The 15th iCC conference took place in Vienna (Austria). The first session introduced into some unusual vehicle applications. Oliver Hrazdera from Rosenbauer reported about the usage of CAN networks in fire-fighting trucks. Several CAN networks are implemented, which are partly interconnected by means of bridges and gateways. For future functional extension (e.g. secure communication), he requested more bandwidth. Gennady Benderman from Porsche came to the same requirement. He presented future electric/electronic (E/E) architectures for front-lights. For future high-resolution headlamps with thousands of pixels using a deeply embedded CAN network, the bandwidth of Classical CAN comes to its limits, because Porsche plans to control the LEDs pixel-wise. James Meer from Microflight reported briefly in an ad hoc presentation about CAN FD standardization in aviation. The responsible working groups in USA decided recently to support CAN FD in the Arinc 825-4 specification.

About 100 participants listened to 22 papers. No doubt, the CAN FD related presentations were of most interest. Other hot topics were security and the Internet of Things (IoT).

Many of the 22 presentations of the 15th iCC were focused on CAN FD

CAN FD related sessions

Magnus-Maria Hell from Infineon provided an update and summary on the discussion made in the last one-and-a-half year. He continued were he stopped at the last iCC. In particular, he explained the parameters introduced in the new ISO 11898-2 high-speed transceiver standard. This standard merges ISO 11898-2, -5, and -6. He explained the consequences for the partial networking respectively the selected wake-up option. Additionally, he discussed some network design options to reduce the ringing, e.g. to terminate all nodes. Another possibility to decrease the ringing in CANFD networks was presented by Denso. Yuuki Horii introduced a ringing suppression circuitry (RSC) based on the idea to change dynamically the overall impedance of the CAN FD network. This RSC is specified in CiA 601-4, which will be released soon.
Of course, you can migrate from Classical CAN to CAN FD strict forward by substituting the CAN hardware, controllers, and transceivers, in all nodes to make benefit of the higher throughput and longer frames. But some users require a more soft transition. NXP introduced in Vienna its FD Shield transceiver, which hides the CAN FD message to the Legacy CAN controller. Tony Adamson promoted the FD Shield as an interim solution for a quick integration of Legacy ECUs and CAN FD nodes in one network as well as a long-term solution for markets, in which a separation of CAN FD and Classical CAN communication is not desired due to the additional costs for the bridge/router device. A similar approach was presented by Kent Lennartsson from Kvaser: His CAN-FD Filter transceiver transforms the CAN FD message to a Classical CAN message with no data content. These two transceiver solutions seemed to be more suitable than the partial networking approach. This is to “switch-off” the Legacy CAN nodes during the CAN FD communication and to wake-up them again. The automotive industry is not in favor of such migration options. The carmakers prefer to migrate completely to CAN FD, in network segments, where higher bandwidth is required and to link those segments by bridge/router devices to segment running Classical CAN communication.

Even if you would like to substitute the entire CAN hardware by CAN FD capable semiconductors, you may need a migration path, because not all micro-controllers support currently CAN FD. Therefore, Wilhelm Leichtfried from Microchip presented a stand-alone CAN FD controller. He said that such external chips can help to minimize development timelines and can be more cost-effective than using high-end MCUs with CAN FD support.

