Raytheon, an RTX Business

CADS
Cyber resiliency for communication buses

Commercial and military aircraft and ground vehicles are more open and connected than ever before. However, these technological advancements also leave them vulnerable to cyberattacks. Most of these mission- and safety-critical platforms use unsecured communication buses designed and built before the rise of cyberattacks and have few modern defenses.

Aircraft cyber protection

Potential threat vectors for modern airframes, ground vehicles, satellites and weapons systems include over-the-air cyberattacks, compromised components delivered through the supply chain and even lateral compromises introduced by infected maintenance equipment.

Any one of these attacks could lead to a direct threat to mission-critical systems in the form of denial of service, unauthorized access to system components, equipment failure or having equipment to deliberately send incorrect information.

Raytheon's CADS directly addresses these threats and increases the cyber resiliency of mission-critical platforms by analyzing internal communication traffic for indications of cyberattack and providing operators with real-time alerts of anomalous behavior and potential compromise.

The CADS solution

CADS is a result of a customer-inspired research and development effort into providing commercial and military pilots with a cyberattack warning system. It is focused on providing real-time anomaly and intrusion detection for the 1553 bus, with a modular design that enables additional protocols such as MIL-STD-1760, ARINC 429 or a controller area network bus to be incorporated with minimal effort. The analytics tools provide long-term performance and cross-fleet analysis of cyber trends.

The system melds Raytheon's cyber expertise with its in-depth understanding of mission-critical system design and is fully tailorable to support the unique needs of a specific platform.

This solution can be procured through Raytheon's GSA IT Schedule 70 contract #GS-35F-204GA.

KEY CAPABILITIES

- Analyzes 1553 data bus traffic in real time for cyberattacks and indicators of compromise.
- Records all communication bus traffic for post-action analysis.
- Supports MIL-STD-1553.
- Modular design enables additional communication protocols to be added with minimal effort.
- Combines machine learning, heuristics and signature approaches to identify cyber-based anomalies.

CADS

How it works

CADS can be deployed as a stand-alone solution running on dedicated hardware or alongside other applications running on existing hardware in order to meet rigorous size, weight and power constraints.

The four main features of CADS provide comprehensive data bus protection through:

- Platform baselining. Using the platform's interface control document and recorded traffic, CADS builds a baseline of normal component communication and behavior.
- Anomaly detection. CADS analyzes all communication traffic for signs of anomalous activity. Whether it is due to a maintenance issue or cyberattack, if a component's behavior deviates from the baseline, CADS will detect it, no matter which attack avenue is taken or attack surface used.
- Real-time alerting. CADS has the ability to send out customizable, real-time alerts and notifications detailing detected anomalies, allowing pilots, ground crew and maintainers to make informed decisions when handling issues seen during a mission.
- Logging and post-mission analysis. CADS provides an easy-to-use interface for viewing and managing all of the data collected. Logs can be compared across fleets, highlighting expected and unexpected communication patterns. Issues and component behavior can be tracked over time, allowing for faster detection of potential faults and predictive maintenance.

CADS

Contact
Raytheon, an RTX Business
1100 Wilson Blvd.
Arlington, VA 22209
cyber.services@rtx.com

Raytheon
An RTX Business

www.RTX.com/cyber