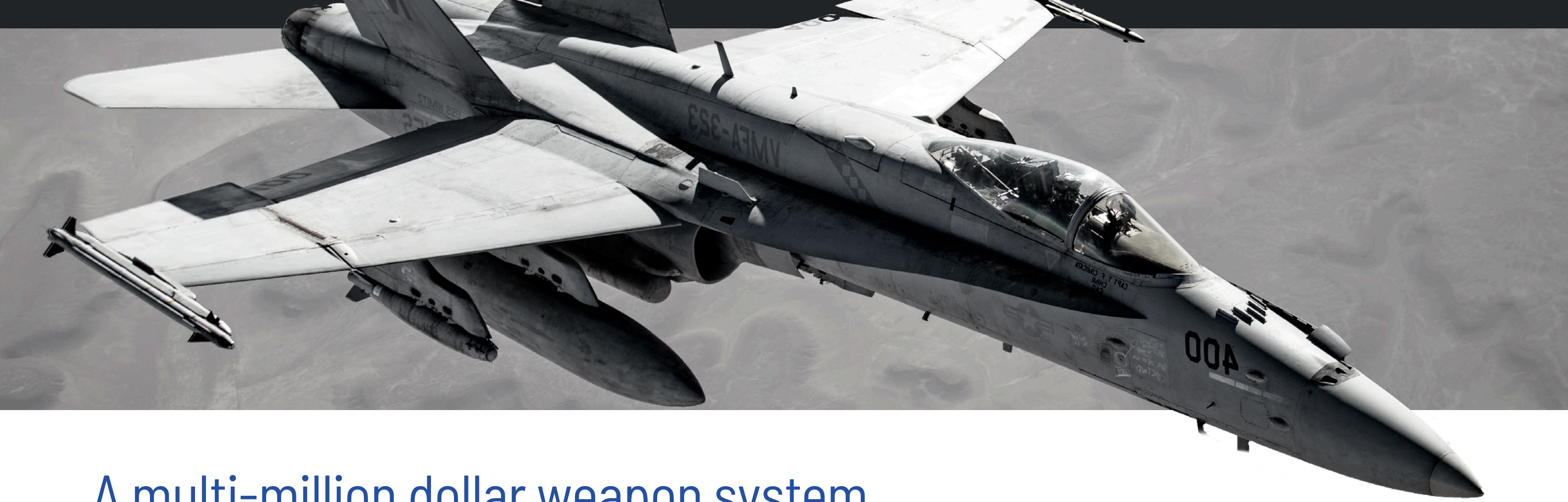
SOLUTION BRIEF

# HOW SHIFT5 SECURES WEAPON SYSTEMS AGAINST CYBER ATTACKS

SHIFT5

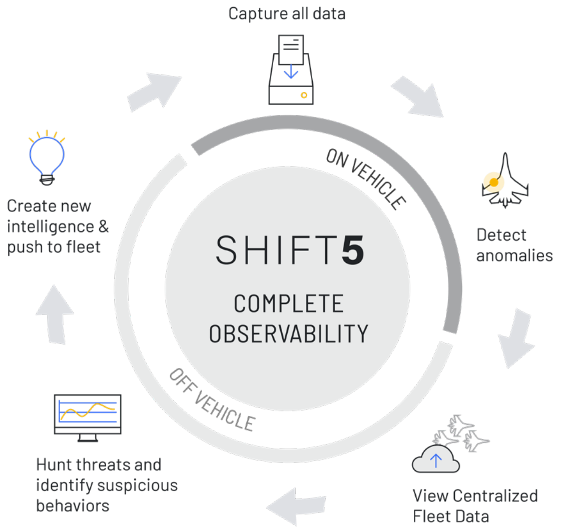
Observe with clarity, know with certainty, decide with confidence.