The developers of software for CAN FD have already started to migrate to CAN FD – in particular, to frames with up to 64-byte payload. Dr. Oliver Hartkopp from Volkswagen presented a comprehensive survey about the integration, configuration, and usability of CAN FD in the Linux operating system. He gave an insight how programming interfaces have been altered in Linux in an evolutionary way without putting the existing application programming concept into question. Some of the presented ideas may be reused in other embedded set-ups – some may be too Linux specific to do so. He also presented the open source implementation of the ISO Transport Protocol as standardized in ISO 15765-2 supporting CAN FD frames. Peter Decker from Vector introduced the dynamic Multi-PDU-to-frame mapping. This approach requires in some cases more bandwidth than an optimized mapping. In the other hand, it is easier to test complex systems and more important it allows very flexible system designs and is supported by Autosar. Holger Zeltwanger presented the CiA 602 application layer, which maps the current SAE J1939 application layer to CAN FD frames. The proposed mapping complies with the Multi-PDU-to-frame mapping introduced by Vector. The CiA 602 proposal is already approved by simulation and requires without optimization just a third of the bandwidth when using Classical CAN.
System design is the most challenging topic in CAN FD. Dr. Marc Schreiner from Daimler provided some general rules and recommendations for the physical network design. He discussed the influencing parameters and critical values of typical components. The main part of his presentation was focused on topologies and the possible bit-rates. He reported about his measurement in different CAN FD topology structures. In his work, the CAN FD signal asymmetries have been analyzed based on the RX as well as on a virtual RX signal based on the differential bus signal. Although the number of assessed variations was huge (approximately 750 in total) of course they cannot cover all kinds of CAN FD topologies that might occur in the field. Nevertheless the presented measurement results gave a good basic overview about the typical behavior of particular topologies and they might be a good help for a CAN FD system designer to configure networks in an appropriate manner. It should be noted that the presented results were valid only at room temperature. Significant changes over temperature have to be expected if PVC cable is used. He stated that the other main impact comes from the transceivers, which can be accounted for by applying the worst-case ISO values. If the CAN FD system design is targeting at 2 Mbit/s and higher in the data phase, he expected that the best results will be achieved with the point-to-point and with the line topology. Especially for conservative system designers, who do not want to tolerate the uncertainty of ringing in the network, the pure line topology is the only safe choice according to the Daimler researcher. Of course, short stubs can be used – but as short as possible, Dr. Schreiner said. According to him, ferrite star topology may work as well, when the branch length is short. The presented graphs are a good source of orientation.

The University of Brighton presented the simulation results using the SAE benchmark message set. The performance analysis was realized for worst-case message delays, average message delays, and bus utilizations. The worst-case message delay analysis has shown that with the CAN FD model based on the SAE benchmark message set, from 1,78 to 3,28 times smaller worst-case message delays on average can be achieved compared to the Classical CAN model. Similarly, from 1,67 to 4,16 times smaller mean message delays on average has been observed with CAN FD. In bus utilization results, almost half the bus utilization values have been observed with CAN FD. The simulation results have revealed that the CAN FD protocol provides considerable performance improvements in message transmission speed and bus utilization compared to Classical CAN.

In order to improve the throughput, Gianluca Cena from the CNR-IEIIT institute presented a method to prevent bit stuffing. The proposal is suitable for CAN FD as well as Classical CAN communication. The zero stuff-bit (ZS) mechanism uses a codec, which can be implemented in software or in hardware. One of the benefits is that there is no time jitter of the messages depending on the content. Each message type has always the same length.

Dr. Arthur Mutter from Bosch explained in detail the performance of the improved error detection mechanisms in the CAN FD protocol. The four main improvements in CAN FD regarding error detection mechanisms are: use of CRC polynomials of higher order, inclusion of dynamic stuff bits into CRC calculation, inclusion of the number of dynamic stuff bits into the frame, and the use of fixed stuff bits in the CRC field of the frame. The results are mainly in the interest of attorneys. They are a proof that CAN FD is more reliable than Classical CAN.

Security and IoT

The two other important topics on the iCC were the Internet of Things (IoT) and secure communication. Amir Spi-vak from Beyond Security opened the discussion with a proposal to test third-party products and applications for unknown vulnerabilities. He used a black box test environment. This means he does not need the source code of the ECU under test. In his research he found out that proprietary protocols are the weakest approach-es to withstand attacks: “The writers of these protocols believe that no one can attack the protocol since its format is unknown. They are very wrong: it’s possible to
Sum from Kvaser presented a wireless replacement for less communication links two CAN segments. Derek "strangers" sent secret data, but should not accept commands from strangers instead of encryption, because the nodes do not work. The proposed solution is based on authentication of a secure communication approach in CANopen networks. Thilo Schumann from CiA presented the first results. "This approach captivates by its simplicity, low complexity and high cost-efficiency, and may be readily implemented without any modifications of off-the-shelf CAN controllers," he stated (see also the detailed article on page 10). Thilo Schumann from CiA presented the first results of a secure communication approach in CANopen networks. The proposed solution is based on authentication instead of encryption, because the nodes do not send secret data, but should not accept commands from "strangers".

