CAN-SEC

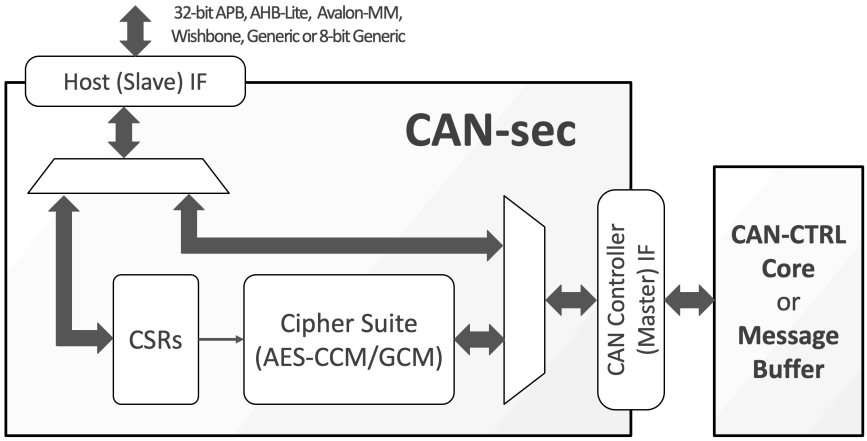
CANsec Acceleration Engine

The CAN-SEC IP core implements a hardware accelerator for the CANsec extension of the CAN-XL protocol, as defined in CiA's 613-2 specification.

The CANsec specification provisions two ciphers with key lengths of 128, 192, or 256 bits to protect CAN XL frames' payload, all of which are supported by the hardware accelerator. Specifically, the core secures frames exchanged over CAN bus networks using AES-CMAC to protect integrity and authenticity and AES-GCM to additionally protect confidentiality. CANsec also secures communication between different groups of nodes physically connected on the same bus using the concept of secure channels, where each channel uses a different encryption key and freshness value. The CAN-SEC core enables its host system to participate in up to 256 secure channels.

This CANsec hardware accelerator has been designed for ease of integration. It presents itself as a peripheral that communicates to the host system via a generic 32-bit memory-mapped slave interface and a configurable interrupt line. The core is delivered with bridges that convert this generic host interface to a generic 8-bit memory mapped interface, or to a 32-bit APB, AHB-Lite, Avalon-MM, or Wishbone interface. Its operation is also rather simple: the host puts the CANsec or CAN XL messages to be processed in a buffer mapped on the core's address space, and the core returns the processed CAN XL or CANsec message to the same buffer and notifies the host. The message buffer can be implemented by means of a simple SRAM attached to the CAN-SEC core via a master memory mapped port. This master port can be used to connect the CAN-SEC core to the CAN-CTRL CAN controller core available from CAST. In this case, the CAN-SEC accesses the CAN controller's message buffers, saving the extra message buffer space and message transfers.

Block Diagram



FEATURES

CANsec Acceleration Engine

- Receives and outputs CAN frames compliant to:
  - CAN XL protocol (CiA 610-1)
  - CAN XL add-oxn services, Part 1: Simple/extended content indication (CiA 613-1)
  - CAN XL add-on services, Part 2: Security (CiA 613-2)
- Implements all ciphers and key sizes provisioned by the specification:
  - AES-CMAC for encryption-only, or
  - AES-GCM for authenticated-encryption
  - Key size of 128, 192, or 256 bits
- Supports up to 256 CANsec secure channels, each equipped with a different key and freshness value.

Easy to Integrate

- Works with any CAN XL controller
  - Optimizes memory usage and bus transfers when used with the CAN-CTRL controller core available from CAST
- Uses a generic 32-bit slave interface & bridges to 32-bit APB, AHB-Lite, Avalon-MM, or Wishbone, or an 8-bit generic microcontroller interface.
- Reports status & error in CSRs and interrupts
  - Supports configuration of interrupt sources

Straightforward to Implement

- Available in LINT-clean, scan-ready, synthesizable RTL source code format or as a targeted FPGA netlist
- Single clock-domain design with no multi-cycle or false paths
- Platform-Independent – Can be implemented on any FPGA device or ASIC technology

Deliverables

Consistent with CAST's quality standards, this core has been rigorously verified, is LINT-clean and scan-ready, and is delivered with everything required for a trouble-free implementation. It is available in System Verilog RTL source code or as a targeted FPGA netlist, and its deliverables include a sophisticated testbench, sample synthesis and simulation scripts, and comprehensive documentation. Software integration is facilitated by a low-level Hardware Abstraction Layer (HAL) and a Linux Driver. A MISRA C bare-metal driver is also optionally available.

Applications

The CAN-SEC core can be used to add a security layer to devices implementing CAN XL interfaces using any CAN controller.

Implementation Results

The CAN-SEC is a purely digital IP core and can be mapped in any ASIC or FPGA technology. The silicon resources required for its implementations depend on the core configuration. The following are sample implementation data for the core configured to support 16 secure channels and when internal memories are implemented with flops.

Target Technology	Area	Clock Freq (MHz)
TSMC 16nm sc7-svt-c16-ssgnp-125c	15,641 um^2 90,526 Gates	80
TSMC 22nm HPC sc9-c35-ss-svt-125c	41,113 um^2 81,573 Eq. Gates	80

These results do not represent the smallest possible area requirements nor the highest possible clock frequency. Please contact CAST to get accurate characterization data for your target application and core configuration.

Support

The core as delivered is warranted against defects for ninety days from purchase. Thirty days of phone and email technical support are included, starting with the first interaction. Additional maintenance and support options are available.

Export Permits

This core implements encryption functions and as such it is subject to export control regulations. Export to your country may or may not require a special export license. Please contact CAST to determine what applies in your specific case.