AVIATION WHITEPAPER

Using NIST CSF to Maintain

CYBER RESILIENCE IN AIRCRAFT SYSTEMS

SHIFT5

Introduction

At any given time, thousands of massive, complex supercomputers travel at 450 knots 36,000 feet above our heads. Tens of thousands more are on the ground awaiting passengers or maintenance. These marvels of interconnected operational and digital technologies are the backbone of an industry that supports over $3.5 trillion in global economic activity (4.1% of global GDP), transports over four billion passengers and 61 million tons of freight per year, and supports over 11 million direct and 75 million indirect jobs around the world.

With so much on the line, it's easy to understand why commercial aircraft need protection from cyber attacks, but it's difficult to understand why they don't have that protection. This eBook discusses the importance of comprehensive observability of the components and networks found on today's digital, connected aircraft to get ahead of risks and eventual new regulations for these types of aircraft. It also explores how and why operators should apply modern principles of IT cybersecurity, like the NIST Cybersecurity Framework (CSF), to connected air fleets to help ensure the safety and security of air travel.

Modern aircraft are flying supercomputers.

As anyone in the aviation industry knows, change happens gradually here, including mindsets. Some still think of commercial aircraft as simple machines because there had been little operational reason—and even less regulatory reason—to think otherwise. That all changed quickly in 2009 with the introduction of the first fully e-Enabled (i.e., connected) aircraft, the Boeing 787 Dreamliner.

Key concepts from modern IT security, Since the Dreamliner, IP-based connectivity has become the backbone of communications for onboard systems and components. Fully-connected, fly-by-wire aircraft rely on modern computer systems to control physical motors and servos. Electronic Flight Bags (EFBs) replaced mounds of paperwork and manuals. Ethernet-based networks replaced or augmented serial-based aircraft networks. Wireless passenger and crew networks that provide services from entertainment to maintenance. Wireless Groundlink systems provide operators with a low-cost IP over cellular alternative to traditionally high-cost ACARS legacy infrastructure.

In addition to an aircraft's core network and computer, today's modern aircraft feature connected systems like

- Wireless Local Area Network units for passengers and crew
- Aircraft Communications Addressing and Reporting
- System (ACARS), and Very High Frequency (VHF)
- Data Link Mode 2 (Basic)
- Broadband satellite communications
- Advanced flight deck technologies, including more software
- Electronic flight bags, including electronic logbooks, onboard performance tools, and document browsers
- Video surveillance systems
- Wireless maintenance, including loadable software airplane parts, aircraft health and condition monitor, continuous logging, configuration management

Modern aircraft need modern cybersecurity.

Most cybersecurity professionals look to the NIST Cybersecurity Framework (CSF) for guidance regarding the security of an organization's IT infrastructure. It uses a common structure of globally-recognized cybersecurity strategies that work effectively today and is equally applicable to and foundational for securing our nation's critical transportation infrastructure.

Key concepts from modern IT security, such as those found in the NIST CSF, can help operators take critical first steps to protect their aircraft from cyber attacks. Here are the five functions of the NIST CSF and an explanation of the categories and subcategories where the Shift5 platform can help you apply these principles to commercial aircraft cybersecurity best practices.

Identify

Begin with gaining observability into the aircraft's networks, systems, and connected components. For example, in the case of AC 119-1's ANSP requirements, this means taking log files from the aircraft, analyzing them for anomalies, and storing them for compliance purposes. Beyond log files, operators should monitor, capture, and normalize operational data from their aircraft, including avionics and serial bus data.

But aircraft are constantly moving, and gaining real-time access to all aircraft data between flight cycles can be challenging. Wireless gatelink systems can provide some data but only do so today while the aircraft is on the ground. This reduces the ability to collect and monitor and detect data in real time, and also narrows the scope of the data to a subset of critical data, rather than the full scope of the data being generated by the aircraft.

