INFORMATION FOR CYBER SECURITY ISSUES RELATED TO AIRCRAFT SYSTEMS REV-A

Peter Skaves
Federal Aviation Administration, Washington, DC

Abstract

Existing FAA regulations, policy and guidance do not specifically address cyber security requirements for aircraft networks and systems. This could result in security related certification criteria that are not standardized and harmonized between domestic and international regulatory agencies.

This paper identifies cyber security threats and the need to address unauthorized and potentially unsafe electronic access to aircraft systems and networks. Unauthorized access could result in the malicious use of networks, and loss or corruption of data (e.g., software applications, databases, configuration files, etc.) brought about by software worms, viruses or other malicious entities (refer to Figure 1).

Figure 1. Security Interconnections

Security Definitions & Risk Management

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. 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 terms network security and systems security for the development of aircraft systems. When developing aircraft systems, risk management should include security risk assessment, risk mitigation and evaluation. Cyber security would be the term used to describe attacks on aircraft networks and systems from hackers.

Introduction

The purpose of this paper is to provide information on cyber security issues related to aircraft systems. This paper is not a FAA official document and is the opinion of the author only. In order to obtain the most recent policy and guidance on cyber security, please contact your local FAA Aircraft Certification Office (ACO).

Certain external and internal data network connections to aircraft systems need to be reviewed for potential cyber security vulnerabilities and threats to aircraft operations. This paper identifies potential threat sources that may require a cyber-security risk assessment of the aircraft networks and systems.

There are many different types of aircraft operating in the United States National Air Space including Transport Category Airplanes, Small Airplanes and Rotorcraft. The rule basis, system architectures and security vulnerabilities are different across these aircraft types. Cyber security guidance should be developed and structured to address different architecture and security vulnerabilities across all aircraft types.

This paper does not address security issues related to individuals who could gain physical access to aircraft with the intent of causing malicious damage to aircraft systems. Physical aircraft security

4A1-1
is enforced by the Department of Homeland Security (DHS) and Transportation and Security Administration (TSA). Security issues related to individuals that could gain access to aircraft to cause malicious damage (e.g., improper maintenance procedures, cutting wire bundles, etc.) are not addressed in this paper.

This paper describes two types of service providers that may receive and transmit information to the aircraft; (1) Air Traffic Service (ATS) providers and (2) non-ATS providers.

**ATS Provider Overview**

ATS providers are managed by United States 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 1370.82A “Information Systems Security Program” and the “FAA Information Systems Authorization Handbook”. Examples of ATS provider services include Global Positioning Systems (GPS), Satellite Based Augmentation Systems (SBAS), Global Positioning Augmentation Systems (GBAS), Air Traffic Control (ATC) data communications, Automatic Dependent Surveillance – Broadcast (ADS-B), and Controller Pilot Data Link Communications (CPDLC).

As the ATS providers are “authorized sources” and the security requirements are the responsibility of the provider, aircraft networks and systems do not require any additional security considerations to ensure that the transmission links are secure.

The assumption in this paper is that the United States ATS provider has addressed all security requirements for the safety, performance and interoperability-related transmissions (e.g., data links) to aircraft systems. 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.

Other international regulatory authorities that do not use the same security processes and standards as the United States 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.

**Non-ATS Provider Overview**

Non-ATS providers are not managed by United States federal agencies and the security standards used by these providers are variable. Aircraft connectivity to non-ATS providers may result in cyber security vulnerabilities to the aircraft networks and systems. As the non-ATS providers “are not authorized sources” and the security standards are variable, the use of these services may require an end-to-end aircraft and provider risk assessment depending in part on aircraft architecture.

The term non-ATS provider also includes any external data network connectivity to the aircraft that is not provided by ATS. Any aircraft modification that adds a Non-ATS Provider active external interface (including cellular and wireless) to the aircraft systems may require a security risk assessment. Wireless aircraft sensors and sensor networks should require a cyber security risk assessment when they are receiving data from non-ATS service providers as illustrated in figure 2.

