: 8 digital outputs with High-side switches

www.peak-system.com

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

PEAK-System Technik GmbH

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

PEAK System

Specifications

Security

Engineering

Imprint

Publisher
CAN in Automation GmbH
Kontumazgarten 3
DE-90429 Nuremberg

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

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

CEO
Reiner Zitzmann

AG Nürnberg 24338

Downloads September issue:
(retrieved November 19, 2019)
2966 full magazine

Editors
pr@can-cia.org
Cindy Weissmueller (cw)
Holger Zeltwanger (hz)
(responsible according
to the press law)

Layout
Nickel Plankermann

Media consultant
Meng Xie-Buchert
(responsible according
to the press law)

Distribution manager
Julia Dallhammer

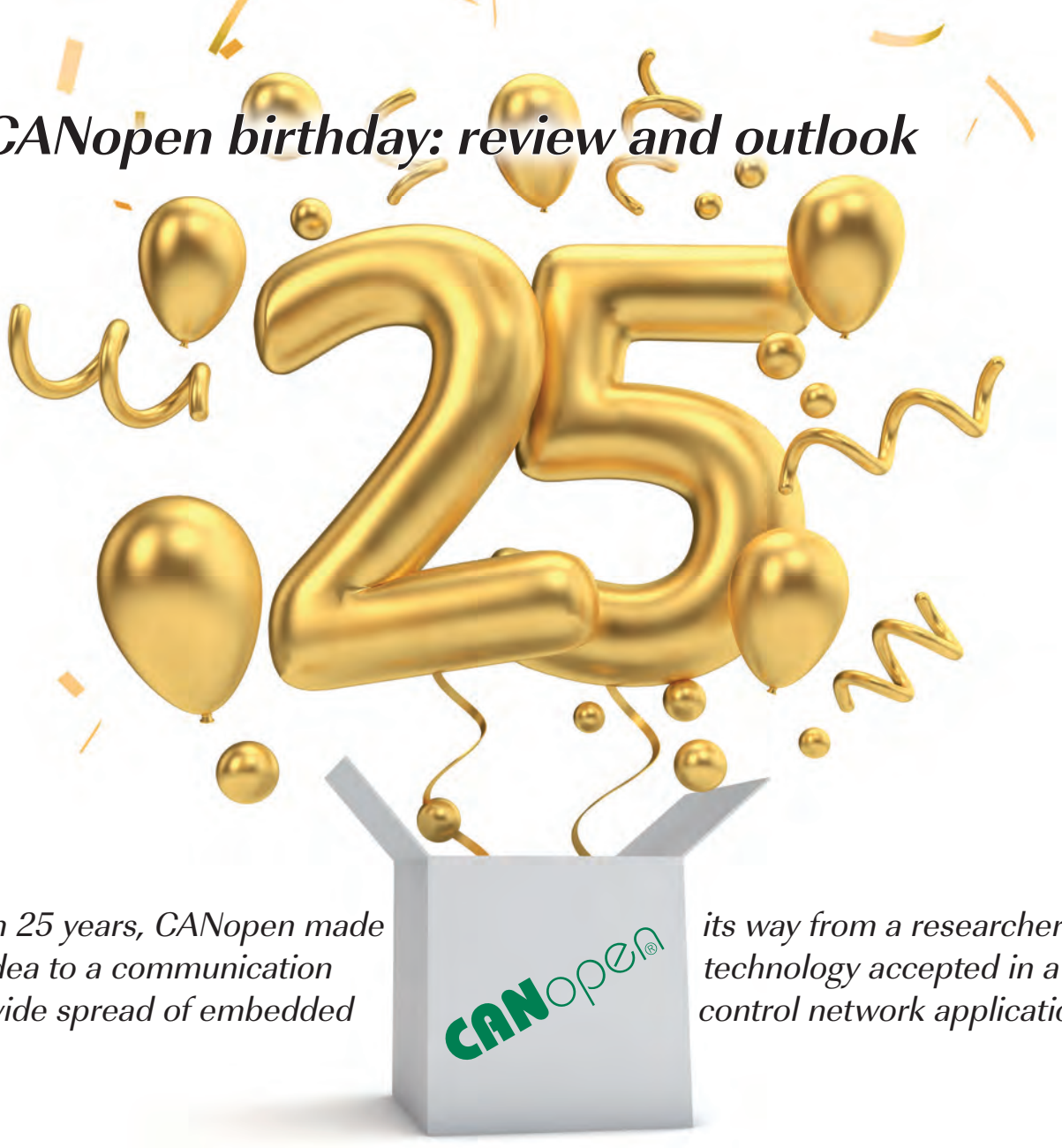
30 years of SPS

This year, SPS tradeshow celebrates its 30th anniversary. CAN in Automation (CiA) has exhibited 27 times on this fair – the first years in Sindelfingen (Germany) and then in Nuremberg (Germany), the hometown of the CAN users' and manufacturers' group. By the way, there is no company that participated more times; just a few others attended also 27 times including some CiA members.

CiA shows on its SPS 2019 stand the migration from classic CANopen to CANopen FD. Additionally, several members exhibit classic CANopen products. CiA's staff would appreciate to discuss new developments in more details with you in hall 5, stand 410.

Our sister-publication, the CAN Newsletter Online already reported about some CAN-related products you can expect at the SPS 2019.

CANopen birthday: review and outlook



Source: Adobe Stock

In 25 years, CANopen made its way from a researchers' idea to a communication technology accepted in a wide spread of embedded control network applications.

In the year 1994, Disney's Lion King with songs from Elton John hit cinema screens. Steven Spielberg won his first directing Oscar for Schindler's List. Nelson Mandela became South Africa's first black president. The IRA declared cease-fire in Northern Ireland. The Internet got real in 1994 with the founding of both Yahoo and Amazon. The Playstation was launched at the tail end of 1994 as well as the CANopen application layer. In the beginning, the title of the CiA (CAN in Automation) specification was a little bit bulky: CAL-based communication profile. The first release end of November comprised just 60 pages.

The CiA document based on the results of the Esprit 7302 European research project. Moog (Ireland) leaded this research activity, which was participated by ADL Automation (France), Bosch (Germany), JL Automation (United Kingdom), STA technology center (Germany), and the University of Newcastle upon Tyne (United Kingdom). The research project was titled ASPIC (Automation and Control Systems for production Units using an Installation Bus Concept). The research results were discussed within CiA. After revising and extending the research report, CiA released the CAL-based communication profile in November 1994. CAL (CAN Application Layer) was the application layer developed by CiA and published as CiA 200 series.

Already six weeks later, in January 1995, CiA released the version 1.1. It provided the missing definitions of data types. End of 1995, after gaining some experiences when implementing prototype devices, the version 2.0 was launched. It was numbered as CiA 301. The next CiA 301 version, version 3.0, published in October 1996, was implemented in real products used in industrial machines. This document was titled CANopen CAL-based communication profile for industrial systems.

The next big step was the release of version 4.0 named CiA 301 CANopen application layer and communication profile. It provided four pre-defined TPDOs and RPDOs, Heartbeat functionality, and many other functional improvements. Especially, medical device manufacturers and military equipment suppliers requested them. This CANopen specification was also the base for the EN 50325-4 standard.

The following CiA 301 versions introduced minor improvements, functional extensions, and corrections as well as clarifications. One of the functional extensions is the Sync counter allowing a more flexible use of the unique Sync protocol triggering PDO communication. The newest CiA 301 specification is the version 4.2.0 released in 2011. This means the CANopen base specification is very mature and stable.

One key of the success: standardized profiles

From the very beginning, there were standardized CANopen device profiles. Already pre-developed were the profiles for modular I/O devices and electrical drives. After reviewing them, CiA published them. The first implemented I/O profile was CiA 401 version 1.3 released in 1995. The CiA 402 motion control and drive profile was partly based on the Drivecom profiles by Phoenix Contact. The first version was published in May 1997 as well as the CiA 406 CANopen device profile for encoders. The CiA 402 profile is internationally standardized in IEC 61800-7-201 and IEC 61800-7-301.

Standardized device profiles enable off-the-shelf interoperability between host controllers and CANopen NMT slave devices. Products compatible with standardized profiles are also partly exchangeable, when they support the same optional functions. The list of CANopen device profiles is long, but not complete. There are still specific device functions, which have not been standardized. The last released device profile, CiA 461, specifies weighing devices.

Device profiles do not support pre-defined cross-communication between CANopen NMT slave devices. This needs to be configured by the system designer. In order to provide a pre-defined system approach, CiA developed CANopen application profiles. The first one was the CiA 407 application profile for passenger information. It was submitted for European standardization and is available as EN documents 13149-4/5/6 (Public transport – Road vehicle scheduling and control systems – General application rules for CANopen transmission buses/CANopen cabling specification/CAN message content). The most successful CANopen application profiles are the CiA 417 profile family for lift control systems and CiA 422 profile family for refuse collecting vehicles (also standardized in EN 16815).

CANopen profiles are also used on other communication technologies. Ethercat, Powerlink, Safetynet, and Varan support CiA profiles more or less officially. Other proprietary network technologies make also use of the CiA profile specifications.

Conformity tests are optional

CiA provides since many years a CiA 301 conformance test plan and a tool, implementing it. This CiA CANopen Conformance tool is available for members free-of-charge. Conformance testing is not mandatory. This has advantages and disadvantages: On the one hand nobody has to spend money for testing, but on the other hand some CANopen named devices contain just traces of CANopen functions. Especially, in the early days, there were many so-called CANopen master devices on the market, which were not compliant to CiA 301. Of course, they were able to control and manage CANopen NMT slave devices. But they were by themselves no CANopen devices. They even did not implement an object dictionary.

Some conformance test plans for device profiles have been developed, but to implement them is costly. Testing device profiles makes only sense, when an upper tester is ▷

Figure 1: Heidelberg printing machines is one of the early users of CANopen as network to connect add-on devices to its Speedmaster machines (Source: CiA/Heidelberg)

implemented. Upper testers depend on the device-under-test. This means they are unique and cannot be used easily to test other devices.

Classic CANopen: a hidden champion

CANopen started as an embedded network in industrial machines including printing machines and textile machines. Early adapters were medical device suppliers. Today many medical devices use embedded CAN networks for different purposes. One of the most penetrated markets is construction machinery. Truck-mounted cranes, excavators, and many other earth-moving and mining machines implement embedded CAN-open networks.

This magazine is full of CANopen application reports. Professional coffee machines, subsea equipment, satellites, and service robots are just a few examples of the broad range of CANopen applications. CANopen is also used in police cars and cabs (CiA 447 series), in building doors (CiA 416 series) as well as in rail vehicles.

Besides the CiA 401 profile for modular I/O devices, the CiA 402 drives and motion control profile seems to be the most implemented one. The number of servo controllers and stepper motors supporting CiA 402 is huge. The CiA 402 specification gives the implementers some freedom to use manufacturer-specific functions. This leads to some interoperability issues, when integrating them with host controllers.

Figure 2: The Toru picker self-driving logistics robot from Magazino using CANopen motion controllers by Faulhaber is a typical example of a modern CANopen application (Source: Magazino/Faulhaber)

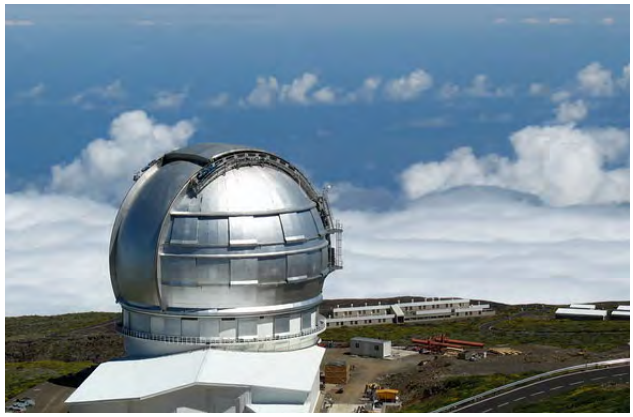


Figure 3: Embedded CANopen networks are also used in exotic applications such as the shown Gran Telescopio Canarias (Source: Flickr/Alberto Perdomo)

CANopen is also used deeply embedded in modular devices such as I/O modules. In such applications it acts as device-internal backbone network. Those deeply embedded networks are not visible. They are so-to-say hidden networks.

Outlook: CANopen FD application layer

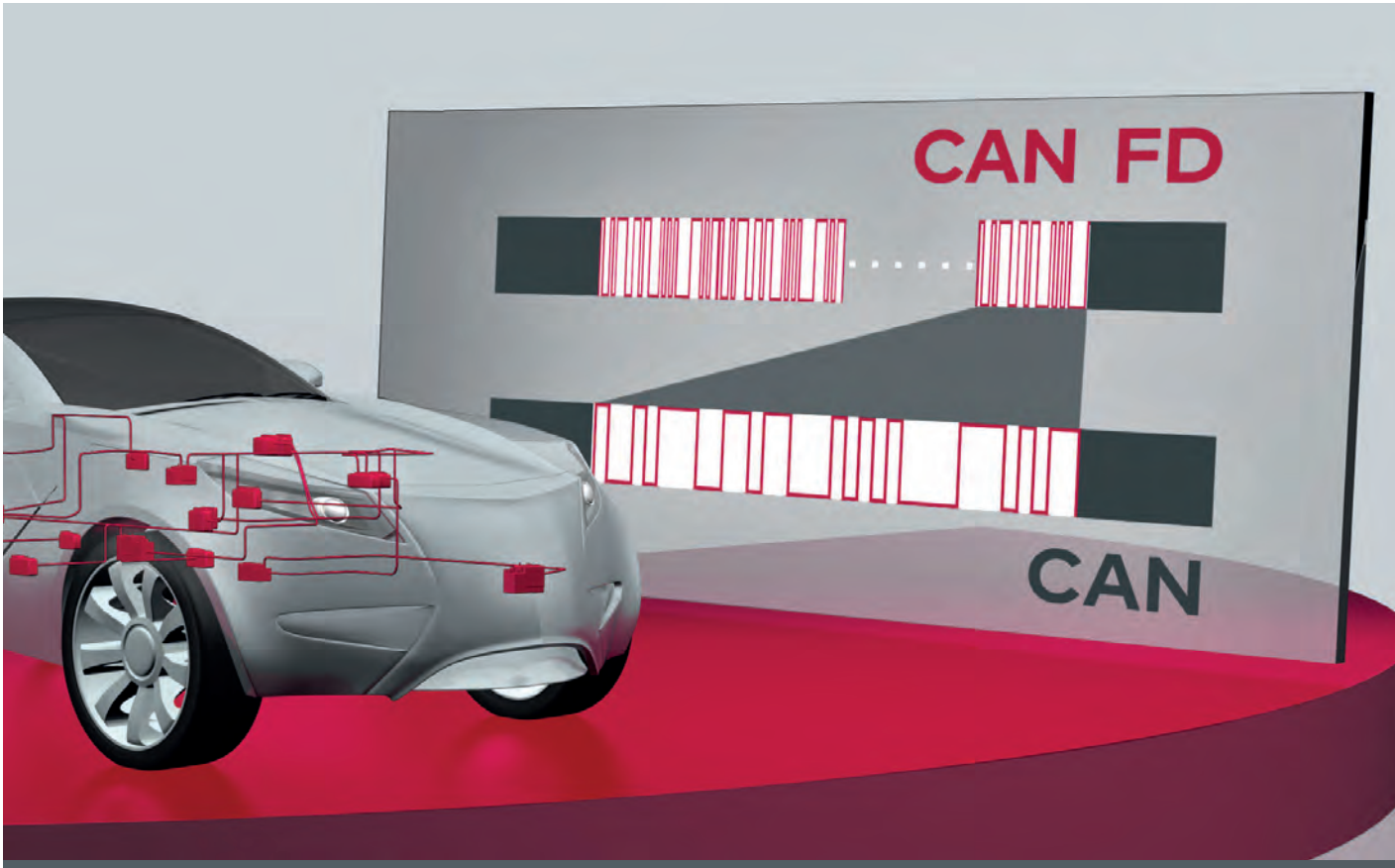
With the introduction of the CAN FD data link layer protocol, CiA started to make use of the higher payload and faster transmission also for CANopen markets. The CiA 1301 CANopen FD application layer is released already. The other necessary building blocks such as electronic data sheet, layer setting services, etc. will follow soon. CANopen FD is specified in a way that it can also be used for the next CAN data link layer generation, which is currently under development in the CiA organization. It will provide payloads up to 2048 byte and will support bit-rate of 10 Mbit/s and above.

