Fraunhofer Institute for Photonic Microsystems IPMS

CAN-XL Security Add-On

CAN-SEC – CANsec Controller IP

In order to extend the CAN-XL protocol with security functions, new standard (CiA613-1 and 2) has been developed by CAN in Automation (CiA). It extends the CAN XL frame with security functions aimed at protecting the integrity and authenticity of the origin and confidentiality of data in CAN-based networks.

The CAN-SEC IP core can be used in a host processor directly between the host processor and a CAN-XL controller core. The CAN-SEC IP core builds up the CANsec structure in the buffers of the CAN-XL core directly before transmission or directly after reception of the frame. The CAN-SEC IP core has internal registers that contain the information (identifier, key and mode) for the safe channels. The registers for up to 16 safe channels can be set by synthesis parameters. Therefore, the station equipped with the CAN-SEC IP core can participate in up to 16 safe channels.

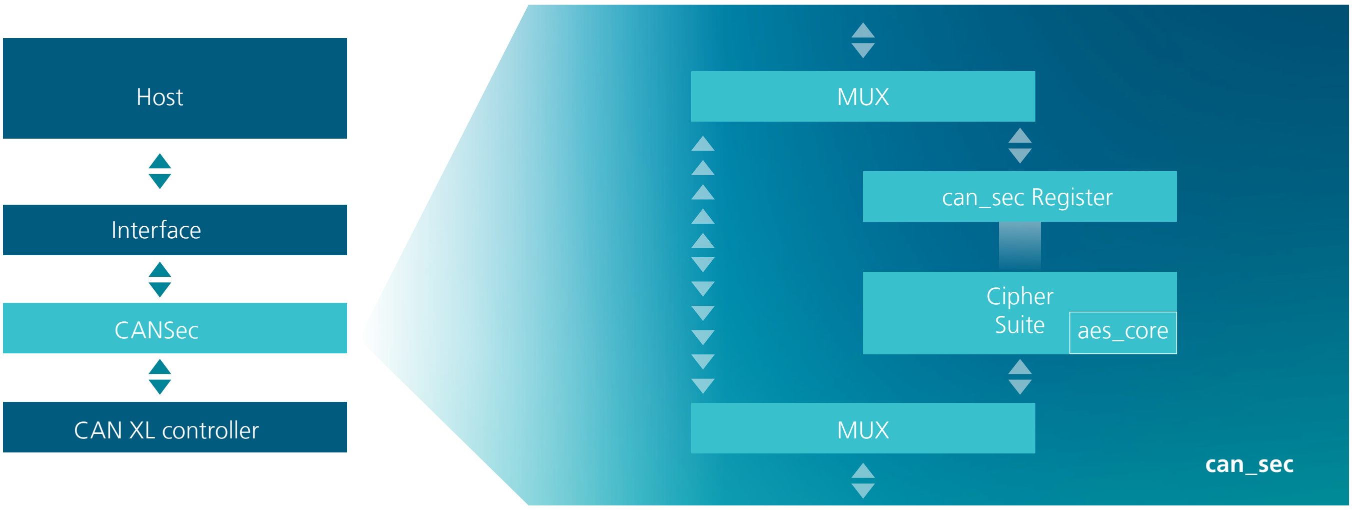
The CAN-SEC is compatible with the CAN XL IP Core (CAN CTRL) of Fraunhofer IPMS but can also be used with several CAN XL IP Cores from other vendors.

Fraunhofer IPMS is a member of CAN in Automation (CiA) and contributes to the development of CiA specifications covering all Open Systems Interconnection (OSI) layers and applications in different areas. CiA representatives actively support the international standardization of CAN-related topics.

Contact

Monika Beck
Technology Transfer
Tel. +49 351 88 23-274
monika.beck@
ipms.fraunhofer.de

Fraunhofer Institute for
Photonic Microsystems
IPMS
Maria-Reiche-Strasse 2
01109 Dresden, Germany
www.ipms.fraunhofer.de



Features

- Fully synchronous HDL design (System Verilog)
- Supports CAN XL specification and CAN XL add-on services (CiA 610-1, CiA 613-1 and 2)
- Supports NIST encryption Standards
  - Advanced Encryption Standard (AES)
  - Cipher-based Message Authentication Code (CMAC)
  - Galois Counter Mode (GCM)
- One clock domain (from host interface)
- Detailed error reporting
- Configurable number of supported Secure Channels up to 16
- Transmit and Receive Buffer used from CAN-XL controller cores
- Supports separate buffer for standalone operations
- Configurable interrupt sources
- Compatible with several CAN XL IP-Cores

Host Controller Interfaces

- 32 bit synchronous host controller interface; wrapper for 8 bit hosts
- 32 bit AMBA APB Protocol Specification v2.0
- 32 bit AMBA 3 AHB-Lite Protocol v1.0
- 32 bit Avalon-MM version 2018.09.26, simple interface (no pipelining)
- 32 bit Wishbone
- Optional application specific interface to the host-controller on request

Deliverables

- Source code Verilog RTL or targeted netlist
- Testbench
- Sample synthesis and simulation scripts
- Comprehensive documentation

Easy System Integration

- Platform independent implementation Xilinx, Intel, Microsemi, Lattice, Gowin FPGAs and any foundry technologies
- Responsive implementation suppor

CAN Controller IP Core CAN CTRL

Fraunhofer IPMS offers a CAN Controller IP Core which carries out serial communication in accordance with the CAN 2.0, CAN FD and CAN XL specification. It is certified as ASIL-D-ready according to ISO 26262 for functional safety.