Autosar SecOC for CAN FD

With the migration to CAN FD, new security concepts have become possible: It enables the Autosar concept Secure Onboard Communication, which detects attacks on the network.

For more than 20 years, CAN has been and still is the dominating communication system in vehicles. With the rising complexity of in-vehicle functions, Classical CAN cannot satisfy the increasing demand for an effective data rate any longer. Therefore, CAN FD was introduced – it allows for a payload up to 64 byte to achieve data rates of 2 Mbit/s and 5 Mbit/s. To exploit this major advantage for advanced functions, challenges of larger network topologies have to be addressed. In particular, the so-called ringing effect has a tremendous impact on the communication reliability. One of the major benefits of CAN FD is that it enables security for single protocol data units using the Autosar concept Secure Onboard Communication (SecOC).

Ringing

In CAN FD networks with more than two nodes, reflections of communication voltage waves, which occur because of impedance mismatches in a network at the signal transition frequencies, generate ringing. The impedance mismatches occur mainly at non-terminated nodes and the junction. When a transmitter outputs a recessive state, the output of the transmitter has a high resistance. Therefore, signal ringing occurs in particular during the transition from recessive-to-dominant. In addition, a negative reflection occurs at the junction because the impedance decreases. This results in a lower impedance than the characteristic impedance. If ringing does not converge below a predetermined voltage until the defined sampling point, a bit malfunction occurs.

To avoid this, we developed the so-called RSC – ringing suppression circuitry. This circuitry detects the change from dominant to recessive state and changes the impedance to 120 Ohm. An internal MOS component detects this falling edge and activates the ringing suppression. This suppression circuit can be seen as a circuit comprised by resistors and switches, which take the energy out of the network. RSC was designed to be compatible to all ISO 11898-2-compliant transceivers. Therefore, it can be used in CAN FD networks and allows engineers to develop software using all technical advantages of CAN FD. RSC is already specified in CiA as CiA 601-4, with ongoing continuous improvement of 601-4 as well as standardization activities on ISO-level (11898-2).

CAN FD to completely enable SecOC

The Autosar concept Secure Onboard Communication (SecOC) was specified to check the authenticity of a single transmitted protocol data unit, in order to detect attacks such as replay, spoofing and tampering. As the recently published hacks have shown, gaining access to the CAN network is typically the only barrier to taking remote control of a vehicle. Once on the bus, the attacker can imitate a legitimate sender and gain control of the behavior of the entire vehicle. With SecOC, the attacker also has to know the sender's secret key. Assuming proper system design, this is only possible by physical access to the vehicle and destruction of the respective control unit. Therefore, such attacks can be prevented.

The SecOC module calculates and adds a message authentication code (MAC) to the protocol data unit. For replay protection, a freshness value has to be included in the cryptographic calculation. The PDU is transmitted together with the MAC and freshness value in one frame. With Classical CAN, only a part of the freshness value for synchronization and only a part of the MAC can be added due to the limited frame size of 8 byte. The receiver then calculates the MAC of the PDU and the freshness value and compares it with the one it (partially) received. If there is no match, the PDU is dropped and ignored.

However, some issues with the application of SecOC to serial products remain. Challenging topics, not dealt with by the standard, are the key management, freshness value handling, and recovery strategy. The recovery strategy for instance is how to deal with failed authentications, how to ensure the functionality or at least the safety of the system in such a case, and how to recover the system operation when participants are out of synchronization. Another critical factor is the Classical CAN frame, which provides only 8 byte of payload. While NIST recommends truncation of the MAC below 64 bits only in conjunction with a careful analysis, a Classical CAN message would be entirely occupied by the MAC and leave ▷

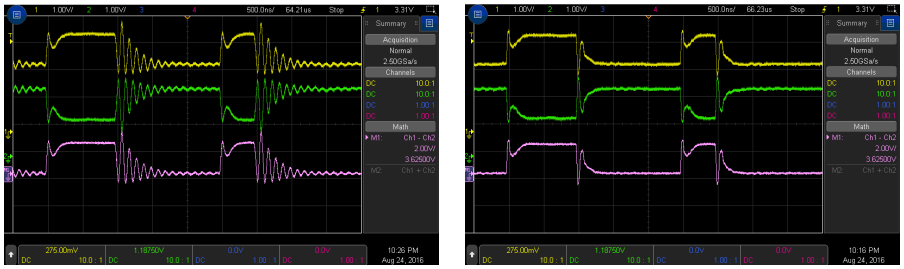


Figure 1: Left: Conventional CAN FD transceiver; right: Denso RSC transceiver (Photos: Denso Automotive Deutschland)

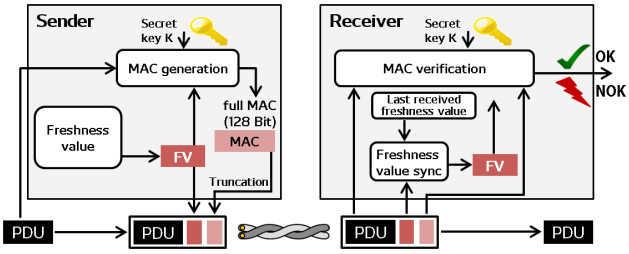


Figure 2: Process of secure onboard communication in Autosar (Photo: Denso Automotive Deutschland)