![E-enabled Architecture & Infrastructure](image)

**Figure 2. E-Enabled Architecture & Infrastructure**

As an example, airport Gate Link networks that receive and transmit information to and from aircraft systems may require a security risk assessment. The
following are examples of external aircraft networks not provided by ATS:

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

Aircraft operators and manufacturers have identified many potential economic and safety benefits using e-enabled technology and software applications. There are many e-enabled applications that will require increased aircraft connectivity to non-ATS providers.

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, Field Loadable Software, Integrated Modular Avionics and Passenger Information and Entertainment Services.

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. Legacy aircraft are now being modified and new aircraft are being developed with Integrated Modular Avionics (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.

Notional Aircraft Domain Concepts

To better understand cyber security threats and vulnerabilities, industry has defined conceptual aircraft architecture block diagrams called domains. 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. Aircraft Communication Addressing and Reporting Systems (ACARS) are used to communicate with both ATC and the Airline Operations Center (AOC). Advisory Circular (AC) 120-7B “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. [1, 2]

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 to a Control Display Unit (CDU) of a Flight Management Computer System (FMCS). The flight planning information is sent from ACARS to the CDU of the 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.

In the United States National Air Space 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 security issues associated with ACARS for the flight planning function.

**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 a 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.

**Aircraft Security Regulations**

Current Title 14 Code of Federal Regulations (CFR 14) regarding security are §129.25 “Airplane Security”, §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 cyber security controls for certain applications that are not specifically required by FAA regulations. Cyber security 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.

Until new regulations on security are published, some aircraft modifications 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 and are not general public rules. When required, a FAA Special Condition should be 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.

Special Conditions may be used to address new and novel technology and methods, such as the increased connectivity between the aircraft and external interfaces. As this paper is for information only and is not regulatory, it is recommended that you contact your FAA ACO for information on specific applicability of cyber security related Special Conditions.

**RTCA Special Committee (SC) 216 Aeronautical Systems Security**

The scope of this committee is to develop industry standards for airworthiness, instructions for continued airworthiness (ICA), and operational implementation of the ICA for certain aircraft systems and networks connected to non-ATS providers. This committee will address conditions where the security of the system interfaces or information crossing those interfaces may cause or contribute to a failure condition that impacts aircraft safety of flight. The committee's scope excludes communication, navigation and surveillance services managed by United States Federal agencies or their international equivalents.

The security assurance and assessment processes and methods for safety-related aircraft systems and the security guidance for continued airworthiness documents are intended to be used by the FAA and other Civil Aviation Authorities (CAA) as an acceptable means of addressing the security-related safety aspects of aircraft systems and networks. It is envisioned that the documents would be invoked by FAA Special Conditions for operating and maintaining a secure aircraft system. The complete Terms of Reference for this committee are provided in RTCA Paper No. 078-11/PMC-888 March 17, 2011. [3]

---

**Risk Management Considerations for Information Technology Systems**

There are many Federal Information Processing Standards (FIPS) and National Institute of Standards and Technology (NIST) documents that could be used during the security risk assessment process [4-11]. This paper will discuss NIST “Special Publication (SP) 800-30 which is a “Risk Management Guide for Information Technology Systems” [4].

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-sources’ 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 Information Technology (IT) systems and their risk assessment includes physical security. Many IT systems are public systems, have internet connectivity and are subject to potential threats from anyone that has internet access world-wide.

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.

For navigation, Transport Category airplanes have multiple sensor inputs including GPS, Distance Measuring Equipment (DME), Very High Frequency (VHF) Omni directional Range (VOR), and Inertial Navigation Sensor (INS). Loss of GPS (intentional or inadvertent jamming of the GPS signal) for these airplanes, while not desirable, would not have significant safety impacts because of the other navigation sensor inputs.

