Securing CAN communication without cryptography

NXP TJA115x Secure CAN Transceiver Family

The NXP TJA115x CAN and CAN FD transceiver family provides a smooth, cost-effective solution for securing classical CAN and CAN FD communication without cryptography.

OVERVIEW

The TJA115x transceiver family is a new generation of automotive high-speed CAN/CAN FD transceivers. These transceivers provide an interface between a classical CAN or CAN FD protocol controller and the physical two-wire CAN bus and offer authentication of CAN communication without cryptography. As long as no security incident is detected, the TJA115x transceiver behaves like standard high-speed CAN transceivers.

The different TJA115x variants are available in standard SO8 or HVSON14 packages.

HOW SECURE CAN WORKS

If a security incident is detected, the message gets invalidated by the TJA115x transceiver by sending an active error frame. This prevents the message from being stored in any receive buffer. If a local host originates the security incident, the TJA115x transceiver also disconnects the local host temporarily from the CAN bus.

Configuration of the TJA115x transceiver, like the CAN identifiers and filter settings, is part of the end-of-line programming. The configuration can either be kept open for future secure updates in the field, or it can be permanently locked.

The TJA115x transceiver facilitates logging and reporting security incidents on the bus and to the local host.

KEY FEATURES

- Supporting high-speed CAN and CAN FD up to 2 Mbit/s
- Available in SO8 or HVSON14 packages
- Footprint compatible with today´s high-speed CAN transceivers
- Detection and containment of following security incidents:
  - Flooding
  - Tampering
  - Spoofing
    - The local host attempts to transmit a CAN message with an unassigned identifier
    - Receiving a CAN message with identifier that is solely assigned to the local host

SYSTEM VALUE AND BENEFITS

Offering inherent security level with minimum system impact

The following system application aspects should be considered when using the TJA115x transceiver:

- Ensures the legitimate sender of a classical CAN or CAN FD message
- Can replace AUTOSAR® "SecOC" or similar for the authentication of local CAN communication which eliminates:
  - Bandwidth overhead
  - Need for crypto key storage/handling
  - Start-up delays
  - Increased latency
  - Additional processor load
- Protects its own configuration update
- Complements in (intrusion) detection system (IDS)
- Provides immediate containment of intrusion

As the security functions are purely hardware based, the TJA115x operates completely independently and isolated from the microcontroller. This means that the TJA115x transceiver provides an inherent level of security and is specifically designed for minimum system impact and to overcome the lack of sender identification in the CAN protocol specification.

The TJA115x transceiver can be stepwise introduced into a network (i.e., ECU by ECU), without impacting other ECUs, or impacting the message latency, the busload or increasing the processor load.

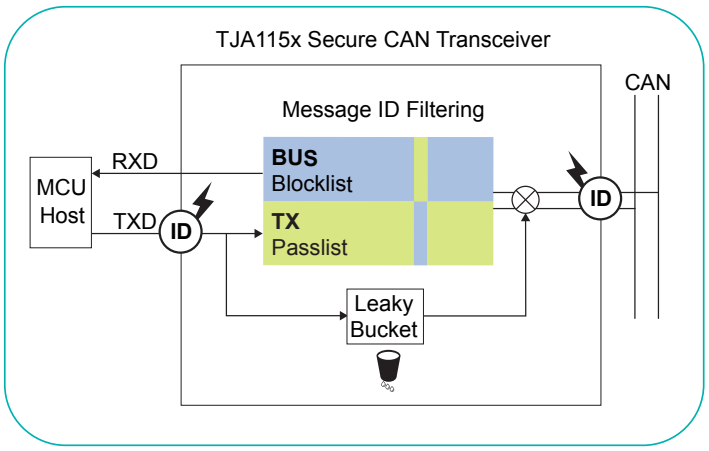
SPOOFING PROTECTION

The implemented spoofing protection mechanism (Transmission Passlist and Bus Blocklist) on the sender makes sure that whenever the target ECU (i.e., message receiver) has received a protected message, the genuine sender has transmitted it. Also, the bus is protected immediately after any activity on the CAN bus. The implemented security mechanisms do not require any initialization (of individual ECUs) or synchronization (of multiple ECUs on a bus).

FLOODING PROTECTION

The TJA115x transceiver measures the duration of frames transmitted by its local host controller. The measured values are added to a "leaky bucket", which overflows when the cumulative bus load exceeds a configurable threshold. A flooding incident is signaled by invalidating the message with an active error frame and switching to Secure mode to disconnect the local host controller from the bus.

TJA115x APPLICATION PRINCIPLE



NXP TJA115x SECURE CAN 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

Flooding is also detected when the sender attempts to occupy the bus for longer than the maximum theoretical frame length.

TAMPER PROTECTION

During a transmission by the local host – authorized according to the Transmission Passlist—the TJA115x transceiver will detect payload modification performed by another node on the CAN bus. According to the CAN specification, the CAN controller of the local host detects and handles such modification in Error Active state. However, in Error Passive state, the modifications are not signaled by an Error Frame leaving tampering opportunities to a malicious node. When tampering protection is enabled, the TJA115x will close the security gap of the Error Passive state by generating the missing (from a security point-of-view).

FROM STANDARD CAN TO SECURING CAN COMMUNICATION—A SMOOTH AND EASY TRANSITION

NXP secure CAN transceivers are a hardware replacement for today's standard high-speed CAN transceivers. They avoid major hardware and/or software modifications of the ECU and do not affect the operation of other ECUs. This approach helps enable a fast, low-effort, non-disruptive and highly cost-effective introduction of security to the CAN bus—either as standalone protection mechanism; or even more advanced, as an extra layer of defense in addition to other security solutions.

www.nxp.com/CAN

NXP and the NXP logo are are trademarks of NXP B.V. All other product or service names are the property of their respective owners.
All rights reserved. © 2020 NXP B.V.

Document Number: SECURCANTRLFUS REV 3