Fraunhofer IPMS

## CAN-XL Security Add-On

# CAN-SEC – CANsec Controller IP

The new standards CiA 613-1 and -2 by CAN in automation (CiA) extends the CAN XL protocol 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 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 secure channels. The registers for up to 256 secure channels can be set by synthesis parameters. Therefore, the station equipped with the CAN-SEC IP core can participate in up to 256 secure channels.

The CAN-SEC is compatible with the CAN XL IP Core (CAN CTRL) of Fraunhofer IPMS and can also be used standalone or with other CAN XL Solutions.

CAN

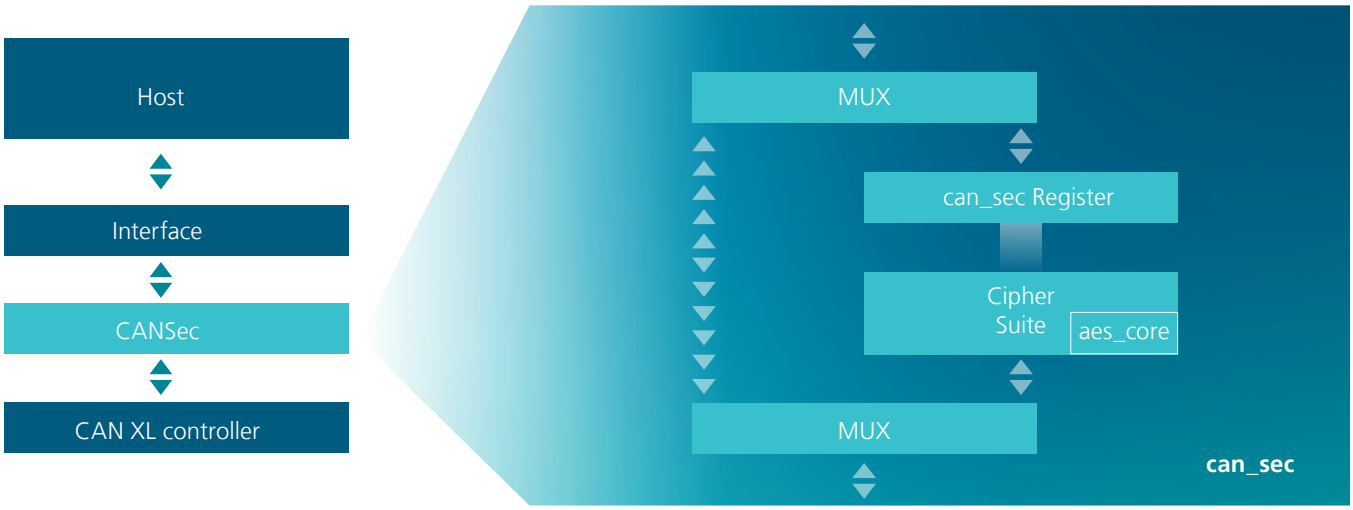
Fraunhofer IPMS is a member of CAN in Automation (CiA) and contributes to the development of CiA specifications covering all Open Systems Interconnection (OSI) layers and applications in different areas. CiA representatives actively support the international standardization of CAN-related topics.

### Contact

Monika Beck
+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

- Supports up to 256 bit key size
- 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
- Detailed error reporting
- Configurable number of supported secure channels (up to 256)
- Transmit and receive buffers used from CAN-XL controller cores
- Supports separate buffers for standalone operations
- Configurable interrupt sources
- Usable 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 or targeted netlist
- Testbench
- Sample synthesis and simulation scripts
- Comprehensive documentation

## Easy System Integration

- Platform independent implementation in any FPGA or foundry technologies
- Responsive implementation support

## 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.

# CAN-CTRL – ISO CAN FD/CAN 2.0B/CAN XL CONTROLLER CORE

The CAN-CTRL IP core is a bus controller that carries out serial communication according to the CAN 2.0, CAN FD specification (ISO 11898-1: 2015 plus earlier ISO and Bosch specification) and CAN XL (CiA 610-1). It is compatible to ISO CAN FD and is certified as ISO 26262 ASIL-D ready.

