Safe and Secure CAN Bus IP Core

Product Overview:

The Safe and Secure CAN Bus IP Core ("**SnS CAN IP**") is an implementation of a CAN BUS 2.0 compliant digital controller interface with built in cyber resilience and circuit failure detection capabilities. The SnS CAN IP offers advanced network security and health monitoring capabilities while maintaining compliance with industry standards and peripherals devices (e.g – CAN transceivers).

Key Features:

- Implements CAN version 2.0B with programmable bit rate up to 1Mbit/sec. ISO 11898-5 compliant.
- Physical CAN layer compliant with ARINC 825 for CAN Aviation
- License options for implementation of a safe and secure CAN controller in FPGA or ASIC designs .
- CPU Interface (PCI/local bus/SPI)
- Standard, Extended and Remote frames supported.
- 8 maskable identifier filters. Filtering on ID and first two data bytes for both Standard and Extended Identifiers.
- Loopback mode for self-test.
- Monitor (Listen-only)
- 32-message Transmit and Receive internal fabric FIFOs.
- Internal 16-bit free running counter for time tagging of transmitted or received messages.
- Permanent dominant timeout protection.
- Re-transmission disable capability.
- Transmit Enable pin.
- Supports any COTS CAN transceiver.

Applications:

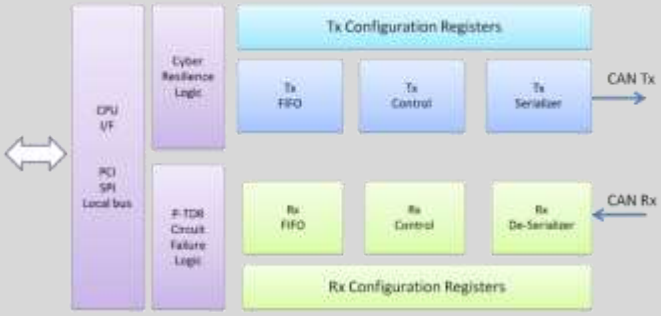
- Automotive
- Aerospace and Military
- Marine
- Industrial
- IoT

Supported FPGA Families:

- Xilinx
- Lattice
- Altera/Intel
- Microsemi

Safe and Secure Enhanced Features:

- Self DoS detection and prevention
- Self-message spoofing detection and prevention
- Rate anomaly notification
- Message Source Validation (in IC mode only)
- Malicious/suspicious message invalidation
- Real-time Passive-TDR info to all ECUs
- Circuit Single Short detection
- Main bus circuit single disconnect detection
- Main bus circuit double disconnect detection



FREE EVALUATION

CONTACT US

Key Benefits:

- Real-time network security and monitoring
- Monitor all ECUs on the network with a single SnS CAN instance
- Flexible licensing options

Core Deliverables:

- FPGA agnostic VHDL Netlist for any clock frequency
- Simulation test bench
- HSID documentation
- API layer – ANSI C code
- Linux AXI bus driver
- Sample application – ANSI C code
- Vivado project files (Xilinx only)

