

CAST 推出首款针对 CAN XL 总线安全的 CANsec IP 核

新的 CANsec 规范的硬件加速引擎为任何 CAN XL 总线系统增加了数据的真实性和保密性

新泽西州伍克里夫湖--**2022 年 9 月 13 日**--半导体知识产权供应商 CAST 今天宣布立即推出一个 IP 核，该 IP 核实现了 CANsec 安全功能，可以更好地保护任何 CAN XL 总线。

CAN 协议定义了一种数据传输总线，在汽车和工业系统中极为流行。然而，它起源于 20 世纪 80 年代，缺乏任何内置的数据保护，使 CAN 总线系统容易受到网络攻击和其他威胁。

最新版本的 CAN 协议，即 CAN XL，提高了传输速度并增加了数据长度的可扩展性。新的 CANsec 协议--由 CAN in Automation (CiA) 开发，作为 613-1 和-2 的规范草案--利用这些 CAN XL 的特点，增加了一层安全性。

新的 CAN-SEC CANsec 加速引擎 IP 核与 CAST 提供的 CAN XL 核或任何其他符合 CAN XL 标准的控制器 IP 核一起工作。它使用两种 NIST 批准的密钥长度高达 256 位的密码来保护 CAN XL 的数据有效载荷。

- AES-CMAC 保护数据的完整性和真实性。
- AES-GCM 还能保护保密性。

该核心保护同一 CAN XL 总线上的多个节点或设备，使用多达 256 个安全通道与 CAN XL 控制器和系统的主处理器通信。

在硬件而非软件中实现 CANsec，CAN-SEC 核心为 CAN XL 总线上的数据增加了可忽略不计的延迟，同时保护这些数据免受已知的网络攻击，包括欺骗、嗅探和重放、拒绝和资源耗尽。

由弗劳恩霍夫 IPMS 开发的 CANsec 核心经过严格的验证和生产，符合 CAST 的 IP 可重用性和质量标准，并已在瑞萨电子公司的演示器中公开使用。它现在可以从 CAST 获得。

CAST 首席执行官 Nikos Zervas 说："正如 2002 年的 CAN、2017 年的 TSN 以太网和 2020 年的 CAN XL 一样，弗劳恩霍夫 IPMS 的先进研发团队使我们能够为一项大有裨益的新技术提供首批可用的 IP 核心之一。CAN XL 有助于应对汽车系统复杂性的急剧增加，现在 CANsec 有助于保护司机和乘客免受日益严重的数字攻击的威胁。"



关于 CAST

计算机辅助软件技术公司 (CAST) 是一家成立于 1993 年的硅 IP 供应商。CAST 的 ASIC 和 FPGA IP 产品线包括微控制器和处理器；数据、图像和视频的压缩引擎；用于汽车、航空和其他应用的接口；各种通用外围设备；以及全面的 SoC 安全模块。