Of course, the classic CANopen profiles need to be updated to provide PDOs with more payloads. This process has been started already. The CiA profiles will be divided in a generic part specifying the application functionality and parts describing the mapping to CiA 301 (classic CANopen) and CiA 1301 (CANopen FD). It is also intended to map the CiA profiles to the J1939 application layers on demand. The first profile supporting CANopen FD is CiA 463-F (CANopen device profile for IO-Link gateway – CANopen FD mapping). The functional behavior and parameters are specified in CiA 463-B. Other profiles will be adapted, too. ◀

Author

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

VECTOR



First Class Solutions
for Your CAN (FD) Projects

Your Universal Tool Chain

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

- > High-professionial tools for testing, flashing and calibrating ECUs
- > Flexible network interfaces
- > New all-in-one network disturbance interface
- > Powerful logging solutions for test fleet operators
- > High performance oscilloscope
- > Proven design tools for network architectures
- > Easy to configure AUTOSAR basic software
- > Worldwide engineering services and trainings

More information: **www.can-solutions.com**

More CAN power by Vector: benefit from 30 years of networking experience.

SAE J1939: 25th anniversary

Figure 1: Originally J1939-compliant networks were used in heavy-duty road vehicles for the U.S. market, today most commercial trucks are equipped with multiple J1939 networks (Source: Adobe Stock)

In 1994, the nonprofit SAE association released the first J1939 documents. In the meantime, application-specific network solutions have been developed, which are based on the J1939-21 application layer.

Originally, it was not intended to map J1939 messages to the CAN data link layer. But the introduction of the CAN extended frame format enabled the mapping of the 8-bit source and the 8-bit destination addresses into the 29-bit identifiers. Even today, the 29-bit CAN-ID data frame format option is often named as CAN 2.0B; although, it was already internationally standardized in ISO 11898:1993 and named Extended Data Frame. In the last revision of ISO 11898-1, it is called Classical Extended Data Frame Format (CEFF). This term should be used; CAN 2.0B is outdated since 1993.

In 1994, SAE released the J1939-11 high-speed physical layer, the J1939-21 application layer (unfortunately, titled wrongly as data link layer), and the J1939-31 network layer specifications. The J1939-21 document also specified the BAM (Broadcast Announcement Message) and the RTS/CTS (Request-To-Send/Clear-To-Send) transport layer protocols, which enabled the transmission of messages with more than 8 byte. In order to provide ECU (electronic control unit) interoperability, the J1939-71 document specified the content of the PDUs (protocol data units). Most of the specified parameter groups (PGs) have a length of 8 byte fitting into Classical CAN data frames. Today most of them are specified in the J1939 digital annex. The PGs are identified by the uniquely assigned PGN (parameter group number). Standardized PGs are not configurable, but user-specific PGs as specified in J1939-74 are configurable. They were introduced in 2004.

J1939 networks were first used in trucks and bus to link powertrain electronic control units (ECUs). Nowadays, nearly all commercial vehicles are equipped with J1939 networks. In the last 25 years, additional J1939 specifications have been developed (see Table 1).

The J1939 application layer was also adapted by other industries. The first one was the stationary generator sets, which used the J1939 recommended practices. Some specific functions are specified in J1939-75 (2002). However, this industry is not very transparent. This means, the SAE J1939 committee, which meets quarterly, has no detailed information about generator set applications.

The agriculture and forestry machine industry makes also use of the J1939 communication technology. The ISO 11783 series, released in 2007, references the SAE specifications and adds some specific functions. Also the transport layer protocol has been adjusted to the specific needs of this industry. ISO 11783 compatible networks are also known as Isobus. They link tractors to so-called implements. Implements comprise tractor add-on devices such as sprayers as well as attachable harvesting machinery. There have been published some Isobus-related articles by this magazine. Interesting is that this industry is well organized in the nonprofit AEF association, which organizes bi-annually so-called plugfest. These events are used to proof the interoperability of Isobus devices. AEF has also developed conformance test tools. Conformance testing is mandatory for Isobus implementations. ▷

Table 1: SAE J1939 documents

Number	Title	First issue	Current issue
J1939	Serial control and communications heavy duty vehicle network – Top level	2000	2019
J1939/1	On highway equipment control and communication network	2000	2011
J1939/2	Agriculture and forestry off-road machinery control and communication network	2006	2019
J1939/3	On-board diagnostics implementation guide	2008	2015
J1939/05	Marine stern drive and inboard spark-ignition engine on-board diagnostics implementation guide	2008	2017
J1939/11	Physical layer, 250 kbps, twisted shielded pair	1994	2016
J1939/13	Off-board diagnostic connector	1999	2016
J1939/14	Physical layer, 500 kbps	2011	2016
J1939/15	Physical layer, 250 kbps, un-shielded twisted pair	2003	2018
J1939/16	Automatic baud rate detection process	2015	2018
J1939/17	CAN FD physical layer – 500 kbps/2 Mbps	*	*
J1939/21	Data link layer	1994	2018
J1939/22	CAN FD data link layer	*	*
J1939/31	Network layer	1994	2018
J1939/71	Vehicle application layer	1994	2016
J1939/73	Application layer – Diagnostics	1996	2019
J1939/74	Application – Configurable messaging	2004	2015
J1939/75	Application layer – Generator sets	2002	2015
J1939/76	SAE J1939 functional safety communications protocol	2018	2018
J1939/81	Network management	1997	2017
J1939/82	Compliance	2008	2015
J1939/84	OBD communications compliance test cases for heavy duty components and vehicles	2008	2017
J1939/90	OBD traceability matrix	2019	2019
J1939/91	Network security	*	*
J1939DA	Digital annex (SP and PG specification)	2013	2019
* under development			

Another industry, which makes use of J1939 technology, is the marine industry. The nonprofit NMEA association developed already in the late 90ties the NMEA 2000 specification. It is since 2008 internationally standardized in IEC 61162-3. This standard is widely used for navigation purpose in small boats as well as ocean vessels. It has been amended several times. Last amendment was released in 2014.

The FMS (fleet management system) mainly developed by European truck makers is also based on J1939. It is developed under the umbrella of the nonprofit ACEA European vehicle makers association. Since 2004, it is used to read in-vehicle network and provide this by means of telecom services to manage a fleet of commercial trucks. The ISO 16844 standard, released already in 2001, specifies a J1939-based communication between tachograph and dashboard.

Table 2: ISO 11783 (Tractors and machinery for agriculture and forestry – Serial control and communications data network) documents

Part-no.	Title	First issue	Current issue
1	General standard for mobile data communication	2007	2017
2	Physical layer	2002	2019
3	Data link layer	1998	2018
4	Network layer	2001	2017
5	Network management	2001	2011[a]
6	Virtual terminal	2004	2018
7	Implement messages application layer	2002	2018
8	Power train messages	2006	2015
9	Tractor ECU	2002	2012[a]
10	Task controller and management information system data interchange	2009	2015
11	Mobile data element dictionary	2007	2016
12	Diagnostics services	2009	2019
13	File server	2007	2016
14	Sequence control	2013	2018
[a] under systematic review			

Figure 2: The J1939-based network for agriculture tractors and implements is standardized in the ISO 11783 series (Source: Adobe Stock)

In another ISO standard, the communication between truck and trailer is specified. There are two point-to-point links standardized: one for brake and running gear (ISO 11992-2) another one for other devices including lane departure functions (ISO 11992-3). These ISO standard series was published first in 1998. Both mentioned networks are based on J1939, but use the dedicated physical layer as specified in ISO 11992-1. Unfortunately, just one transceiver IC has been implemented, which is not available openly on the market. If several trailers or dollies are connected, you need multiple ISO 11992 network-segments. In Europe, the brake and running gear network as specified in ISO 11992-2 is required by an ECE (Economic Commission for Europe) regulation.

Under development is a network linking commercial vehicle body control systems such as tail lifts, truck-mounted cranes, cooling systems as well as complex body applications for refuse-collecting vehicles or fire-fighting trucks to telematics gateways. This DIN 4630 standard links also in-vehicle network gateways and FMS gateways. This German standard is written in English language and is mainly developed by body system suppliers in co-operation with some truck and trailer OEMs (original equipment manufacturers).

Other standards and specifications make also use of the J1939 application layer. Currently, the earth-moving machine manufacturers are standardizing autonomous driving vehicles using J1939-based networks to detect and avoid collisions. The Chinese e-vehicle charging standard (GB/T 27930) is also based on J1939.

J1939 and CAN FD

In 2016, CiA started to develop a J1939 application layer using CAN FD. CAN FD is a data link layer option providing data fields with up to 64 byte. The related CiA 602-2 specification introduced a multi-PDU concept allowing the mapping of multiple PGs into one CAN FD data frame. The CiA 602-2 specification was given to SAE for further extension and integration into the new J1939-22 application layer. This specification also introduces a new transport layer and is still under development. It is expected that J1939-22 will be released in 2020. SAE is also developing the J1939-17 physical layer specifying a 500 kbit/s arbitration speed and a 2-Mbit/s dataphase bit-rate. Also this SAE document will be released beginning of next year. ◀

+++ EDITORIAL +++ EDITORIAL +++ EDITORIAL +++

Hard to read for newcomers

The different standards based on J1939 are developed independently. There is no harmonization, so far, regarding terminology and description. Sometimes, the same functions are specified in two standards. I think, it would be better to make reference to avoid differences in the descriptions. It would be also more than nice to harmonize terms. This would decrease the chance of misunderstanding and misinterpretations. These problems are addressed and need to be fixed in the next revision of J1939-related specifications and standards. As the convener of an ISO working group responsible for the ISO 11992 and ISO 16844 series, I am working on the avoidance of double-specifications. I am doing the same as liaison officer for the ISO 11783 series. To improve all J1939-related documents is a giant task, which I cannot do alone. Everyone can do one simple thing: Use terminology consistently and correctly. For example, the PGN (parameter group number) is just a number and not the PG (parameter group). A J1939 message comprises the PGN and the PG. The PG is the assembly of suspect parameters (SPs). Do not use PGN as synonym for PG. Let us make the documents easier to read and to understand. Newcomers should not be challenged.

Holger Zeltwanger

Author

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

KVASER

Welcome to the new Kvaser Memorator Light v2

Simple to use. No configuration or software setup required. Ideal for monitoring intermittent faults. More than enough memory to capture an entire test drive.

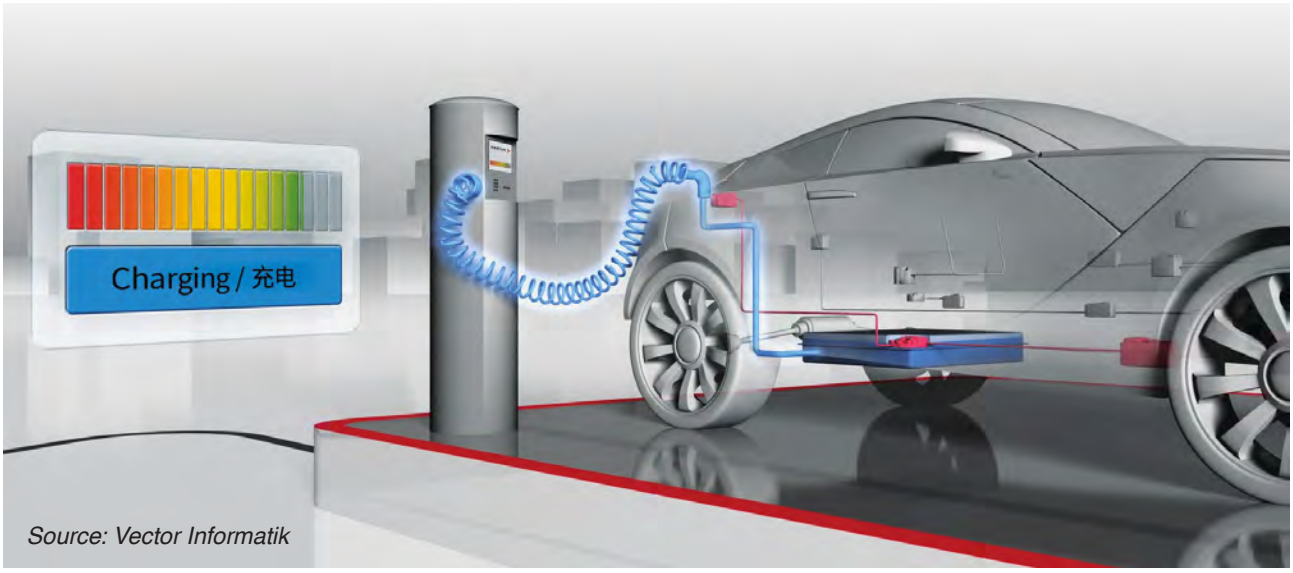
Features include:

- Autobaud function automatically determines CAN bus bit rate.
- Silent mode: Log traffic without interfering on the bus.
- Rugged & Reliable: the memory card is attached to the PCB.
- Two FIFO buffers: Log all messages & the messages before and after an error frame.
- A built-in real time clock with battery backup.

