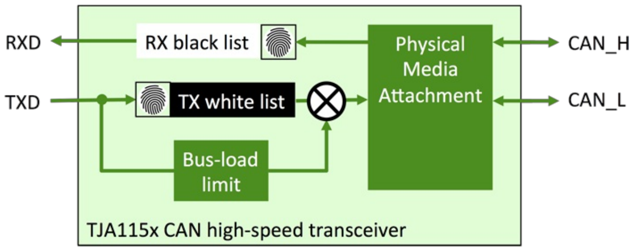
CAN Newsletter Online

CAN TRANSCEIVER

Securing CAN without cryptography

NXP has launched the TJA115x series of CAN high-speed transceivers. They provide some data link layer security controls.



The TJA115x series implements several security controls (Photo: CAN Newsletter)

The CAN data link layer security controls have a name: TJA115x series. Already introduced a couple of years ago, NXP is going to ship so-called “smart” CAN transceivers featuring protection against spoofing, tampering, and flooding attacks. The components are available as drop-in replacement for high-speed CAN transceivers in SO8 and HVSON14 packages. If no cyber security incident has been detected, the TJA115x transceivers behave like TJA104x transceivers (difference is e.g. that the TJA115x features “auto biasing”). In case a cyber security incident is detected the frame gets invalidated on the bus in the end-of-frame field by an active error flag. This happens before it is stored in any receive buffer. For an incident caused by the local host, the transceiver disconnects the local host temporarily from the CAN network.

The simple exchange of the high-speed transceiver is possible without the need to modify the software in the host controller. Additional effort during production needs to be considered to configure basic parameters like: CAN identifiers or filter settings. The configuration can either be kept open for further secure updates in the field, alternatively it can be locked out. The TJA115x has abilities to facilitate logging and reporting security incidents on the network and to the local host.

The secure CAN transceiver can be used in Classical CAN as well as in CAN FD networks. It protects its own configuration update. The concept proposed by NXP is implemented entirely in hardware. It operates independently and in isolation from the host-controller. This means it provides an inherent level of security and is specifically designed for minimum system impact to overcome the lack of sender identification in the CAN protocol. It can be introduced into a network in a stepwise approach (ECU by ECU), without impacting other devices, or impacting the message latency, the busload or increasing the processor load.

The implemented spoofing protection mechanism makes sure that whenever the target ECU receives a protected frame, the expected sender has transmitted it. Also, the network is protected immediately after turning on the ignition – as the implemented security mechanisms do not require any initialization (of individual ECUs) or synchronization (of multiple ECUs on a bus). Denial-of-Service incidents are counter-measured by means of limiting the bus access to a configured permitted bandwidth. Such bandwidth limitations are also known as “inhibit” times, for example in CANopen (PDO and EMC).

hz