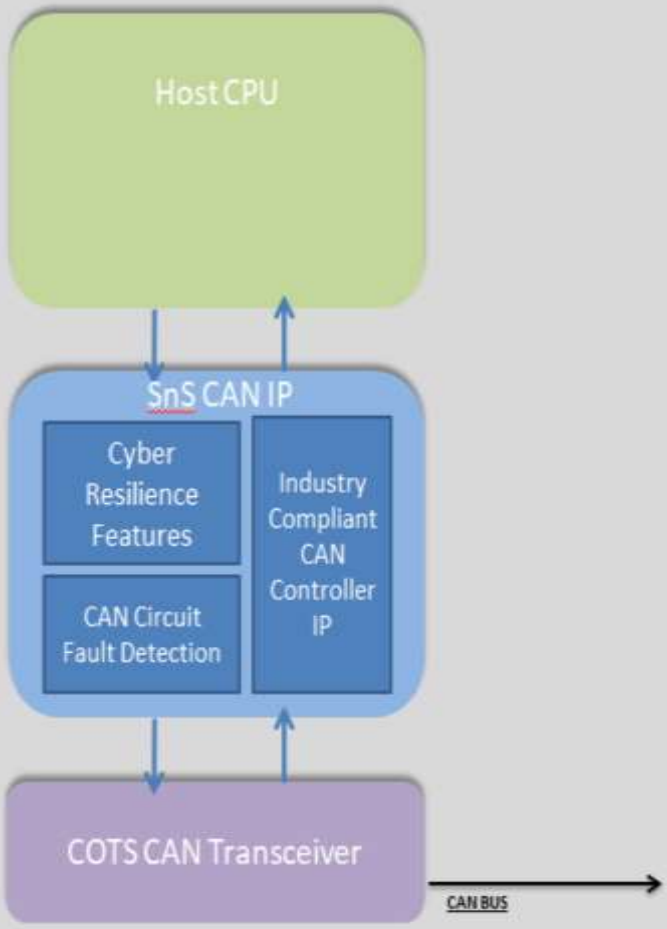
Safe and Secure Features Overview

Sital's CAN Bus IP Core ("**Sn CAN IP**") includes security features to overcome inherent gaps in the CAN/CAN-FD protocol.

Since the SnS CAN IP functions as an industry compliant CAN controller it can be implemented in any IC requiring CAN connectivity (e.g – ECU). A single SnS CAN node can monitor the entire CAN network and provide network security detection and prevention from without impacting other ECUs, or impacting the message latency, the busload or increasing the processor load.

Sital's SnS CAN solution includes 3 major components:

- **Industry Compliant CAN Controller IP**
- **SnS CAN IP core**
  - White List
  - Black List
  - Timing Monitoring
  - Self DoS Detection and Prevention
- **CAN Circuit Fault Detection Sensor**
  - TDR information
  - Shorted CAN circuit detection
  - Open CAN single circuit detection

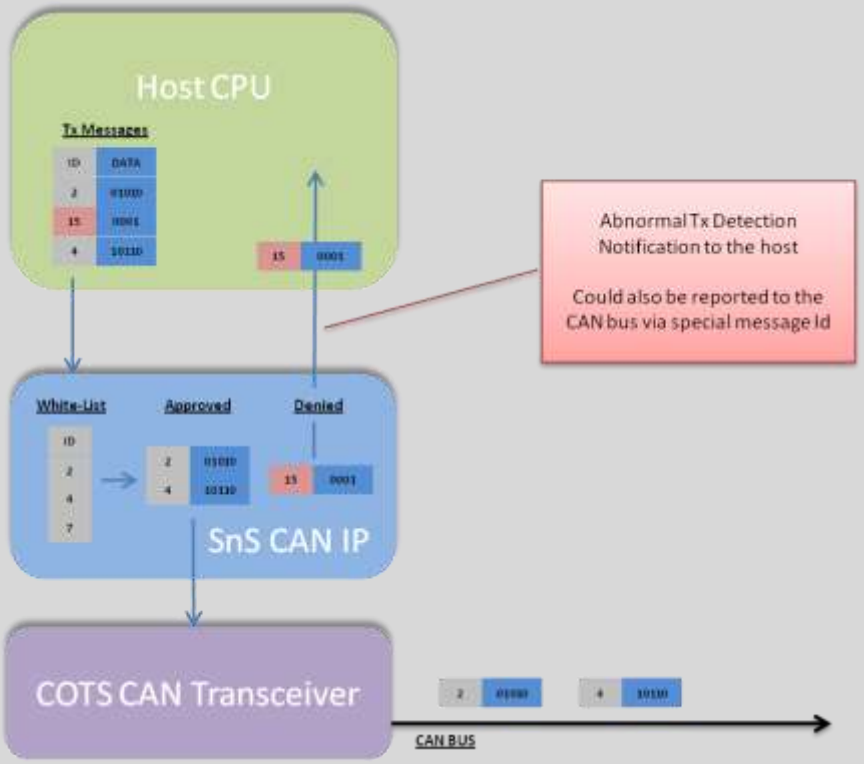


Security and Cyber Resilience Features Overview

Tx White List

User configurable list of valid message IDs allowed for transmission by the host CPU. Sital's SnS CAN Bus IP Core will trigger a notification in real-time on any attempts to transmit messages outside the whitelist configuration both to the host CPU and to all other ECUs connected to the network. The real-time notification includes meaningful forensic information for security playbook execution.

In addition, the SnS CAN IP can be configured to prevent such anomalies from ever reaching the CAN transceiver and thus prevent such attacks without contaminating the bus. The filtering will be done prior to transmitting any of the message bits to the transceiver and thus does not affect the bus or create any collateral communication "damage" (e.g – error out messages).