To find out more, visit **www.kvaser.com/kvaser-memorator-light-hs-v2**

Charging communication in Chinese

Manufacturers around the world who want to sell electric cars in China have to comply with the Chinese standard GB/T 27930. Vector simplifies development and testing GB/T 27930 compliant electric vehicles and charging stations.



Source: Vector Informatik

In China, as everywhere else in the world, the success of electric mobility is closely linked to the availability of a large number of charging stations and optimal compatibility between vehicles and the charging infrastructure. For communication between charging stations and on-board battery management systems, the Chinese standard GB/T 27930 has been established for use in the People's Republic. This is why European, American, and any other manufacturers around the world who want to sell electric cars in China have to comply with this standard. Development for the Far East can be significantly accelerated through the use of corresponding testing and simulation tools and ready-to-use embedded solutions for GB/T 27930 based charging communication.

Like virtually no other nation, China is advancing electric mobility with tremendous effort. The numbers are impressive: In 2018 alone, more than one million electric vehicles were purchased by Chinese consumers. If this trend continues, more than five million electric cars will be on China's roads by 2020. An armada of electric vehicles like this is also going to need an adequate supply of power. At present, around 200 000 charging stations have been installed – and the number is rapidly rising. The growth rate of stations is even noticeably higher than that of the electric vehicles themselves. In order for charging processes to run smoothly everywhere, standardized communication between electric cars and charging stations is essential. This has been described in the Chinese GB/T 27930 standard for charging systems. It defines the communication between a charging station (charger) and the battery management system (BMS) in an electric car for conventional cable charging.

Additional smart charging functions, such as those described in ISO 15118, are not supported by the Chinese communication standard. GB/T 27930 also gives no information about possible uses of the standard. Only the high-level document GB/T 18487.1-2015 mentions that buses, trains, utility vehicles, and off-road machines aren't supported. According to information from China, though, it seems to be common practice to charge all electric vehicles at the same charging stations, regardless of whether they are cars, trucks, or buses. Obtaining accurate information in this regard can be difficult, as hardly any information on GB/T 27930 is freely available on the Internet.

GB/T 27930: Based on J1939

The current version of the standard is GB/T 27930-2015 from 2015, which replaced version GB/T 27930-2011. GB/T 27930 is based on SAE J1939 and accordingly uses a CAN network as a point-to-point connection between the charger and the BMS. Direct connections to other CAN systems in the vehicle, such as the Powertrain CAN, do not exist. A transmission rate of 250 kbit/s is used by default. If the line quality is poor or external interference fields are influencing communication, a reduction to 50 kbit/s ▷

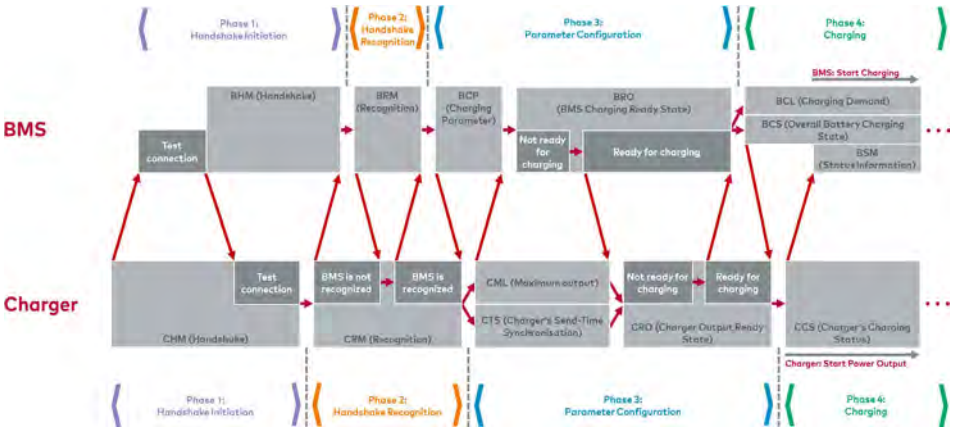


Figure 1: The charging process - Phases 1 through 4 with all relevant messages and state transitions (Source: Vector Informatik)

is possible. The layout of the CAN identifiers adheres to the rules of J1939, and GB/T 27930 supports the transport protocol for directed data transfer from J1939-21 (RTS/CTS or CMDT). Diagnostic options are also provided, for which the standard defines six diagnostic messages designated DM1 through DM6.

Differences between GB/T 27930 and J1939

However, GB/T 27930 differs in several aspects from J1939, such as the lack of address arbitration according to J1939-81. As a result, parameter groups for address claiming, commanded address, and name management are not defined. This is logical and consistent, as the charging station and vehicle's BMS are always the only participants involved in charging communication. The specification clearly defines their addresses: 86 (56_h) for the charger and 244 ($F4_h$) for the BMS, which are conflicting with predefined addresses of J1939. Since the Request mechanism from J1939-21 is used solely for diagnostics, neither the ACKN (PGN $E800_h$) nor Request2 (PGN $C900_h$) nor Transfer (PGN $CA00_h$) parameter group is present.

In addition, GB/T 27930 uses the names DM1 through DM6 and packs the information on arising problems into DTC (diagnostic trouble code) blocks as described in J1939-73, but the function and parameter group numbers (PGNs) are defined differently from J1939, and the DTCs do not start with byte 3, but rather byte 1. In deviation from the recommendations of J1939, GB/T 27930 also uses messages with message lengths (DLCs) shorter than eight.

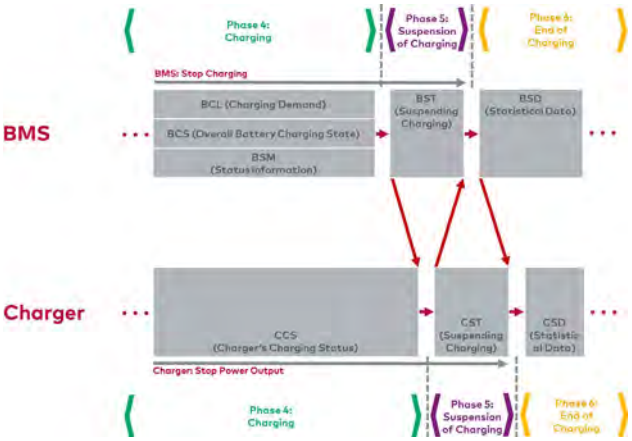


Figure 2: Ending of the charging process initiated by the BMS (Source: Vector Informatik)

Communication phases

Charging communication primarily involves both the battery management system and the charging station agreeing on the energy requirements of the vehicle and both the amperages and voltages used during charging. Following successful connection establishment, the vehicle electronics notifies the charging station of the desired charging current and voltage (request). If the charging station is able to provide the desired energy, the charging process begins with the desired parameters. If insufficient power is available on the power grid overall, for example because too many vehicles want to charge at the same time, the charging station reduces the current and communicates this to the BMS. Based on the boundary conditions, the charging electronics adjusts to different charging currents in this way.

Each charging process can be divided into the following six phases:

1. Handshake initiation
2. Handshake recognition
3. Parameter configuration
4. Charging
5. Suspension of charging
6. End of charging

Phases 1, 2, 3, 5, and 6 work according to the same principle. The charging station begins sending a data record, e.g. a CHM (charger handshake message). The BMS then receives the CHM and carries out the corresponding action, e.g. by checking the connection. To signal that it has carried out the action successfully, the BMS begins sending a BHM (BMS handshake message) to the charging station. As soon as the charging stating has received the BHM, it starts the corresponding action on its part and checks compatibility, for example. Once the task is complete, it begins sending another message. The procedure is like a soccer game, in which two players reach the opponent's goal or target by continually passing the ball back and forth to one another (Figure 1).

Messages during energy transfer

During phase 4, the actual charging process, communication is considerably clearer, as there are no longer any state transitions. The BMS and charger send their messages back and forth cyclically and independently. The vehicle initiates the charging process, sends the requirements to the charging station using the BCL (battery charging demand) message, and informs it of its own state using the BCS (overall battery charging status) and BSM (power storage battery status information) messages and other messages. The charging station, on the other hand, sends the CCS (charger's charging status) message and informs the vehicle of its status, the current being provided and the maximum voltage which can be generated.

There are also three optional messages with which the vehicle can provide additional information on its internal status to the energy source while charging: BMV (single power storage battery voltage), BMT (temperature of power storage battery), and BSP (reserved message of power storage battery). The charging process lasts until either the battery management system or the charging station initiates the end of charging. This happens either when the battery is fully charged, the specified charging duration is reached, or the passengers wish to continue traveling without a fully charged battery (Figure 2).

Problems and faults while charging

Problems during charging can be classified as communication faults or technical faults. The first group generally includes timeouts, such as when a state transition does not occur within the prescribed time or when cyclical messages are received too late. Overheating, line breakage, deviations from the target current and voltage values, and similar issues are classified as technical faults. As a response to ▷

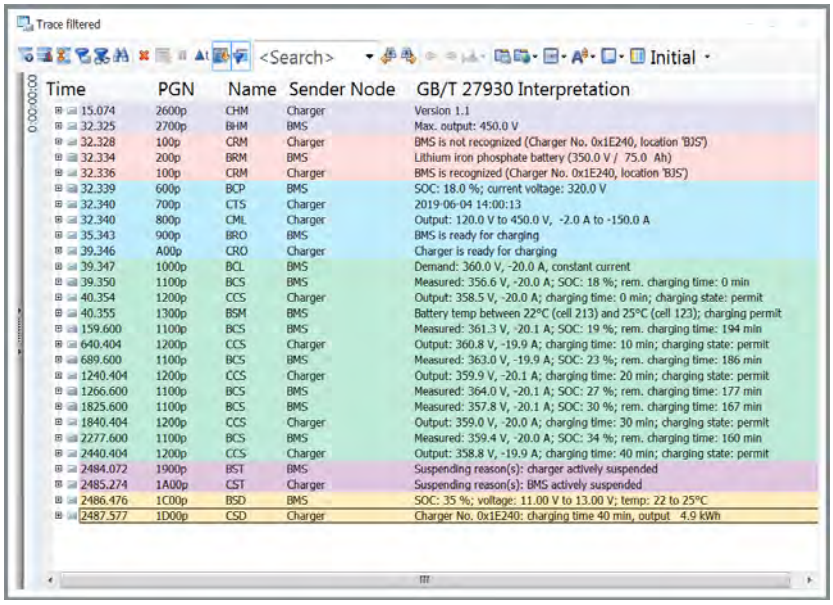


Figure 3: Typical communication between a charging station and an electric car: All six phases are simulated with CANoe 12.0 and represented in a reduced form in the Trace Window through intelligent filtering (Source: Vector Informatik)

DIY CAN TOOL
WITH COLOR TOUCHSCREEN

Meet VividCAN!

- Affordable, versatile, & customizable CAN tool
- Use as a field service tool with a simple touchscreen
- Perfect for field diagnostics, such as factory resets, configurations and localizations
- Ideal driver's aid for displaying drive profiles compared to actual values
- Use for executive display

Key Features

- 60 FPS highly responsive display
- Capacitive display technology for easy and reliable operation
- Simple to configure with Vehicle Spy software
- Very quick startup (under 500 ms) with auto wakeup and startup features

Find out more: www.intrepidcs.com/vivid

INTREPID
CONTROL SYSTEMS
www.intrepidcs.com

+49 (0)721 1803083 -1 icsgermany@intrepidcs.com

USA Germany UK Japan Korea China India Australia

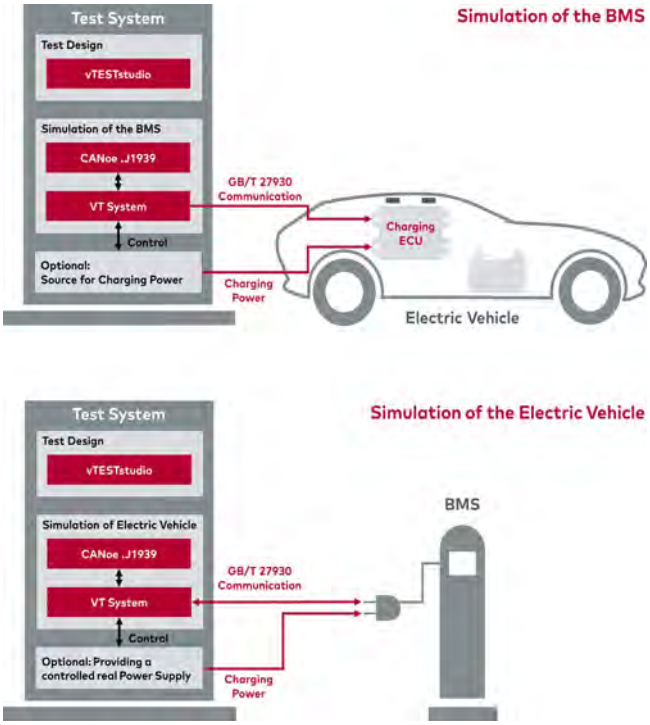


Figure 4: A GB/T 27930 compliant simulation solution (Source: Vector Informatik)

faults, the system either cancels connection establishment or stops the energy output or intake, depending on which side detected a fault. This ends the charging process.

Testing development in an efficient way

In principle, communication as per GB/T 27930 is not unusually complex, but it is characterized by certain pitfalls and quirks. This is made more difficult by the fact that there are a large number of charging station manufacturers in China. Many cities and municipalities have what essentially amounts to their own local charging station production, which bears the risk of each one interpreting the standard in their own way, potentially differing in some small detail.

Because of this, it is in the best interest of everyone who develops electric vehicles for the Chinese market to comprehensively test the vehicle electronics. The required depth of testing can only be realized through systematic tests and corresponding test automation. A GB/T 27930 reference is also required, against which testing can be carried out. Electric vehicles are to be tested as expected using suitable charging station electronics (Figure 3). Manufacturers of charging stations, on the other hand, require a vehicle battery management system which corresponds to the standard.

Automated testing against simulated remote stations

Based on CANoe and the modularly configurable VT System as testing hardware, Vector has developed a GB/T 27930 compliant simulation solution which can simulate either the charging station or the electric vehicle's BMS. CANoe is responsible for sequence control and serves as the user interface for the convenient creation of test scripts with C-like syntax (CAPL) and for checking test reports. The respective simulated system receives and transmits messages according to the GB/T 27930 standard. This makes it possible to simulate rising and falling charging amperages and to request higher or lower current. Also, the temperatures and temperature fluctuations of individual battery elements can be simulated, and the charging duration can be estimated (Figure 4).