If we assume the worst possible case, whatever that might be, then the cost to add security controls could be prohibitive. For this reason, certain aircraft system applications that could provide safety benefits
would not be installed in aircraft due to economic reasons. Threat source likelihood, aircraft potential vulnerabilities and mitigation should be taken into account when developing a security risk assessment. Cyber security guidance needs to be developed on how to scope the problem to reasonable proportions.

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. 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. The standards, guidance and regulations to design and manufacture ground based IT systems and aircraft avionics systems are very different which makes it challenging to conduct an end-to-end system safety assessment when information is exchanged between these two entities.

Aircraft avionics manufacturers typically use the Society of Automotive Engineers (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” [12, 13].

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 “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 [14, 15].

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, 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.

RTCA SC-216 for Aeronautical Communications Security and other related committees determined that the best approach was to create new document standards without revising existing standards. This committee has published RTCA DO-326 “Airworthiness Security Process Specification” which provides guidance on the security risk management process. RTCA DO-326 incorporates many of the processes described in the SAE and RTCA documents referenced above. A new RTCA SC-216 document on security methods is scheduled for publication during the second quarter of 2014.

For new or modified aircraft avionics designs, this paper proposes that the systems requirements are not a separate process from the cyber security requirements process. The cyber security requirements should be part of the system design and be developed at the same time as the rest of the system requirements.

The challenge is that we are now integrating two separate set of standards; (1) the Information Technology standards, and (2) the aircraft avionics systems standards. Normally, engineers are experts in either Information Technology standards or aircraft avionics standards, but in general are not experts in both areas. The new RTCA SC-216 industry cyber security standards are intended to integrate the aircraft and infrastructure processes.
Current Policy and Plans for Aircraft Systems Security

Until new cyber security rules are published, the FAA is issuing Special Conditions for new aircraft or aircraft modifications that could create aircraft system vulnerabilities. Based on the results of the risk assessment, the FAA may issue a Special Condition to ensure that the cyber security issues have been addressed.

The Special Condition addresses potential cyber security threats to aircraft safety and operations by entities that could inadvertently or intentionally transmit data on networks which could compromise data integrity and aircraft safety. The FAA plans to replace the Special Conditions with new regulations on cyber security in the future. Currently, the FAA is not planning on publishing new rules that would affect existing previously certified aircraft unless unsafe conditions are identified.

In support of the FAA Special Conditions, RTCA Special Committee 216 is working jointly with EUROCAE to develop guidance material for identifying and mitigating aircraft systems security vulnerabilities. Once the RTCA Special Committee documents are published, the current plan is to invoke these documents with FAA Issue Papers using an FAA Special Condition as the rule basis. These Special Conditions could be used as the basis for the certification and continued airworthiness for certain aircraft systems. The FAA Issue Papers on cyber security will provide supplemental information on the use of the RTCA documents and additional guidance for using alternative methods.

Commercial-Off-The-Shelf Electronic Hardware Devices

Over 95% of the components used in aircraft systems are Commercial-Off-The-Shelf (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 being made 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 3 provides an example of a COTS multi-function display.

Figure 3. 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 bus 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 [15]. 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
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.

Field Loadable Software (FLS) Security Considerations

Aircraft maintenance procedures are becoming increasingly e-enabled and field loadable software is being used to replace floppy discs for wireless uploading of thousands of electronic parts. FLS could be used to update software programs in any aircraft system across domains.

AC 20-115B invokes RTCA DO-178B “Software Considerations in Airborne Systems” which provides guidance for Field Loadable Software. FAA AC 20-153 “Acceptance of Data Processes and Associated Navigation Data Bases” provides guidance on databases used in aircraft systems and invokes RTCA DO-200A [14, 16].

RTCA DO-178B Field-Loadable Software Guidance

Field-loadable airborne software refers to software or data tables that can be loaded without removing the system or equipment from its installation. 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.

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, 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. If AC 20-115B is used in combination with other industry FLS standards (e.g., ARINC security controls) then additional security considerations may not be required.