Secure communication is needed, when a wireless communication links two CAN segments. Derek Sum from Kvaser presented a wireless replacement for

Dr. Andreas Müller from Bosch presented for the first time an approach for establishing and refreshing symmetric cryptographic keys between different nodes in a CAN network in a plug-and-play manner. “Our approach captivates by its simplicity, low complexity and high cost-efficiency, and may be readily implemented without any modifications of off-the-shelf CAN controllers,” he stated (see also the detailed article on page 10). Thilo Schumann from CiA presented the first results of a secure communication approach in CANopen networks. The proposed solution is based on authentication instead of encryption, because the nodes do not send secret data, but should not accept commands from "strangers".

Secure communication is needed, when a wireless communication links two CAN segments. Derek Sum from Kvaser presented a wireless replacement for

15th ICC Focus on CAN FD
About 100 attendees listened in Vienna to 22 presentations and one ad hoc paper. Many talks were related to CAN FD technology.

CAN FD products
Microchip goes automotive
Microchip has pre-announced its CAN FD stand-alone controller and transceiver. Its daughter company, K2L has launched interface devices supporting CAN FD to be used with the company’s software tools.

Transceiver
Filters CAN FD messages
NXP has presented an idea on how to run Classic CAN controllers in a CAN FD network. It is based on a transceiver able to filter CAN FD messages and also the Error frames caused by the Classic CAN chip.

CAN FD
Recommended practice
CiA has released part 1 of the CiA 601-1 CAN FD node and system design recommended practice. The series fills the gap between the ISO standards for CAN FD and the system design specifications.

IP solution
Non-ISO CAN FD solution for automobiles
Arasan’s Total IP Solution implements the Classical CAN protocol, as well as the non-ISO CAN FD protocol compliant to Bosch. The company plans the development of CAN FD transceivers, too.

attack (as demonstrated by the black box test approach) and when attacked, weaknesses are immediately exposed.”

Dr. Andreas Müller from Bosch presented for the first time an approach for establishing and refreshing symmetric cryptographic keys between different nodes in a CAN network in a plug-and-play manner. “Our approach captivates by its simplicity, low complexity and high cost-efficiency, and may be readily implemented without any modifications of off-the-shelf CAN controllers," he stated (see also the detailed article on page 10). Thilo Schumann from CiA presented the first results of a secure communication approach in CANopen networks. The proposed solution is based on authentication instead of encryption, because the nodes do not send secret data, but should not accept commands from "strangers".

Secure communication is needed, when a wireless communication links two CAN segments. Derek Sum from Kvaser presented a wireless replacement for

15th ICC Focus on CAN FD
About 100 attendees listened in Vienna to 22 presentations and one ad hoc paper. Many talks were related to CAN FD technology.

CAN FD products
Microchip goes automotive
Microchip has pre-announced its CAN FD stand-alone controller and transceiver. Its daughter company, K2L has launched interface devices supporting CAN FD to be used with the company’s software tools.

Transceiver
Filters CAN FD messages
NXP has presented an idea on how to run Classic CAN controllers in a CAN FD network. It is based on a transceiver able to filter CAN FD messages and also the Error frames caused by the Classic CAN chip.

CAN FD
Recommended practice
CiA has released part 1 of the CiA 601-1 CAN FD node and system design recommended practice. The series fills the gap between the ISO standards for CAN FD and the system design specifications.

IP solution
Non-ISO CAN FD solution for automobiles
Arasan’s Total IP Solution implements the Classical CAN protocol, as well as the non-ISO CAN FD protocol compliant to Bosch. The company plans the development of CAN FD transceivers, too.

attack (as demonstrated by the black box test approach) and when attacked, weaknesses are immediately exposed.”

Dr. Andreas Müller from Bosch presented for the first time an approach for establishing and refreshing symmetric cryptographic keys between different nodes in a CAN network in a plug-and-play manner. “Our approach captivates by its simplicity, low complexity and high cost-efficiency, and may be readily implemented without any modifications of off-the-shelf CAN controllers," he stated (see also the detailed article on page 10). Thilo Schumann from CiA presented the first results of a secure communication approach in CANopen networks. The proposed solution is based on authentication instead of encryption, because the nodes do not send secret data, but should not accept commands from "strangers".

