Sital Technology – Safe and Secure (SnS)
Solutions for MIL-STD-1553 and ARINC-429 Buses

The following bullets provide a descriptive overview about Sital's Safe and Secure (SnS) technology:

- For MIL-STD-1553 and ARINC-429 buses, 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 receivers to detect impersonating, or "spoofing" transmitters based on the characteristics of received signals. The need for this is critical for safety-related operations such as navigation and flight control, and mission critical applications such as weapons deployment.

- In addition, Sital's SnS enables the detection and location determination of wiring faults such as open and short circuits in MIL-STD-1553 or ARINC-429 bus and stub cabling, (for MIL-STD-1553) bus couplers, and connected LRUs. 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 1553 or ARINC-429 buses.

- For the case of ARINC-429, in addition to including SnS capability in all receiving nodes, Sital also proposes to connect receivers to transmitter outputs, allowing them to monitor their own transmissions. With the addition of an ARINC-429 receiver, a transmitting node is also able to detect "rogue" or "spoofing" transmitters on a bus prior to initiating its own ARINC-429 message transmission. Further, this also allows a transmitting node to monitor reflections from its own transmission, enabling it to detect wiring faults on the ARINC-429 bus. As an alternative to adding an ARINC-429 receiver for each transmitting node, for an additional NRE charge, Sital would consider the use of a quad RS-485 transceiver. This would improve the SnS authentication and wire fault detection capabilities by providing indications of rise and fall times.

- 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 the transmitter's signal characteristics. This result of this approximately 4-second process is the SnS hardware "sensor" and 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 also 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 receiving or transmitting MIL-STD-1553 or ARINC-429 node is now prepared to monitor all future message transmissions.

- In operation, all receivers on a MIL-STD-1553 or ARINC-429 bus, including for ARINC-429 the receiver in the transmitting node, will continuously measure and compute the attribute values of the signal for all received messages. The values of the measured/computed attributes for each message are compared with the "expected" values determined during the learning phase and possibly adjusted thereafter. If the measured value(s) of one or more attributes falls out of tolerance, the API 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, host processor 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 a MIL-STD-1553 or ARINC-429 bus or some other interface. Such actions may be necessary to mitigate against the risk of flight or mission failure.

- In addition to detecting spoofing nodes, the Sital's SnS will also provide wire fault detection. Electrical wiring faults such as arc faults, fraying wires or failing connectors are capable of taking down MIL-STD-1553 and ARINC-429 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 attributes, without the need for sending potentially disruptive pulses down a bus.

- Following each message received, Sital's SnS API provides two sets of attribute values to application 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 will supply POC with source code for the MIL-STD-1553 and ARINC-429 SnS APIs. In addition, since the topologies for different MIL-STD-1553 and ARINC-429 buses can be dis-similar, Sital will be available to collaborate with POC and/or POC's customer(s) on the development of software to detect and locate electrical faults for specific MIL-STD-1553 and ARINC-429 bus and stub structures.

By so doing, it should be possible to develop software that’s optimized for each application’s specific bus topology.