**ARINC Project Report 835 Frequently Asked Questions on FLS**

ARINC Project Report 835 provides the following information on frequently asked questions:

**What is a digital signature?**

A digital signature is a value computed with a cryptographic algorithm and appended to a data object in such a way that any recipient of the data can use the signature to verify the data’s origin and integrity.

**What is a Loadable Software Part?**

A Loadable Software Part, in the most general terms, is a collection of files associated with a part number which are intended to be loaded into an aircraft system. More specific information about Loadable Software Parts, their types and formats may be found in ARINC publications 665 and 667.

**What is a Digital Signature on a Loadable Software Part?**

A digital signature is added to a Loadable Software Part to guarantee the identity of the creator to the recipient. It ensures that a function on the aircraft can determine the software part came from a recognized, valid source.

**Does a Digital Signature Provide encryption of the software files?**

No, the application of a digital signature to a Loadable Software Part does not provide encryption of the digital files. It only encrypts the data of the signature to ensure security and verify the origin and integrity.

**Why are Digital Signatures being applied to Loadable Software Parts?**

The correct function of software in an aircraft system is, in part, dependent upon clear identification of software part pedigree. Software parts contain CRC or other information to provide the recipient with integrity checks. CRC algorithms, for various reasons, do not exclude unintended parties from being able to correctly create them and thus cannot be used to identify the creator. Digital signatures provide the necessary pedigree.

The significant potential increase in field loadable software parts in today’s airplanes (up to 1000 software parts to be managed) demands increasing levels of secure electronic processing for purely electronic software parts, in addition to physical security of software parts distributed on physical transport media, including automatic
electronic comparison, configuration management, packaging and un-packaging [17, 18].

Using industry standards for FLS should minimize the effort required for security risk assessments.

**Users-Modifiable Software**

FAA AC 20-115B invokes RTCA DO-178B “Software Considerations in Airborne Systems” which provides guidance for User-Modifiable Software as follows.

A modifiable component is that part of the software that is intended to be changed by the user and a non-modifiable component is that which is not intended to be changed by the user. User-Modifiable software may vary in complexity. Examples include a single memory bit used to select one of two equipment options, a table of messages, or a memory area that can be used for programmed, compiled and linked for aircraft maintenance functions. Software of any level can include a modifiable component.

Guidance for designing user-modifiable software includes:

The non-modifiable component should be protected from the modifiable component to prevent interference in the safe operation of the non-modifiable component. This protection can be enforced by hardware, by software, by the tools used to make the change, or by a combination of the three.

The applicant-provided means should be shown to be the only means by which the modifiable component can be changed. If the User-Modifiable Software component protection is enforced by software, then a security risk assessment is required. Based on the results of the security risk assessment a Special Condition may be required. If the User-Modifiable Software component protection is not enforced by software, then a security risk assessment and Special Condition may not be required.

**Integrated Modular Avionics (IMA) Systems**

AC 20-170 “Integrated Modular Avionics, Development, Verification, Integration, and Approval using” RTCA DO-297, “IMA Design Guidance and Certification Considerations” and Technical Standard Order-C153 provides guidance in the following areas [19, 20]:

- IMA Module, Application, System, and Integration Acceptance
- Aircraft installation Approval of IMA Systems including TSO Authorized Components
- Software Loading Procedures
- Field-Loadable Software
- Electronic Identification Guidance of IMA parts (Electronic Part Marking)
- Automated, Robust Configuration Management
- Non-Automated, Robust Configuration Management

IMA systems are highly integrated and complex and contain unique security vulnerabilities that are different from other aircraft systems. The current recommendation is that IMA systems include a cyber security risk assessment for high speed bi-directional inter connectivity between aircraft systems and domains to address propagation of faults.

**Electronic Flight Bag (EFB) Systems**

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 and some EFB systems transmit information to aircraft avionics systems.

