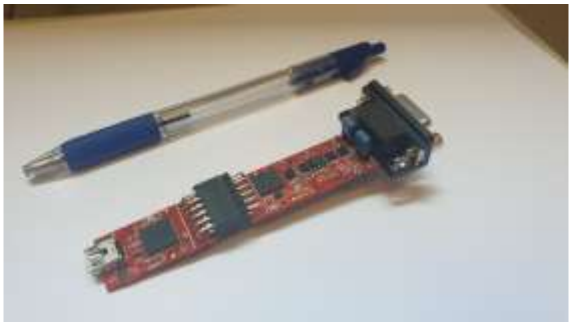
CAN Sequencer GRIP and PhysiCAN SnS GRIP



Sital Technology’s CAN Sequencer GRIP and PhysiCAN SnS GRIP are portable USB testers for CAN bus, CAN-FD and ARINC-825-4. The PhysiCAN SnS GRIP version includes Sital’s patented Safe and Secure (SnS) technology. Both boards support 11-bit and 29-bit CAN messaging and provide capability for transmitting and receiving messages for various lower-level and higher-layer protocols including ISO-11898, CAN 2.0, CAN-FD, ARINC-825-4, CANopen, SAE J1939, and DeviceNet4. These boards can be used for detecting electrical (wire) faults and cyber authentication violations for commercial automotive, military ground vehicle, aircraft, and industrial applications. This includes for engineering development, assembly line and in-use environments.

The boards, which can operate at data rates up to 4 Mb/s, include configurable options to support CAN bus and ARINC-825-4 standards. These include support for Standard, Extended and Remote frames; 8 maskable identifier filters with filtering based on the Message_ID field and first two data bytes, self-test loopback mode, Monitor (listen-only) mode, and an internal free-running counter for time tagging of received and transmitted messages. The boards include FIFO memory structures, with capacity for 16 transmit data buffers and 16 receive data buffers.

The boards may be connected to a USB port on a desktop, laptop or tablet computer and are supplied with Windows GUI software and a Windows API/library/driver. If needed, Sital could port its GUIs to Linux or other operating systems.

For support of CAN-FD and ARINC-825-4, the boards provide a CAN-FD-compliant physical layer that can operate at data rates up to 4 Mb/s. In addition to industry standard transceivers, this includes enabling different data rates for arbitration and data transfers, along with compliance with CAN-FD’s bit timing requirements. The boards also implement the CAN-FD frame structure, including 64-byte data fields; operation of the FDF, IDE, RRS, BRS and SRR bits; delays before and after the ACK (acknowledgement) bit and options for either 17-bit or 21-bit CRCs.

The boards also provide an option for the ARINC-825 modified DLC (data link control) field, Identification Service, and CAN bus bandwidth management. Sital’s bandwidth management includes support of both synchronous, periodic messages and asynchronous messages; implementing minor and major synchronous frames; balancing bus loading; controlling the transmission rate of each node; and performing bus load calculations. The boards also provide the ARINC-825-4 Periodic Health Status Message (PHSM) and Management Information Base functionality.

Safe and Secure. The PhysiCAN SnS GRIP version includes Sital's Safe and Secure (SnS) technology. By means of enhanced physical layer monitoring, Sital's PhysiCAN SnS GRIP sensor provides continuous real-time detection and location of intermittent or continuous open or short circuit wire faults, along with capability to detect cyber authentication "spoofing" (impersonation) violations.

Sital's SnS electrical fault detection feature enables the detection of intermittent open-circuit and short circuit faults in cables, connectors, terminators and devices. The capability to detect intermittent faults at an early stage enables preventive maintenance prior to the occurrence of a continuous, catastrophic failure.

The detection of a cyber authentication "spoofing" (impersonation) violation indicates that a CAN frame (message) for a specific Message_ID was transmitted by an unauthorized sender; i.e., there was a second transmitter for the particular Message_ID. During system development, this can be the result of a hardware or software engineering error. During production, the detection of such a violation could be the result of an assembly line manufacturing error. Subsequent to manufacturing, such violations could be evidence of a transmitter sending malicious messages on a CAN bus.

Sital's SnS technology used in PhysiCAN is the only available product on the market that can both detect authentication violations and identify the violating transmitter; *and* detect and locate electrical faults. Further, it can reliably distinguish between these two types of fault conditions is able to defend a CAN bus from a single point.

The PhysiCAN's SnS API/library software includes source code. The inclusion of source allows users to customize the SnS software to meet their specific application requirements.

PhysiCAN GUI. Sital's PhysiCAN board is supplied with two separate Windows graphical user interface (GUI) programs:

1. One GUI may be used for detecting and locating electrical faults; and
2. A second GUI, for cyber authentication; that is, for detecting the occurrence of "spoofing" (impersonating) messages sent by unauthorized transmitters.

For both programs, users are able to enter their bus topology data into the GUI by means of a simple text format. The electrical fault detection GUI then uses the PhysiCAN SnS GRIP to detect and locate intermittent or continuous electrical faults and indicate its findings as notifications on a diagram of the monitored CAN bus's topology.

Similarly, following detection of a "spoofing" (impersonating) messages, the cyber authentication GUI will indicate the Message_ID and physical node on the bus that was violated. In addition, if the software determines that the violating (spoofing) node was transmitted by a different known node on the bus, the GUI will also indicate the violating node.

Both the electrical fault detection and location, and the cyber authentication operations are based on enhanced physical layer monitoring of all received messages. During system initialization (approximately the first four seconds following power-up), Sital's SnS sensors make measurements to determine the fingerprints (or signatures) for all nodes on the CAN bus. The individual fingerprints consist of a set of parameters for each respective node on the bus. There can be one or more Message_IDs associated with each node on the bus.

Following the initialization period, the GUI and API/library/driver software programs detect electrical or authentication faults by determining the occurrence of mismatches between the expected fingerprint parameter values associated with individual Message_IDs and the actual measured parameter values for each message received.

The PhysiCAN and its GUIs may also be used as a development platform for embedding Sital's CAN bus SnS IP into embedded automotive, military ground vehicle, aircraft and industrial systems with CAN bus networks. For this purpose, it's possible to initially implement, test and debug topology files using PhysiCAN and then re-use the same files for the embedded applications.

Sital Technology Ltd
Tel: +972-9-7633300
Fax: +972-9-7663394
Email: info@sitaltech.com
Web: www.sitaltech.com