FAA AIRCRAFT SYSTEMS INFORMATION SECURITY PROTECTION OVERVIEW

Peter Skaves, Chief Scientific & Technical Advisor for Advanced Avionics, FAA, Renton, WA

Background (FAA)

The Federal Aviation Administration (FAA) has various lines of business and coordinates security activities with other organizations such as the Department of Homeland Security and Transportation and Security Administration. All aspects of security are addressed by various organizations including but not limited to physical security, infrastructure, Aircraft Systems Information Security Protection and aircraft operations. The scope of this paper is to address electronic Aircraft Systems Information Security Protection. For completeness the following is a brief overview of the FAA origin and scope.

The FAA is the national aviation authority of the United States (U.S.), and as an agency of the U.S. Department of Transportation (DOT), it has the authority to regulate and oversee all aspects of American Civil Aviation. The Federal Aviation Act of 1958 created the organization under the name Federal Aviation Agency. The agency adopted its current name in 1966 when it became a part of the U.S. DOT.

The FAA is divided into four "lines of business" (LOB) [1]. Each LOB has a specific role within the FAA as follows:

1) Airports (ARP) -- Plan and develop projects involving airports, overseeing their construction and operations.
2) Air Traffic Organization (ATO) --The primary duty is to safely and efficiently move air traffic within the National Airspace System (NAS). ATO employees manage air traffic facilities including Airport Traffic Control Towers and Terminal Radar Approach Control Facilities.
3) Aviation Safety (AVS) -- Is responsible for aeronautical certification of personnel and aircraft, including pilots, airlines, and mechanics.
4) Commercial Space Transportation (AST) -- Ensures protection of U.S. assets during the launch or reentry of commercial space vehicles.

Abstract

The purpose of this paper is to provide an overview of Aircraft Systems Information Security Protection (ASISP) from an FAA AVS perspective. Increased aircraft connectivity to aircraft systems and networks to Air Traffic Service (ATS) providers, including NextGen and public networks (e.g., Internet), may require additional security risk considerations. When the aircraft connects electronically to the infrastructure the safety, performance and interoperability requirements of both the aircraft and the systems that the aircraft are connected to should be considered.

The FAA solution set includes safety, security, and environment. Improving safety, security, and the environment is an inherent part of the FAAs overall mission and is embedded in the activities of individual programs agency-wide. This solution set involves activities directly related to ensuring that NextGen systems contribute to steadily reducing risks to safety and information security while mitigating adverse effects on the environment and ensuring environmental protection that allows sustained aviation growth [2].

Security issues related to individuals that could gain physical access to aircraft to cause malicious damage to the aircraft systems (e.g., improper maintenance procedures, cutting wire bundles, etc.) are not addressed in this paper. Physical aircraft security is enforced by the Department of Homeland Security (DHS) and Transportation and Security Administration (TSA) [3].

This paper is not a FAA official document and is the opinion of the author only. The pictures and figures contained in this paper were obtained from various internet sites, including the FAA NextGen program office. A list of acronyms and references used herein are included in the back of this paper.

Security Definitions

The terms aircraft network security, systems security, and cyber-security are not precisely defined and are often used interchangeably, which may cause confusion as to their intended meaning. The FAA Transport Airplane Directorate (TAD) uses the term network security in the publication of Special Conditions and Issue Papers [4, 5]. Aircraft network security includes the data link, internal aircraft data bus connections, switches, and routers. Aircraft system security risk assessments are required in combination with network security. This paper proposes to use the term Aircraft Systems Information Security Protection (ASISP) which includes aircraft networks and systems. Cyber-security is the term used for potential electronic security threats which may require ASISP. Figure 1 provides additional information on security terminology.

Figure 1 – Piecing Together Security Terminology

Aircraft Security Regulations

Current Title 14 Code of Federal Regulations (14 CFR) regarding security are §121.538 and §129.25 "Airplane Security", §121.313 "Miscellaneous Equipment" (Flight Deck Doors), §129.28 "Flight Deck Security", and §25.795 "Security Considerations". These regulations do not specifically address security requirements for networks and aircraft systems. This could result in non-standardized agreements between the various applicants and the various regulatory agencies for developing an acceptable process and means of compliance for ensuring safe, secure, and efficient aircraft systems certification.

Certain airborne avionics manufacturers and operators are adding ASISP controls for certain applications that are not specifically required by FAA regulations. ASISP controls that are implemented in the aircraft systems design are part of the aircraft systems "intended function" and must meet 14 CFR §xx.1301 and §xx.1309.

FAA Special Conditions, Issue Papers and Policy Statement

Until new regulations on security are published, certain aircraft avionics architectures may require a FAA Special Condition on security for systems and networks protection from unauthorized external and internal access. FAA Special Conditions are airplane model specific rules and are not general public rules. When required, a FAA Special Condition is applied for each specific aircraft model type. These special conditions contain the additional safety standards that the FAA Administrator considers necessary to establish a level of safety equivalent to that established by the existing airworthiness standards.

When issuance of a special condition is required, the proposed rule is published in the Federal Register for public comment. A companion issue paper (project specific policy or guidance on meeting the regulatory standard) that describes the FAA expectations for compliance to address cyber-security vulnerabilities and ASISP is also issued to the applicant. The ASISP Special Conditions and companion issue paper covers regulations, policy, and guidance used to address cyber-security threats.

14 CFR does not specifically define how we address electronic cyber-security vulnerabilities for any aircraft operating in the U.S. NAS. To address this issue, the Design, Manufacturing, and Airworthiness Division issued policy statement PS-AIR-21.16-02 "*Establishment of Special Conditions for Cyber Security*", which describes when issuance of special conditions are required for aircraft systems that directly connect to external services or networks under specific conditions.

Aviation Rulemaking Advisory Committee (ARAC) for ASISP

As a result of the December 18, 2014 ARAC meeting, the FAA assigned and ARAC accepted a task establishing the ASISP working group [6]. This new task will provide recommendations regarding ASISP rulemaking, policy, and guidance on best practices for airplanes and rotorcraft, including both certification

and continued airworthiness. The issue is that without updates to regulations, policy, and guidance to address ASISP, aircraft vulnerabilities may not be identified and mitigated, thus increasing exposure times to security threats. In addition, a lack of ASISP specific regulations, policy, and guidance could result in security related certification criteria that are not standardized and harmonized between domestic and international regulatory authorities. Unauthorized access to aircraft systems and networks could result in the malicious use of networks and loss or corruption of data (e.g., software applications, databases, and configuration files) brought about by software worms, viruses, or other malicious entities.

