Peraton

BUS DEFENDER™ PRODUCTS

BUS DEFENDER | MAINTENANCE DEFENDER | BUS OFFENDER

A proven solution for total cyber resiliency for warfighting system using the MIL-STD-1553 data bus

PRODUCT LINE

Fielded warfighting systems utilizing MIL-STD-1553 buses are vulnerable to destructive cyberattacks from multiple entry points on aircraft, vehicles, ships, and space platforms. Successful 1553-based cyberattacks can propagate over the data bus with catastrophic results – not only mission failure and loss of life and material, but also harnessing a warfighting system to execute adversarial action.

The 1553 Bus Defender product line addresses this demonstrable lack of security on the 1553 bus and the in-line systems connected to it, to deliver proven cyber resilience.

- **Bus Defender™** for on-platform cyber defense to defeat attacks launched or spread over the MIL-STD-1553 data bus
- **Maintenance Defender™** for off-platform defense to provide protection during maintenance, test and software loading, and secure the supply chain
- **Bus Offender™** leverages the powerful traffic generation capabilities of Bus Defender to easily create novel cyberattacks and identify vulnerabilities

BUS DEFENDER
FOR ON-PLATFORM PROTECTION

Bus Defender performs real-time, low-delay network protection to actively defend weapons platforms and stop attacks launched or propagated over the MIL-STD 1553 data bus. Leveraging patented, sophisticated security processing algorithms, Bus Defender can identify 1553 messages that violate policy and block them in real-time. It protects against diverse run-time attacks, including zero-day attacks and known vulnerabilities, and prevents a compromised line-replaceable unit (LRU) or weapons replaceable assembly (WRA) from attacking other LRUs/WRAs or conducting malicious activities via other LRUs or WRAs.

Features and advantages

- Hardware-in-line module requires no modification to LRUs, WRAs, system software or configurations (in-LRU/WRA configurations are also available)
- Detects, prevents, and mitigates attacks in real-time
- Stops zero-day attacks as well as known vulnerabilities
- Protects against diverse attacks (sniffing, denial of service, spoofing/impersonation, etc.)
- Upholds MIL-STD 1553 delay constraints for real-time control systems
- Cannot be turned off like a software solution — making it extremely difficult to disable
- Supports multilevel security objectives to protect against untrusted LRUs/WRAs

PROVEN PERFORMANCE

Bus Defender has proven performance in preventing cyberattacks at diverse DoD test and evaluation events including:

- Achieved Acquisition Milestone B (TRL-6) based on System Integration Laboratory (SIL) testing
- Proven to prevent cyberattacks by DoD red team testers from all services in five separate test events
- Integration, SIL, and on- platform demonstration and testing on five platforms, including aircraft, fighter jet, ground vehicle, and helicopter
- Awarded contract to mature, adapt, and qualify the Bus Defender product for potential future integration and flight testing on the MQ-8C Fire Scout.
- Supporting three branches of DoD on efforts to mature, harden, and evaluate to protect platforms for the Navy, Air Force, and Army

Development hardware and features

- Available in diverse models including LRU/WRA-to-coupler: 2-port model supporting a distributed topology
- Bus-to-Bus Multi-LRU/WRA: supports in-bus topology protecting LRUs/WRAs on one side of the bus from the other side
- High-Profile 6-port secure coupler: supports a centralized topology, similar to a multi-port coupler
- Ruggedized variant: tested -55° to +85°C, random vibration, 40G shock
- Lab Standard 1553 TRB triax connectors, with platform-specific adapters available as needed
- 28V DC power (13-18W depending on model)
- Hardware bypass on switch, power fail, or software command
- Dual-redundant bus circuitry for mission critical independent A/B functionality
- General purpose SoM for anomaly detection and administration
- Two 1 Gb/s Ethernet ports for administration and logging

BUS DEFENDER RUGGEDIZED 2-PORT MODEL

FUTURE BUS DEFENDER REDUCED SWaP CONNECTOR MODEL

MAINTENANCE DEFENDER
FOR MAINTENANCE, TEST, AND DATA LOADING APPLICATIONS

Maintenance Defender is an off-platform device that protects data uploads and maintenance as well as test access via the 1553 bus-based maintenance port on an aircraft or a vehicle.

Significant cyber risks for weapons platforms arise from data loading and access via testing and maintenance terminals used in the field. Maintenance terminals are a lower-barrier target for cyber criminals and can introduce malware into the platform causing catastrophic failures.

Maintenance Defender prevents attacks such as a maintenance laptop inserting malware into an operational flight program (OFP) that will be loaded into an LRU or WRA, and it protects 1553 systems from deliberate or inadvertent compromise during maintenance and test activities.

Features and advantages

- Detects and blocks malware from being introduced during maintenance and test operations
- Eliminates propagation of malware from compromised LRU/WRA via automated test equipment (ATE)
- Secures the supply chain and prevents loading of malicious or compromised OFPs or other data
- Operates transparently, requiring no modification to test equipment, platform, LRUs, or WRAs
- Can be manufactured in three configurations—connector, hardened unit, or integrated into ATE

BUS OFFENDER
FOR EFFICIENT DEVELOPMENT OF ADVANCED, NOVEL CYBERATTACKS

Bus Offender improves cyber resiliency by efficiently creating novel 1553-based cyberattacks to test 1553 weapons systems and identify vulnerabilities. It enables the development of new cyberattacks — including sophisticated and platform-tailored attacks — without requiring the developer to track operational conditions through waveforms and bits.

Leveraging Peraton Labs' powerful 1553 traffic generation capability, Bus Offender develops new attacks much faster and more easily than current systems, and without requiring FPGA or C-level development. A key capability of Bus Offender is its black box LRU/WRA 1553 fuzzer at the physical level, which can vary inter- and intra-bit transmission strength, timing, and Manchester bit encoding to attack analog-to-digital circuits, clock recovery, and state tracking.

Bus Offender includes a Python-based API with constructs for a variety of attack techniques expressed in a high-level, concise, and readable format. It also includes a mechanism to tailor attacks for a specific target weapon system — that is, actions to interact directly and conveniently with interface control document (ICD)-defined messages for the LRUs or WRAs used in the target. Bus Offender is connected to the system-under-test using laboratory standard Triaxial BNC (TRB) connectors and uses wall power.

The 1553 Bus Defender work was sponsored by the Defense Advanced Research Projects Agency (DARPA), the Air Force Research Laboratory (AFRL), the Naval Air Warfare Center (NAVAIR), and Ground Vehicle Systems Center (GVSC) under project agreement issued by U.S. Army Contracting Command – Warren to the Defense Automotive Technologies Consortium (DATC). The views, opinions and/or findings expressed are those of the author(s) and should not be interpreted as representing the official views or policies of the Department of Defense or the U.S. Government.

Peraton

ABOUT PERATON

Peraton drives missions of consequence spanning the globe and extending to the farthest reaches of the galaxy. As the world's leading mission capability integrator and transformative enterprise IT provider, we deliver trusted and highly differentiated national security solutions and technologies that keep people safe and secure. Peraton serves as a valued partner to essential government agencies across the intelligence, space, cyber, defense, citizen security, health, and state and local markets. Every day, our employees do the can't be done, solving the most daunting challenges facing our customers.

Scan to learn more at peratonlabs.com/**bus-defender**