If desired, the testing system can confront the test object with software and hardware faults. Artificial line breakage and short circuits can be created by the user by way of the VT System. Controllable power supplies and electronic loads can also be connected up if charge testing with actual amperages and voltages is desired. The graphical interface enables convenient operation and monitoring on the screen, and users can also define their own panels as they see fit.

Additional components and outlook

Complete embedded solutions from the Microsar product line are also available for GB/T 27930 compliant charging communication. Users are able to integrate them directly into their development environment with minimal effort, thus achieving the required level of product maturity as quickly as possible. At the same time, Vector is continuing work on a comprehensive GB/T 27930 testing solution so that compliance tests can also be carried out in the future, for example. ◀

Author

Dipl.-Phys. Wladimir Schnaper
Vector Informatik
info@vector.com
www.vector.com

COMPLETE HARVESTER CONTROL SOLUTIONS.

UKMADE

DSE**M240**
CAN Slave Module (44 I/O)

DSE**M640**
Programmable Controller (68 I/O)

DSE**M643**
Programmable Controller (34 I/O)

DSE**M840**
4.3" Programmable Display

DSE**M870**
7" Programmable Display

DSEControl® M-Series

DSE has been delivering world-class control solutions to its customers for over 40-years. During this time the company has developed a reputation across the globe for its UK engineering and manufacturing excellence.

The **DSE M-Series** builds on this reputation. The innovative collection of programmable controllers & displays and CAN slave modules provide customers with complete harvester control solutions.

To learn more about **DSE M-Series** products, visit **www.deepseaelectronics.com**

VISIT US AT

CONEXPO-CON/AGG 2020

MARCH 10-14, 2020
BOOTH: **B93602**

DEEP SEA ELECTRONICS LTD
Highfield House, Hunmanby Industrial Estate Hunmanby, North Yorkshire, YO14 0PH, UK
TELEPHONE: +44 (0) 1723 890099

CiA 601-4: CAN signal improvement

New CAN FD SIC (signal improvement capability) transceivers will remove some limitations and accelerate CAN FD far beyond what was previously possible, opening up new possibilities. This article reviews the background, the new CiA 601-4 version 2.0.0, and the future implications for CAN.

CAN FD was introduced as an extension of Classical HS-CAN that enabled more data to be exchanged at faster bit rates. Whilst clearly boosting the throughput of Classical CAN, the accelerated bit rates created new signal integrity problems, significantly limiting its application in the topologies that car makers ultimately required. New CAN FD SIC transceivers will remove these limitations and accelerate CAN FD far beyond what was previously possible, opening up new possibilities for this technology. This article reviews the background, the new CiA 601-4 version 2.0.0, and the future implications for CAN.

CAN FD - accelerating to 2 Mbit/s

Getting faster bit rates through a CAN network is not a new problem. Communication bandwidth is always in demand and as many automotive networks have evolved over time, they have slowly reached their bandwidth capacity. The maximum bit rate a CAN network can reliably operate at has been traditionally limited by the loop delay, a timing parameter defined in the ISO11898-2 standard. Essentially, it equated to a simple principle: faster bit rates enforce smaller networks. Specifically, a shorter maximum distance between any two nodes.

This limit derives from the arbitration phase, where all nodes need to correctly receive every other nodes' signal to collectively agree on who has priority to send.

CAN FD, by comparison, could accelerate to higher bit rates by only doing so in the data phase of communication, when arbitration has completed and there is just one node sending. Here the loop delay requirement no longer applies, although it does still apply unchanged during the arbitration phase of CAN FD. As a result, every CAN FD network has two defined bit rates: the bit rate during the arbitration phase (typically similar bit rates to previous HS-CAN networks) and the data phase – or fast phase – bit rate, when the payload is sent and when faster bit rates can be achieved.

While CAN FD was defined up to 5 Mbit/s in the fast phase in the ISO11898-2:2016, quickly a new speed limit was encountered when networks were evaluated at these higher bit rates. This time, it was achieving a stable signal during the recessive bit, which became distorted due to two topology effects: signal ringing, created by unterminated stubs (or branches) in the wiring harness, and signal plateaus, created by a lower characteristic cable impedance. These both disturbed the signal at the beginning of the recessive bit and delayed it from becoming stable below a differential voltage of 0,5 V. This 0,5 V is the minimum receiver threshold – the point at which all transceivers must interpret the signal as recessive.

These effects were not new creations of CAN FD and already existed in traditional HS-CAN networks. However, the bit rate in the fast phase meant bit times were significantly shorter and so the effects which were normally small artifacts way ahead of the sample point, now became significant roadblocks to reliable communication.

To mitigate these effects, network architects had to limit the complexity of their topologies, by avoiding long, unterminated stubs and remaining instead with a reduced number of nodes in a typically linear (or daisy-chain) network. While this allowed communication to be guaranteed, it came with several side-effects: an increase in network branches leading to more complex gateways, more ▷

Figure 1: Signal ringing examples at 500 kbit/s (left) and 2 Mbit/s (right). The horizontal lines show the minimum and maximum receiver thresholds. To guarantee reliable communication, the signal must be stable underneath the minimum receiver threshold by the sample point, typically around 70 % to 80 % of the bit time. In the 2 Mbit/s example, the signal still peaks above this limit, preventing reliable communication to occur. (Source: NXP)

connectors, more cabling being routed through a vehicle, and more complex installation and test during vehicle production. A simple illustration of this would be routing a cable to a roof module. With a linear topology, the cable now needs to both stretch up 1 m to 2 m up to the roof, and then back down again, instead of just having a one-way stub. This adds more cost and weight to the cable harness. Even with these mitigations however, CAN FD became effectively limited to 2 Mbit/s communication, outside of point-to-point connections.

CAN signal improvement capability

The problem of controlling the signal during recessive bit was initially tackled in the CiA 601-4 version 1.0.0 specification. A receiver-based approach was proposed, which monitored the bus and tried to identify a recessive bit transition. Once detected, it would actively bring the signal to 0-V differential for a period of time. This solution showed good results on bench tests, with multiple nodes acting simultaneously to improve the ringing and increasing the potential topology size at 2 Mbit/s. It did not, however, fully address concerns on how to reliably distinguish genuine bit transitions from temporary signal distortions (such as glitching on the bus or by EMC effects) and plateau effects were shown to risk delaying activation.

A receiver-based approach also has inherent limitations on its speed of activation. Fast activation is a key parameter to quickly eliminate energy in the ringing and get the signal stable below the 0,5-V threshold. By reacting on the bus signal, additional delay is introduced to ensure accurate detection, with any additional filtering of glitches slowing down the reaction time further. Certainly, when considering bit-rates beyond 2 Mbit/s, the reaction time would become a major bottleneck for such an approach. Finally, any receiver-, or feedback-based concept has an inherit problem of ensuring system stability, especially if a critical node lost power and was no longer able to improve the signal, then communication in the entire network could be affected.

NXP proposed an alternative feedforward-based solution. Activation is based on the TXD input, which is both reliable and allows a significantly faster activation time, since this triggers the signal improvement even before the internal propagation delay of the transceiver. Faster activation of the signal improvement means ringing is controlled earlier in the bit time, guaranteeing communication in networks with more severe ringing (thus more complex topologies) or in a network with even faster bit rates. System predictability is straightforward since there is only one sender applying signal improvement. This avoids having possibilities for unpredictable interactions between nodes and since each node manages their own signal, should any node lose power, its impact would be limited only to that node.

The CiA 601-4 working group reviewed both these concepts leading to a set of requirements for any solution. With thanks to major contributions from several car makers and silicon vendors, this resulted in a basic set of requirements that can be summarized as follows:

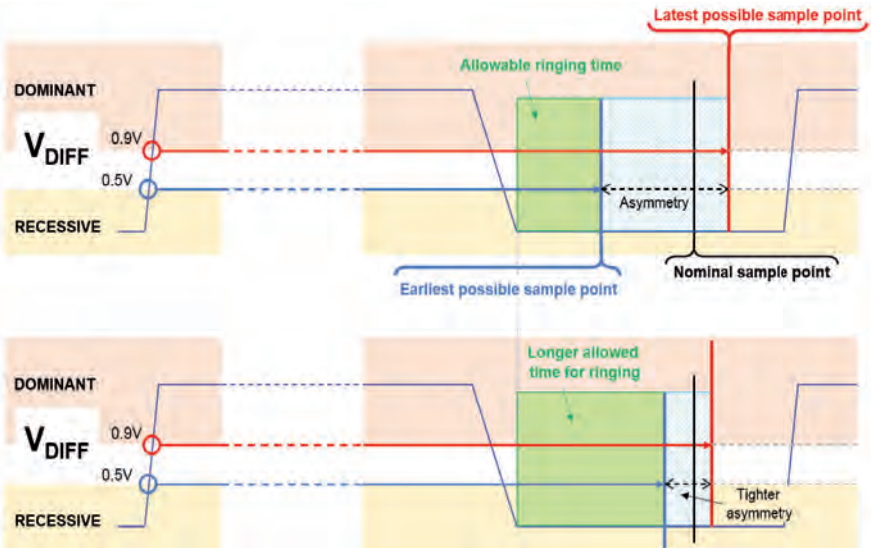


Figure 2: A reduced asymmetry a smaller deviation on when a sample point may occur, which means the earliest possible sample point is later. In turn, this means more time for ringing to occur without affecting network communication. (Source: NXP)

- All mechanics of the existing CAN FD protocol shall be fully guaranteed, especially arbitration, frame acknowledgement, and error handling.
- Solutions should be as fast as possible and bit rate independent. Up to 8 Mbit/s shall be considered.
- Solutions should be fully backwards compatible with conventional HS-CAN transceivers and footprint compatible, to enable easy adoption.
- Solutions should have the same robustness to EMC (electromagnetic compatibility), ISO pulses, and ground shifts as of today.
- Networks with signal improvement shall have a predictable system response, also in case a node fails or loses power.

From this work, specification points were derived and captured in the new CiA 601-4 version 2.0.0 specification, which relate to the transceiver symmetry, the length of signal improvement time and EMC testing. Collectively, these define the basic criteria any CAN signal improvement solution should fulfill, independent of its precise approach.

Transceiver symmetry explained

The transceiver symmetry is highly relevant to the overall capabilities of a CAN FD network. Simply, it defines how much timing deviation is seen on successive bit edges from TXD to the CAN network, and from the bus to RXD. This is relevant because all CAN controllers synchronize on a dominant bit transition, and any transceiver asymmetry will introduce potential timing differences for when nodes make their sample point. Since guaranteeing reliable communication relies on a signal being stable at the sample point, it is important to calculate when the earliest sample point may occur, including these deviations, and assess the signal stability at that moment. Before that time, no sample point will ever occur, so signal distortions are no problem. This can be referred to as the “allowable ringing time”, shown in Figure 2.

Transceiver symmetry is a significant component in the total asymmetry calculation within a network. Thus tightening the symmetry specification means less possible spread and the earliest sample point will appear relatively later. This in turn increases the allowable ringing time before that earliest sample point. Unlike the ISO11898-2:2016, which defined symmetry values for 2 Mbit/s and 5 Mbit/s, the CiA 601-4 version 2.0.0 defines bit-rate independent values with a much tighter symmetry specification. This enables CAN FD to tolerate significantly more ringing, allows significantly shorter bit times, extending the maximum bit rate CAN FD can operate to even beyond 10 Mbit/s.

Additional specification points and next steps

Further to the symmetry specification, the CiA 601-4 version 2.0.0 introduces a limit on the duration of signal improvement time, required to respect arbitration rules. If multiple senders all concurrently are trying to bring a recessive signal to 0-V differential while another node is sending a dominant signal, all nodes should agree the bus is dominant. To achieve this, the maximum signal improvement time limit is set, defining effectively a maximum arbitration bit rate for networks with signal improvement, with an associated limit on maximum node distance. The CiA 601-4 version 2.0.0 specification provides a generous operating area however, with 48 m supported at 500 kbit/s bit rate, and a maximum arbitration bit rate of 727 kbit/s.

Finally, a new EMC test proposal is made in order to provide evidence that any CAN FD SIC transceiver is not creating any EMC issues. Additional emission and immunity tests are defined, to introduce differential ringing into the EMC test set-up. This ringing still needs to be eliminated, even under harsh RF injection.

With the publishing of the CiA 601-4 version 2.0.0 specification, the basis of this technology is now defined. Interoperability tests (IOPT) are now under development, based on the current HS-CAN IOPT.

NXP’s CAN FD SIC technology

NXP has played a key role with other industry players in the development of the CiA 601-4 version 2.0.0 specification, promoting a feedforward-based CAN FD SIC solution. This solution has been extensively evaluated globally by car makers and demonstrated to reliably operate complex networks beyond 5 Mbit/s. At 2 Mbit/s, it significantly boosts potential network topology dimensions and our experience broadly shows a topology validated at 500 kbit/s can be operated at 2 Mbit/s. An additional advantage of the NXP CAN FD SIC solution is that it is bit-rate independent, with one device able to serve any bit rate. NXP is now sampling ▷

this technology and we expect the first vehicles using this technology to be on the road in 2020.

CAN signal improvement also really extends what is feasible with CAN FD and 5 Mbit/s becomes a definite reality for car makers to consider in their future technology choices. With vehicle network architectures undergoing major changes in the next generations of vehicles, this positions CAN FD as a highly relevant and meaningful technology to consider, givens its proven reliability and cost.

Although signal improvement can theoretically go way beyond 5 Mbit/s, accelerating the fast phase to even higher bit rates comes with diminishing returns, given the arbitration phase remains unchanged. Therefore, there is, a natural link from signal improvement technology towards CAN XL, which intends to significantly increase the payloads and removing limitations in the current CAN FD protocol that would enable more physical layer improvements of the signals. That technology step will require new protocol controllers in the micro-controller – something not required with signal improvement transceivers of today – but with this promising technology targeting 10 Mbit/s communication and 2 kbit/s frames, it extends the potential and relevance for CAN even further within new vehicle networks.

Author

Tony Adamson
NXP Semiconductors
info@nxp.com
www.nxp.com

CAN security case in small aircrafts

Source: Adobe Stock

In July, the US Department of Homeland Security (CISA) has issued a security alert warning owners of small aircrafts about vulnerabilities that can be exploited to alter airplane telemetry.

The vulnerabilities reside in avionics (electronic equipment fitted in an aircraft), and more specifically inside a small aircraft's CAN network. The attacker needs to have physical access to the CAN network to inject false data, resulting in incorrect readings in avionic equipment reported CISA. This in mind, such an attack is not very likely, because the access to aircrafts is highly regulated and controlled in most countries. Rapid7 examined two small aircrafts, but not discovered the brand names.