The ASISP Working Group is tasked to:

1) Provide recommendations on whether ASISP-related rulemaking, policy, and/or guidance on best practices are needed and, if rulemaking is recommended, specify where in the current regulatory framework such rulemaking would be placed.
2) Provide the rationale as to why or why not ASISP-related rulemaking, policy, and/or guidance on best practices are required for the different categories of airplanes and rotorcraft.
3) If it is recommended that ASISP-related policy and/or guidance on best practices are needed, specify (i) which categories of airplanes and rotorcraft such policy and/or guidance should address, and (ii) which airworthiness standards such policy and/or guidance should reference.
4) If it is recommended that ASISP-related policy and/or guidance on best practices is needed, recommend whether security-related industry standards from Aeronautical Radio Incorporated (ARINC), Federal Information Processing Standards (FIPS), International Standards Organization (ISO), National Institute of Standards and Technology (NIST), Radio Technical Commission for Aeronautics (RTCA), Society of Automotive Engineers (SAE) Aerospace Recommended Practices (ARP) 4754a and/or SAE ARP 4761 would be appropriate for use in such ASISP-related policy and/or guidance.
5) Consider European Aviation Safety Agency (EASA) requirements and guidance material for regulatory harmonization.
6) Develop a report containing recommendations on the findings and results of the tasks explained above.
    a) The recommendation report should document both majority and dissenting positions on the findings and the rationale for each position.
    b) Any disagreements should be documented, including the rationale for each position and the reasons for the disagreement.
7) The working group may be reinstated to assist the ARAC by responding to the FAA's questions or concerns after the recommendation report has been submitted.

Schedule - The recommendation report should be submitted to the FAA for review and acceptance no later than fourteen months from the date of the first working group meeting which is currently planned for late April, 2015.

ATS Service Providers

ATS providers include NextGen capabilities and are managed by the U.S. federal agencies or their international equivalents and provide secure “authorized services”. FAA ATS providers have been certified and accredited in accordance with the Federal Information Security Management Act (FISMA), FAA Order 1370.86 “AVR Information System Security Protection” and the “FAA Information System Authorization Handbook”. In order to evaluate potential aircraft ASISP vulnerabilities the connectivity between the ATS providers and the aircraft need to be considered.

Other international regulatory authorities that do not use the same security processes and standards as the U.S. may require additional end-to-end aircraft/ATS provider security risk assessments. This could result in additional security requirements for aircraft that operate in certain international airspace.

Examples of ATS provider connectivity to aircraft systems and networks include the following:

- Global Positioning Systems (GPS)

- Ground Based Navigation Aids (NavAid) (e.g., Distance Measuring Equipment (DME), Very High Frequency (VHF) Omni-Directional Radio-range (VOR)) which provide range and bearing information to the aircraft
- Instrument Landing Systems (ILS) (Localizer and Glideslope for lateral and vertical guidance)
- Voice Communication (VHF, High Frequency (HF), and Satellite Communications)
- Aircraft Communication Addressing and Reporting System (ACARS)
- Controller Pilot Data Link Communications (CPDLC) (e.g., text messages between the Air Traffic Control (ATC) controller and flight crew)
- NextGen Data Communications
- Automatic Dependent Surveillance – Broadcast (ADS-B)

An important consideration is that the ATS provider boundary ends at the transmission and does not include aircraft antennae, receiver, display unit, and airplane interfaces. These additional interfaces should be addressed by aircraft certification, maintenance, and operational requirements.

GPS is funded and controlled by the U.S. Department of Defense (DOD) [7]. GPS provides specially coded satellite signals that can be processed in a GPS receiver, enabling the receiver to compute position, velocity, and time. The FAA AVS service has published various advisory circulars (ACs) and technical standard orders (TSOs) for the use of GPS in civil aircraft. These FAA documents contain requirements to detect and mitigate certain GPS failure modes. Security controls are contained in the GPS constellation architecture (refer to figure 2), including health monitoring and fault reporting. Commercial transport category aircraft use GPS in combination with other navigation sources (e.g., ground based navigation aids) to provide navigation position information during GPS outages.

Multi-constellation Global Navigation Satellite Systems (GNSS) receiver technology (e.g., combined GPS and GLONASS, GPS/Galileo) is one of the areas of ongoing research and standards development.

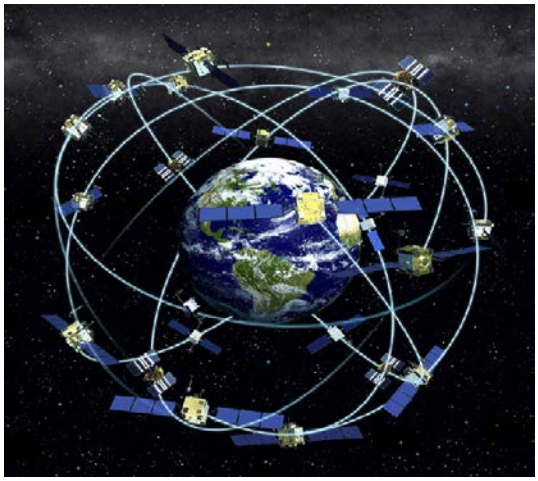

Figure 2 - GPS Satellite Constellation

ACARS Security Considerations

The classic (and almost universally used) ACARS protocol, apart from basic message integrity checks, has no provisions in the protocol for security of content or authentication of sender or receiver. Most aircraft communication management systems are not equipped to use ACARS encryption. The basic questions that need to be addressed during the compliance review are as follows:

1) Is ACARS, when functioning as intended, sufficiently safe to use when considering the possibility of unauthorized access?
2) Does the ACARS specification, when operating as intended in the cyber-security environment, contain correct and complete requirements to work safely and reliably?
3) Do systems that implement ACARS communication functions contain any vulnerability that would allow hackers with unauthorized access to ACARS message transmissions to disrupt or otherwise interfere with airplane systems by causing unintended or functional failures?

The ACARS security risk assessment identifies vulnerabilities and allows credit for pilot-in-the-loop operational procedures and cross checks to mitigate these vulnerabilities. As an example, a security risk assessment was conducted on the flight plan information that was transmitted from an Airline Operations Center (AOC) to a Control Display Unit (CDU) of a Flight Management Computer System (FMCS). The flight crew is required to review the information on the CDU display before manually

transferring the information from the CDU to the FMCS. After the new flight plan information is uploaded, the flight crew is required to use aeronautical charts to assist in navigation of the aircraft.