# A multi-million dollar weapon system should have better cybersecurity than a $500 laptop.

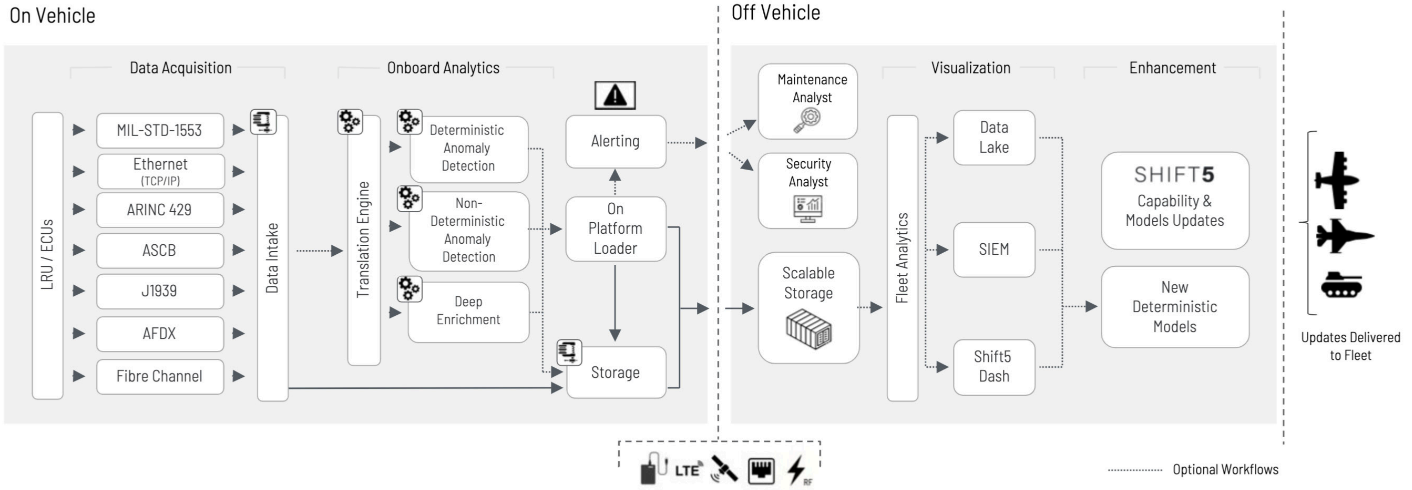
A 2018 GAO report found that the Department of Defense (DoD) faces mounting challenges in protecting its weapon systems from cyber threats[1], and at the same time, cyber-attacks from our adversaries are ramping up in both efficacy and in volume.[2 3]

DoD weapon systems are more advanced and computerized than ever before, but they lack a basic onboard sensor capable of onboard real-time digital anomaly detection capabilities. Digital anomaly detection enhances platform survivability against cyber threats by monitoring onboard computers and data buses for cyber intrusion, digital anomalies, and unauthorized configuration changes. Simultaneously, it enhances fleet readiness by providing maintainers the ability to identify, triage, and monitor digital systems for issues above and beyond the capability of current data recorders.


Capture all data
ON VEHICLE
Detect anomalies
SHIFT5
COMPLETE OBSERVABILITY
View Centralized Fleet Data
OFF VEHICLE
Hunt threats and identify suspicious behaviors
Create new intelligence & push to fleet

# The Shift5 Platform

Shift5's unique platform is hardware, bus, and protocol agnostic, and can perform passive, full-take data capture from any onboard source — every frame, every bus, every protocol. The platform captures, stores, and analyzes serial bus data on the platform in real time on the edge, providing anomaly detection and operational intelligence required to act. Our insights provide real-time alerting and historical trends to assure mission readiness and cyber survivability.



[1] "Weapon Systems Cybersecurity: DOD Just Beginning to Grapple with Scale of Vulnerabilities." GAO-19-128. Oct 2018
[2] "'Aggressive' China cyberattacks are the 'defining threat' of our time, top U.S. cyber official says". CNBC. Dec 2023.
[3] "Russia's Wartime Cyber Operations in Ukraine: Military Impacts, Influences, and Implications" Jon Bateman, Carnegie Endowment for International Peace. Dec 2022.

# RuBI-200, Ruggedized Mission Computer

## OVERVIEW

RuBI™ (Ruggedized Bus Interface) is a customizable, Shift5-built hardware solution that provides passive, full-take onboard data capture, analysis, and enrichment to provide real-time alerting.

RuBI is adaptable to specific application requirements and has been tested against the most stringent environmental conditions, such as RTCA DO-160G and the U.S. Department of Defense Test Standards including, but not limited to, MIL-STD-810H, MILSTD-61G, and MIL-STD-704F.

