使用GMSL隧穿对远程汽车外设进行身份验证

摘要

身份验证可应用于汽车环境，旨在保护外围组件免遭第三方器件假冒。本应用指南详细介绍如何使用千兆多媒体串行链路(GMSL)实现汽车身份验证。

简介

随着汽车设计日益复杂，电子控制单元(ECU)与车内远程外设之间的新通信方式不断开发推出。在这些远程外设负责任务关键型决策的场景，例如构成高级驾驶辅助系统(ADAS)的传感器或摄像头，确保这些外设是经过授权的高质量组件非常重要。ADI公司提供了一种将千兆多媒体串行链路(GMSL)串行器/解串器(SerDes)对与DS28C40结合的解决方案，用于支持外设（如ADAS摄像头或传感器）中嵌入的安全认证器与需要验证外设真实性的ECU之间的通信。

GMSL设计与技术

GMSL是ADI公司特有的汽车SerDes实现技术，已进入汽车通信市场。GMSL技术是一种低功耗、高带宽的串行器和解串器对，具有非常高的数据完整性和可靠性。

GMSL使用同轴电缆供电(PoC)，通过单根同轴电缆传输电力和数据。这意味着ECU侧的电源可以通过同轴电缆传输，从而同时为远程摄像头或传感器以及认证器供电。图1说明了PoC如何融入GMSL设计。

DS28C40是一种合理且简单的解决方案，可为ECU与远程设备（如摄像头或传感器）之间采用GMSL进行通信的任何应用添加安全和身份验证功能。这些应用可能需要身份验证，因为在维修店进行例行维修期间，劣质仿冒器件可能会在驾驶员毫不知情的情况下添加到车辆中。例如，假冒的ADAS摄像头可能没有正确的视场范围、分辨率或校准信息，无法为ECU提供准确的数据，因此可能会带来重大安全风险，甚至导致事故。上电时，ECU可以并行对多个摄像头和/或传感器进行身份验证，以确保所有任务关键型外设都是经过授权的组件。DS28C40的添加非常简单，无需复杂的配置或操作，因为GMSL设备在正确连接和配置后会自动搜索I²C总线上的任何主动监听设备。与评估套件一起使用时，这些I²C设备会自动出现在GMSL GUI中。