Using these charts and other tools, pilots are able to determine their position, safe altitude, best route to a destination, navigation aids along the way, alternative landing areas in case of an inflight emergency, and other information such as radio frequencies and airspace boundaries. Charts used for Instrument Flight Rules (IFR) contain an abundance of information regarding locations of waypoints, known as "position fixes" which are defined by measurements from electronic ground based navigation aids or GPS, as well as the routes connecting these waypoints. The flight crew is able to manually update the flight planning information at any time during flight and is able to disconnect this automatic navigation function used to provide steering commands to the autopilot if deemed necessary.

In the U.S. NAS we have excellent radar surveillance which enables Air Traffic Controllers to monitor aircraft conformance to assigned flight plan information. This surveillance information is independent of the aircraft navigation function. In summary, these operational procedures and flight crew cross checks address and mitigate security issues associated with ACARS for the flight planning function.

Aircraft Avionics Industry Standards

Aircraft avionics manufacturers use industry standards such as RTCA documents which address safety, performance, and interoperability when connecting to the ATS providers [8]. These RTCA documents are typically invoked by FAA Technical Standard Orders (TSOs). These industry standards and FAA TSOs have been harmonized world-wide with other international civil aviation authorities and avionics manufacturers.

The aircraft avionics systems are required to implement robustness checks and be able to detect when certain ATS provider services are unavailable or corrupt. As the cyber-security threat environment is constantly changing and ever-evolving, the FAA and industry are monitoring security threats in real-time and, when required, will provide updates to address any mitigations required to reduce vulnerabilities to an acceptable level. Mitigations could include updates to ATS provider services, industry aircraft avionics standards, and updates to ATS or flight crew procedures.

Standards and Guidance for Aircraft Systems Information Security Protection

Industry, FAA, EASA, and other international civil aviation authorities were involved in the publication of the following documents for use on Transport Category Airplanes with greater than 19 passenger seats:

1) RTCA DO-326A "Airworthiness Security Process Specification", published July 8, 2014. This document provides process assurance guidance and requirements for the aircraft design regarding systems information security.
2) RTCA DO-355, "Information Security Guidance for Continuing Airworthiness", published June 17, 2014. This document provides guidance for assuring continued safety of aircraft in service in regard to systems information security.
3) RTCA DO-356, "Airworthiness Security Methods and Considerations", published September 23, 2014. This document provides analysis and assessment methods for executing the process assurance specified in DO-326A.

Aircraft Security Risk Assessments Considerations for using ATS Provider Services

There are many different types of aircraft operating in the U.S. NAS including Transport Category Airplanes, Small Airplanes, and Rotorcraft. The rule basis, system architectures, and security vulnerabilities are different across these aircraft types. ASISP should be developed and structured to address different architecture and security vulnerabilities across all aircraft types.

It is estimated that 10 thousand large transport category airplanes, 7 thousand business jets, 250 thousand general aviation aircraft, and thousands of military aircraft are currently using the U.S. ATS

provider services. Although the cyber-security threat environment is constantly changing and ever-evolving it is **not possible or practical** to have the operators of these hundreds of thousands of aircraft to **individually conduct** and monitor security threats and propose mitigation strategies for the use of ATS service providers. This concept would also apply to new avionics and aircraft manufactures that **would not be required to conduct individual security threat evaluations** when connecting to ATS service providers.

To address the constantly changing and ever-evolving cyber-security threat environment, this paper recommends development of a AVS strategic plan to monitor security threats and, if required, develop recommendations for additional security controls for ATS service providers, industry aircraft avionics standards, and updates to ATS or flight crew procedures. Existing aircraft industry standards that provide information on connectivity with ATS provider communication, navigation, and surveillance services should be reviewed to ensure that adequate security guidance are in place. As an example, certain industry standards such as data communication and database requirements are being reviewed by RTCA committee team members to determine if additional security guidance is needed [9]. The FAA has chartered an ARAC which could provide additional recommendations on the development of a national plan to further address this proposal.

ATS Provider Services & Aircraft Systems Redundancy Management

ATS providers and aircraft systems have fault tolerant designs and use redundancy management and independent back-up systems to address and mitigate failure conditions caused by inadvertent or intentional system degradation. Commercial airplane operations are extremely reliable and safe, based in part on the ATS providers and aircraft systems architectures including redundancy management and back-up systems.

Communication

Commercial Transport Category Airplanes typically have three independent radios that use VHF, HF, or satellite communications. Voice communication between ATC and the flight crew is used in the U.S. NAS. CPDLC may be used in the oceanic environment. Multiple independent failures would need to occur to cause loss of all communication between the flight deck and ATC. If all of the aircraft communications systems fail, the flight crew is able to continue safe flight and landing in coordination with ATC procedures.

Navigation

Commercial Transport Category Airplanes have layers of redundancy and also use independence to address ATS provider failure modes. As an example, by federal regulations, Transport Category Airplanes are required to have at least two independent long range navigation sensors (e.g., GPS, Inertial navigation systems (INS), VOR, and DME). During GPS outages the aircraft could default to INS or ground based navigation aids (VOR/DME) to obtain navigation position information for the aircraft systems. The NAS has approximately 4,500 ground based navigation aids and multiple independent failures would be required to adversely affect aircraft navigation operations. In the worst case scenario, when all of the aircraft navigation sensor inputs fail during operations, the flight crew is able to continue safe flight and landing in coordination with ATC procedures. As an example, ATC could provide radar vectors for aircraft heading information.

Surveillance

The U.S. NAS infrastructure provides excellent radar coverage. The radar provides range and azimuth and the aircraft reports altitude and aircraft identification. A new surveillance capability called ADS-B also reports position information to ATC. The ATC automation tools receive both Radar and ADS-B position information and display aircraft position information to ATC. The combination of radar and ADS-B position information provides seamless surveillance monitoring of aircraft by ATC for NAS operations.

In summary, we have independence, redundancy, and back-up systems for the communication, navigation, and surveillance functions, which would require multiple failures to affect the safety of airplane operations. Airplane avionics systems also have health monitoring and integrity checks typically called

built-in-test which provides additional capability to detect and report fault conditions including intentional degradation caused by certain cyber-security attacks. As the cyber-security attacks evolve and become more sophisticated, addition security controls to detect and mitigate new cyber-security threat sources may be required.