Secure communication is needed, when a wireless communication links two CAN segments. Derek Sum from Kvaser presented a wireless replacement for

15th ICC Focus on CAN FD
About 100 attendees listened in Vienna to 22 presentations and one ad hoc paper. Many talks were related to CAN FD technology.

CAN FD products
Microchip goes automotive
Microchip has pre-announced its CAN FD stand-alone controller and transceiver. Its daughter company, K2L has launched interface devices supporting CAN FD to be used with the company’s software tools.

Transceiver
Filters CAN FD messages
NXP has presented an idea on how to run Classic CAN controllers in a CAN FD network. It is based on a transceiver able to filter CAN FD messages and also the Error frames caused by the Classic CAN chip.

CAN FD
Recommended practice
CiA has released part 1 of the CiA 601-1 CAN FD node and system design recommended practice. The series fills the gap between the ISO standards for CAN FD and the system design specifications.

IP solution
Non-ISO CAN FD solution for automobiles
Arasan’s Total IP Solution implements the Classical CAN protocol, as well as the non-ISO CAN FD protocol compliant to Bosch. The company plans the development of CAN FD transceivers, too.

attack (as demonstrated by the black box test approach) and when attacked, weaknesses are immediately exposed.”

Dr. Andreas Müller from Bosch presented for the first time an approach for establishing and refreshing symmetric cryptographic keys between different nodes in a CAN network in a plug-and-play manner. “Our approach captivates by its simplicity, low complexity and high cost-efficiency, and may be readily implemented without any modifications of off-the-shelf CAN controllers," he stated (see also the detailed article on page 10). Thilo Schumann from CiA presented the first results of a secure communication approach in CANopen networks. The proposed solution is based on authentication instead of encryption, because the nodes do not send secret data, but should not accept commands from "strangers".

Secure communication is needed, when a wireless communication links two CAN segments. Derek Sum from Kvaser presented a wireless replacement for

15th ICC Focus on CAN FD
About 100 attendees listened in Vienna to 22 presentations and one ad hoc paper. Many talks were related to CAN FD technology.

CAN FD products
Microchip goes automotive
Microchip has pre-announced its CAN FD stand-alone controller and transceiver. Its daughter company, K2L has launched interface devices supporting CAN FD to be used with the company’s software tools.

Transceiver
Filters CAN FD messages
NXP has presented an idea on how to run Classic CAN controllers in a CAN FD network. It is based on a transceiver able to filter CAN FD messages and also the Error frames caused by the Classic CAN chip.

CAN FD
Recommended practice
CiA has released part 1 of the CiA 601-1 CAN FD node and system design recommended practice. The series fills the gap between the ISO standards for CAN FD and the system design specifications.

IP solution
Non-ISO CAN FD solution for automobiles
Arasan’s Total IP Solution implements the Classical CAN protocol, as well as the non-ISO CAN FD protocol compliant to Bosch. The company plans the development of CAN FD transceivers, too.

attack (as demonstrated by the black box test approach) and when attacked, weaknesses are immediately exposed.”

Dr. Andreas Müller from Bosch presented for the first time an approach for establishing and refreshing symmetric cryptographic keys between different nodes in a CAN network in a plug-and-play manner. “Our approach captivates by its simplicity, low complexity and high cost-efficiency, and may be readily implemented without any modifications of off-the-shelf CAN controllers," he stated (see also the detailed article on page 10). Thilo Schumann from CiA presented the first results of a secure communication approach in CANopen networks. The proposed solution is based on authentication instead of encryption, because the nodes do not send secret data, but should not accept commands from "strangers".

Secure communication is needed, when a wireless communication links two CAN segments. Derek Sum from Kvaser presented a wireless replacement for
cables in CAN network systems. The idea is not new. He discussed the general requirements on security and timing behavior, especially the real-time behavior, as well as the data consistency.

Secure communication is also required when cloud-based maintenance and services should be used. Dr. Heikki Saha from TK Engineering shared his thoughts on the example of CANopen-based control systems. He reported about first CANopen pilot projects proving the proposed system integration framework for management process, device, tool, and service ecosystem into a web-based cloud environment. Further development in the near future will concentrate on the improvement of information logistics from design into assembly line and field service. Configuration packets are already automatically generated from corresponding CANopen design projects, but measurement setup creation from the projects shall be implemented. One of the missing links for diagnostics is the mapping of CANopen services to the ODX standard used by the automotive industry. This would be helpful in particular for the mobile machine industry and other off-highway vehicle fleets.

