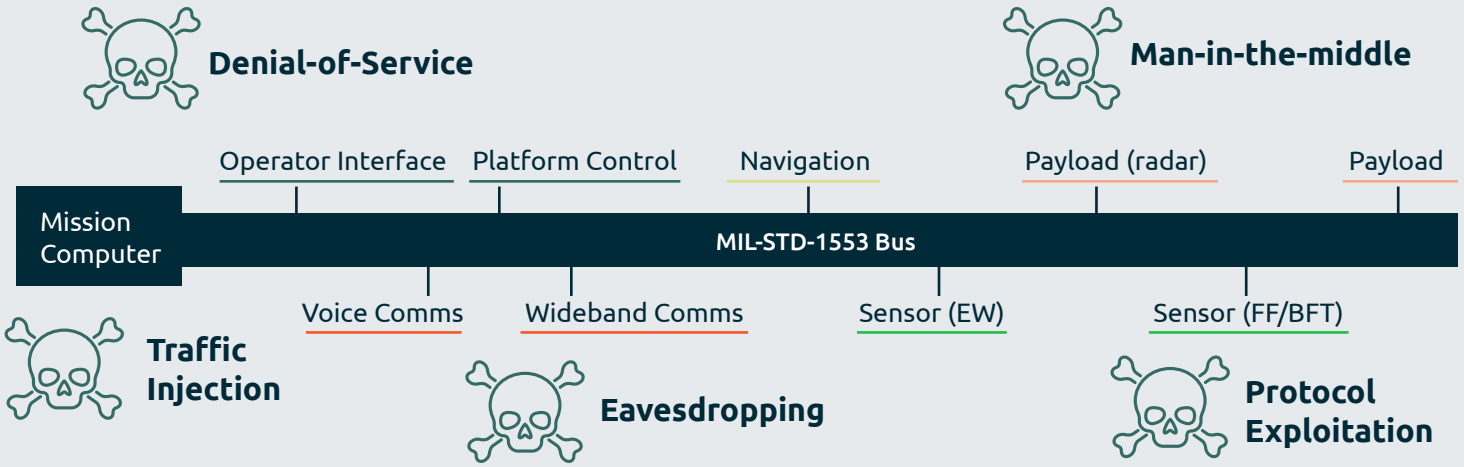
IDAHO SCIENTIFIC

BusCop
MIL-STD-1553B Cybersecurity



What problem does this solve?

The MIL-STD-1553 bus is used on most civilian and military aircraft and many other types of military vehicles. It was designed for electrical reliability but is vul-nerable to attack, introspection, or modification. BusCop protects a device from being infected by a bad bus and/or a bad device from infecting the bus.

How does it work?

BusCop sits between a device and the bus to provide security services including traffic monitoring, firewalling, encryption and authentication. BusCop can be integrated as firmware in compatible existing hardware or as a form, fit replacement for the existing bus network interface card.

Is the 1553 Bus a validated threat?

Several publications, including from Government laboratories, have affirmed the vulnerability of the 1553 bus. With each box on a platform having a unique and complex supply chain, the likelihood exists that one box could contain get taint-ed and then infect the remaining boxes on the bus.

Why BusCop?

- No SWAP impact – no bump in the wire, replaces existing 1553 hardware, no change to the 1553 bus protocol
- Proven Performance – Government validated and proven by Programs of Record
- More Flexibility – scalable protection for the entire platform or protect only the most sensitive boxes platform

Benefits

- **Proven Security** through extensive testing in Government System Laboratories and third-party evaluation
- **Simple Integration** thanks to industry-standard tools
- **No SWAP impact** to the platform thanks to a firmware addition to existing hardware or a form, fit hardware replacement
- **No impact to latency or throughput** possible; operates transparent to the bus

Features

- Shim between PHY/MAC and memory/application interface to provide security on ingress/egress
- Implemented as IP soft core integrated in FPGA/ASIC or form/fit hardware replacement for existing Network Interface Card (XMC, PMC, PCI)
- Cyber detection, firewalling and mitigation if integrated on one terminal
- Encryption/decryption, authentication if integrated on two or more terminals
- Authentication and encryption uses NIST-compliant AES-GCM
- Out-of-band status signal notifies system of suspicious behavior; system designer or operators decides on countermeasure rules
- No impact to latency of 1553 traffic

Deliverables

- Xilinx IP-XACT Package (VHDL)
- Software interface for BusCop configuration
- Product Documentation
- Example design with tutorial
- Technical support

Idaho Scientific

- Trusted U.S. Supplier
- Employees are cleared U.S. citizens
- Secure facilities
- No Foreign Ownership, Control, Influence (FOCI)

XILINX ALLIANCE PROGRAM MEMBER

DPA

FAQs

Compatibility

- **Can it be used for other bus architectures (ARINC 429, CAN)?** The current version of BusCop is specific to 1553 but the security features would work well in other bus architectures. It would take some work to ensure compatibility but nothing in the design prevents it from being applied to other bus architectures.
- **Can BusCop only be used in Xilinx devices?** The cores are tested and validated in Xilinx devices. Nothing in the design prevents porting to FPGAs and SoCs from other vendors.
- **What version of the 1553 standard is supported?** 1553B Notice II.

Performance

- **What is the latency impact to bus traffic?** None. BusCop's security features are implemented in the programmable logic fabric, where the logic is operating at a frequency an order of magnitude higher than the frequency of the bus. Therefore, no latency is introduced to bus transactions.

Security

- **What types of attacks can BusCop prevent?** Eavesdropping via ingress firewall pigeonhole, command injections/Bus Controller takeover via egress firewall, ICD based attacks, attacks through maintenance/configuration ports, man-in-the-middle attacks.
- **How/when does the firewall get configured?** The firewall gets configured via the Security Interface Manager (SIM) API function calls. The API allows a host to transfer signed configuration files into the SIM (configuration files are signed off-host in a secure environment and transferred to the host). The SIM then authenticates the signature and configures the firewall accordingly. The firewall can be configured at any point during the lifetime of the system.

Verification

- **What verification and testing has been done on BusCop?** BusCop's security features have been validated in Government System Integration Labs and have been successfully evaluated by third parties. BusCop also passes Society of Automotive Engineering (SAE) AS4111 Remote Terminal (RT) Validation Test Plan, which is the industry gold standard to validate functionality of a 1553 RT on a 1553B bus.

Ease of Integration

- **What is actually delivered?** For the soft IP version, Idaho Scientific mails a CD with BusCop IP_XACT VHDL encrypted IP Cores, drivers, documentation, a reference design, and a simulated test bench. If the hardware form factor is preferred, Idaho Scientific mails a NIC in the desired form factor (XMC, PMC, PCI), drivers, and documentation. Idaho Scientific also provides the driver stack, a reference design, and complete documentation to simplify the integration process.
- **How much time should I plan to get BusCop setup and running?** BusCop is delivered with industry standard interfaces (AXI-based interface for the soft implementation, and XMC/PMC/PCI for hardware implementation). If you run into any issues along the way, Idaho Scientific engineers are waiting by the phone in Boise, Idaho.

Idaho Scientific: Solve the Problem, Not the Symptom

Named as a 2019 Top 10 Security Company by Enterprise Security Magazine, Idaho Scientific is a specialized, embedded security firm with a proven track record of solving the hardest anti-tamper and cyber security problems for the Pentagon and National Labs with novel and scalable solutions. We prevent exploits at the device level, keeping your sensitive information and intellectual property safe from reverse engineering.

Learn more at idahoscientific.com or email us at info@idahoscientific.com to start a conversation.

IDAHO SCIENTIFIC