Patrick Kiley from the Rapid7 cybersecurity company was one of the researchers, who investigated in CAN network integrity in avionics systems: “After performing a thorough investigation on two commercially available avionics systems, Rapid7 demonstrated that it was possible for a malicious individual to send false data to these systems, given some level of physical access to a small aircraft’s wiring.” Such an attacker could attach a device to an avionics CAN network in order to inject false measurements and communicate them to the pilot. These false measurements can include the following:

- incorrect engine telemetry readings
- incorrect compass and attitude data
- incorrect altitude, airspeed, and angle of attack (AoA) data

“In some cases, unauthenticated commands could also be injected into the CAN network to enable or disable autopilot or inject false measurements to manipulate the autopilot’s responses,” said Kiley. A pilot relying on these instrument readings would not be able to tell the difference between false data and legitimate readings, so this could result in an emergency landing or a catastrophic loss of control of an affected aircraft.

As mentioned, physical access to the CAN network was needed to perform the attack. The CAN data frames were injected by a USB dongle linked to the CAN networks. The frames from the avionics devices were recorded using a Linux operating system running the CAN-utils software. “The system was reverse engineered by sending individual recorded CAN frames back onto the avionics bus and observing what effects they had with the various nodes,” explained Kiley. This reversing technique is particularly effective in CAN explorations compared to other networking environments, since CAN network implementations are often susceptible to replay attacks. In addition, Rapid7 modified various CAN data frames to observe any interesting effects.

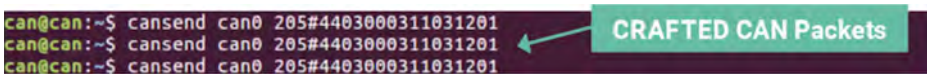


Figure 1: Crafted oil pressure CAN data frame (Source: Rapid7)

Findings in the first aircraft

The first examined avionic CAN network included the following devices:

- 10-inch glass panel combining the primary flight display (PFD) and the multi-function display (MFD)
- avionics concentrator
- engine Instrumentation controller
- electronic magnetometer (compass)
- attitude and heading reference system (AHRS)

Rapid7 researchers found out that CAN-ID 205_h contains the oil pressure, the oil temperature, and two cylinder head temperature values. “By sending crafted data frames using this CAN-ID, we were able to send false oil pressure, oil temperature, and cylinder head readings to the display,” said Kiley.

The compass uses the CAN-ID 241_h. The attitude and heading reference system (AHRS) transmits the CAN-IDs 281_h to 284_h with the AHRS acting as node 1. Nodes 2, 3, and 4 produce the CAN-IDs 291_h to 294_h, $2A1_h$ to $2A4_h$, and $2B1_h$ to $2B4_h$, respectively. The AHRS data frames were reverse engineered by spoofing messages from nonexistent AHRS units until the displayed aircraft attitude was changed, indicating an incorrect aircraft orientation.

The used higher-layer protocol does not provide any kind of built-in authentication mechanism. This is what makes the CAN communication easy to implement, but it also removes any assurance that the sending device was the actual originator of the provided data.

Finding in the second aircraft

The second examined avionic CAN network comprised the following devices:

- 10-inch combined PFD and MFD
- AHRS sensor
- electronic magnetometer (compass)
- autopilot servo
- engine Instrumentation controller
- flap/trim electronics controller

In this aircraft 29-bit CAN-IDs are used. The CAN-ID 10342200_h contains the oil pressure. By sending crafted data frames with this CAN-ID, Rapid7 engineers were able to send false oil pressure values to the display.

“We also identified that the CAN-IDs responsible for attitude and heading were part of a more complicated, non-standard CAN message format.

The electronic compass uses the CAN-IDs $10A8200_h$ and $10A82100_h$ to transmit the altitude and heading data. The data frame with the CAN-ID $10A8200_h$ acts as a header packet, with the third byte used to indicate the length of ▷

the message. "We reverse engineered the magnetic heading, time, and magnetic field strength fields by fairly standard protocol analysis techniques," explained Kiley.

The payload of the AHRS data frames were also reverse engineered and turned out to be very similar to the messages described above. The AHRS sent 52- and 60-byte messages with CAN IDs 10242000_h to 10242200_h.

Rapid7 engineers were able to both replay messages as well as craft data frames that would then indicate on the PFD an incorrect altitude, attitude heading, or airspeed. This attack could then be combined with one against the autopilot system. It was identified that the autopilot could be engaged and disengaged (see Figure 6).

Figure 2: Spoofed CAN data frames from AHRS nodes 2 and 3 (Source: Rapid7)

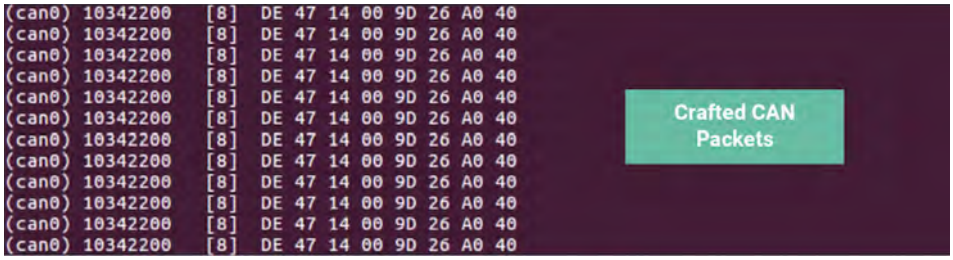


Figure 3: Crafted CAN data frames with false oil pressure values (Source: Rapid7)

An attack against the autopilot and attitude indicator could lead to an unusual attitude and potentially loss of control of the aircraft, given that forged CAN data frames can create disastrous scenarios very quickly.

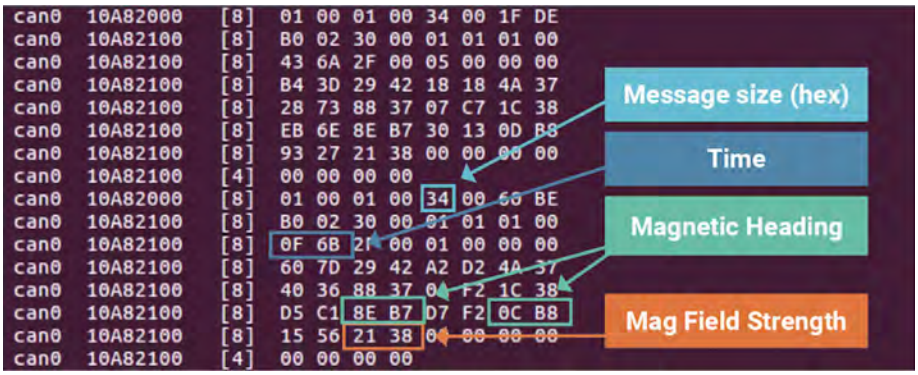


Figure 4: Example of the GMU 11 Magnetic Compass data frame (Source: Rapid7)

Conclusion and recommendations

In commercial and military aviation the physical access to aircrafts is limited and controlled. But still this is a single point of failure. In security engineering, it is well understood that relying on a single dimension of security for protection is precarious. In particular, in cybersecurity, it is generally frowned upon to rely on only securing the environment of the systems, rather than addressing vulnerability of the system itself.

"For example, while the most correct solution to a given database software vulnerability may be to apply a patch from a ▷

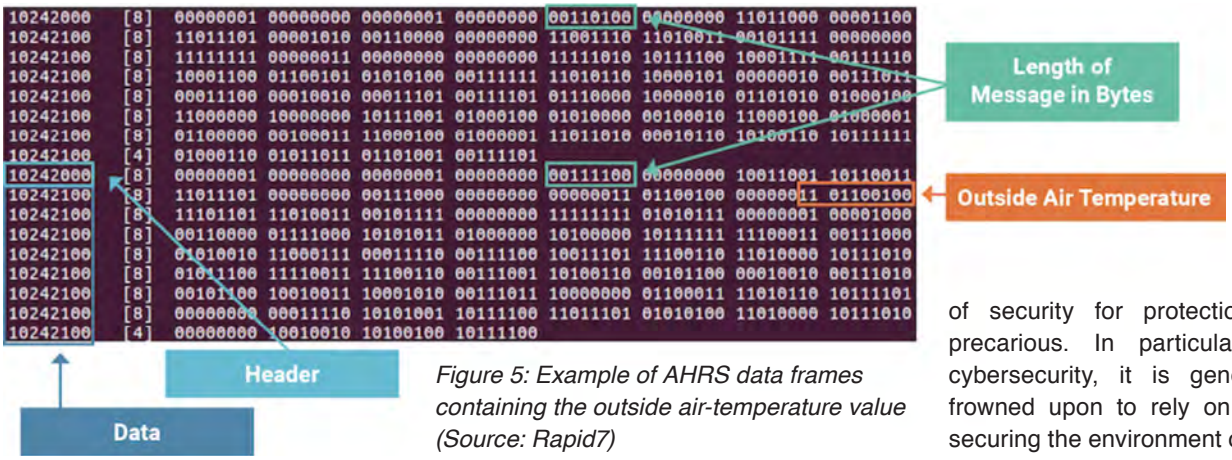


Figure 5: Example of AHRS data frames containing the outside air-temperature value (Source: Rapid7)

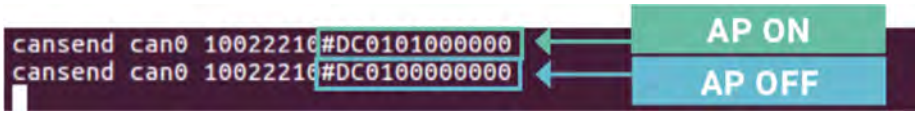


Figure 6: Autopilot data frames (Source: Rapid7)

vendor, a better solution would involve patching as well as limiting network access to that software through an operating system firewall and a local network firewall, and limiting physical on-keyboard access to authorized personnel. That way, if one of these systems happens to fail – a patch is skipped, a firewall rule is mistyped, or a physical door to a data center is left ajar – other defensive measures are in place to help prevent disaster," explained Kiley.

The CAN data link layer lacks modern network security design considerations, such as cryptographic assurances of data frame sources or authenticity. More critically, CAN-based networks often do not consider the threat model of an attacker with physical access to the shared wiring of the system. "While the physical security of airplanes is both well regulated and well tested, this reliance on physical controls may, in fact, be a leading cause as to why aviation CAN security has not matured at a pace similar to more traditional security or even automotive CAN security," said Kiley.

One solution to detect unauthorized access to the CAN network is the Stinger transceiver by NXP. However, the proposed solutions using CAN-specific filtering, whitelisting, and firewalling, do not appear to have gotten much traction in avionics networking, at least in the avionics systems favored by pilots of small aircraft, stated Patrick Kiley. He added: "This is due, in part, to the emphasis on physical security in aircraft; after all, even small, personal aircraft are rarely parked in unmonitored, open areas like open parking lots or public streets."

Small-aircrafts are also increasingly seeing similar enhancements with consumer technologies such as Bluetooth and Wi-Fi. These wireless interfaces are additional vulnerabilities. Rapid7 did not test this interface as a part of this research. "Given these realities, we offer two suggestions to reduce the risk of avionics CAN networks attacks based on false messages: Segment the CAN network from other networks and encourage secure designs for CAN network itself," explained Kiley.

"The open-ended nature of CAN should be seen as an invitation for security innovation. In particular, our research indicates that a message authentication protocol would strengthen defenses against attacks that leverage forged CAN messages," said Kiley. He proposed to use CAN FD with a payload of up to 64 byte: "Some of that extra space can now be used for security-critical features such as replay protection and cryptographic hashing. There is no reason to think that CAN could not enjoy a leveling-up of secure design if manufacturers, framers, regulators, and users demand it." ◀

hz

Classical CAN/CAN FD security threats

The authors already have introduced various technical solutions for distinct security threats. In this issue of their quarterly articles, they want to take a step back to look at the bigger picture of CAN security.

We've already introduced you to various technical solutions for distinct security threats: black- and whitelisting technologies for Classical CAN/CAN FD transceivers, CANcrypt for authenticated and/or encrypted Classical CAN/CAN FD communications and (D)TLS for secure end-to-end security in remote access applications. However, choosing the right one largely depends on the application's needs and the manufacturer's design goals. Some might be more worried about their intellectual property being copied while others fear unauthorized access to their systems the most.

Classical CAN or CAN FD is used in so many different applications that it will be close to impossible to find a common security solution for all use cases. In our past CiA (CAN in Automation) security meetings it has become clear that we need to collect a list of security threats for Classical CAN/CAN FD systems and address them individually. We don't claim this list to be comprehensive but rather a starting point for further explorations:

Vandalism (denial-of-service)

Vandalism often has a random component – sometimes, the affected system is just at the wrong place at the wrong time. With physical access, an attacker may destroy connectors or cut wires of the CAN network, among other damage. With remote access they might just try to flood the CAN network with high-priority messages, causing a denial-of-service attack (DOS). Either way, the system will likely malfunction or fail.

Bypassing limitations, using unauthorized spare parts (variation of jailbreaking)

This category includes all system manipulations done by a user or owner for the purpose of functional or financial gain, such as tweaking run time or total distance counters or the odometer of a moving system or using a vehicle outside its specified parameters for "tuning" it. Practical examples discovered in the field include taximeter manipulations or manipulations of the weighing system in a truck to be able to overload it. The spare parts and service business is another use case: many manufacturers want to allow only authorized workshops to install authorized spare parts. For the system designer and the required security techniques all these examples are challenging because usually the owner or user of a machine has full physical access to the machine. They can easily add or replace components on the CAN network.

Unauthorized data collection

The data communicated via the CAN network may be sensitive and include personal data, for example diagnostic measurements in medical applications or location data from any moving vehicle application. The value of the collected data is steadily increasing the more it is collected, especially when combined with large-scale networking and cloud technologies like envisioned in Industry 4.0. There are already artificial-intelligence algorithms that rate a vehicle driver as "good" or "bad" based on collected CAN vehicle data. Other systems try to collect so much data from different sources that operators can be alerted in advance that machinery components are about to fail. All the above is information that is owned by a person or a company. A leaking of this information is not in the interest of that party or even prohibited by law and must therefore be prevented.