U.S. National Airspace System Overview

The purpose of this section is to provide a brief overview of the NAS architecture in order to further illustrate the connectivity between the ATC information services and aircraft. This paper uses the terms ATC information services and ATS providers interchangeably. The NAS architecture includes the ATS providers and has over 34,000 pieces of maintainable equipment [10]. The NAS architecture includes but is not limited to the following:

- 18,300 airports
- 21 Air Route Traffic Control Centers (ARTCC)
- 197 Terminal Radar Approach Control Facilities (TRACON)
- 460 Airport Traffic Control Towers (ATCT)
- 75 Flight Service Stations (FSS)
- 4,500 ground based navigation facilities
- Global Navigation Satellite Systems (GNSS)

With more than 7,000 takeoffs and landings per hour, and more than 660 million passengers and 37 billion cargo revenue miles of freight a year, ATO safely guides 50,000 aircraft through the NAS system every day. Figure 3 provides an overview of the U.S. NAS architecture.

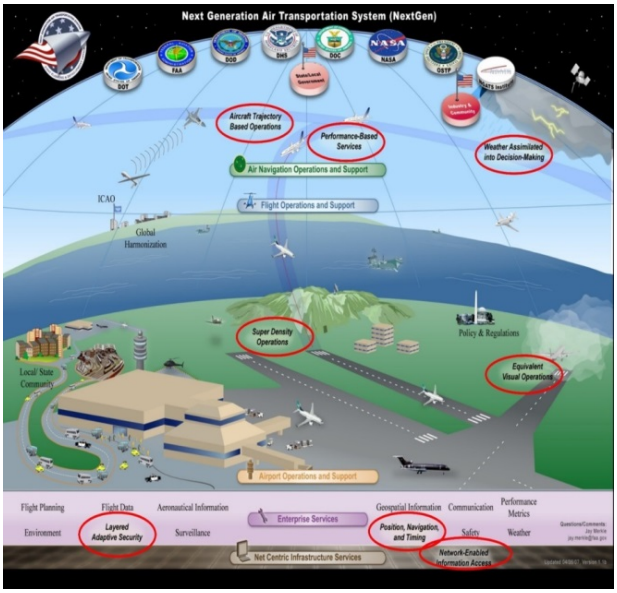

Figure 3 - U.S. National Airspace System (NAS) Architecture

As described in previous sections of this paper, the FAA AVS oversees the development of aircraft systems industry standards for safety, performance, and interoperability for connecting to the ATC communication, navigation, and surveillance services. These aircraft industry standards are typically invoked by FAA TSOs.

The ATO, the operational arm of the FAA, implements and oversees cyber-security measures for NAS services. The ATO's Authorizing Official Designated Representative (AODR) and NAS Cyber Operations Organization have responsibility for cyber-security on all NAS ATC systems, including continuous monitoring, threat response coordination, and policy. The AVS oversees the connectivity of aircraft systems to the ATC information services. The scope of this paper is to provide information on the aircraft systems connectivity to ATC information services. ATC information services in general, are described in other publications such as the FAA NextGen implementation plan.

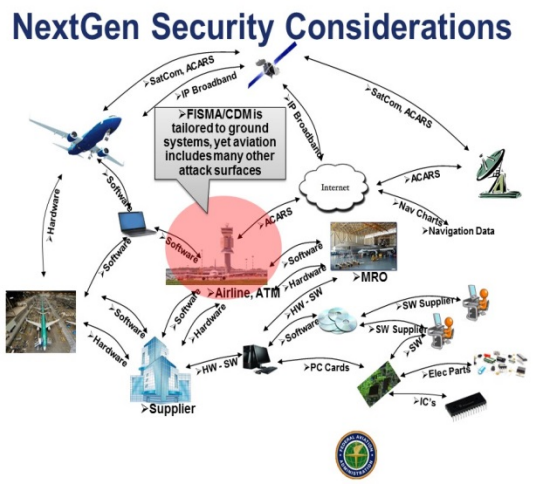

Figure 4 – NextGen Overview and Security Considerations

Figure 4 provides an illustration of NextGen and security considerations.

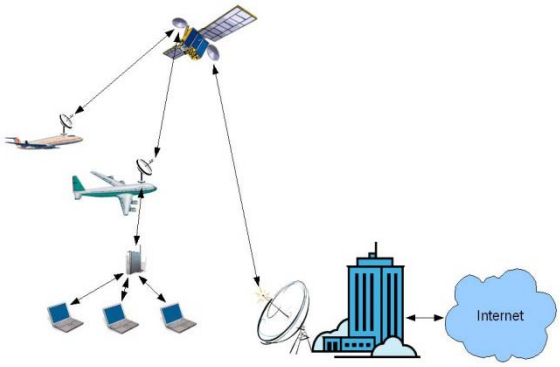

Figure 5 - Aircraft Connectivity to the Internet

Aircraft operators and manufacturers throughout the world are expanding their use of information technology (IT) within their maintenance, engineering, and flight operations organizations. The use of IT to integrate aircraft systems is sometimes called "e-Enabling". Many potential economic and safety benefits using e-Enabled technology and increased connectivity to the internet have been identified. Figures 5 and 6 provide an overview of aircraft connectivity to the internet, public and airline networks.

The following are examples of non-ATS provider services:

- AOC communications
- Airport Gate Link Networks
- Public Networks (e.g., internet)
- Portable Electronic Devices (PEDs) including Laptops and iPADS
- Electronic Flight Bags
- Wireless Aircraft Sensors and Sensor Networks
- Wireless Ground Support Equipment (GSE)
- Universal Serial Bus (USB) devices
- Satellite Communications
- Maintenance lap tops

Aircraft connectivity to non-ATS providers may result in cyber-security vulnerabilities to the aircraft networks and systems. Non-ATS provider services are not managed by U.S. federal agencies and the security standards used by these providers are variable. As the non-ATS providers "are not authorized sources" and the security standards are variable, the use of these services requires an ASISP risk assessment. Many IT systems are public systems, have internet connectivity, and are subject to potential threats from anyone that has internet access world-wide. IT connectivity to aircraft systems provides great benefits but also enables great risk if ASISP has not been properly addressed. Of particular concern is the ability to gain unauthorized access of onboard avionics through internet protocol (IP) connected devices in the cockpit or cabin, or during maintenance.