- Intel Atom C3708, 8 Cores running at 1.7 GHz
- 64 GB DDR4 RAM with ECC
- 2 TB SSD capacity
- LUKS for full disk encryption, meets CNNSP 11 requirements
- 4x Mini PCIe3 Slots
- 2x USB
- 8x GPIOs

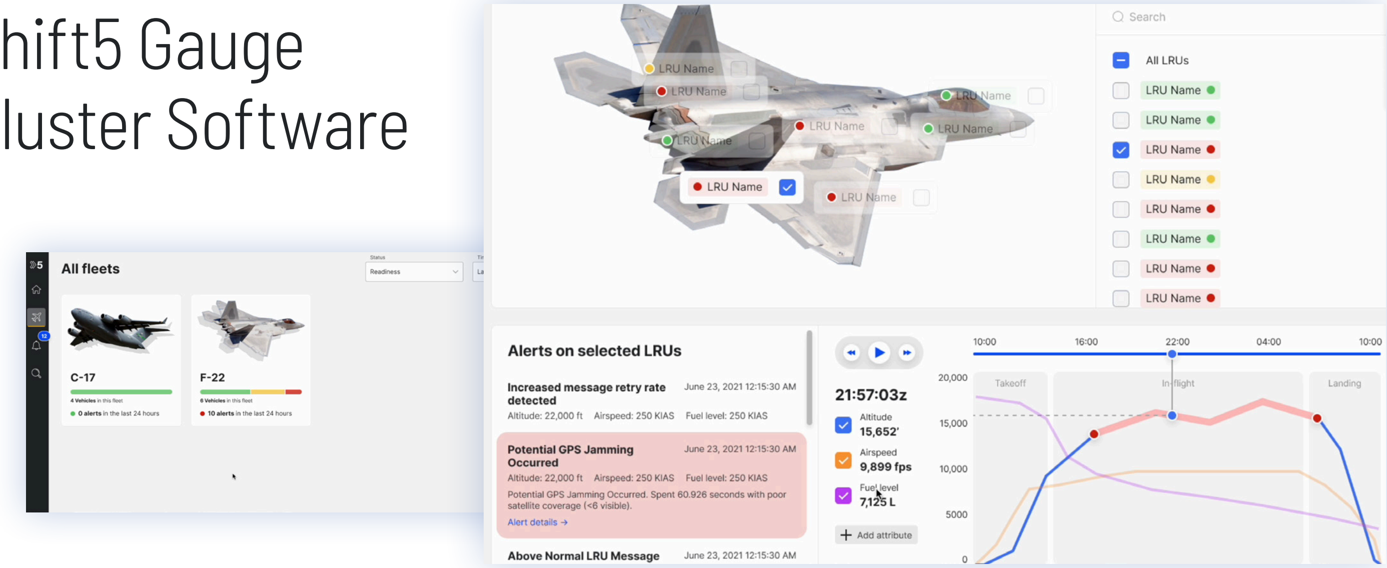
## ENVIRONMENTAL CONDITIONS AND HOUSING

- Dimensions: 6.0 in x 4.5 in x 2.4 in
- Weight: ~ 4 lbs
- Connectors: MIL-C-38999 compliant rugged circular connectors
- Input power: 18 -32V DC
- Reduced power dissipation: 20W
- Operating temperature range: -40°C to 71°C with natural convection
- Category A, for vibrations: RTCA/DO-160G
- Vibration: 7.7 Grms 1hr/axis
- Altitude: 70,000 Feet
- Humidity: 30C-60C @ 95% RH 10-24hr cycles

## INTERFACES AND CONNECTORS

- Ruggedized circular connectors (MIL-C-38999)
- ARINC 429 (13 receive, 13 transmit)
- Customizable I/O module (26 discrete I/Os)
- Power and test connector interface
- Analog audio I/O (2x stereo outputs)
- RS-232 or RS-422 standard (16 receive, 16 transmit)
- 10/100 BASE-T Ethernet ports (2x)
- HD-SDI video interfaces (3x receive and 3x transmit)
- Analog video inputs (3x)
- MIL-STD-1553B (1x)