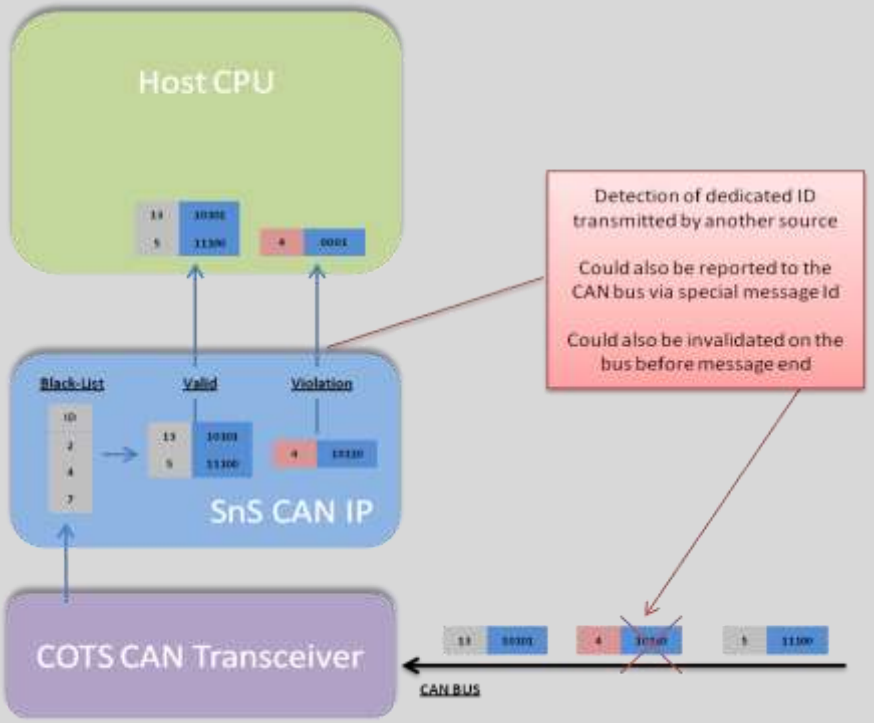
White List Anomaly Detection Example

Black List

list of message IDs that are **dedicated** for this CAN controller and are **not allowed** for transmission by any other ECU on the bus.

Receiving such a CAN message with an identifier that exists in the black list will trigger a real-time notification and **can also be invalidated on the bus** before the end of the message.

The real-time notification is transmitted both to the Host ECU and to all other ECUs and enables the execution of a security playbook.

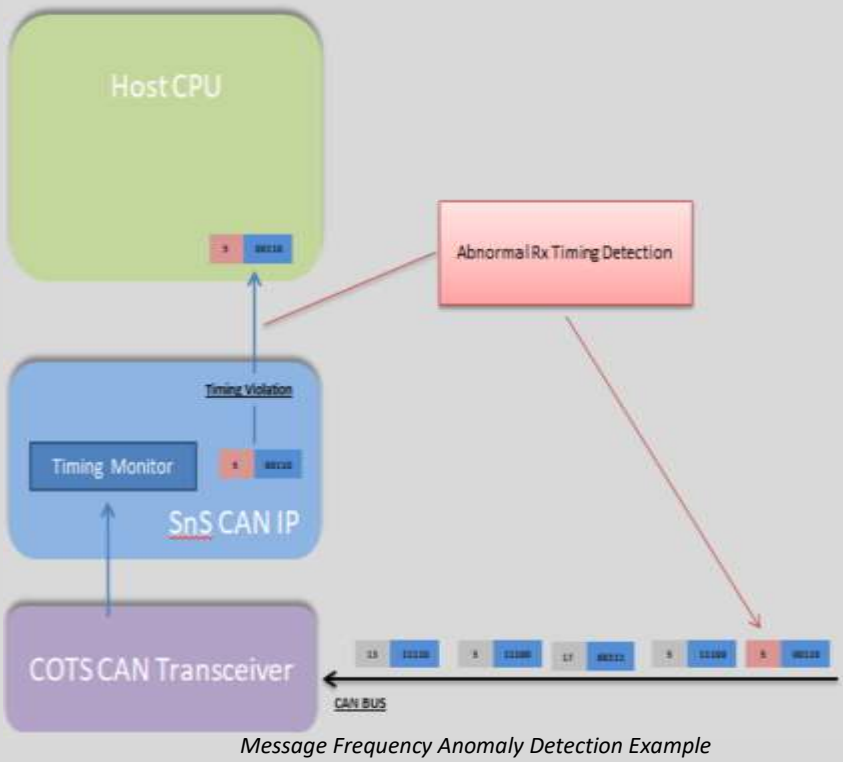


Black List Anomaly Detection Example

Message Timing/Frequency Monitoring

The SnS CAN IP can profile message frequency (Rx intervals). Once a message is appearing on the bus in an "out of bounds" frequency (e.g – too fast or too slow) a real-time notification is trigged to the host CPU or to the bus with forensic anomaly information regarding the message ID and it's info for security playbook execution.