In the past, legacy aircraft had closed avionics architectures with zero or very limited IT connectivity. Aircraft avionics systems that do not have IT connectivity are not subject to threats from the internet because they are physically isolated and do not have access points for hackers to attack. Prior to the availability of e-Enabled technologies, legacy aircraft have used federated architectures with limited wired or wireless connectivity to non-Air Traffic Service (ATS) providers. This is rapidly changing as legacy aircraft are now being modified to add Wi-Fi, Electronic Flight Bags (EFB), Field Loadable Software (FLS), Integrated Modular Avionics (IMA) and Passenger Information and Entertainment Services [11].

With increased aircraft connectivity to IT systems, security risk assessments should be required when connecting to non-ATS providers in order to identify threats, determine potential safety vulnerabilities, and provide mitigations to reduce or eliminate these threats.

Federated architectures with single direction data busses (e.g., ARINC-429) are less vulnerable to the propagation of inadvertent or malicious cyber-security attacks across aircraft systems [12]. Legacy aircraft are now being modified and new aircraft are being developed with IMA systems with increased connectivity to non-ATS providers. IMA systems typically use bi-directional high speed data busses with connectivity to many aircraft systems across aircraft domains which could increase vulnerability to cyber security attacks.

The standards, guidance, and regulations to design and manufacture aircraft avionics systems and networks are very different than IT systems which make it challenging to conduct an end-to-end system safety assessment when information is exchanged between these two entities. The security threat vulnerabilities for IT systems are different than aircraft systems and networks.

One of the most difficult tasks is determining the sophistication and capabilities of the threat sources and types of malicious attacks that could occur. The safety effect on aircraft systems is much more severe if the cyber-security attacks result in misleading information to the flight crew rather than loss of certain aircraft functions. As many aircraft systems have layers of redundancy and independent back-up systems, the malicious attack, in some cases, would have to affect multiple aircraft systems to cause reduction in safety margins.

The best way to address this issue is during the development of the aircraft/systems requirements. The aircraft/systems design and maintenance procedures should be developed to ensure that any cyber-security attack from non-ATS providers will not impact safety of operations regardless of the sophistication and capabilities of the attacker. Developers should identify security vulnerabilities first, and then development mitigation strategies to reduce or eliminate the effect of cyber-security attacks.

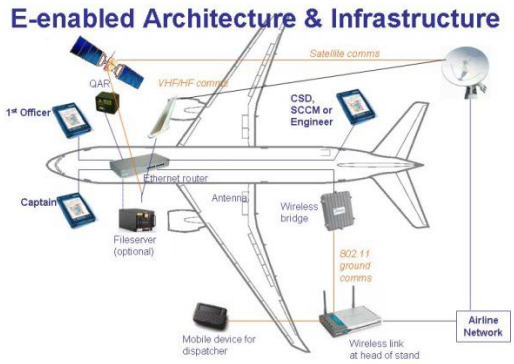

Figure 6 – e-Enabled Architecture & Infrastructure

FLS Security Considerations

Field-loadable airborne software refers to software or data tables that can be loaded without removing the system or equipment from its installation. Some airplanes such as the B787 are able to upload software parts via the internet anywhere in the world. The safety-related requirements associated with the software data loading function are part of the system requirements. If the inadvertent enabling of the software data loading function could cause erroneous loading of software parts, then a safety-related requirement for the software data loading function should be specified in the system requirements [13].

System safety considerations relating to field-loadable software include:

- Detection of corrupted or partially loaded software
- Determination of the effects of loading the inappropriate software
- Hardware/software compatibility
- Software/software compatibility
- Aircraft/software compatibility
- Inadvertent enabling of the field loading function
- Loss or corruption of the software configuration identification display.

Unless otherwise justified by the system safety assessment process, the detection mechanism for partial or corrupted software loads should be assigned the same failure condition or software level as the most severe failure condition or software level associated with the function that uses the software load.

If a system has a default mode when inappropriate software is loaded, then each partitioned component of the system should have safety-related requirements specified for operation in this mode which address the potential failure condition.

The software loading function, including support systems and procedures, should include a means to detect incorrect software and/or hardware, and should provide protection appropriate to the failure condition of the function. If the software consists of multiple configuration items their compatibility should be ensured.

If software is part of an airborne display mechanism that is the means for ensuring that the aircraft conforms to a certified configuration, then that software should either be developed to the highest software level of the software to be loaded, or the system safety assessment process should justify the integrity of an end-to-end check of the software configuration identification.

The following are examples of FLS networks and applications:

- External Data Networks for EFB Downloads/Uploads
- Portable Data Loader (Wired/Wireless)
- Web Site Access of Electronic Parts and Databases
- Data Distribution Software Loaders
- Data Base updates (e.g., Flight Management Computer Navigation Data Bases and Terrain Awareness and Warning Systems)

RTCA DO-178B section 2.5 provides guidance for FLS. The ARAC committee will provide recommendations on whether AC 20-115B should be used in combination with other industry FLS standards (e.g., ARINC security controls) [14, 15].

Risk Management Considerations for IT Systems

There are many FIPS and NIST documents that could be used during the security risk assessment process. NIST Special Publication (SP) 800-30 which is a "Risk Management Guide for Information Technology Systems".

According to SP 800-30, risk management encompasses three processes: risk assessment, risk mitigation, and evaluation and assessment. Risk is a function of the likelihood of a given threat-source exposing a particular vulnerability, and the resulting impact of that adverse event on the organization. In general, NIST and FIPS documents provide recommendations and standards for ground based IT systems and their risk assessment includes physical security.

Transport category aircraft avionics manufacturers typically use the SAE Aerospace Recommended Practices (ARP) 4754a "Guidelines for Development of Civil Aircraft and Systems" and SAE ARP 4761 "Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment" [16, 17].

SAE ARP 4754a provides guidance for development of civil aircraft and addresses the development cycle for aircraft systems, taking into account the overall aircraft operating environment and functions; this includes validation of requirements and verification of the design implementation for certification and product assurance. SAE ARP 4754a is used in combination with SAE ARP 4761 which provides guidance for the safety assessment process.

