Aviation Business Solutions

The Aircraft Network Security Program (ANSP)

Newer Planes Warrant Newer Plans

Introduction

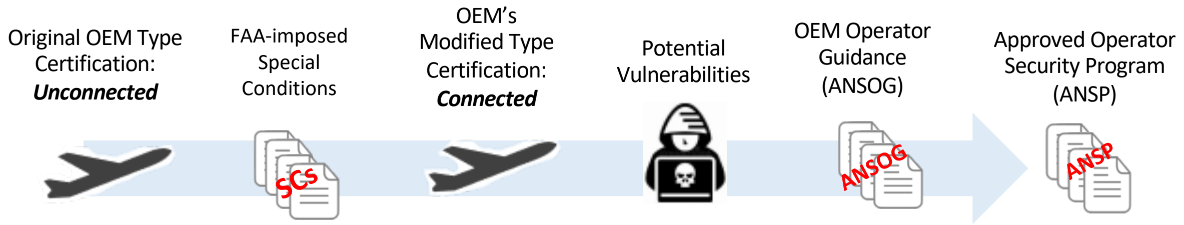
According to the International Civil Aviation Organization (ICAO), passenger transport is predicted to reach approximately 10 billion by 2040, up from roughly 4 billion in 2018. Protection and safety from cyberattacks is an imperative for the industry.

Though policies, processes, and procedures for the protection of *ground-based information* and network systems may exist, if protection of *avionics systems on the airplane* are not considered in the security program, the organization may be susceptible to operational risks.

Modern avionics systems have come a long way from traditional information security networks, whose initial purpose was to enable communication internally amongst onboard systems. Modern avionics systems have one or more onboard networks connected to external networks, either airborne or ground-based, that enable electronic data flow between the aircraft, other aircraft, flight crews, maintenance crews, air traffic controllers, and even passengers, designating them as e-Enabled. However, while the industry's evolution from legacy standards to modernized connected aircraft (i.e. e-Enabled) design has created much-needed efficiencies, it has also introduced new security requirements. Traditional aircraft information networks were only equipped for physical connectivity and were certified accordingly. To address cybersecurity risks of such novel design features, the Federal Aviation Authority (FAA) imposed Special Conditions (SCs) that retroactively modified the original type certification regulations for these legacy aircraft.

Additionally, Boeing released its Universal Airplane Network Security Operator Guidance (UANSOG), created specifically to address e-Enabled aircraft security, as it pertains to internal networks of Boeing aircraft models, and external connectivity. The UANSOG outlines security objectives for aircraft operators to develop an Aircraft Network Security Program (ANSP) and serves as a means of compliance with SCs. Not only does the U.S. FAA require an approved ANSP via issuance of an operations specification (OpSpec), EASA, ICAO, and other industry bodies are moving in the same direction. This white paper describes how an ANSP securely integrates an organization's aircraft internal networks, external connections, and cybersecurity as it relates to continued airworthiness.

Evolution of Connected Aircraft, Security Risks, and Regulatory Requirements


Original OEM Type Certification: ***Unconnected***
FAA-imposed Special Conditions
SCs
OEM's Modified Type Certification: ***Connected***
Potential Vulnerabilities
OEM Operator Guidance (ANSOG)
ANSOG
Approved Operator Security Program (ANSP)
ANSP

Risks of Connectivity

Aircraft connectivity will continue to evolve for operational efficiency, safety, and security, so accounting for all connections to the aircraft is vital to identifying any vulnerabilities. Boeing's Chief Security Officer, Richard Puckett, issued a caution about the influx of interconnected avionics systems saying, "Increasing requests for sensors on almost every working part of the aircraft makes it more efficient, but it also makes it more vulnerable because anything that sends or receives a signal can be hacked."

Traditional information technology (IT) systems, using the same hardware and software components, are subject to vulnerability exploits that result in "billions of dollars in damages," as noted by the Government Accountability Office; avionics system components for e-Enabling are not exempt.

