Overview of Sital Technology – Safe and Secure (SnS) Solutions for CAN bus/ARINC-825-4

This document provides a descriptive overview about Sital's Safe and Secure (SnS) technology for CAN bus/ARINC-825-4:

- For CAN bus/ARINC-825-4, Sital's Safe and Secure (SnS) technology consists of methods to perform physical layer monitoring for providing continuous, real time authentication on all received messages. Real time authentication enables CAN bus receiving nodes to detect impersonating, or "spoofing" transmitters based on the physical layer characteristics of received signals.

- In addition, Sital's SnS enables detection and location determination of wiring faults such as open and short circuits in bus and stub cabling, bus couplers (for MIL-STD-1553) and connected LRUs for multi-drop data buses. This provides users with the capability to identify and correct such faults while they're still intermittent, before they become continuous and capable of bringing down the data buses such as CAN bus.

- Following power turn-on, each node's SnS logic initiates its local "learning" process. The purpose of this process is to develop the fingerprint or "signature" of each transmitter's signal characteristics. This result of this approximately 4-second process is the SnS hardware "sensor" and low-level software computing an array of attributes to characterize each transmitter, or for ARINC-429, the single transmitter on the bus. This process involves measuring various pulse widths and other timing parameters by means of a high-frequency sampling clock and performing calculations. As an option, application software may compare the measured attribute values following power turn-on with the ones last determined during the previous power cycle. If a mismatch is detected, this anomaly can be reported to the system's security playbook software to possibly take further action. Once the learning process has been completed, the CAN bus/ARINC-825-4 node is now prepared to monitor all future message transmissions.

- In operation, receivers on a CAN bus will continuously measure and compute the parameter values of the signal for all received messages. The values of the measured/computed parameters for each message are compared with the "expected" values determined during the learning phase and adjusted very slowly thereafter to accommodate changes due to temperature and operating voltage. If the measured value(s) of one or more parameters for a received message are determined to be out of tolerance, Sital's software will categorize that message as an anomaly and notify the application software that there's a potentially impersonating or "spoofing" node transmitting on the bus. Following such notifications, application software can then execute its security playbook and take the appropriate actions. This can include shutting down certain processes at the local system level and/or communicating about the anomalies' occurrence over the multi-drop bus or some other interface. Such actions may be necessary to mitigate against the risk system-level failure.

- In addition to detecting spoofing nodes, the Sital's SnS also provides wire fault detection. Electrical wiring faults such as arc faults, fraying wires or failing connectors are capable of taking down ARINC-825/CAN data buses. Detecting such faults in real time while they're still intermittent allows corrective action to be taken before the faults become continuous and potentially catastrophic. The wire fault detection methods are based on Sital's patented passive time domain reflectometry (PTDR) technology. Similar to detecting spoofing nodes, this is based on changes in measured/computed signal parameters, without the need for sending potentially disruptive pulses down a CAN bus.

- Following each message received, Sital's SnS API provides two sets of parameter values to higher level software:
  (1) the "normal" set of attributes originally determined during the "learning" process, and which can get slightly adjusted over time; and
  (2) the attributes measured for the most recent message.
  Software will then be able to determine whether the message indicated the occurrence of an anomaly such as an open or short circuit. Short circuit faults will truncate transmitted pulses, while open circuit faults will modify the timing of reflected voltages. By analyzing such changes, it's possible to detect the occurrence of open and short circuit faults in the ARINC-429 bus and stub wire cabling. In addition, it's also possible to determine the approximate ***location*** of the wire faults. Detecting and correcting these faults early increases equipment availability, mission readiness and flightworthiness; and reduces maintenance costs.

- Sital Technology supplies source code for its SnS software. In addition, since the topologies for different CAN buses can be dis-similar, Sital will be available to collaborate with customers on the development of software to detect and locate electrical faults for specific bus and stub structures. By so doing, it should be possible to develop software that's optimized for each application's specific bus topology.

- In addition to cyber authentication and wire fault detection, Sital's SnS CAN IP core also includes a built-in mechanism to prevent DoS attacks. If a CAN bus interface using this core attempts to continuously transmit more than a numerical threshold of consecutive messages from Sital's patented CAN transmitter and its transmit FIFO isn't empty, the IP will transition into its anti-DoS mode. In this mode, the transmitter automatically lowers the priority of all messages in its transmit FIFO until the FIFO is empty. Following that, it will resume normal operation. This reduction of priorities for all vying transmit message allows other nodes on the CAN bus to transmit their messages normally. If all transmitters on a CAN bus use the SnS CAN IP core, this will eliminate the possibility of software-initiated DoS attacks on that CAN bus.