The CAN protocol uses a multi-master bus configuration for the transfer of frames between nodes of the network and manages error handling with no burden on the host processor. The core enables users to set up economic and reliable links between various components. It appears as a memory-mapped I/O device to the host processor, which accesses the CAN-CTRL core to control the transmission and reception of frames. Optionally a stream interface can be used which allows to efficiently handle large amount of data and to reduce the size of the memory inside the core.

The core is easy to integrate: it offers a simple generic processor interface and additional wrappers to allow the integration into AMBA AHB or APB bus systems. CAN-CTRL is flexible but still easy to use: it provides programmable interrupts, data and baud rates as well as a configurable number of independently programmable acceptance filters. It implements a flexible memory scheme, allowing fine-tuning of the core size to the requirements of each specific application. The number of storable reception frames can be configured prior to synthesis. Two types of transmit buffers are implemented: a high-priority primary transmit buffer (PTB) and a lower-priority secondary transmit buffer (STB). Optionally the core can be configured to include a stream based message interface. They can be included into or excluded from an implementation using configuration parameters.

The PTB can store one message, while the number of included buffer slots for the STB is synthesis-time configurable. The STB can operate in FIFO mode or in priority mode where automatically the message with the highest priority is transmitted first.

Moreover, an optional wrapper instantiating multiple CAN controller cores eases the integration in cases where multiple busnodes need to be controlled by the same host processor.

## CAN Specifications Support

- Classic CAN 2.0B
- CAN FD (ISO 11898-1:2015)
- CAN XL (CiA 610-1)

## Applications

The CAN-CTRL core can be integrated in devices that use CAN or higher-layer CAN-based communication protocols.In addition to traditional automotive applications, such devices are used in industrial (e.g. the CANopen and the DeviceNet protocols), aviation (e.g. the ARINC-825 and CANaerospace protocols), marine (e.g. the NMEA 2000 protocol) and other applications.

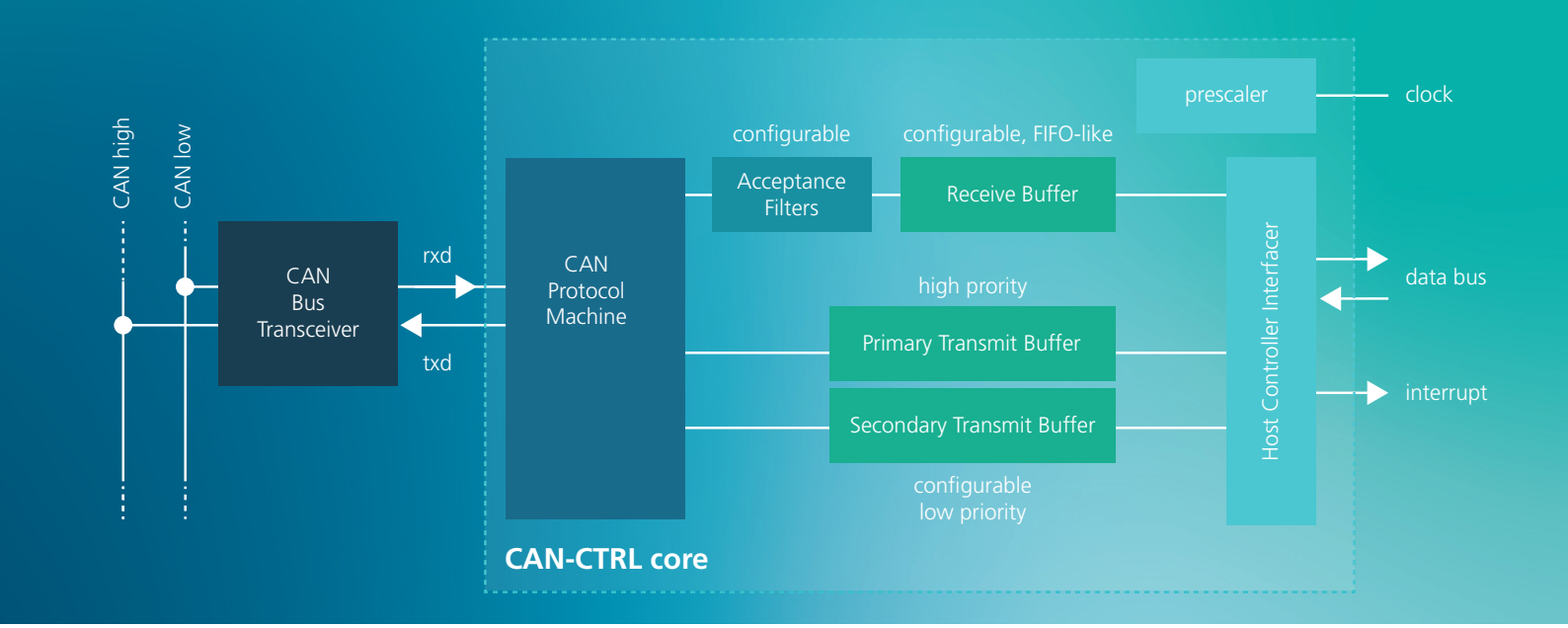
With its safety enhanced package it is also suitable for devices and systems in automotive, airborne, space, medical and other safety critical applications.