Erik Halvordsson from HMS Industrial Networks talked about the Industrial Internet of Things (IIoT). He gave examples (e.g. straddle carriers getting remotely orders via the web) on today’s integration of CAN-controlled systems into the IT world. Another example was predictive machine analysis using CANopen data streamed to SAP’s web-based database.

All papers are documented in the 15th ICC proceedings, which can be purchased from CiA office in Germany. The presentation slides are available for participants and buyers of the proceedings as PDF files.

The tabletop exhibition

As usual, the 15th ICC was accompanied by a tabletop exhibition. Besides already launched products, the participating companies presented also some new semiconductors, devices, and tools. Of course, everyone was looking for CAN FD controllers. Microchip presented its stand-alone CAN FD controller and its MCP2561(FD) transceiver family. The products will be available via distribution in the next year. Microchip plans also a single-chip comprising CAN FD controller plus transceiver. Renesas showed first samples of its RH850/F1K micro-controller featuring six CAN FD modules and an additional Classical CAN module. These chips suitable for gateway solutions will be available also in 2016. Cypress presented in Vienna its Traveo MCU family with CAN FD on chip. All these products support the ISO CAN FD protocol. The Fraunhofer IPMS exhibited its CAN FD core, which complies also with ISO 11898-1:2015. This core supports the non-ISO CAN FD protocol, too. Vector and K2L presented their tools supporting Classical CAN and CAN FD.
Hardware for CAN FD Applications & Development

PCAN-Router FD
Programmable Converter for CAN FD and CAN

The new PCAN-Router FD has two CAN channels that support the CAN FD standard in addition to the conventional CAN 2.0 specification. The module behavior and the data exchange between the two channels are freely programmable. Thus, for example, a conversion of CAN to CAN FD and vice versa is possible and new CAN FD applications can be integrated into existing CAN 2.0 networks.

- ARM Cortex M4F microcontroller
- 4 kByte On-chip EEPROM and 4 MByte SPI flash
- Two High-speed CAN channels (ISO 11898-2)
  - Comply with CAN specifications 2.0 A/B and FD
  - CAN FD support for ISO and Non-ISO standard
  - CAN FD bit rates for the data field up to 12 Mbit/s
  - CAN bit rates from 25 kbit/s up to 1 Mbit/s
- 1 I/O-connection: digital input and output
- RS232 serial data transfer, alternatively 2 digital inputs
- Available in aluminum casing with two 9-pin D-Sub connectors or one 10-pole screw-terminal strip (Phoenix)
- Extended operating temperature range from -40 to 85 °C
- Galvanic isolation up to 500 V
- Scope of supply includes:
  - PCAN-View: Software for monitoring CAN and CAN FD busses for Windows (32/64 bit)
  - PCAN-Basic: API for developing applications with CAN and CAN FD connection for Windows (32/64 bit)

PCAN-USB FD
CAN FD Interface for High-Speed USB 2.0

- Adapter for High-speed USB 2.0
- Time stamp resolution 1 µs
- CAN bus connection via D-Sub, 9-pin (in accordance with CiA® 102)
- Complies with CAN specifications 2.0 A/B and FD
- CAN FD support for ISO and Non-ISO standard switchable
- CAN FD bit rates for the data field up to 12 Mbit/s
- CAN bit rates from 25 kbit/s up to 1 Mbit/s
- Measurement of bus load including error frames and overload frames on the physical bus
- Induced error generation for incoming and outgoing CAN messages
- CAN termination and 5-Volt supply at the CAN connection can be activated through solder jumpers
- Galvanic isolation up to 500 V
- Extended operating temperature range from -40 to 85 °C
- Scope of supply includes:
  - CAN FD interface drivers for Windows 10, 8.1, 7, Vista and Linux (32/64 bit)
  - PCAN-View: Software for monitoring CAN and CAN FD busses for Windows (32/64 bit)
  - PCAN-Basic: API for developing applications with CAN and CAN FD connection for Windows (32/64 bit)
Powerful Control Units for High-Safety Applications: HY-TTC 500 Family

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

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

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

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

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

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