For example, airplanes have become increasingly dependent on commercial off-the-shelf hardware and software. While not all aircraft software can be updated, software is a common target, especially outdated software. As with other wi-fi-based connections, airplane software synchronization via ground-based Gatelink systems at airports require diligent security protocols. Interference with such systems could result in delays or malfunction to maintenance, baggage, and other related operations.

To further examine the significance of hardware and software risks, operators must analyze internal supply chains, as vulnerabilities can be exploited at multiple touchpoints within the airline operations ecosystem. Part-loading devices can be malware-compromised and sent directly from vendors to operators. Upon receipt, operators can unwittingly connect compromised devices to ground systems or aircraft. Furthermore, various communications networks and surveillance systems that utilize satellite navigation technologies can extend the potential attack surface.

> *"Increasing requests for sensors on almost every working part of the aircraft makes it more efficient, but it also makes it more vulnerable because anything that sends or receives a signal can be hacked."* - Boeing CSO

Any of these scenarios can lead to denial of service, ransomware, or other attacks, resulting in costly operational disruptions, including regulatory and reputational implications. The results of such incidents could cause reduced customer satisfaction or damage to the company brand. There are many other scenarios that highlight consequences of insecure systems, driving the requirement for an FAA-approved ANSP for the issuance of an OpSpec. ANSP compliance is prescribed in Advisory Circular (AC) 119-1A.

Mitigating Risks: The ANSP

By closely adhering to the FAA's ANSP requirements and industry best practices, customers can develop and execute an effective program to support Entry into Service and/or continued airworthiness efforts. As an example of where to start, the FAA adopted the National Institute of Standards and Technology's (NIST) Cybersecurity Framework as a fundamental component of an operator's organization risk management process, requiring aircraft-related systems, components, and associated risks to be diligently assessed. NIST and other cybersecurity frameworks include similar fundamentals of securing IT systems. Those fundamentals follow a logical sequence of detecting potential risks, and then deploying protection, identification, response, and recovery protocols. Aligning with these frameworks and applying them to aircraft and airline ground-based systems, the FAA issued Advisory Circular (AC) 119-1A defines a means of compliance for an approved ANSP. For non-U.S. operators, regulatory requirements and standards vary, but are moving in a similar direction.

The ANSP: A Process

Without a thorough ***organizational risk assessment***, organizations could have gaps in their operation that negatively impact their operations. Once risks are identified in the assessment, an ***Incident Response Plan (IRP)*** outlines processes, procedures, and personnel assignments that will restore normal operations. Some customers have sought non-aviation related, third-party services to evaluate the effectiveness of their IRPs. Effective airline IRPs often require additional training for IT-staff to ensure they are familiar with strategic objectives of the airline operation.

Other requirements for an ANSP include technology and processes that ensure ***e-Enabled part security*** and the ability to ***manage aircraft logs***. Yet, it is not always cost-effective for operators to hire and retain the required hybrid of IT and Avionics expertise. A key component of securely managing software airplane parts for e-Enabling is implementing Public Key Infrastructure. Software authenticity and integrity must be maintained by utilizing digital signatures, then encryption measures can be implemented to ensure confidentiality. Operators are required to develop a security log file policy to define how security events are managed. Supplemental training and services should be acquired as needed. Often, airlines will download aircraft logs, but are unable to interpret the complex data elements of various systems and sensors. Assistance from the OEM may be required.

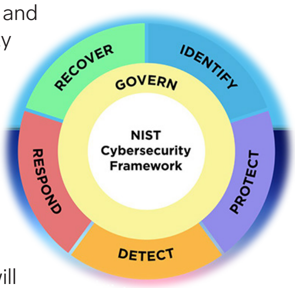


Table 1 summarizes typical ANSP mitigation strategies.