Category	Subcategory	How the Shift5 Platform Helps
Risk Assessment (ID. RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	**ID.RA-1:** Asset vulnerabilities are identified and documented	Monitors network traffic on aircraft, including data traversing serial networks, to identify and record vulnerabilities.
	ID.RA-2: Cyber threat intelligence is received from information-sharing forums and sources	Uses threat intelligence feeds from multiple sources, including open-source, paid, and proprietary threat research.
	ID.RA-3: Threats, both internal and external, are identified and documented	Using the threat intelligence from ID.RA-2, monitors network traffic on aircraft, including data traversing serial networks, to identify and record threats.
	ID.RA-4: Potential business impacts and likelihoods are identified	Calculates severity of the vulnerability or threat based on business impact.
	ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk	Uses risk modeling provided by manufacturers, users, and proprietary research to calculate the likelihood and impact of a particular risk.
	ID.RA-6: Risk responses are identified and prioritized	Uses risk modeling provided by manufacturers, users, and proprietary research to prioritize risk.
Risk Management Strategy (ID.RM): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	**ID.SC-1:** Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders	Identifies assets and can identify and block the installation of corrupted LRU firmware.
	ID.SC-2: Suppliers and third-party partners of information systems, components, and services are identified, prioritized, and assessed using a cyber supply chain risk assessment process	Identifies assets and can identify and block the installation of corrupted LRU firmware.
	ID.SC-3: Contracts with suppliers and third-party partners are used to implement appropriate measures designed to meet the objectives of an organization's cybersecurity program and Cyber Supply Chain Risk Management Plan.	Uses risk modeling provided by suppliers and third-party partners to calculate the likelihood and impact of a particular risk.
	ID.SC-4: Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations.	Shift5 routinely undergoes assessments and can provide a report of those assessments to help customers meet their obligations.
	ID.SC-5: Response and recovery planning and testing are conducted with suppliers and third-party providers	Shift5 partners with customers to develop and meet their appropriate disaster recovery goals.

Protect

With access to your fleet's operational and security data, you now need to understand it better by normalizing and analyzing the data, then prioritizing any identified risks. One recommendation is to break down data by its potential impact. For example, prioritize data coming from flight-critical systems like full authority digital engine controls (FADEC) or from passenger comfort and entertainment systems.

From there, stack ranking the severity of any risks and automatically assigning responsibility to an appropriate owner or team of owners is a best practice for proactively identifying and mitigating risks and vulnerabilities. Risks might not share the same severity or the same owners, so it's essential to know which should be looked at first and by whom.

However, accurately identifying and scoring risks requires a comprehensive understanding of information from more than one source. For example, correlating information found in core network log files with Flight Data Recorder records (ARINC 647), or data from Onboard Boeing Electronic Distribution Systems (OBEDS), can surface unique insights that help more accurately detect, score, and assign anomalies.

Category	Subcategory	How the Shift5 Platform Helps
Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.	**PR.DS-2:** Data-in-transit is protected	Monitors data moving across a network for anomalous behavior. Encrypts data moving across the Shift5 platform's internal components.
	PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity	Performs an integrity check on files moved from a supported vehicle to the Shift5 cloud. Shift5 also performs integrity checks of its own software deployed at customer sites.
	PR.DS-8: Integrity checking mechanisms are used to verify hardware integrity	Fingerprints data from devices to identify components on a supported vehicle.
Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures.	**PR.MA-1:** Maintenance and repair of organizational assets are performed and logged, with approved and controlled tools	Allows customers to add notes in the interface for an asset to indicate planned maintenance for a component.
	PR.MA-2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access	To the extent data about maintenance events is broadcast across a Shift5-monitored network, Shift5 can catalog those activities and indicate which, if any, are anomalous.
Protective Technology (PR.PT): Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.	**PR.PT-1:** Audit/log records are determined, documented, implemented, and reviewed in accordance with policy	To the extent that data about login events is broadcast across a Shift5-monitored network, Shift5 can log that activity.
	PR.PT-4: Communications and control networks are protected	Enables customers with visibility into and detection of anomalous communications.

Detect

Operators must also catch events outside of manageable risk, like targeted attacks. Solutions you deploy should continuously monitor aircraft network data in real-time using behavioral heuristics and advanced statistical methods to detect even the slightest anomalies that could indicate compromise. They should also provide context about an event to give analysts the information they need to understand the event thoroughly and to help them reduce their mean time to respond.

For example, how critical is the affected component? Can the component or system rely on backups until someone can address the event? With an automated process to detect suspicious behavior or unauthorized change in aircraft state, you can react and respond to threats more quickly to protect your assets and the flying public.