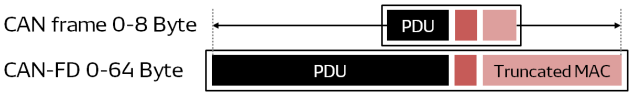


Figure 3: CAN FD has the potential to increase both security and efficiency (Photo: Denso Automotive Deutschland)

no space for the actual payload. To retain a decent communication efficiency, the MAC must be truncated to a shorter length, which also reduces the level of security the MAC can provide. The MAC could also be sent in another frame, which improves the security but has quite an impact on the busload and communication effort. By switching to CAN FD, the payload of up to 64 byte allows the transmission of a reasonable amount of data in conjunction with a "secure" MAC length. Ultimately, the limitations of Classical CAN hinder the wider and more effective introduction of essential security technology. Therefore, CAN-based mission-critical communication should follow the evolution to CAN FD in order to accelerate the inevitable introduction of new features. RSC enables the design of large CAN FD networks to make full use of CAN FD's advantages.

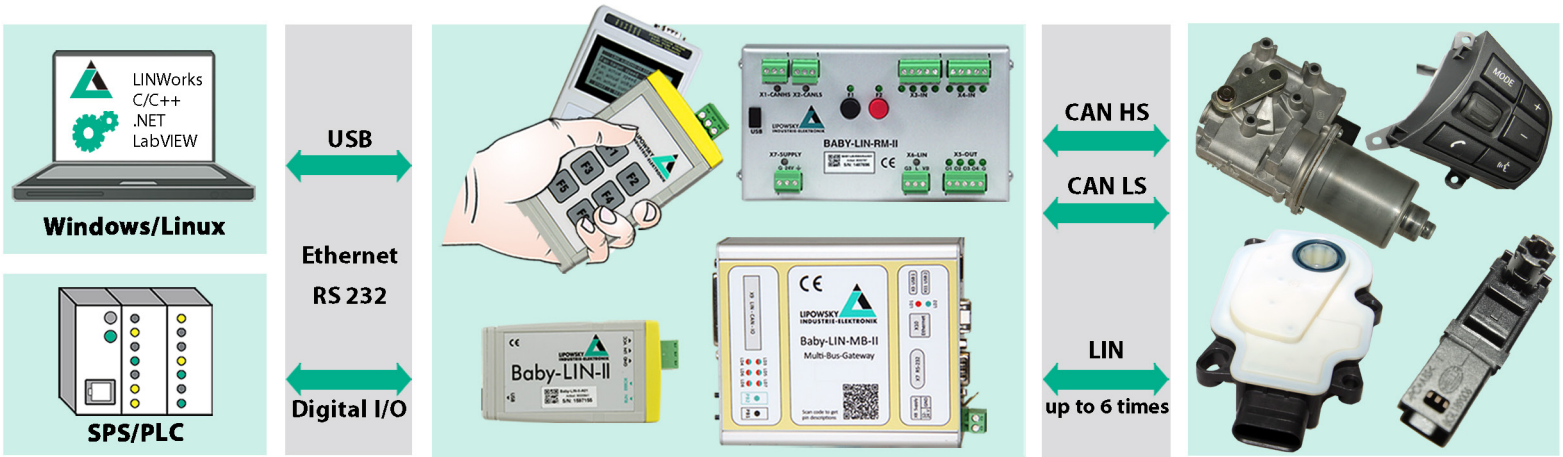
Summary

Autosar Secure Onboard Communication is limited in Classical CAN networks due to its payload of only 8 byte. With CAN FD, SecOC can be used without limitation such as MAC truncation and omission of freshness synchronization. However, CAN FD cannot be deployed as easily as Classical CAN. For larger networks, either the topology has to be reduced in complexity or other technologies have to be applied to attenuate ringing effects. The use of RSC simplifies the upgrade to CAN FD for any existing (Classical CAN) topology and also allows for more freedom in the topology design.

Authors

Dr. Tobias Islinger, Yasuhiro Mori, Jennifer Neumüller,
Martin Prisching, Dr. Robert Schmidt
Denso Automotive Deutschland GmbH
t.islinger@denso-auto.de
www.denso-auto.de

LIN&CAN Tools for test and production



Configure - Connect - Operate
We support you all the way!
+ 49 6151 93591-0

SINCE 1986
ISO 9001 : 2008

www.lipowsky.com info@lipowsky.de

LIPOWSKY INDUSTRIE-ELEKTRONIK

Distribution China: Hongke Technology Co., Ltd Ph: +86 400 999 3848 sales@hkaco.com www.hkaco.com
Distribution USA: FEV North America Inc. Ph: +1 248 293 1300 marketing_fev@fev.com www.fev.com