Stealing intellectual property

Sometimes CAN communications include the exchange of intellectual property. This can be complex configuration schemes or tables, for example when multiple large electrical drives are controlled using specific acceleration ramps. ▷

Table 1: The table shows a summary of the attack vectors for the listed categories

Attack via	physical access	remote access
Vandalism, denial-of-service	cut wires	DOS (inject high prior frames)
Bypass limitations, jailbreaking	add/swap electronics	inject targeted frames
Unauthorized data collection	add sniffer	log all CAN frames
Stealing intellectual property	add sniffer	log all CAN frames
Unauthorized remote control	add electronics	inject targeted frames
Extortion, sabotage, ransomware	add/swap electronics	inject targeted frames

Table 2: The table shows possible protection options for attack cases

Attack via	physical access	primary remote access	secondary remote access
Vandalism, denial-of-service	lock access	Stinger (ltd)	Stinger
Bypass limitations, Jailbreaking	DTLS, Auth & Encr	DTLS, Auth & Encr	Stinger/DTLS, Auth & Encr
Unauthorized data collection	lock access	CANcrypt Encr (ltd)	Stinger/CANcrypt Encr
Stealing intellectual property	lock access	DTLS, Auth & Encr	DTLS, Auth & Encr
Unauthorized remote control	lock access	DTLS, Auth & Encr (ltd)	Stinger/CANcrypt Auth
Extortion, sabotage, ransomware	lock access	DTLS, Auth & Encr (ltd)	Stinger/CANcrypt Auth & Encr

Many CAN-connected devices also allow code updates through CAN. If the protection of the updating process is minimal or non-existing, a simple sniffer device might be sufficient to generate a copy of the entire firmware image and use it to clone the device.

Unauthorized remote control

An attacker with write access to a Classical CAN/CAN FD system can inject CAN frames to actively trigger controls. Past hacks have shown that more and more vehicles have active control components like power steering and power brakes that hackers can potentially trigger remotely. In industrial environments, this would translate to manipulating actuators, robots, valves etc.

Extortion, sabotage, ransomware

Ransomware-style attacks are designed to specifically cause real damage and either use it as a threat for extortion or to perform sabotage. They could start with slight manipulations of production parameters that lower the quality of your product but otherwise can go unnoticed for a long time and end with a complete halt of your production line if parameters are screwed up completely. To exercise that level of control, simply capturing CAN traffic or inject messages typically won't be enough but you'd have to replace hardware or firmware. Past hacks have already demonstrated that if the firmware update process over CAN is understood well enough, it can be used to remotely alter the firmware of devices in a way that makes them the gateway to launch further, more far-reaching attacks.

Attack vectors and security protection options

Table 1 shows a summary of the attack vectors for the listed categories. An attacker with physical access to the CAN system can cut wires and remove, add, or replace electronic components. With any sort of remote access, e.g. by hacking into a component that has both Internet and CAN access, the attackers' intermediate goal would be to get access to be able to read all CAN frames communicated and to inject any CAN frame desired at any time.

In Table 2 we list protection options for these cases. We distinguish between secondary and primary remote access, where primary remote access is the access to a main control device that actively sends cyclic control commands. A secondary remote access goes to a device that does not perform active control algorithms. Typically, this would be a generic gateway between CAN and some other network or the Internet.

The security options referred to are:

- Stinger: Hardware protection based on the CAN ID using black- and whitelist filtering, as provided by the NXP TJA115x secure transceiver devices for example.
- CANcrypt: Software layer including secure grouping of multiple CAN devices providing encryption and/or authentication based on a symmetric key.
- DTLS: Software datagram transport layer security for end-to-end security providing encryption and/or authentication based on a public/private key pair.

"Lock access" means that no full physical access to the system shall be granted or possible. Full physical access by an attacker is the worst-case scenario as they might not even need CAN network access to obtain collected data collected intellectual property – instead, they may just lift it from embedded flash memory directly for example. In some cases, DTLS can still protect the system if the private keys can't be extracted and one of the communication end points of the DTLS connection is outside of the system. For example, code updates only happening through an encrypted and authenticated DTLS connection between the manufacturer's secure server and the target system.

If an attacker has successfully hacked into a component that does primary controls ("primary remote access" in table), then security options at the CAN communication level are limited in their effectiveness. If the device was authorized to send control messages and is equipped with appropriate keys in the beginning, then it will keep its authorization, even when hacked. All private keys stored on that device must be considered "compromised" at that point.

Conclusion

The bad news is that no matter what we do to add security to a CAN system, there will be always some cases left that cannot be protected with reasonable effort. We must work under the assumption that an attacker with unlimited physical access might be able to extract private keys stored in the devices. That would result in unlimited access to the protected CAN network, if the used security methods are based on these keys. There are several micro-controllers offering secure key storage that can't be extracted but while they are getting more common they are not yet extremely widespread. Also, if we learned anything from the past, it will only be a matter of time until new extraction methods are found.

But remotely-exercised attacks are a serious threat, too. A main control unit that is authorized to produce all CAN commands and has possession of all used keys will still be able to actively participate in any protected CAN communications. Therefore, the number one recommendation we can give you for any remote access to CAN: do not realize it via the main control unit. Any remote access should be implemented using a dedicated gateway where it is less challenging to configure it to also act as a firewall and better protect a CAN-based system.

The good news is that with a combination of Stinger, CANcrypt, and DTLS technologies you can still effectively protect your system from many attack vectors. The combination of Stinger and CANcrypt alone ensures that exploitation attempts by a determined attacker that manages to obtain CAN read and write access can do no harm. ◀

Related articles

- Olaf Pfeiffer, Christian Keydel (Emsa): Status summary of CAN security specifications
- Olaf Pfeiffer, Christian Keydel (Emsa): Smart-bridging CANopen and CANopen FD
- Olaf Pfeiffer, Christian Keydel (Emsa): CAN security: How small can we go?
- Olaf Pfeiffer, Christian Keydel (Emsa): CANopen FD multi-level security demonstrator
- Olaf Pfeiffer, Christian Keydel (Emsa): No excuses for not securing your CAN FD communication!
- Olaf Pfeiffer, Christian Keydel (Emsa): Security expectations vs. limitations

Authors

Olaf Pfeiffer, Christian Keydel
Emsa (Embedded Systems Academy)
info@esacademy.com
www.esacademy.de

Products for mobile automation

WARRANTY 5 years on ifm products

Maximum reliability for extreme conditions

If there is one thing we know after many years of experience with sensors and control systems:
Products used in mobile machines must be extremely robust. Exposed to heat, cold, moisture, dust and vibrations, they must guarantee maximum reliability – even if the going gets tough. This is why we offer corresponding solutions for operation, communication and remote maintenance. The result: increased uptime and maximum reliability of your machines. ifm – close to you!

Go ifmonline
ifm.com/gb/mobile

HIL test systems in the automotive industry

Multi-domain simulations with HIL systems are standard in aviation. But automotive OEMs (original equipment manufacturers) also benefit from real-time simulations. This requires a powerful and standardized test system.

Advanced driver assistance systems (ADAS), in modern vehicles are becoming increasingly complex and autonomous. The more authority these systems have, the more they need to be considered as highly critical safety applications. This leads to new challenges for the automotive industry, especially in terms of sensor fusion. To ensure reliable qualification, the systems need to be tested and validated according to ISO 26262. Lab tests in simulated hardware in the loop (HIL) real-time scenarios, which have been a standard procedure in aviation for quite some time now, are becoming increasingly important for the automotive industry. The growing complexity of ADAS in turn is resulting in higher technological and quality requirements for test systems.

Lab-based HIL validation with real-time scenarios

Hardware in the loop test systems enable an ex ante testing of the ADAS qualifications in the lab. Test drives on the road are not only expensive, time-consuming and hardly adaptable, but they also entail certain risks. Consequently, there are numerous advantages to have these systems validated in advance using real-time scenarios: The procedure is not time dependent; it reduces test times on the road and in turn also shortens development cycles. As a result, it is more cost-efficient and comes with a minimum risk for damages.

The lab enables a flexible creation of test cases with arbitrary changes to the scenario and a possible introduction of errors. This approach results in the elimination of gross errors and faulty functions right from the start, in order to proceed to real test drives after a successful lab validation. For as long as it is impossible to prove that HIL simulations are fully comparable to reality, the final validation will be done in a real driving situation on the road. Yet, the more these test drives lead to the same results as previously found in the lab, the higher the confidence level in connection with lab tests will be.

Multi-domain simulations

In aviation, multi-domain simulations using HIL systems have been part of the standard procedure for quite some time now. Real-time simulations on the original equipment are used for large parts of the validation and verification processes, e.g. to simulate the plane behavior in real-time to the line replacement units (LRUs).

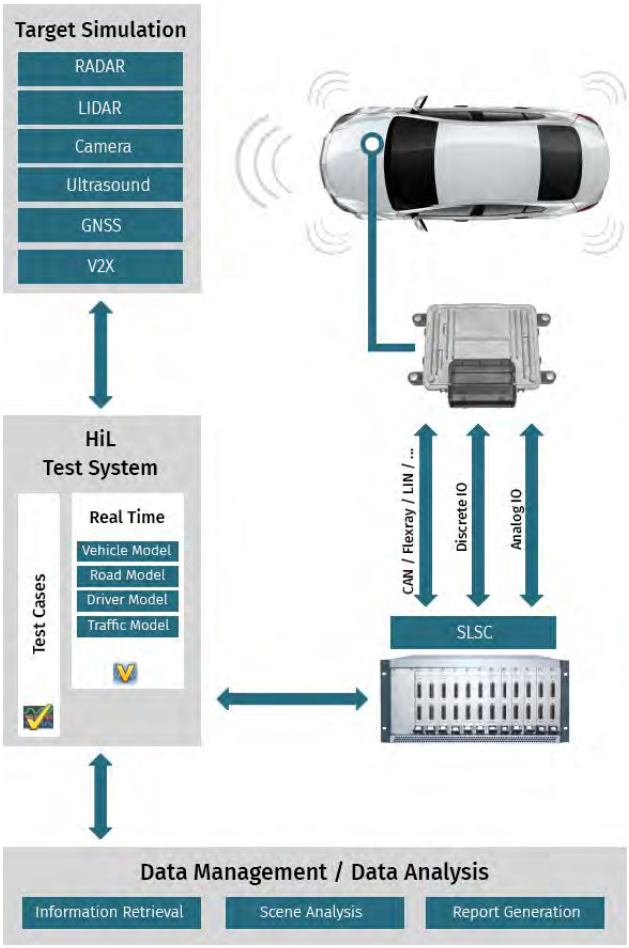


Figure 1: ADAS iiT one stop test solution (Source: SET)

Every plane natively uses sensor fusion. Every flight control system applies sensor fusion by taking the various sensor values to then validate and verify them before inferring and implementing the correct reaction.

The automotive industry also looks back on a long-standing tradition to use HIL simulations for validations. Previously, it was, however, not necessary to come up with such precise, complex, and detailed scenario models for the vehicle environment as it is now. In order to test sensor fusion systems in HIL environments, the models need to precisely convey the vehicle's surfaces and inertia, road situations as well as traffic environments and the behavior by others in traffic.

Not every manufacturer uses the same scenario model for simulations. Consequently, HIL systems need to be able to operate various scenario models by different ▷

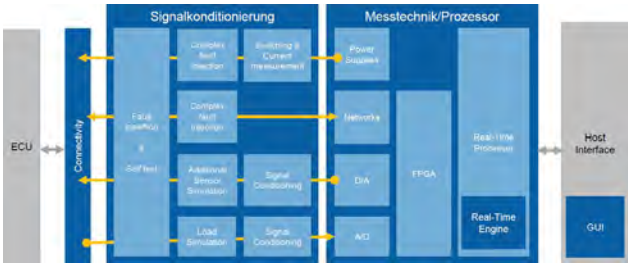


Figure 2: HIL architecture with electronic control unit (Source: SET)

manufacturers in parallel – e.g. IPG Carmaker as one scenario model together with other models like Tass Prescan. This requirement calls for flexibility, as it should be possible to flexibly convey error modes on all levels with arbitrary changes to the scenarios.

Cross-linked domains, interfaces, and gateways

The complexity of individual control devices and the interdependent cross-links of domains are increasing massively as well. To provide all relevant data to the sensor fusion unit of the vehicle, the sensors not only need more but also more detailed information on their surroundings. To test high-resolution sensors, the target simulators in the scenario models of the HIL test system consequently need to become more complex and need to provide a higher resolution.

Physical domains, interfaces, and gateways are also exponentially increasing and are subject to rapid changes. Additionally, backbone communications in testing are undergoing transformation as well: It's no longer only the Classical CAN network, but also CAN FD, Flexray, Ethernet, and BroadR-Reach or Mostbus that is used.

Depending on the application, the Classical CAN will continue to be used in vehicle development, but thanks to its higher transmission rate, CAN FD is much faster and can transport much larger data volumes – instead of eight bytes for the CAN network, this is 64 bytes. With Flexray and Ethernet solutions, speeds, and capabilities are increasing exponentially, but with a much higher degree of complexity – and thus rising costs.

The special challenge in the HIL testing of ADAS functions, especially in terms of sensor fusion functions, is to synchronously simulate these more strongly interconnected functions in a real-time environment. In other words, the algorithms of the sensor fusion unit used to evaluate the vehicle surroundings need to perceive these simulations as real and they also need to simultaneously see the same scenario in real-time everywhere.

This development has led to a rapidly increased complexity of HIL systems in all dimensions. Meeting these new challenges requires powerful, standardized, and modular test systems, which enable flexible adaptation to the needs and testing requirements at hand. One of the main advantages with open platforms is that they enable modular expansion and that they are provider independent. ▷

Figure 3: Modular system architecture using SLSC (Source: SET)

Standardized measurement technology platforms like PXI can be used to convey a multitude of signal types. A standardized signal conditioning like SLSC (switch load and signal conditioning) enables complex functions like fault insertion or sensor simulation – which means that it is no longer necessary to develop these functions on a per project basis. Thanks to these two open platforms, it is also possible to integrate necessary special functions without having to change the underlying architecture.

Closed loop test scenarios for validation

It is actually possible to simulate the entire sensor system used for the car's ADAS functions on the electronic and physical interfaces of HIL systems. Either the sensors are electronically simulated in real-time systems on the interface level or the actual sensors are physically stimulated by target simulations.

Through simultaneous emission of radar signals, simulating targets for Lidar sensors and projecting an image for the camera, for instance, multi-level and multi-domain simulations synchronously provide the sensor fusion unit with the same scenario from all interfaces. In real-time, all this information is collected from the simulated car surroundings. Vice versa, the reactions by the sensor fusion control device are synchronously returned to the simulated surroundings to adapt the simulation accordingly and to achieve closed loop scenarios. Multiple options for the testing environment enable fault insertion on a physical, protocol, and model level allowing for a reproducible showcasing of complex errors, to ensure the sample's systemic reaction in light of various fault situations.

Procedure according to ISO 26262

As ADAS are starting to act more autonomously, they increasingly need to be considered as highly critical safety applications. To provide solid proof for their reliability and safety, these systems need to be tested and validated according to ISO 26262. Depending on their importance, corresponding risks are given an ASIL rating between A and D.

