Secure CAN communication without cryptography

NXP® TJA115x Secure CAN Transceiver Family

NXP's new secure CAN/CAN FD transceiver family TJA115x provides a seamless and very efficient solution to secure Classical CAN and CAN FD communication without using cryptography.

OVERVIEW

The TJA115x high-speed CAN FD transceiver family provides an interface between a Classical CAN and CAN FD protocol controller and the physical two-wire CAN bus.

The TJA115x transceivers belong to a new generation of automotive high-speed CAN/CAN FD transceivers from NXP Semiconductors, offering Cyber Security functions. They are available as drop-in replacement for standard CAN transceivers in SO8 and HVSON14 packages. If no cyber security incident has been detected the TJA115x transceivers behave like TJA104x standard transceivers (difference is e.g. that the TJA115x features "auto biasing").

In case a cyber security incident is detected the message gets invalidated on the bus in the end-of-frame field by an active error flag, this is before it is stored in any receive buffer. For an incident caused by the local host, the TJA115x transceiver disconnects the local host temporarily from the CAN bus.

The simple exchange of a TJA104x standard transceiver by a TJA115x transceiver is possible without the need to modify the SW 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 bus and to the local host.

KEY FEATURES

- Available for high-speed CAN & CAN FD up to 2 Mbps
- Available in SO8 and HVSON14 packages
- Foot print compatible with today´s CAN transceivers
- The Cyber security incidents that can be detected and contained are:
  - Flooding
  - Tampering
  - Spoofing
    - The local host attempts to transmit a CAN message with an identifier that is not assigned
    - Receiving a CAN message with an identifier that is assigned for transmission by local host
- AEC-Q100 qualified to Grade 1 requirements
- Dark green product

SYSTEM VALUE AND BENEFITS

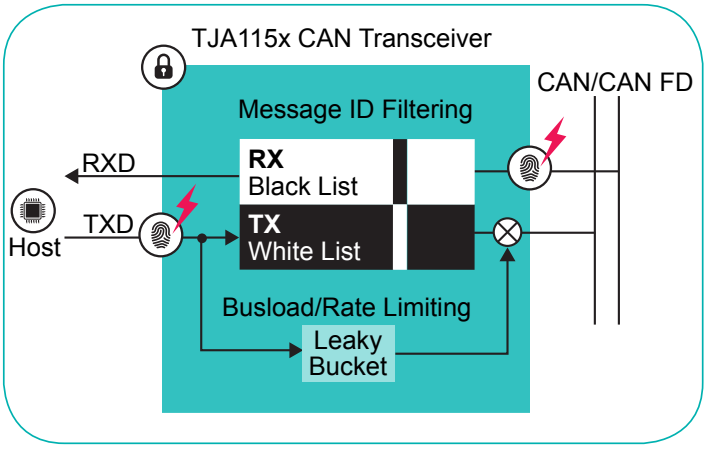
The following system application aspects should be considered when using TJA115x. The secure CAN transceiver:

- Guarantees the legitimate sender of a Classical CAN or CAN FD message
- Can replace AUTOSAR "SecOc" on CAN branches – removing bandwidth overhead, removing the need for crypto key storage/handling, removing start-up delays, removing increased latency and reducing processor load
- Can protect its own configuration update
- Can be used as an Intrusion Detection System (IDS)
- Provides containment of intrusion
- Is drop-in replacement to many standard CAN transceivers

The concept proposed by NXP is implemented entirely in hardware in the form of a secure CAN transceiver. It operates completely independently and in isolation from the microcontroller (µC). 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 CAN protocol specification. It can be introduced into a network in a stepwise approach (ECU by ECU), without impacting other ECUs, or impacting the message latency, the busload or increasing the processor load. The implemented spoofing protection mechanism makes sure that whenever a protected message is received by the target ECU (i.e.: message receiver) it has been transmitted by the expected sender. Also, the bus 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).

Such secure CAN transceivers are provided as a hardware replacements of today's standard CAN transceivers, avoiding major hardware and further software changes on the ECU and do not affect the operation of other ECUs. This makes the proposed approach a fast, low-effort, non-disruptive and highly cost-effective way to introduce security to the CAN bus – either as standalone protection mechanism, or better, as an extra layer of defense in addition to other security solutions.

TJA115x APPLICATION PRINCIPLE



NXP SECURE CAN TJA115x TRANSCEIVER FAMILY

Type	Package	Description
TJA1152AT	SO8	8-pin transceiver with Standby mode and V_{IO} pin
TJA1152BT	SO8	8-pin transceiver with Standby mode
TJA1153ATK	HVSON14	14-pin transceiver with Sleep mode and V_{IO} pin

Document Number: SECURCANTRLFUS REV 0