CAN IP core for FPGAs and ASICs

The SI-825H IP (intellectual property) core by Sital Technology is suitable for CAN CC and CAN FD communication. It can be configured to support the Arinc 825 higher-layer protocol.

(Source: Adobe Stock)

The IP core is intended for FPGAs and ASICs used in airborne ECUs (electronic control units). The functional safe and cybersecure product features a built-in cyber resilience and network health monitoring functionality. This approach ensures communication reliability and protection as required for AGVs (automated guided vehicles), UAVs (unmanned aerial vehicles), and other mission-critical applications. The IP core is delivered as VHDL netlists for compatibility across many FPGA and ASIC implementations. It complies with ISO 11898-1 and is DO-254 DAL A certifiable. The product features eight maskable filters (CAN-ID and two data field bytes) and a loopback mode for self-testing. It supports up to 32 frame FIFOs (first-in, first-out). There are several interface options to the host controller: PCI, SPI, and a local bus. A listen-only mode is supported. The IP core provides an internal 16-bit free running counter for time tagging of transmitted or received data/remote frames. It is protected against a permanent dominant timeout. To achieve cyber resilience the IP core can white-listing CAN-IDs and monitors the CAN communication from a single instance on the network. Other features include real-time source authentication (IC license mode), real-time anomaly detection and reporting as well as an optional IPS security (IC license mode) mode.

Board-level products

The company uses an implementation of its CAN IP core on a USB (universal serial bus) dongle. This dongle enables CAN CC/FD frame transmissions and supports several higher-layer protocols (e.g., CANopen, DeviceNet, J1939, and Arinc 825-4). The board can operate at data rates up to 4 Mbit/s. It provides a data/remote frame FIFO memory with capacity for 16 transmit data buffers and 16 receive data buffers. The dongle can be connected to a USB port on a host controller and comes with Windows API/library/drivers. Optionally, the product supports the Sital's patented Safe and Secure (SnS) technology. This includes a physical layer monitoring, providing a continuous real-time detection of cyber authentication "spoofing" (impersonation) violations, along with the capability to detect and locate intermittent or continuous open or short circuit wire fault detection for the CAN network lines. This wire-fault detection feature provides continuous fault monitoring, enabling the detection of intermittent open-circuit and short circuit faults in cables, connectors, termination circuitry, and other connected devices. By detecting such faults at the early stage, this enables preventive maintenance, prior to the occurrence of a continuous, catastrophic failure. This SnS feature comes with an API/library software including the source code. The inclusion of source code allows users to customize the SnS software to meet the specific requirements of their applications.

hz