无需使用加密技术
即可保障CAN通信
安全

恩智浦TJA115x
安全CAN收发器系列

恩智浦TJA115x CAN和CAN FD收发器系列提供了一个经济高效的平稳解决方案，无需使用加密技术，即可保障经典CAN和CAN FD通信安全。

概述

TJA115x收发器系列是新一代汽车高速CAN/CAN FD收发器。该系列收发器可在经典CAN或CAN FD协议控制器与物理双线CAN总线之间提供接口，并提供无需使用加密技术的CAN通信认证。只要未检测到安全事件，TJA115x收发器的行为就与标准高速CAN收发器类似。

TJA115x提供采用标准SO8或HVSON14封装的不同版本。

安全CAN的工作原理

如果检测到安全事件，TJA115x收发器将通过发送主动错误帧，使该报文无效。这样就可以防止将该报文存储到任何接收缓冲区中。如果本地主机引发了安全事件，TJA115x收发器还会暂时断开本地主机与CAN总线的连接。

TJA115x收发器的配置（如CAN ID和过滤器设置）既可以将该配置保持为开放状态，以供将来进行现场安全更新，也可以将其永久锁定。

TJA115x收发器有助于在总线上和向本地主机记录和报告安全事件。

主要特性

- 支持高速CAN和CAN FD（高达2 Mbit/s）
- 提供SO8封装或HVSON14封装
- 与当今的高速CAN收发器尺寸兼容
- 检测并遏制以下安全事件：
  - 泛洪攻击
  - 篡改
  - 欺骗
    - 本地主机试图发送带有未分配ID的CAN报文
    - 接收带有ID（仅分配给本地主机）的CAN报文

系统价值和优势

提供固有的安全级别，将对系统的影响降至最低

使用TJA115x收发器时，应考虑以下几个系统应用因素：

- 确保由合法发送方发送经典CAN或CAN FD报文
- 可替代AUTOSAR®“SecOC”或类似方案，进行本地CAN通信认证，以消除：
  - 带宽开销
  - 加密密钥存储/处理的需要
  - 启动延迟
  - 延迟增加
  - 额外的处理器负载
- 保护自身配置更新
- 完善（入侵行为）检测系统(IDS)
- 立即遏制入侵行为

由于安全功能完全基于硬件，TJA115x完全独立运行并与微控制器隔离。这意味着TJA115x收发器具备固有的安全级别，并且专为将系统影响降至最低而设计，并能够克服CAN协议规范中缺少发送方身份的问题。

TJA115x收发器可以逐步引入网络（例如逐个电子控制单元），不会影响其他电子控制单元，也不会影响报文延迟、总线负载或增加处理器负载。

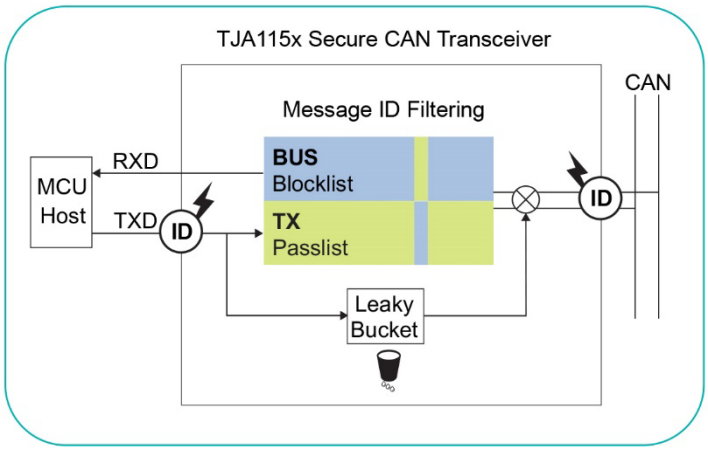
欺骗保护

在发送方实施的欺骗保护机制（发送ID列表和总线阻止ID列表）可确保目标电子控制单元（即消息接收方）所接收的受保护报文均由真实发送方发送。另外，在CAN总线上发生任何活动后，总线会立即受到保护。实施的安全机制不需要任何初始化（各个电子控制单元）或同步（总线上的多个电子控制单元）操作。

泛洪攻击保护

TJA115x收发器测量其本地主机控制器所发送帧的持续时间。测量值将添加到“漏桶”中，当累积总线负载超过可配置阈值时，该“漏桶”会溢出。通过主动错误帧使报文无效并切换到安全模式，从而断开本地主机控制器与总线的连接来发送泛洪攻击事件通知。

TJA115x应用原理



恩智浦TJA115x安全CAN收发器系列

类型	封装	说明
TJA1152AT	SO8	8引脚收发器，具有待机模式和V_{IO}引脚
TJA1152BT	SO8	8引脚收发器，具有待机模式
TJA1153ATK	HVSON14	14引脚收发器，具有睡眠模式和V_{IO}引脚

当发送方试图占用总线的时间超过最大理论帧长度时，也会检测到泛洪攻击。

防篡改保护

在本地主机传输过程中（根据发送ID列表授权），TJA115x收发器将检测CAN总线上另一个节点执行的有效载荷篡改。根据CAN规范，本地主机的CAN控制器在主动错误状态下检测并处理此类修改。然而，在被动错误状态下，不会发送主动错误帧，从而给恶意节点留下了篡改机会。启用防篡改保护时，TJA115x将通过生成缺失信息（从安全角度来看）来弥补错误认可状态的安全漏洞。

从标准CAN到安全CAN通信——平稳轻松的过渡

恩智浦安全CAN收发器可作为当今标准高速CAN收发器的硬件替代产品，无需修改电子控制单元上的主要硬件和/或软件，并且不会影响其他电子控制单元的运行。这有助于以一种快速、省力、非破坏性且具有高成本效益的方式向CAN总线引入安全性——既可以作为独立的保护机制，甚至也可作为更先进的保护功能，为其他安全解决方案增加第二道安全防线。

www.nxp.com/CAN

文档编号：SECURCANTRLFUS REV 3