Guidance for software development is detailed in Document (DO)-178B/C "Software Considerations in Airborne Systems and Equipment Certification". Guidance for airborne electronic hardware development (e.g., integrated circuits) is detailed in RTCA DO-254 "Design Assurance for Airborne Electronic Hardware". These Standards for software and airborne electronic hardware do not specifically address cyber security for aircraft systems [18].

The FAA and industry have considered several options for addressing and publishing cyber-security guidance. Discussions ranged from adding cyber-security requirements to SAE ARP 4754a, SAE ARP 4761, RTCA DO-178B/C, RTCA DO-254 or creating new stand-alone documents that could be used in combination with these documents. The reason that SAE ARP 4754a, SAE ARP 4761, RTCA DO-178B and RTCA DO-254 are referenced in this paper is because of the inter-relationships between these documents and the security risk assessment process. Industry published RTCA-DO-326A, RTCA DO-355 and RTCA DO-356 standards and guidance for ASISP which are intended to be used in combination with other documents referenced in this section.

The challenge is that we are now integrating two separate set of standards; (1) the IT standards, and (2) the aircraft avionics systems standards. Normally, engineers are experts in either IT standards or aircraft avionics standards, but in general are not experts in both areas. Leveraging and communicating information between IT standards and aircraft avionics standards continues to be work in progress.

Change Impact Analysis

A Change Impact Analysis is required for modifications to aircraft interfaces which permit electronic access by non-ATS providers either during operations or maintenance. Additional Aircraft interfaces could be physical, wireless, or logical. ED-79A/ARP 4754A describes the aircraft and systems modification process. Aircraft and systems manufacturers may use their original system and safety development processes as the baseline.

The Change Impact Analysis is an iterative document, which is updated as changes to the modification plans are made. The analysis should also be updated following validation and verification activities. The Change Impact Analysis accounts for the effects on the aircraft by the new or modified system, but also effects on the new or modified system by the connected systems. Unplanned modifications resulting from the modification process should be discussed and their impact also addressed. The effort required can vary greatly from a small task to a complete rework of the security risk assessment data, dependent on the extent of modification planned.

A change impact analysis is simplified for legacy aircraft using federated systems and uni-directional ARINC-429 data busses. For IMA aircraft using bi-directional high speed data busses across aircraft domains, involvement and coordination with the original aircraft manufacturer may be required.

In general, the Change Impact Analysis should verify that:

1) The aircraft and its systems, networks, and other assets are protected from unauthorized electronic interaction. If protection cannot be verified, then the risk should be assessed as being acceptable or mitigated by additional security controls.

2) Procedures exist to ensure the continuing airworthiness of the Aircraft.

3) Malicious or inadvertent threats to aircraft systems and networks required for safe flight and operations are prevented.

4) Previously approved aircraft security measures are maintained.

Aircraft Level versus System Level Security Risk Assessment Determination

For every aircraft modification, a Change Impact Analysis is required. The results of the Change Impact Analysis may be used to determine if aircraft level or system level Security Risk Assessment is required. Security Risk Assessment can be relatively simple or complex depending on the aircraft architecture and intended function of the information technology applications.

As an example, threat evaluation of EFBs that are not connected or have read–only access to aircraft systems are less complicated than the devices that have read-write access. When they are receiving data, wireless or wired aircraft systems and networks should require a security threat evaluation when connected to non-ATS providers to ensure that the data is not intercepted or corrupted. The installation requirements for a security system should consider the aircraft avionics architecture, such as federated systems versus highly integrated modular avionics systems using bi-directional data busses to aid in determining if aircraft level or system level Security Risk Assessment is required.

In most cases, federated avionics systems with unidirectional data busses (e.g., ARINC-429) that connect to aircraft systems and networks should have system level, not aircraft level, Security Risk Assessment. System Security Risk Assessment should show that threats are mitigated by the system(s) to which the threat of non-ATS providers is connected. If it is not possible to determine if mitigations are adequate at the system level, then Aircraft Security Risk Assessment will be required. Also, if the unidirectional nature of a bus cannot be guaranteed, then the mitigation measures should address all possible sources of data or interference on the data-bus.

When non-ATS providers are connected to bi-directional data busses (e.g., Avionics Full-Duplex Switched Ethernet (AFDX)) on highly integrated aircraft with integrated modular avionics systems, in most cases Aircraft Security Risk Assessment is

required. The Supplemental Type Certificate (STC) applicant may obtain a data package or services from the Original Equipment Manufacturer (OEM) of the aircraft or system through a specific arrangement as required. Based on this data package, the STC applicant should provide evidence that the modification does not adversely impact safety based on the original Type Certificate (TC) approval. The applicant is responsible to obtain all necessary information and documentation in support of their proposed modification.

Commercial-Off-The-Shelf (COTS) Electronic Hardware Devices

Over 95% of the components used in aircraft systems are COTS based. COTS devices include integrated circuits generally produced in large quantities by commercial manufacturers including Intel, Advanced Micro Devices, LSI Logic, Texas Instruments, etc. These COTS devices are not designed or built in FAA approved manufacturing facilities.

COTS hardware suppliers sometimes make minor and major changes to the integrated circuit manufacturing process (size reductions in integrated circuits) without changing the part number which makes configuration control monitoring difficult. Figure 7 provides an example of a COTS multi-function display.

Airborne avionics manufactures do not have access to specific design data associated with these devices, but do have access to components specification regarding their use in computer systems. Examples of COTS integrated circuits and applications include the following:

- General Purpose Integrated Circuits
- Microprocessors
- Data buss and network components, such as controllers, switches, relays, etc.
- Networks
- Operating Systems
- Application Programs

RTCA DO-254 provides FAA policy for "Design Assurance Guidance for Airborne Electronic Hardware" for Application Specific Integrated Circuits (ASIC) and Programmable Logic Devices which are typically designed for aircraft systems. The FAA does not have specific cyber-security policy and guidance for the use of COTS devices in aircraft systems. COTS devices are required to meet CFR §xx.1301 and §xx.1309 when installed in aircraft systems.

Manufacturer's quality control systems often contain requirements for obtaining aircraft parts from trusted sources and ensure configuration control throughout the parts procurement process and final integration into the aircraft systems. Manufacturers that obtain aircraft parts from COTS suppliers should include cyber-security controls to ensure counterfeit parts are detected and eliminated during the procurement and tracking processes.

One of the key assumptions is that COTS devices are obtained from "aircraft manufacturers approved suppliers" and that the information obtained is correct and valid. The second key assumption is that if the COTS devices are inadvertently or intentionally corrupted, these anomalies will be detected at receiving inspection or during the airborne systems final acceptance tests prior to installation in aircraft.

