Engineering samples are available

NXP has developed a CAN FD transceiver with cyber security features. This includes an ID whitelist and a bus-load measuring capability.

Demonstrator of the secure CAN FD transceivers qualified for 5 Mbit/s (Photo: CiA)

At the 16th international CAN Conference (iCC), Bernd Elend presented the secure CAN transceiver functions in detail. The products protect against spoofing attacks. The node capture by a software attack doesn't send CAN-IDs, which have not been hardware-configured in a safe area by the OEM or Tier1. There is also such a hardware-configured whitelist for received messages owned by the receiver. Detecting such a CAN-ID causes the transmission of an active Error Flag, which destroys the spoof-message. This helps also against tampering the message data. Of course, this leads to multiple error conditions. But at the end, the attacked and captured node goes bus-off.

Bernd Elend: "These security functions can also be implemented on CAN controllers." (Photo: CiA)

In order to avoid flooding by a compromised node, the transceiver has hardware-configured bus-load limit (e.g. 6 %). The secure transceivers are pin-compatible to generic products. There is no need to update the application software or to exchange keys. "It is complementary to other security measures," summarized Elend. Engineering samples are already available. NXP presented at the iCC a demonstrator.

hz