Airlines have been authorized to use iPADS as portable EFB equipment, to which the airlines have purchased over 30,000 iPADS. AC 120-76B “Guidelines for the Certification, Airworthiness and Operational Approval of Electronic Flight Bag Computing Devices” provides guidance for the use of over seventy applications [21].

Avionics manufacturers are proposing to use PEDs with certain applications to control passenger reading lights and seat adjustments. AC 120-76B
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 4 provides an illustration of an EFB system in the flight deck.

![Figure 4. EFB Flight Deck System](image)

The FAA does not currently have prescriptive guidance or policy for EFB system security. Operators are required to demonstrate that adequate security measures are in place to obtain suitability of operations approval from the FAA Principal Inspector (PI) on a case-by-case basis. Depending on the types of software applications hosted on the EFB system platform the safety effect on airplane operations will vary based on intended function.

Certain airlines are allowing the pilots to use the iPAD for both airplane applications and personal use. This process has advantages as it encourages pilots to become familiar with iPAD use in general. Apple does provide security controls including authentication for the use of iPADS. Various companies provide iPAD applications including Jeppesen which provides electronic charts. Software applications that are used in the flight deck require configuration control and a 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 Airlines Electronic Engineering Committee (AEEC) is developing a standard for portable electronic equipment (e.g., iPAD) connectivity to aircraft systems called an Aircraft Interface Device (AID). The AID is being developed for legacy aircraft using the ARINC-429 data bus architecture which is single-direction bus architecture. The AID standard will not support connectivity to high speed bi-directional data busses.

The AID will have four ARINC-429 receivers and two ARINC-429 transmitters. The AID will require an FAA aircraft certification design approval. The portable EFB equipment that connects to the AID will not require an FAA aircraft certification design approval. The portable EFB equipment will be able to transmit information to a flight deck printer and ACARS used for airline administration communications.

The FAA is in the process of issuing Change 1 to EFB AC 120-76B which will allow moving maps with own-shop position for surface operations as a Type “B” application for portable EFB equipment. This should streamline the approval process for surface moving maps with own-ship position.

The current FAA policy does not require a security assessment for Portable EFB Class I and II systems with access to read-only information from aircraft avionics systems.

Portable EFB systems are authorized to read-write information to the Airline Service (e.g., ACARS) and Passenger Information and Entertainment Service Domains. The FAA does not currently have specific security policy on EFB connectivity to these aircraft domains. A draft industry proposal for “FAA guidance for EFB System Security Considerations and Intended Function” is currently under review by the FAA [22]. Current FAA plan is to develop performance based general security guidance and not prescriptive one-size fits all specific solutions for EFB systems.

A security risk assessment should be required for EFB Class III systems that are connected to an external network link and authorized to read-write information to the aircraft control domain. Based on the results of the security risk assessment, a Special Condition may be required.
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 buss) with faster and lighter bi-directional data busses. [23] The guidance in this AC is intended for new type certificate or major changes of aircraft installations with highly-integrated and complex data buss technology.

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

A security risk assessment should be required for new bi-directional data busses that are connected to an active external non-ATS Provider network and the Aircraft Control Domain.

Adding read-write connectivity to a high speed bi-directional data buss to a non-governmental service provider may require an aircraft level cyber security assessment. Adding read-write non-governmental connectivity to a single-direction ARINC-429 data buss may require a systems level cyber security assessment, but in most cases will not require an aircraft level cyber security assessment.