Applicants and aircraft systems manufacturers are required to have configuration control on items purchased by suppliers and are responsible for traceability to ensure that counterfeit parts are screened, detected, and rejected during the quality control process.

Another key assumption is that aircraft systems may have built-in-test software, real time monitors, and/or voting planes that should be able to detect and isolate most integrated circuit malfunctions or failures caused by inadvertent or intentional degradation. These assumptions need to be validated by the avionics manufacturers to ensure that COTS hardware security vulnerabilities have been mitigated.

Figure 7 – Example of a portable COTS multi-function display

Aircraft Domains and Internal Aircraft Data Buss Connectivity

AC 20-156 "Aviation Data Buss Assurance" provides guidance on replacing point-to-point wiring and unidirectional data busses (for example, ARINC 429 data-bus) with faster and lighter bi-directional data busses. The guidance in this AC is intended for new type certificate or major changes of aircraft installations with highly-integrated and complex data-bus technology.

Aircraft systems may be connected to aircraft electronics networks which are private, public, or managed by ATS Providers. Some late model aircraft have novel or unusual design features associated with the architecture and connectivity capabilities of the airplane's systems and networks.

Notional Aircraft Domain Concepts

To better understand cyber-security threats and vulnerabilities, industry has defined conceptual aircraft architecture block diagrams called domains for transport category airplanes. This paper will describe these domains as an aid to conducting security risk assessments with the understanding that aircraft architectures vary widely and few if any will meet this exact model.

Aircraft Control Domain

The Aircraft Control Domain (ACD) provides guidance and control related to continued safe flight during all flight phases including takeoff and landing. Automatic Flight Guidance and Control Systems (AFG&CS) and flight control computers, yaw damper, auto thrust, flight director, and primary flight displays are part of the ACD. A security risk assessment should be conducted for all non-ATS provider connectivity that has write access to the ACD.

Airlines Information Services Domain

The Airline Information Service Domain (AISD) provides airline administrative and non-safety related airline communications. ACARS are used to communicate with both ATC and the AOC. AC 120-70B "Operational Authorization for Use of Data Link Communications Systems" and AC 20-140A "Guidelines for Design Approval of Aircraft Data Link Communications Supporting ATS" provide guidance for the AISD. [19, 20]

Passenger Information and Entertainment Services Domain

The Passenger Information and Entertainment Services domain (PIESD) provides entertainment and communications (e.g., email, voice, internet connectivity) directly to the passengers.

A security risk assessment should be required for any non-ATS external network connected to the PIESD domain that has write access and is physically connected to the ACD and/or AISD. If the PIESD domain is not connected to the ACD or AISD domain (physically isolated), then an aircraft level security risk assessment is not required.

The FAA does not currently require a security risk assessment for information displayed to the passengers via the entertainment system and internet. Threatening or hostile messages that could be sent to the passengers via an aircraft internet connection are under study for potential safety impacts. To date, no significant safety impacts of passenger internet use during flight have been identified.

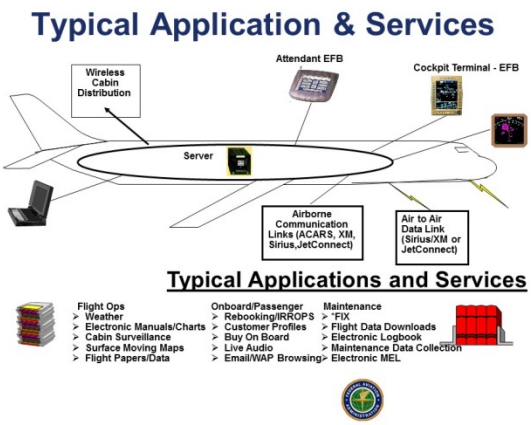

Figure 8 - Typical EFB Applications and Services

EFB Systems

Both portable and installed EFB systems authorized for use through the appropriate Flight Standards District Office / Certificate Management Office that have certificate oversight authority of Title 14 of the Code of Federal Regulations 91 subpart K (part 91K), 121, 125 including Letter of Deviation Authority and 135 certificate holders. EFB systems are now being used for many applications including display of aeronautical charts, weather products, aeronautical information publications, aircraft maintenance manuals and weight and balance calculations. Most EFB systems have internet connectivity with very limited transmit capability to aircraft avionics systems.

Airline operators have been authorized to use iPads as portable EFB equipment, and have purchased over 40,000 iPads. AC 120-76C "Guidelines for the Certification, Airworthiness and Operational Use of Electronic Flight Bags" provides guidance for the use of over seventy software applications [21]. Some of these software applications are available from the Apple store and may be downloaded into iPads for use by the flight crew.

Avionics manufacturers are proposing to use EFB systems with certain applications to control passenger reading lights and seat adjustments. AC 120-76C provides the following general guidance for security considerations. "The operator should identify a means to demonstrate that adequate security measures are in place to prevent malicious introduction of unauthorized modifications to the EFB operating system, its specific hosted applications, and any of the databases or data links used to enable its hosted applications. EFB systems need to be protected from possible contamination from external viruses." Figure 8 provides an illustration of typical EFB applications and services.

Certain airlines are allowing flight crew members to use the iPads for both airplane applications and personal use. This process has advantages as it encourages pilots to become familiar with iPads use in general. Apple does provide security controls including authentication for the use of iPads. Various companies provide iPADS applications including Jeppesen which provides electronic charts. Software applications that are used in the flight deck require configuration control and a Principal Inspector (PI) evaluation to determine suitability for operations. Other software applications (Pilot personal software applications) that are not used in the flight deck do not require PI evaluations except for non-interference.

The National Institute of Standards and Technology (NIST) has approved certain Apple iPads operating systems to Federal Information Processing Standards (FIPS) 140-2, certification level 1. The FIPS 140-2 is a U.S. government computer security standard used to accredit cryptographic modules [22]. The U.S. DOD has officially approved Apple iPhone and iPads for connectivity to secure government networks.

The Airlines Electronic Engineering Committee (AEEC) has developed a standard for portable electronic equipment (e.g., iPads) connectivity to aircraft systems called an Aircraft Interface Device (AID) [23]. The AID has been developed for legacy aircraft using the ARINC-429 data-bus architecture which is uni-directional. The AID standard will not support connectivity to high speed bi-directional data-busses. The AID includes a data-bus converter which allows the iPads to directly communicate with the ARINC-429 data-bus protocol.