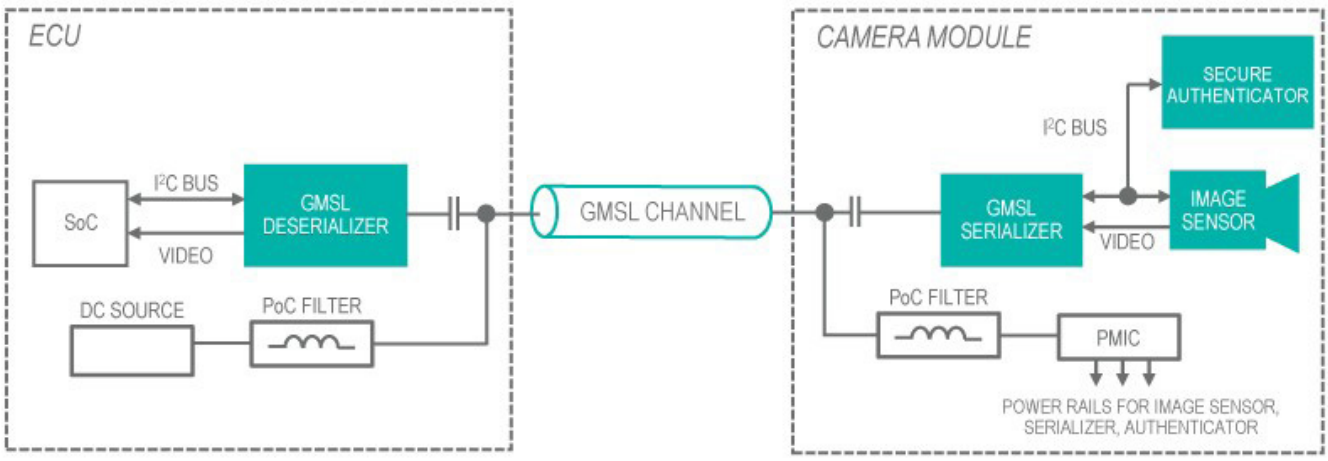

图1. 使用GMSL通道的标准I²C总线与安全认证器通信

GMSL设备具有一个主控制通道和两个直通通道，直通通道让I²C或通用异步收发器(UART)信号隧穿穿过GMSL链路。主控制通道可以访问串行器或解串器的寄存器，但直通通道是纯隧穿通道，无法控制SerDes I²C寄存器。在这种情况下，DS28C40不使用UART，但可以使用主控制通道或直通通道。要配置直通通道并让I²C信号能够使用隧穿功能，串行器和解串器的IIC_1_EN或IIC_2_EN位必须设置为1，具体取决于两个通道中哪个通道正在使用。即使对于直通模式，也需要上拉电阻来实现I²C通信。用于隧穿的引脚对于通道1是SDA1_RX1和SCL1_TX1，对于通道2是SDA2_RX2和SCL2_TX2。如果多个传感器与一个解串器一起使用，GMSL SerDes芯片组提供的I²C地址重新分配和转换功能可避免I²C地址冲突。

为外设（如ADAS摄像头或传感器）添加身份验证的简单方法是将DS28C40嵌入到外设中，并使用I²C隧穿功能通过GMSL通道与ECU进行通信。这样可以降低复杂性，因为不需要对寄存器进行编程，用户能够轻松地利用GMSL系统的硬件通过I²C快速开始通信。图2展示了该实现方案，其中显示了ECU对摄像头模块的身份验证。请注意，仅外设侧需要DS28C40认证器，因为它是使用非对称算法的公钥设备，本文对此有详细说明。因此，主机ECU可以仅使用公钥来验证摄像头身份，只需添加一个设备就能增强安全性。同时，通过GMSL直通通道的数据通信对于I²C主机和DS28C40来说是完全透明的。

DS28C40使用非对称椭圆曲线数字签名算法(ECDSA)加密技术对每个外围组件进行身份验证。ECDSA是一种公钥算法，每个认证器都有唯一的公钥-私钥对。私钥嵌入在认证器中，永远不会离开设备。相应的公钥存储在设备的一次性可编程(OTP)存储器中，可由ECU自由读取。此公钥用于完成ECDSA计算，以确保认证器提供正确的数据来证明它以及嵌入它的设备是系统的有效部分。设备有效性得到进一步检查，因为每个身份验证器都包含唯一证书，这将确保设备是系统认可的一部分，并且已由正确的证书颁发机构进行编程。此外，每次DS28C40生成签名时，它都会包含由ECU发送的唯一质询，以防范重放攻击（在这种攻击中，静态值可能会被发现并重复使用）。

如前所述，身份验证有两个主要步骤。首先，主机验证DS28C40证书是系统的有效部分。其次，要求DS28C40对随机质询进行签名。证书颁发机构使用DS28C40上不存在的系统范围私钥对DS28C40的唯一公钥进行签名，从而在每个设备中创建并安装唯一证书。因此，虽然伪造者可以直接复制证书，但无法使用正确的私钥对来自主机的随机质询进行签名。另一方面，伪造者可以使用唯一密钥对实现ECDSA算法，并响应来自主机的随机质询，但这种类型的伪造者无法产生由系统范围私钥签名的有效证书。因此，身份验证过程非常稳健可靠，ECU使用系统范围的公钥和DS28C40的唯一公钥，而无需安全主机。ADI公司的教程5767（椭圆曲线数字签名算法详解）更详细地描述了如何使用ECDSA进行身份验证。

图2. 使用GMSL I²C隧穿功能在ECU和摄像头之间进行通信

除了仅使用一个IC即可增强汽车外设的安全性之外，实现上述两个身份验证步骤的ECU主机命令序列也相对简单。DS28C40评估套件和免费软件可以帮助客户更快地熟悉设备操作。由于GMSL直通模式对I^2C主机和DS28C40是透明的，因此身份验证命令序列开发不需要相应的GMSL评估套件。

随着越来越多的原始设备制造商(OEM)开始选择将通信和安全保护嵌入ADAS外设的方法，了解各种设备是否相互兼容非常重要。幸运的是，DS28C40安全认证器和GMSL SerDes对的组合久经考验，既能提供强大的安全性，又能确保可靠的数据通信。

结语

本应用笔记介绍了如何利用GMSL在汽车环境中添加身份验证功能。文中阐述了保护外设免遭假冒的重要性，以及如何实施这种安全保护的细节。