Secures CAN without cryptography

NXP has announced a CAN transceiver family which provides several cyber security features. It complements crypto-based security solutions with an additional layer in a Defense-in-Depth (DiD) concept, or as a stand-alone option.

(Photo: NXP)

Already introduced unofficially at the 16th international CAN Conference, NXP announced the development of its secure CAN transceiver. It is a milestone in protecting CAN networks against cyber attacks. Security solutions on the market today protect CAN communication with message authentication code (MAC) based on cryptography and complex key management, but they require increased busload, message latency, or computing power consumption. Additionally, it is not always possible to upgrade devices to support secure CAN messages, when the processors do not have sufficient computing power. With secure CAN transceivers, however, you can secure messages from devices already installed in systems by means of exchanging the transceiver. “NXP´s secure CAN transceivers signal a disruptive approach compared with the status quo,” said Jens Hinrichsen from NXP. “This translates to more efficiency and a reduction in the vital system resources needed for increasingly complex cars.”

The transceiver prevents spoofing on the transmit side. It filters CAN messages based on allowed CAN-IDs. If a compromised device tries to send a message with an ID that is originally not assigned to it, the secure CAN transceiver can refuse to transmit it to the network. There is also a spoofing prevention on the receive side: A complementary protection is used to invalidate messages on the network with a CAN-ID assigned for transmission. This method means each device has the ability to protect its own IDs in the eventuality that a rogue device manages to send a message with the same ID. The transceiver also prevents communication tampering: The transceiver invalidates CAN messages by means of CAN error frames. Another feature is the flooding prevention and rate limit control. Limiting the number of transmitted messages per ECU from the sender side at any time, helps prevent flooding the bus but leaves the busload open for certain types of critical tasks.

hz