Acronyms and Abbreviations

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>AC</td>
<td>Advisory Circular</td>
</tr>
<tr>
<td>ACARS</td>
<td>Aircraft Communication Addressing and Reporting System</td>
</tr>
<tr>
<td>ACD</td>
<td>Aircraft Control Document</td>
</tr>
<tr>
<td>ACO</td>
<td>Aircraft Certification Office</td>
</tr>
<tr>
<td>ADS-B</td>
<td>Automatic Dependent Surveillance-Broadcast</td>
</tr>
<tr>
<td>AEEC</td>
<td>Airlines Electronic Engineering Committee</td>
</tr>
<tr>
<td>AFG&amp;CS</td>
<td>Automatic Flight Guidance &amp; Control Systems</td>
</tr>
<tr>
<td>AISD</td>
<td>Airlines Information Services Domain</td>
</tr>
<tr>
<td>AOC</td>
<td>Airline Operations Center</td>
</tr>
<tr>
<td>ARINC</td>
<td>Aeronautical Radio Incorporated</td>
</tr>
<tr>
<td>ARP</td>
<td>Aerospace Recommended Practices</td>
</tr>
<tr>
<td>ASIC</td>
<td>Application Specific Integrated Circuit</td>
</tr>
<tr>
<td>ATC</td>
<td>Air Traffic Control</td>
</tr>
<tr>
<td>ATS</td>
<td>Air Traffic Service</td>
</tr>
<tr>
<td>ATS-P</td>
<td>Air Traffic Service-Provider</td>
</tr>
<tr>
<td>CAA</td>
<td>Civil Aviation Authorities</td>
</tr>
<tr>
<td>CDU</td>
<td>Control Display Unit</td>
</tr>
<tr>
<td>CFR</td>
<td>Code of Federal Regulations</td>
</tr>
<tr>
<td>COTS</td>
<td>Commercial Off-The-Shelf</td>
</tr>
<tr>
<td>CPDLC</td>
<td>Controller Pilot Data Link Communications</td>
</tr>
<tr>
<td>CRC</td>
<td>Cyclic Redundancy Check</td>
</tr>
<tr>
<td>DHS</td>
<td>Department of Homeland Security</td>
</tr>
<tr>
<td>DME</td>
<td>Distance Measuring Equipment</td>
</tr>
<tr>
<td>DO</td>
<td>Document</td>
</tr>
<tr>
<td>EFB</td>
<td>Electronic Flight Bag</td>
</tr>
<tr>
<td>FAA</td>
<td>Federal Aviation Administration</td>
</tr>
<tr>
<td>FIPS</td>
<td>Federal Information Processing Standards</td>
</tr>
<tr>
<td>FLS</td>
<td>Field-Loadable Software</td>
</tr>
<tr>
<td>FMCS</td>
<td>Flight Management Computer System</td>
</tr>
<tr>
<td>GBAS</td>
<td>Ground Based Augmentation Systems</td>
</tr>
<tr>
<td>GNSS</td>
<td>Global Navigation Satellite Sensor</td>
</tr>
<tr>
<td>GPS</td>
<td>Global Positioning System</td>
</tr>
<tr>
<td>GSE</td>
<td>Ground Support Equipment</td>
</tr>
</tbody>
</table>
ICA Instructions for Continued Airworthiness
ILS Instrument Landing Systems
IMA Integrated Modular Avionics
IT Information Technology
NIST National Institute of Standards and Technology
PED Portable Electronic Devices
PIESD Passenger Information and Entertainment Services Domain
SAE Society of Automotive Engineers
SBAS Satellite Based Navigation Systems
SC Special Condition
TSA Transportation and Security Administration
TSO Technical Standard Order
UMS User Modifiable Software
USB Universal Serial Buss
VHF Very High Frequency
VOR VHF Omni directional Range

References
[12] Society of Automotive Engineers (SAE) Aerospace Recommended Practices (ARP) 4754a “Guidelines for Development of Civil Aircraft and Systems”
[21] Advisory Circular 120-76B “Guidelines for the Certification, Airworthiness, and Operational
Approval of Electronic Flight Bag Computing Devices”

[22] Draft FAA Guidance for EFB Security Considerations, Mr. Dave Allen, The Boeing Company

[23] Advisory Circular 20-156 “Aviation Data Bus Assurance”

Email Addresses
Peter.Skaves@faa.gov

32th Digital Avionics Systems Conference
October 6-10, 2013