Table 1: Risk Mitigations Enabled by an ANSP

Risk	ANSP Mitigation Strategy
Unawareness of vulnerabilities	Risk Assessment
Lack of cyber breach recovery plan	Incident Response Plan
Network traffic breach	Airplane Log File Monitoring
Personnel response readiness	Table-Top Exercises

Furthermore, process-and-procedure mapping to any existing IT policies should be assessed. New and supplemental policies and procedures may need to be established. An operator in Central Asia noted their existing policies were applicable only to their general IT computer networks. The operator's leadership directed staff to either create new policies for e-Enabled part and log file management or integrate those policies with their existing IT policies. Simply completing a documented checklist of requirements will not suffice for regulatory compliance; the FAA requires substantial evidence of trained staff and a functional program to earn their stamp of approval. An ANSP must outline governing policies and procedures and account for how the organization will take action to reduce cyber risk in its e-Enabled aircraft environment before regulators will approve the operation as safe and airworthy.

Conclusion

Avionics system connections will continue to advance with the progression of technology, and each new efficiency will result in added risks of cyber threats. Implementing protective measures that enable confidentiality, integrity, and availability of the systems is critical to risk mitigation. As regulators work diligently to provide an acceptable means of compliance for newer airplanes, it is the operator's responsibility to establish associated security measures through the development and execution of an ANSP.

References and further reading

FAA Regulations:

- 14 CFR Part 25, Airworthiness Standards: Transport Category Airplanes
- 14 CFR Part 26, Continued Airworthiness and Safety Improvements for Transport Category Airplanes

FAA Advisory Circular (AC) 119-1A
https://www.faa.gov/documentLibrary/media/Advisory_Circular/AC_119-1A.pdf

DO-355A/ED-204A, Information Security Guidance for Continued Airworthiness
https://standards.globalspec.com/std/14335560/rtca-do-355

Boeing Document: D925W704-04, ANSOG Rev B (Contact Boeing for availability)

Government Accountability Office (GAO)-21-86, Aviation Cybersecurity: FAA Should Fully Implement Key Practices to Strengthen Its Oversight of Avionics Risks
https://www.gao.gov/products/gao-21-86

MDPI, Cyber-Security Challenges in Aviation Industry: A Review of Current and Future Trends
https://www.mdpi.com/2078-2489/13/3/146

National Institute of Standards and Technology (NIST) Cybersecurity Framework
https://www.nist.gov/cyberframework

Resecurity, The Aviation and Aerospace Sectors Face Skyrocketing Cyber Threats
https://www.resecurity.com/blog/article/the-aviation-and-aerospace-sectors-face-skyrocketing-cyber-threats

World Economic Forum. Cybersecurity in aviation: Building a resilient future
https://www.weforum.org/impact/cybersecurity-in-aviation/

Biography

Denisha Ward-Swanigan is a Certified Information Systems Security Professional, adding her 25 years of cyber-security experience to the Aviation Business Solutions (ABS) team. Denisha specializes in security of information and information systems with an emphasis in cyber security governance, risk, and compliance.

A veteran of the United States Air Force, Denisha served as Installation Command Chief at the 412th Test Wing, Edwards Air Force Base, leading personnel in the execution of developmental test and evaluation programs.

Today, Denisha volunteers as a mentor for the Veterans Cybersecurity Group and The National Society of Leadership and Success.

To learn more about Denisha's work and discover how Aviation Business Solutions can help your operation, please visit services.boeing.com/aviation-business-solutions-consulting.

About Boeing Aviation Business Solutions

Aviation Business Solutions (ABS) was established by Boeing Global Services in 2011 in response to growing requests from customers for strategic and technical advisory services. ABS recruited former airline/aviation executives, licensed/certified pilots, dispatchers, mechanics, cyber security professionals and engineers to provide improved operational efficiency solutions through applied data-analytics and disciplined cost control. By combining Boeing's industry-leading tools and subject matter expertise with global customer insight and a growing list of subsidiaries and partners, ABS provides consulting solutions to your most pressing needs. Aviation Business Solutions currently has five fleet agnostic practice areas:

- Aviation Operations
- Maintenance & Engineering
- Information Technology & Cybersecurity
- Military Aviation
- Results Management

Contact:
For more information on Aviation Business Solutions
Email: aviationbusinesssolutions@boeing.com