The AID architecture supports four ARINC-429 receivers and two ARINC-429 transmitters. The AID will require an FAA aircraft certification design approval as it is connected to and is considered part of the aircraft. The portable EFB equipment that connects to the AID will not require an FAA aircraft certification design approval but will require a review of suitability of operations by the FAA PI. The portable EFB equipment will be able to transmit information to a flight deck printer and ACARS used for Airline Administration Communications.

EASA has published Acceptable Means of Compliance (AMC) 20-25 for EFB systems used in commercial transport category aircraft [24]. This AMC provides guidance on security considerations for EFB systems which is in the process of being harmonized with the FAA and should result in updates to future FAA policy and guidance in this area.

Contact Information

Peter Skaves

Peter.Skaves@faa.gov

425 917-6700 (w)

425 802-0395(c)

2015 Integrated Communications

Navigation and Surveillance (ICNS) Conference

April 21-23, 2015

Appendix I

Acronyms and Abbreviations

AC	Advisory Circular
ACARS	Aircraft Communication Addressing and Reporting System
ACD	Aircraft Control Document
ACO	Aircraft Certification Office
ACD	Aircraft Control Domain
ADS-B	Automatic Dependent Surveillance - Broadcast
AEEC	Airlines Electronic Engineering Committee
AFDX	Avionics Full-Duplex Switched Ethernet
AFG&CS	Automatic Flight Guidance & Control Systems
AID	Aircraft Interface Device
AISD	Airlines Information Services Domain
AMC	Acceptable Means of Compliance
AOC	Airline Operations Center
ARAC	Aviation Rulemaking Advisory Committee
ARINC	Aeronautical Radio Incorporated
ARP	Aerospace Recommended Practices
ARINC	Aeronautical Radio Incorporated
ARTCC	Air Route Traffic Control Centers
ASIC	Application Specific Integrated Circuit
ASISP	Aircraft Systems Information Security Protection
AST	Commercial Space Transportation
ATC	Air Traffic Control
ATCT	Airport Traffic Control Towers
ATO	Air Traffic Organization
ATS	Air Traffic Service
ATS-P	Air Traffic Service-Provider
AVS	Aviation Safety
CAA	Civil Aviation Authorities
CDU	Control Display Unit
CFR	Code of Federal Regulations
COTS	Commercial Off-The-Shelf
CFR	Code of Federal Regulations
CPDLC	Controller Pilot Data Link Communications
CRC	Cyclic Redundancy Check
CST	Commercial Space Transportation
DHS	Department of Homeland Security
DME	Distance Measuring Equipment
DO	Document
DOD	Department of Defense
ED	European Document
EFB	Electronic Flight Bag
E.G.	As an Example
FAA	Federal Aviation Administration

FIPS	Federal Information Processing Standards
FLS	Field-Loadable Software
EASA	European Aviation Safety Agency
FISMA	Federal Information Security Management Act
FMCS	Flight Management Computer System
GBAS	Ground Based Augmentation Systems
GNSS Systems	Global Navigation Satellite
GPS	Global Positioning System
GSE	Ground Support Equipment
ICA	Instructions for Continued Airworthiness
ILS	Instrument Landing Systems
IMA	Integrated Modular Avionics
INS	Inertial Navigation System
ISO	International Standards Organization
IT	Information Technology
LOB	Line of Business
NAS	National Air Space
NextGen	Next Generation
NIST	National Institute of Standards and Technology
OEM	Original Equipment Manufacturer
PED	Portable Electronic Devices
PIESD	Passenger Information and Entertainment Services Domain
RTCA	Radio Technical Commission for Aeronautics
SAE	Society of Automotive Engineers
SBAS	Satellite Based Navigation Systems
SC	Special Condition
SP	Special Publication
STC	Supplemental Type Certificate
TAD	Transport Airplane Directorate
TC	Type Certificate
TRACON	Terminal Radar Approach Control Facilities
TSA	Transportation and Security Administration
TSO	Technical Standard Order
UMS	User Modifiable Software
U.S.	United States
USB	Universal Serial Buss
VHF	Very High Frequency
VOR	VHF Omni directional Range

Appendix II

References

[1] www.faa.gov/about

[2] NextGen Implementation Plan, August 2014

[3] www.tsa.gov

[4] FAA Issue Paper, Aircraft Electronic Systems Security Protection from Unauthorized External Access

[5] FAA Issue Paper, Isolation or Aircraft Electronic System Security Protection from Unauthorized Internal Access

[6] www.gpo.gov [FR Doc No: 2015-01918]

[7] www.defense.gov

[8] www.rtca.org

[9] FAA Advisory Circular 20-153 "Acceptance of Data Processes and Associated Navigation Data Bases"

[10] https://www.faa.gov/air_traffic/nas/

[11] Advisory Circular 20-170 "Integrated Modular Avionics, Development, Verification, Integration, and Approval Using RTCA DO-297 "IMA Design Guidance and Certification Considerations"

[12] FAA Technical Center Report "Potential Cybersecurity Issues for the ARINC 429 Avionics Data Bus and Line Replaceable Units (LRUs)", dated August 29, 2014

[13] RTCA DO-178B, "Software Considerations in Airborne Systems and Equipment Certification"

[14] ARINC 665-2, "Loadable Software Standards"

[15] ARINC 667-1 "Guidance for the Management of Field Loadable Software"

[16] Society of Automotive Engineers (SAE) Aerospace Recommended Practices (ARP) 4754a "Guidelines for Development of Civil Aircraft and Systems"

[17] SAE ARP 4761, "Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment"

[18] RTCA DO-254, "Design Assurance Guidance for Airborne Electronic Hardware"

[19] Advisory Circular 120-70B "Operational Authorization for Use of Data Link Communication Systems"

[20] Advisory Circular 20-140A "Guidelines for Design Approval of Aircraft Data Link Communication Supporting ATS"

[21] Advisory Circular 120-76C "Guidelines for the Certification, Airworthiness, and Operational Use of Electronic Flight Bags"

[22] FIPS Publication 140-2 "Government Computer Security Standard used to accredit Cryptographic Modules"

[23] ARINC 759 Aircraft Interface Device [AID]

[24] AMC 20-25 "Airworthiness and Operational Approval Considerations for Electronic Flight Bags