CAST News

CAST introduces the First CANsec IP Core for CAN XL Bus Security

Hardware acceleration engine for the new CANsec specification adds data authenticity and confidentiality to any CAN XL bus system

Woodcliff Lake, New Jersey — September 13, 2022 — Semiconductor intellectual property provider CAST today announced the immediate availability of an IP core that implements CANsec security features to better protect any CAN XL bus.

The CAN protocol defines a data transmission bus that is extremely popular in automotive and industrial systems. Originating in the 1980s, however, it lacks any built-in data protection, making CAN bus systems vulnerable to cyberattacks and other threats.

The latest version of the CAN protocol, CAN XL, increases transmission speed and adds data length scalability. The new CANsec protocol — being developed by CAN in Automation (CiA) as draft specification 613-1 and -2 — takes advantage of these CAN XL features to add a layer of security.

The new CAN-SEC CANsec Acceleration Engine IP core works with the CAN XL core available from CAST or any other CAN XL standard-conforming controller IP core. It protects the CAN XL data payload using two NIST-approved ciphers with up to 256-bit key lengths:

- AES-CMAC protects data integrity and authenticity, and
- AES-GCM additionally protects confidentiality.

The core protects multiple nodes or devices on the same CAN XL bus using up to 256 secure channels to communicate with the CAN XL controller and the system’s host processor.

– more –

Implementing CANsec in hardware rather than software, the CAN-SEC Core adds negligible delay to data on the CAN XL bus while protecting that data from known cyber-attacks including spoofing, sniffing and replay, repudiation, and resource exhaustion.

The CANsec core developed by Fraunhofer IPMS was rigorously verified and produced to meet CAST's IP reusability and quality standards and has been publicly used in a demonstrator from Renesas Electronics Corporation. It is available now from CAST.

"As with CAN in 2002, TSN Ethernet in 2017, and CAN XL in 2020, the advanced research and development team at Fraunhofer IPMS has enabled us to provide one of the first available IP cores for a hugely-beneficial new technology," said Nikos Zervas, chief executive officer at CAST. "CAN XL helps answer the demanding increases in automotive system complexity, and now CANsec helps protect drivers and passengers from the rising threat of digital attack."

About CAST

Computer Aided Software Technologies, Inc. (CAST) is a silicon IP provider founded in 1993. CAST's ASIC and FPGA IP product line includes microcontrollers and processors; compression engines for data, images, and video; interfaces for automotive, aerospace, and other applications; various common peripheral devices; and comprehensive SoC security modules. Learn more by visiting www.cast-inc.com.

# # #

Media Contact:
Artemis Couroupaki, a.couroupaki@cast-inc.com