ISO 26262 includes in detail requirements, which OEMs and suppliers must meet in terms of development processes and how these processes need to be documented. These requirements also cover qualification and validation depths and go all the way to include a description of safety items of systems with a critical effect on safety. In turn, this has had a huge effect on development processes in the automotive sector.

Increasing safety requirements for assistance systems go hand in hand with an increased complexity and safety evaluation during validation. With a high likelihood, this step needs to ensure that images, simulations, and simulation tools actually correspond to the expectations of the control device.

ISO 26262 also results in a growing similarity between development and testing processes for systems in the automotive branch and for aviation systems with their highly critical safety impact. Due to the high autonomy of flight systems, these safety features are tested according to the strict regulations in RTCA DO-178 and RTCA DO-254. As a matter of fact, flight control systems, capable of flying a plane on their own have actually been around for quite some time now.

So far, the automotive branch has yet to come up with control device capable of driving a car completely autonomously. There are, however, plans to introduce autonomous level 3 and level 4 systems to drive a car autonomously, which would have complete control over steering, acceleration, and braking. The logical consequence: With increased complexity, these systems would also have to significantly step up in terms of safety.

Figure 4: Scenario model IPG on a HIL system (Source: SET)

When comparing the standards, they show a vast similarity, e.g. in terms of development processes for software and hardware, for test cases, safety levels, or requirements in terms of reliability. The only differences can usually be found in the probabilities. Where a flight control system in aviation holds complete authority, its safety rating for reliable operation needs to be 10^{-12} – in automotive the corresponding value is 10^{-8}.

In aviation, there is an authority to monitor that the prescribed processes are maintained. Manufacturers of aviation electronics need a license for development and subsequently the licensing authority checks for every project if the company processes have been applied correctly or not. So far, the automotive branch lacks a corresponding body: There is no institution to assist OEMs or suppliers in terms of correct implementation of processes according to ISO 26262. Going forward, it remains to be seen if such verification will be done voluntarily by an institution purposely created or by a true authority comparable to FAA in aviation. One thing, however, can be said for sure: In light of the outlook on autonomous driving, the correct implementation of the safety regulations according to ISO 26262 will become inevitable.

Author

Frank Heidemann
SET – Smart Embedded Technologies
info@smart-e-tech.de
www.smart-e-tech.de

Displaying vehicle information with Raspberry PI

Introduction of the open source project "OBD display" for the world of Internet-of-Things (IoT) including an app.

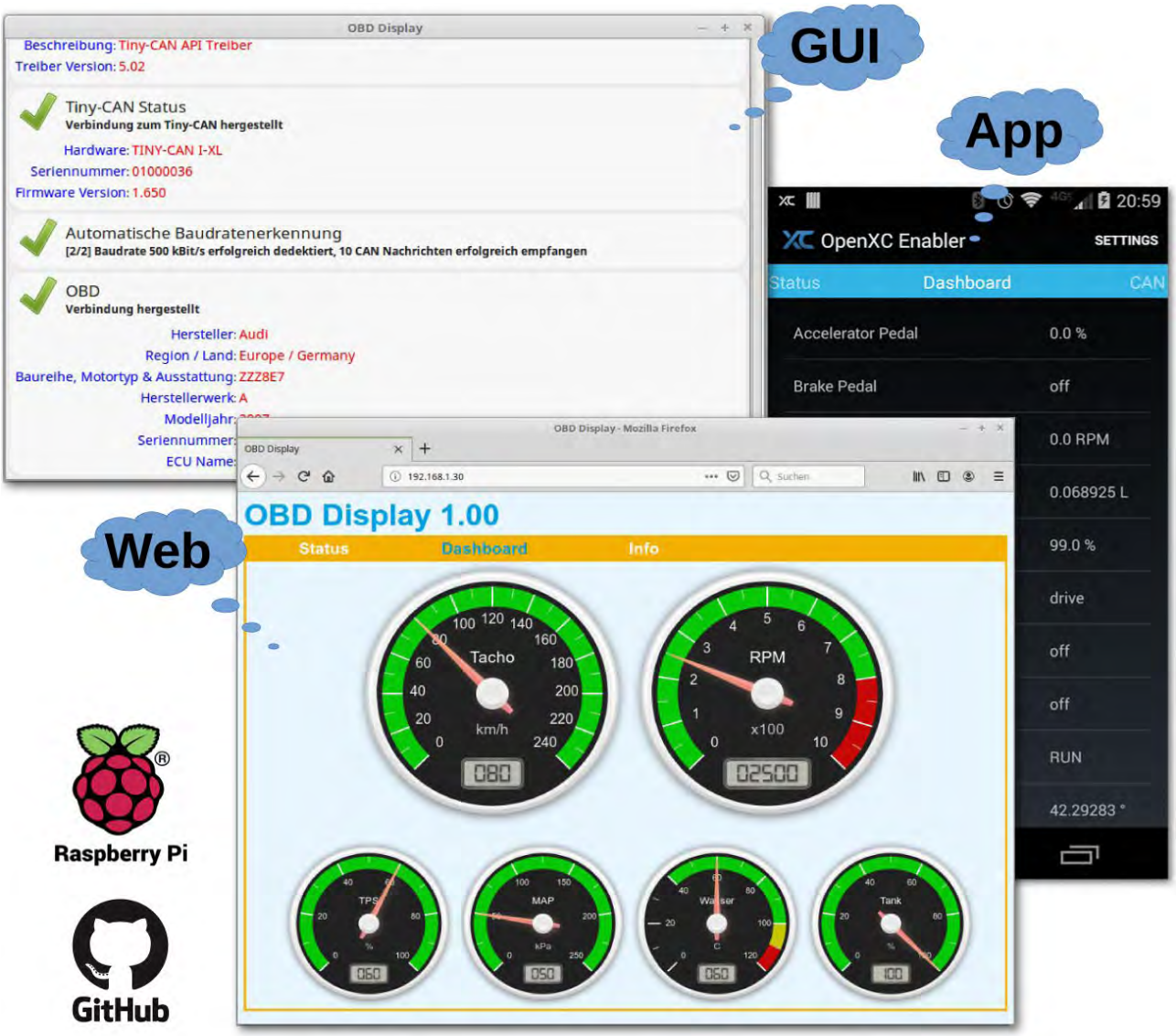


Figure 1: OBD display interfaces (Source: MHS-Elektronik)

Via the OBD-II interface, measurement data (SID 01_h), vehicle information such as chassis number/vehicle identification number (SID 09_h) and fault memory (diagnostic trouble codes, SID 03_h are queried via a CAN network. A list of all values that can be displayed is shown in the appendix. A Tiny-CAN is used as an interface adapter from the CAN network to the USB network. By using a standard USB-CAN adapter, the program can be used on any Linux PC. The software is written in C. GTK+ is used as GUI (graphical user interface). The graphic illustrates the functionality in a very simplified way.

The program flow even more detailed:

1. Load CAN API driver libmhstcan.so, query information about driver and Tiny-CAN hardware, configure and open CAN interface, forward received CAN messages and send CAN messages (can_device.c)
2. Monitor the connection and disconnection of the Tiny-CAN interface (can_dev_pnp.c)
3. Driver for the ISO-TP protocol (isotp.c), sending of single and segmented ISO-TP messages with data flow control. Receive single and segmented ISO-TP messages, including generated CAN messages for data flow control
4. Establish OBD connection, read VIN and supported PIDs, cyclically read the life data and read the error memory, errors are not deleted.

The vin_db.c module contains utility functions for breaking down the VIN in manufacturer, country, etc. The ▷

Table: List of all values that can be displayed. The prerequisite, of course, is that the vehicle also provides the data. The provided data is determined via supported PIDs

Value	Mode	PID
Supported PIDs in the range 01 - 20	01_h	00_h
Monitor status since DTCs cleared	01_h	01_h
Freeze DTC	01_h	02_h
Fuel system status	01_h	03_h
Calculated engine load	01_h	04_h
Engine coolant temperature	01_h	05_h
Short term fuel trim Bank 1	01_h	06_h
Long term fuel trim Bank 1	01_h	07_h
Short term fuel trim Bank 2	01_h	08_h
Long term fuel trim Bank 2	01_h	09_h
Fuel pressure (gauge pressure)	01_h	$0A_h$
Intake manifold absolute pressure	01_h	$0B_h$
Engine RPM	01_h	$0C_h$
Vehicle speed	01_h	$0D_h$
Timing advance	01_h	$0E_h$
Intake air temperature	01_h	$0F_h$
MAF air flow rate	01_h	10_h
Throttle position	01_h	11_h
Commanded secondary air status	01_h	12_h
Oxygen sensors present	01_h	13_h
Oxygen sensor 1	01_h	14_h
Oxygen sensor 2	01_h	15_h
Oxygen sensor 3	01_h	16_h
Oxygen sensor 4	01_h	17_h
Oxygen sensor 5	01_h	18_h
Oxygen sensor 6	01_h	19_h
Oxygen sensor 7	01_h	$1A_h$
Oxygen sensor 8	01_h	$1B_h$
OBD standards this vehicle conforms to	01_h	$1C_h$
Oxygen sensors present in 4 banks	01_h	$1D_h$
Auxiliary input status	01_h	$1E_h$
Run time since engine start	01_h	$1F_h$
Supported PIDs in the range 21 - 40	01_h	20_h
Distance traveled with malfunction indicator lamp on	01_h	21_h
Fuel rail pressure (relative to mainfold vacuum	01_h	22_h
Fuel rail gauge pressure (diesel, or gasoline direct injection)	01_h	23_h
Oxygen sensor 1	01_h	24_h
Oxygen sensor 2	01_h	25_h
Oxygen sensor 3	01_h	26_h
Oxygen sensor 4	01_h	27_h
Oxygen sensor 5	01_h	28_h
Oxygen sensor 6	01_h	29_h

Value	Mode	PID
Oxygen sensor 7	01_h	$2A_h$
Oxygen sensor 8	01_h	$2B_h$
Commanded EGR	01_h	$2C_h$
EGR error	01_h	$2D_h$
Commanded evaporative purge	01_h	$2E_h$
Fuel tank level input	01_h	$2F_h$
Warm-ups since codes cleared	01_h	30_h
Distance traveled since codes cleared	01_h	31_h
Evaporative system vapor pressure	01_h	32_h
Absolute barometric pressure	01_h	33_h
Oxygen sensor 1	01_h	34_h
Oxygen sensor 2	01_h	35_h
Oxygen sensor 3	01_h	36_h
Oxygen sensor 4	01_h	37_h
Oxygen sensor 5	01_h	38_h
Oxygen sensor 6	01_h	39_h
Oxygen sensor 7	01_h	$3A_h$
Oxygen sensor 8	01_h	$3B_h$
Catalyst temperature, bank 1, sensor 1	01_h	$3C_h$
Catalyst temperature, bank 2, sensor 1	01_h	$3D_h$
Catalyst temperature, bank 1, sensor 2	01_h	$3E_h$
Catalyst temperature, bank 2, sensor 2	01_h	$3F_h$
Supported PIDs in the range 41 - 60	01_h	40_h
Monitor status this drive cycle	01_h	41_h
Control module voltage	01_h	42_h
Absolute load value	01_h	43_h
Fuel-air commanded equivalence ratio	01_h	44_h
Relative throttle position	01_h	45_h
Ambient air temperature	01_h	46_h
Absolute throttle position B	01_h	47_h
Absolute throttle position C	01_h	48_h
Accelerator pedal position D	01_h	49_h
Accelerator pedal position E	01_h	$4A_h$
Accelerator pedal position F	01_h	$4B_h$
Commanded throttle actuator	01_h	$4C_h$
Time run with MIL on	01_h	$4D_h$
Time since trouble codes cleared	01_h	$4E_h$
Get DTCs	01_h	00_h
Supported PIDs	01_h	00_h
VIN message count	01_h	01_h
Get VIN	01_h	02_h
ECU name message count	01_h	09_h
Get ECU name	01_h	$0A_h$

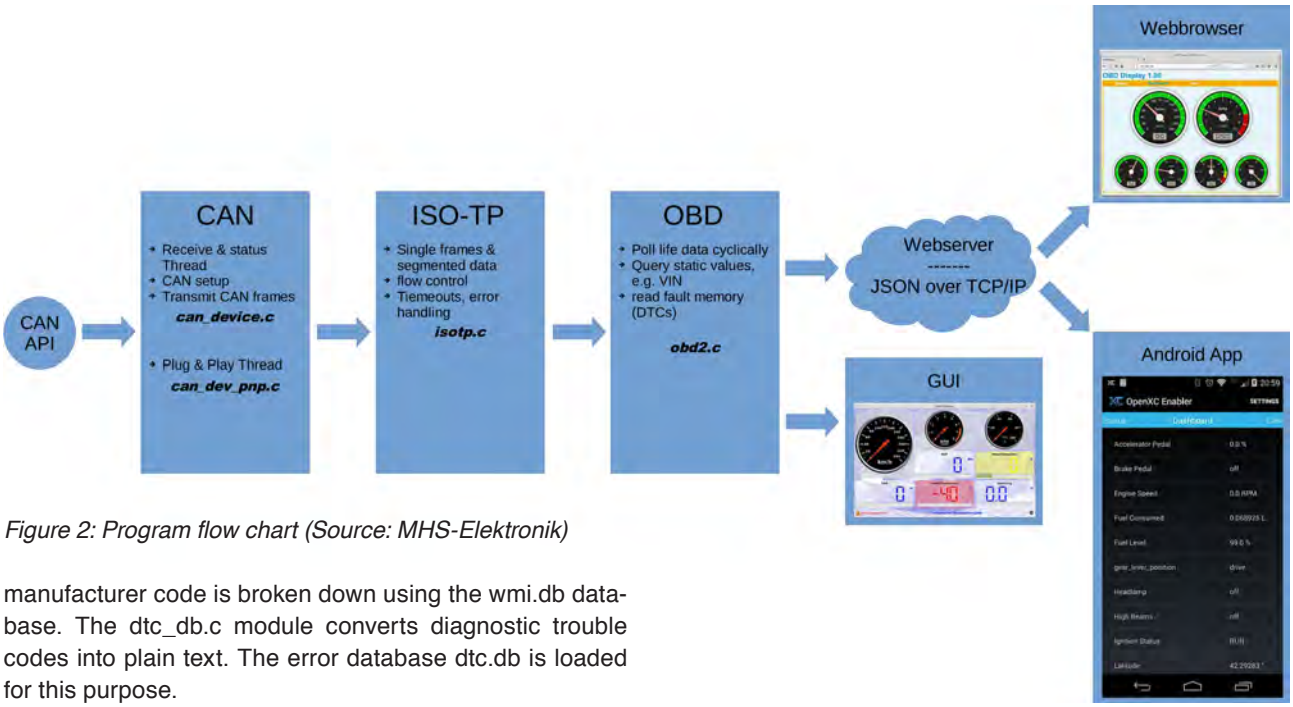


Figure 2: Program flow chart (Source: MHS-Elektronik)

manufacturer code is broken down using the wmi.db database. The dtc_db.c module converts diagnostic trouble codes into plain text. The error database dtc.db is loaded for this purpose.