This capability enables a quick detection of various types of cyber attacks including possible DoS or message invalidation ("killing messages on the bus") ECU software malfunction and more.



Message Frequency Anomaly Detection Example

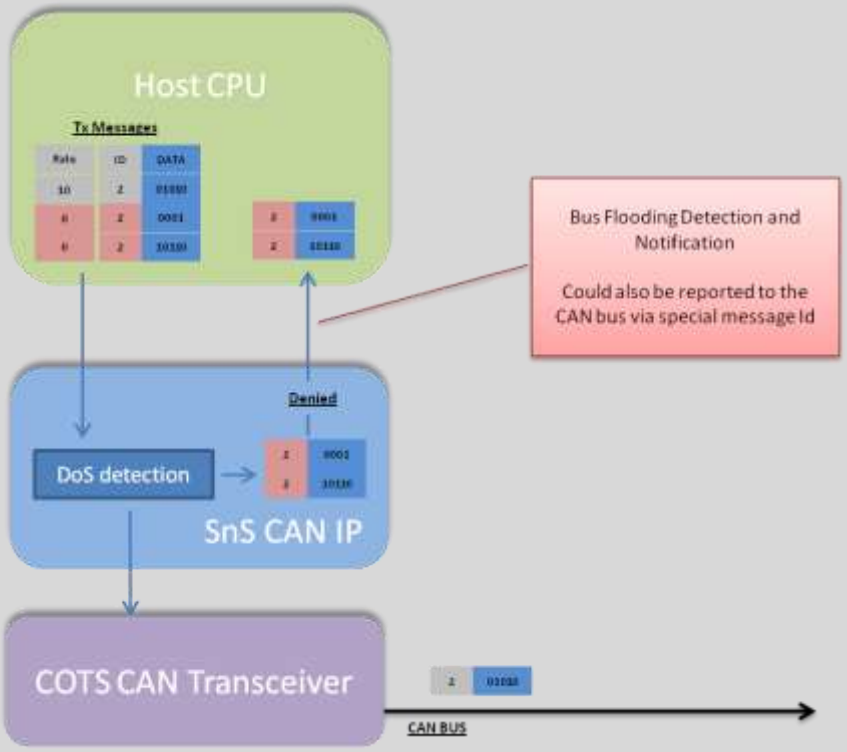
Self Denial of Service Detection and Prevention

The SnS CAN IP has a built-in mechanism to detect self-transmitted bus flooding attempts by the host CPU, and has the capabilities to notify the system and the host CPU on such attempts.

In addition, the SnS CAN IP also has a configurable option to reduce self-transmitted bus load in case DoS is detected to relief the symptoms of such an attack to improve ECU communication and functionality under the attack.

A real-time notification is streamlined to the host CPU and all other ECUs on this bus with forensic information and enables the execution of a security playbook concerning this attack.

DoS attacks are particularly harmful as they block the entire communication network and prevent critical information exchange between ECUs. The SnS CAN IP Core provides a real-time detection, notification and the required minimal network bandwidth to sustain basic communication for safety related systems even under DoS attack.



Message Frequency Anomaly Detection Example

CAN Circuit Fault Detection (CCFD)

Physical network malfunctions are hard to debug especially when they are intermittent. The Sital SnS CAN IP provides real-time detection and notifications on open or shorted CAN circuits and faults, and continuously monitors the physical health of the CAN network out-of-the-box.

The CCFD constantly provides real-time TDR information for critical network circuitry health conditions.

This information is very helpful in chasing the location of CAN bus circuit faults, enables high network reliability and provides early stage failure prognosis.

ADDITIONAL RESOUECES:

- SnS CAN IP Free Evaluation Request
- SnS CAN IC – turnkey module with enhanced cyber resilience and bus circuit monitoring features
- Talk to an expert on how your design may benefit from the SnS CAN IP