# Shift5 Gauge Cluster Software



**Alerts on selected LRUs**

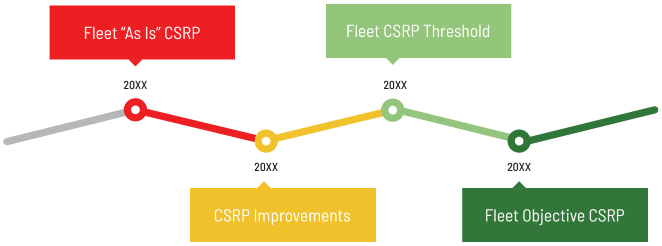
**Increased message retry rate detected** June 23, 2021 12:15:30 AM
Altitude: 22,000 ft Airspeed: 250 KIAS Fuel level: 250 KIAS

**Potential GPS Jamming Occurred** June 23, 2021 12:15:30 AM
Altitude: 22,000 ft Airspeed: 250 KIAS Fuel level: 250 KIAS
Potential GPS Jamming Occurred. Spent 60.926 seconds with poor satellite coverage (<6 visible).
Alert details →

**Above Normal LRU Message** June 23, 2021 12:15:30 AM

# Cyber Survivability Attribute Mapping

## Shift5 Solutions Automatically Drive CSRP Improvements and POA&Ms to Meet Requirements



In 2015, the Deputy Secretary of Defense directed Joint Staff to develop a Cybersecurity KPP. The staffed result was the addition of a Cyber Survivability Endorsement (CSE) to the Joint Staff's System Survivability Key Performance Parameters (SS-KPP). The CSE is meant to be a marked goal for cyber resilience that is specific and achievable, while making sense in context of the realities of the mission.

Any given platform is given a Cyber Resiliency Risk Category (CSRC) based on platform characteristics and mission context (e.g. mission type, threat environment, etc.) that indicate the degree to which cyber survivability is required. The assessed Cyber Survivability Risk Posture (CSRP) must meet the standards of the platform CSRC, otherwise additional mitigations must be put in place. The CSRP of a platform is assessed using ten Cyber Survivability Attributes (CSA) to help PMs cover all the categories of cyber risk.

Shift5 products are focused on helping improve a platform's CSRP by addressing CSAs.

✓ **Control Access**

- Continuous serial data bus monitoring detects and records system access
- Assured Code Delivery provides validation, anti-tamper, and code integrity
- Cyber IDS improves availability and confidentiality
- User interfaces provide fleet situational awareness and operator feedback

✓ **Reduce System Cyber Detectability**

- Continuous serial data bus monitoring identifies adversary monitoring and exfil
- Forensically identify state of the system during emanations

X **Secure Transmission and Communications**

- Shift5 products do not provide encryption capabilities

✓ **Protect System Information From Exploitation**

- Continuous bus monitoring detects and alerts on both data exfiltration and exploits
- Assured Code Delivery prevents data modification

X **CSA 5 – Partition and Ensure Critical Functions at Mission Completion Performance Levels**

- Shift5 products do not offer system partitioning if added after original platform design

✓ **Minimize and Harden Attack Surfaces**

- Continuous monitoring identifies and logs active services and protocols
- Assured Code Delivery provides configuration management
- Cyber IDS monitors platform attack surfaces and alerts on cyber events

✓ **Baseline/Monitor Systems and Detect Anomalies**

- Continuous serial bus monitoring provides foundational data for platform baseline
- Heuristics, trained machine learning models, and AI provide a quantifiable & configurable baseline for anomaly detection per platform
- Cyber IDS provides alerts for anomalies and cyber-events
- User interfaces provide health status and anomaly reports
- Cyber Survivability Risk Assessments support CSRP assessment and reporting
- On-edge detection can be tuned to meet T and O reporting time requirements

✓ **Manage System Performance if Degraded by Cyber Events**

- Alerts provide event information and remediation recommendations where possible
- User Interface provides real-time information to inform commander's decisions

✓ **Recover System Capabilities**

- Assured Code Delivery provides restoration to known-good configuration
- The Manifold provides a trusted, out-of-band source for system recovery

✓ **Actively Manage the System's Configurations to Achieve and Maintain an Operational CSRP**

- Continuous monitoring detects changes in CSRP and anomalous component behavior
- Regular updates to Cyber IDS help prioritize and mitigate system vulnerabilities
- Cyber Survivability Risk Assessments identify CSRC, assess the adversary cyber threat, prioritize vulnerabilities, and identify a POA&M to an operational CSRP
- Assured Code Delivery maintains known-good system state and configurations

For more information, visit **shift5.io.**

SHIFT5