Without IoT (Internet-of-Things), nothing runs today. The most important vehicle data is provided as HTML5 page via an Apache web server. A JSON over TCP/IP interface is available for apps.

The xml_database.c cyclically writes the dashboard.xml and status.xml files with the current measured values via the XMLDatabaseUpdate function. Here is an excerpt from the XML file:

```
<?xml version="1.0" encoding="utf-8"?>
<dashboard>
<Speed> 0</Speed>
<Rpm> 0</Rpm>
....
</dashboard>
```

Since the XML files are only simple static one-dimensional structures, no XML library was used to write the files. Instead g_strdup_printf and the standard file I/O functions are used.

A Java script of the HTML page cyclically triggers a GET request, which reads the corresponding XML file according to the displayed page. The two modules sock_lib.c und open_xc.c are responsible for TCP/IP communication. The sock_lib.c module creates its own thread in which new socket connections and received data are processed. The open_xc.c module also generates an auxiliary thread that triggers the cyclic transmission of the OBD data. The used JSON message format is compatible to the open source project Open XC of Ford Bug Labs, so the Android, iOS libraries and apps of Open XC can be used. As soon as an app opens the TCP/IP socket, the OBD data is also transferred cyclically. Example of a data record:

```
{"name": "vehicle_speed", "value": 45}\0
```

A data record is completed with \0. It is also possible to send several data records in one package. Example:

```
{"name": ...}\0{"name": ...}\0
```

The app can also send commands to the software. Here is an example of a command and its response:

```
{"command":"platform","unix_time":0,"bypass":
false," bus":0,"enabled":false}\0
{"command_response": "platform", "message":
"Tiny-CAN & Pi", "status": true}\0
```

The open source project is hosted on Github and is licensed under the MIT license. The GIT project homepage describes the compilation, the required hardware, and the packages to be installed. Also the license text, numerous useful tips, e.g. how to turn off the mouse pointer, and some screenshots can be found there. The sources of the libmhstcan.so (Tiny-CAN API) are included in the Tiny-CAN software package and not part of the GIT repository. ◀

Author

Klaus Demlehner
MHS-Elektronik
info@mhs-elektronik.de
www.mhs-elektronik.de

Meet and discuss latest
CAN-related solutions with CAN experts
March 17 to 18, 2019
Register at www.can-cia.org/icc

Tuesday, March 17, 2020		
09:30 - 09:45	Holger Zeltwanger (CiA)	Conference opening
Keynote session **Chairperson: Holger Zeltwanger (CiA)**		
09:45 - 11:00	Carsten Schanze (VW)	Future of CAN from the prospective of an OEM
Session I: Physical layer **Chairperson: Carsten Schanze (VW)**		
11:00 - 11:30	Magnus-Maria Hell (Infineon)	The physical layer in the CAN XL world
11:30 - 12:00	Patrick Isensee (C&S Group)	The challenge of future 10-Mbit/s in-vehicle networks
12:00 - 12:30	Johnnie Hancock (Keysight)	Characterizing the physical layer of CAN FD
12:30 - 14:00		*Lunch break*
Session II: CAN XL data link layer **Chairperson: Reiner Zitzmann (CiA)**		
14:00 - 14:30	Florian Hartwich (Robert Bosch)	Introducing CAN XL into CAN networks
14:30 - 15:00	Dr. Arthur Mutter (Robert Bosch)	CAN XL error detection capabilities
15:00 - 15:30	Dr. Christian Senger (University of Stuttgart)	CRC error detection for CAN XL
15:30 - 16:00		*Coffee break*
Session III: CANopen testing **Chairperson: Uwe Koppe (Microcontrol)**		
16:00 - 16:30	Mark Schwager (Vector)	A new approach for simulating and testing of CANopen devices
16:30 - 17:00	Oskar Kaplun (CiA)	CANopen FD conformance testing – today and tomorrow
Session IV: CANopen FD **Chairperson: Christian Schlegel**		
17:00 - 17:30	Uwe Wilhelm (Peak), Christian Keydel (Emsa)	A simplified classic CANopen-to-CANopen FD migration path using smart bridges
17:30 - 18:00	Alexander Philipp (Emotas)	A theoretical approach for node-ID negotiation in CANopen networks
18:00 - 18:30	Yao Yao (CiA)	CANopen FD devices identification via new layer setting services (LSS)

Wednesday, March 18, 2020		
Session V: CAN FD lower layers **Chairperson: Dr. Frank Deicke (Fraunhofer IPMS)**		
09:00 - 09:30	Tony Adamson (NXP)	CAN signal improvement and designing 5-Mbit/s networks
19:30 - 10:00	Fred Rennig (ST Microelectronics)	A lightweight communication bus based on CAN FD for data exchange with small monolithic actuators and sensors
10:00 - 10:30	Kent Lennartsson (Kvaser)	Improved CAN-driver
10:30 - 11:00		*Coffee break*
Session VI: Engineering **Chairperson: Kent Lennartsson (Kvaser)**		
11:00 - 11:30	Nikos Zervas (Cast)	Designing a CAN-to-TSN Ethernet gateway
11:30 - 12:00	Dr. Heikki Saha (TKE)	Automated workflow for generation of CANopen system monitoring graphical user interface (GUI)
12:00 - 12:30	Dr. Christopher Quigley (Warwick)	Benchmarking of CAN systems using the physical layer – car, truck, and, marine case studies
12:30 - 14:00		*Lunch break*
Session VII: Security **Chairperson: Torsten Gedenk (Emotas)**		
14:00 - 14:30	Thilo Schumann (CiA)	Embedded security recap
14:30 - 15:00	Prof. Dr. Axel Sikora (Hochschule Offenburg), Georg Olma (NXP), Olaf Pfeiffer (Emsa)	Achieving multi-level CAN (FD) security by complementing available technologies
15:00 - 15:30	Vivin Richards, Allimuthu Elavarasu (Infineon)	CAN XL made secure
15:30 - 16:00		*Coffee break*
Session VIII: CAN XL higher layers **Chairperson: Dr. Arthur Mutter (Robert Bosch)**		
16:00 - 16:30	Peter Decker (Vector)	IP concepts on CAN XL
16:30 - 17:00	Holger Zeltwanger (CiA)	Multi-PDU concept for heterogeneous backbone networks

For details regarding sponsorship, please contact CiA office:
Phone: +49-911-928819-22 • email: conferences@can-cia.org

Sponsors

emotas embedded communication · GEMAC · PEAK System · VECTOR

The role of telematics in self-driving transportation

It is amazing to think how far cars have come, and the technology keeps advancing. New concepts appear and the self-driving transportation technology becomes an emerging market at global level.

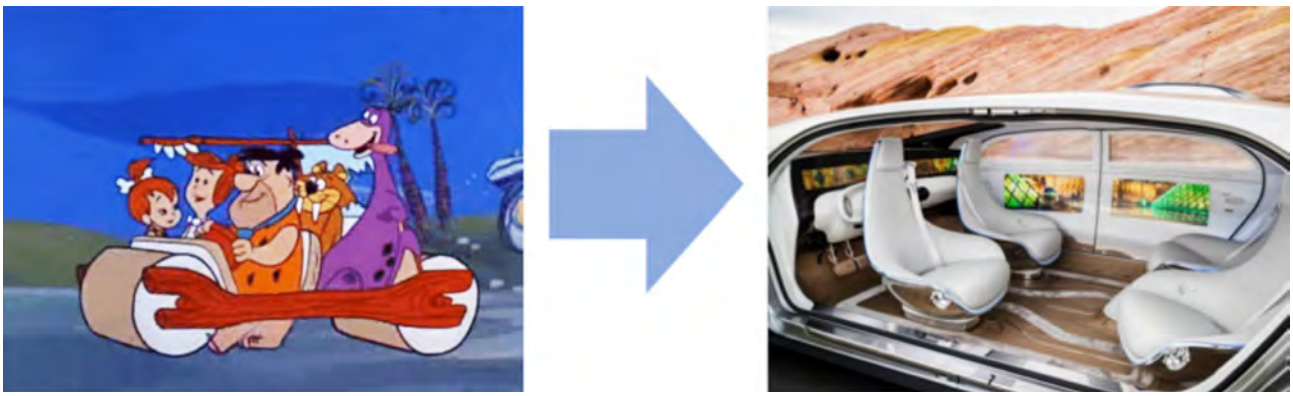


Figure 1: Then and now (Source: Daimler/Cango)

If we think at the first car ever created probably, we have the image of Fred Flintstone driving his family and pets in a stone wheel open car. Then the movies with Charlie Chaplin appeared and some vehicles were present. Moving forward to the 80ies or 90ies, keyless entry systems, electric doors and windows, sunroofs, and CD players began to gain popularity and at the beginning they were seen like something related to high-end technology. And here we are, in the nowadays transportation industry with MP3 players, hard drives, USB ports, memory card slots, advanced safety systems, GPS, navigation screens, cruise control, braking assistance, and even the ability to parallel park themselves. Seems crazy, but it is true. In this age, cars come standard with features that were once a luxury (or did not even exist at all). It is amazing to think how far cars have come, and the technology keeps advancing. New concepts appear and the self-driving transportation technology becomes an emerging market at global level. The estimations, studies, or reports are showing a growing trend and numbers seem to get higher from year to year. Car market for partially autonomous-driving will be around $36 billion by 2025.

But when it comes to automation there are six levels already defined and already known in the industry. Level 0 is considered a car which requires the full attention and action of the driver and level 5 is allocated for the fully automated vehicles. Since these levels do not mean much to people outside the industry, car makers often don't talk about their technology in these specific SAE terms.

As vehicles move towards level 3, where a driver can take his hand off the steering wheel, the dependency on telematics will increase. Vehicle speed, health, weather and road conditions, location, etc. will need to be constantly monitored to ensure safety and efficiency. Finally, for fleets to move synchronously autonomous vehicles will have to transmit their whereabouts and sync with the leading vehicle, which will happen through telematics.

It is nice to talk about autonomous-driving but there are some questions that rise:

- Will autonomous vehicles make driving safer?
- Will autonomous vehicles make a better environment for us?
- Will autonomous vehicles make our lives easier and help to increase quality?
- Are we going to trust autonomous vehicles when it comes to take an immediate decision on the road?

The answer to all this question we have is telematics which enables the mobility services and is the instrument for a better, safer, self- and autonomous environment. Because without a solid telematics knowledge the autonomous transportation will not be as we envision it.

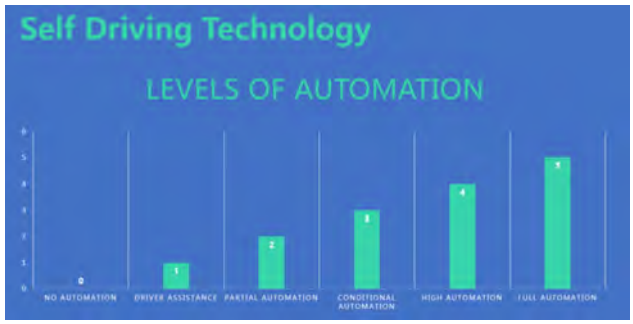


Figure 2: The estimations, studies, or reports are showing a growing trend and numbers seem to get higher from year to year; Car market for partially autonomous-driving will be around $ 36 billion by 2025 (Source: Cango)

Figure 3: PAP concept (Source: Cango)

In self-driving transportation the focus was so far around four main pillars: car sensors outside and inside the vehicle, car positioning and GPS, connected vehicles, machine learning, and artificial intelligence. With so many information and inputs there were still accidents and some of them are well-known and implied important brands in the industry. Which brings us the idea that the autonomous transportation is not complete if it is not safe and efficient.

Safety and efficiency are two points that can be solved for sure with telematics. Telematics is not only about trace and tracking. It is about diagnose the vehicle, the engine, correlate the data with what comes from the sensors, see in real-time what is happening with the engine and verify the safety features used by the passengers.

Telematics gets back to CAN which is for the vehicle like the blood system for the humans. Through the CAN network all the information, data and details, circulate and give command to the vehicle to behave in a certain way on the road.

When the safety issues will be solved and the efficiency targets will be reached then the costs with autonomous-driving will decrease. If we are moving forward with the self-driving transportation we expect that the vehicle will act at least like the known vehicles today: Speed, safety, features and functionality, entertainment, efficiency, parking management, and more are the key elements which contribute to the reduction of the costs with mobility.

Cango has 10 years experience in the CAN network area and so far developed many application for open platform hardware telematics units which are used in different projects related to mobility. Soon we will talk about city as a service, car as a service, vehicle as a market place, and each of it will be customized with different apps that the final user will be able to add on the same platform. The key is to be an open-platform hardware. Once the car manufacturers will become open, everything will be easier, for each participant of the transportation industry or at the traffic.

The easiest example is related to car sharing industry or car rental projects. Cango apps are developed so they command the vehicle from distance, immobilize the engine, lock-unlock the doors, lock-unlock the trunk, close the windows, etc.

The concept the company is launching related to self-driving transportation is called PAP (planning, anticipation, projection). Planning is always important and based on it, there can be developed concepts or algorithms related to anticipation of the actions. Moving forward, combining anticipation with machines learning, sensors, artificial intelligence we get to projections which help us build and imagine the future ecosystem for self-driving transportation and smart mobility environment. Then, based on projections the applications are build and there is just one more step until going into action.

Being prepared for the future is the key element in adopting new technologies when they will become mature. No matter how much the technology will advance, the CAN data are crucial for any project that involves autonomous-driving. CAN and telematics are the first layer for any solid base for autonomous-driving platform or vehicle. ◀

Author

Bianca Barbu
Cango
office@cango.ro
www.cango.ro

CAN in Automation

The non-profit CiA organization promotes CAN and CAN FD, develops CAN FD recommendations and CANopen specifications, and supports other CAN-based higher-layer protocols such as J1939-based approaches.

Join the community!

- Initiate and influence CiA specifications
- Get credits on CiA training and education events
- Download CiA specifications, already in work draft status
- Get credits on CiA publications
- Receive the exclusive, monthly CiA Member News (CMN) email service
- Get CANopen vendor-IDs free-of-charge
- Participate in plugfests and workshops
- Get the classic CANopen conformance test tool
- Participate in joint marketing activities
- Develop partnerships with other CiA members
- Get credits on CiA testing services

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

www.can-cia.org