Category	Subcategory	How the Shift5 Platform Helps
Anomalies and Events (DE.AE): Anomalous activity is detected and the potential impact of events is understood.	**DE.AE-1:** A baseline of network operations and expected data flows for users and systems is established and managed	Analyzes data to develop models for expected patterns and behaviors and alerts customers if deviations are detected.
	DE.AE-2: Detected events are analyzed to understand attack targets and methods	Provides managed services to help customers understand threats and to assist with threat investigations.
	DE.AE-3: Event data are collected and correlated from multiple sources and sensors	Provides a mechanism for integrating customer data from multiple sources.
	DE.AE-4: Impact of events is determined	Reports severity of an anomalous event, based on its potential impact, that the customer can integrate into their own risk modeling.
	DE.AE-5: Incident alert thresholds are established	Enables customers to set their own threshold and to determine when they want to be alerted.
Security Continuous Monitoring (DE.CM): The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures	**DE.CM-1:** The network is monitored to detect potential cybersecurity events	Monitors supported networks continuously for anomalous data or behaviors that could indicate a cybersecurity event.
	DE.CM-4: Malicious code is detected	Detects malicious code based on anomalies in data transmitted on supported networks.
	DE.CM-5: Unauthorized mobile code is detected	Detects unauthorized mobile code based on anomalies in data transmitted on supported networks.
	DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed	Detects unauthorized access based on anomalies in data transmitted on supported networks.
Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.	**DE.DP-3**: Detection processes are tested	Provides deployment services that include testing the platform in the customer's environment and tunes the platform if adjustments are necessary.
	DE.DP-4: Event detection information is communicated	Presents events in the Shift5 portal and can alert via email and text, depending on a customer's configuration.
	DE.DP-5: Detection processes are continuously improved	Provides professional services to use historical detection information to improve the detection capabilities of the platform.

Respond

Response to potential threats to commercial aircraft must be swift, and it must be thorough. How your team handles response can provide a critical time advantage to protect backup systems before they become compromised. Solutions you deploy should ease or even automate the forensic assessment of how an event occurred and the responsible adversary. Sometimes you may need to share information beyond your airline operations with external parties like the Aviation ISAC or FAA. In those cases, it's critical to have solutions in places that can package and deliver information about events quickly and concisely.

Category	Subcategory	How the Shift5 Platform Helps
Analysis (RS.AN): Analysis is conducted to ensure effective response and support recovery activities.	**RS.AN-1:** Notifications from detection systems are investigated	Provides threat detection information inside the Shift5 platform and can export data to a customer's preferred investigation platform.
	RS.AN-3: Forensics are performed	Provides threat detection information inside the Shift5 platform and can export data to a customer's preferred forensics platform.
Mitigation (RS. MI): Activities are performed to prevent the expansion of an event, mitigate its effects, and resolve the incident.	**RS.MI-2:** Incidents are mitigated	Provides threat detection information inside the Shift5 platform, including granularity needed to understand the full extent of an incident, and can export data to a customer's preferred enforcement platforms.

Recover

Lastly, you need to get operations back online after an event. But that's not as easy as flipping a switch and involves much more than simply restoring capabilities or services. Recovery includes debriefing your executive and internal business teams, potentially regulatory agencies, and manufacturers about any events impacting flight operations or safety. For that reason, it's important you can rely on the solutions you deploy to provide clear, concise information everybody can understand. This information will also be essential later for post-event assessments and training teams on how to respond to similar threats in the future and is a critical part of maintaining the public's trust.

About Shift5

Shift5 is the onboard OT data and cybersecurity company for planes, trains, and tanks. Created by founding members of the U.S. Army Cyber Command who pioneered modern weapons system cyber assessments, Shift5 defends military platforms and commercial transportation systems against malicious actors and operational failures. Customers rely on Shift5 to detect threats and maintain the readiness and availability of today's planes, trains, tanks, and weapons systems and tomorrow's next-generation vehicles. For more information, visit shift5.io.

Next Steps

Every new generation of aircraft includes increasingly complex and connected technologies. As these aircraft replace their predecessors in your fleet, it becomes increasingly important to gain observability into the onboard components and networks that power them, and to seize the opportunity to capture and use the valuable data they create. **To learn more about the possibilities, go to shift5.io to schedule a briefing.** Classified briefings are available to organizations with the proper security clearance.

SHIFT5

shift5.io

"Using NIST CSF to Maintain Cyber Resilience in Aircraft Systems"
Version 2.0 // Nov 2022