**Contact**

Monika Beck
+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


0821049DB_DCC_CANControllerCore




## Features

- Support for CAN 2.0B up to 8 bytes payload
- Support for CAN FD up to 64 bytes payload
- Support for CAN XL up to 2048 bytes payload
- Error Analysis features enabling diagnostics, system maintenance and system optimization: last error type, arbitration lost position, error warning limit
- Listen-Only Mode enables CAN bus traffic analysis and automatic bit-rate detection
- Single Shot Transmission Mode
- 2 clock domains for CAN protocol machine and host controller interface enable usage of an optimal clock for CAN communication independent from the host clock (clock domain crossing)
- Time-triggered operation (TTCAN, ISO 11898-4)
- Supports ECC for SRAM & spatial redundancy for inner logic protection
- Time-stamping support, compliant to CiA's 603 specification
- Loop back mode for self-testing
- Optional stream interfaces for transmission and reception of frames

## Flexible Message Buffering and Filtering

- Configurable number of receive buffers
- One high-priority transmit buffer
- Configurable number of lower-priority transmit buffers
- 1 to 16 independently programmable 29-bit acceptance filters
- FIFO or priority mode for transmit buffers
- Optional memory protection using ECC

## Easy System Integration

- Platform independent implementation into any FPGA or foundry technologies
- Programmable data rate up to 1 Mbit/s with CAN 2.0 and several Mbit/s with CAN FD or CAN XL option
- Programmable baud rate prescaler: 1 up to 1/256
- Flexible programmable interrupt sources
- Generic 32-bit host controller interface AHB and APB (32 bit), generic 8-bit and 16-bit optionally
- Memory can be implemented as Distributed-RAM or Block-RAM
- A single host can control multiple CAN bus nodes via an optional Multi-CAN wrapper
- Available in RTL, and portable to ASIC and FPGA technologies
- Compatible with CAN 2.0/FD/XL PHYs from NXP, MicroChip, OnSemi, Infineon, etc.

## Verification

The core has been tested by a Bosch reference model and is extensively proven in a large number of production designs.
It has been embedded in several shipping customer products, and is proven in both ASIC and FPGA technologies.

## Safety Enhanced Package

- SAM and FDMEA certified ISO-26262 ASIL D ready
- ISO-26262 documentation package.

## Deliverables

- Verilog RTL source code or targeted FPGA netlist
- Testbenches (behavioral, post-synthesis verification)
- Simulation and synthesis scripts
- Safety enhanced version available
  ISO26262 ASIL-D Ready safety package
- Linux driver
- Documentation

## CANsec Controller IP Core

Fraunhofer IPMS offers a CANsec IP Core controller (CAN-SEC) an extension to the newly developed CAN XL protocol. It specifies a Layer 2 CAN security protocol that aims to protect the integrity and authenticity of the origin and confidentiality of data in CAN-based networks. It can be used with the CAN-XL IP Core (CAN-CTRL) of Fraunhofer IPMS, with any other CAN IP Core or in standalone operations.