workers have a duty to ensure safe operating practices to prevent accidents. To ensure all workers, regardless of employer, will take appropriate action whenever necessary, Congress should amend the Outer Continental Shelf Lands Act or specific safety statutes to provide the same whistleblower protection that workers are guaranteed in other comparable settings."

F. Program Evaluation

One commenter requested that BTS report the results of the program to stakeholders at least once a year and that the program be evaluated after two years of operation. The frequency of public reports will depend on how many near miss reports are reported to the system. To comply with CIPSEA, reports of aggregated data must be prepared in such a way that no third party could determine the identity of a reporter, directly or indirectly. BTS expects to issue public reports at least once per year and potentially more often, as appropriate.

With regard to re-evaluating the program after two years, as demonstrated by near miss reporting in the aviation industry, it took a commitment of several years before employee reporting increased sufficiently to allow for a robust program evaluation. BTS agrees that "formative evaluation" is essential in developing a successful data collection program and will conduct such evaluation as soon as there is sufficient quantitative information in the near miss data system to allow for such analysis. However, the potential value of sharing data in a confidential manner is worth the investment of time and effort because the continuation of environmental and human losses is an unacceptable alternative to the public and the government.

G. Intent of the National Commission Report

One commenter correctly noted that the National Commission Report on the BP Deepwater Horizon Oil Spill was issued in 2011, not 2013 as the 60-day notice inadvertently stated. BTS, however, does not agree with the commenter's suggestions that the National Commission Report did not envision a government-managed system for near miss reporting, or that the Commission's recommendation for an industry "self-policing institute that would gather incident and performance data" would satisfy the recommendation for a near miss reporting program. In fact, the two recommendations are contained in different parts of the 2011 report, and it was in that part of the report directed to the Department of the Interior (DOI) that the National Commission recommended that DOI: "Develop more detailed requirements for incident reporting and data concerning offshore incidents and 'near misses.' Such data collection would allow for better tracking of incidents and stronger risk assessments and analysis."

Issued On: January 28, 2015.

Rolf Schmitt,

Deputy Director, Bureau of Transportation Statistics, Office of the Assistant Secretary for Research and Technology.

[FR Doc. 2015–02053 Filed 2–2–15; 8:45 am]

BILLING CODE 4910–9X–P

DEPARTMENT OF TRANSPORTATION

Federal Aviation Administration

Aviation Rulemaking Advisory Committee—New Task

AGENCY: Federal Aviation Administration (FAA), DOT.

ACTION: Notice of new task assignment for the Aviation Rulemaking Advisory Committee (ARAC).

SUMMARY: The FAA assigned the Aviation Rulemaking Advisory Committee (ARAC) a new task to provide recommendations regarding Aircraft Systems Information Security/Protection (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.

This notice informs the public of the new ARAC activity and solicits membership for the new ASISP Working Group.

FOR FURTHER INFORMATION CONTACT: Steven C. Paasch, Federal Aviation Administration, 1601 Lind Ave. SW., Renton, WA 98057–3356, Email: *steven.c.paasch@faa.gov*, Phone: (425) 227–2549, Fax (425) 227–1100.

SUPPLEMENTARY INFORMATION:

ARAC Acceptance of Task

As a result of the December 18, 2014, ARAC meeting, the FAA assigned and ARAC accepted this task establishing the ASISP Working Group. The working group will serve as staff to the ARAC and provide advice and recommendations on the assigned task. The ARAC will review and approve the recommendation report and will submit it to the FAA.

Background

The FAA established the ARAC to provide information, advice, and recommendations on aviation related issues that could result in rulemaking to the FAA Administrator, through the Associate Administrator of Aviation Safety.

The ASISP Working Group will provide advice and recommendations to the ARAC on ASISP-related rulemaking, policy, and guidance, including both initial certification and continued airworthiness. 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. 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. 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.

There are many different types of aircraft operating in the United States National Air Space (NAS), including transport category airplanes, small airplanes, and rotorcraft. The regulations, system architectures, and security vulnerabilities are different across these aircraft types. The current regulations do not specifically address ASISP for any aircraft operating in the NAS. To address this issue, the FAA has published special conditions for particular make and model aircraft designs. The FAA issues Special Conditions when the current airworthiness regulations for an aircraft do not contain adequate or appropriate safety standards for certain novel or unusual design features including ASISP. Even though the FAA published special conditions for ASISP, an update to the current regulations should be considered. International civil aviation authorities are also considering rulemaking for ASISP and the ASISP Working Group could be used as input into harmonization of these activities.

The FAA has issued policy statement, PS–AIR–21.16–02, *Establishment of*

Special Conditions for Cyber Security, which describes when the issuance of special conditions is required for certain aircraft designs. This policy statement provides general guidance and requires an update to address the ever evolving security threat environment.

A companion issue paper is published in combination with each FAA ASISP Special Condition. The issue paper provides guidance for specific aircrafts and models and contains proprietary industry information which is not publically available. These issue papers, with industry input, could provide additional guidance and best practices recommendations and could be used as input into the development of national policy and guidance (*e.g.*, advisory circular). The FAA has not published guidance on the use of security controls and best practices for ASISP, thus ARAC recommendations in this area are highly desirable.

There are many industry standards addressing various security topics, such as Aeronautical Radio Incorporated (ARINC), Federal Information Processing Standards (FIPS), International Standards Organization (ISO), and National Institute of Standards and Technology (NIST) standards. There are also industry standards addressing processes for requirements development, validation, and verification, such as Society of Automotive Engineers (SAE) Aerospace Recommended Practices (ARP) 4754a and SAE ARP 4761. In addition, there are standards from RTCA such as (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.

The ASISP Working Group recommendations as to the usability of these standards in ASISP policy and/or guidance are highly desirable.

The Task

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 ARINC, FIPS, International Standards Organization (ISO), NIST, SAE ARP 4754a and/or SAE ARP 4761 would be appropriate for use in such ASISP-related policy and/or guidance.

5. Consider 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.

Working Group Activity

The ASISP Working Group must comply with the procedures adopted by the ARAC, and are as follows:

1. Conduct a review and analysis of the assigned tasks and any other related materials or documents.

2. Draft and submit a work plan for completion of the task, including the rationale supporting such a plan, for consideration by the ARAC.

3. Provide a status report at each ARAC meeting.

4. Draft and submit the recommendation report based on the review and analysis of the assigned tasks.

5. Present the recommendation report at the ARAC meeting.

6. Present the findings in response to the FAA's questions or concerns (if any) about the recommendation report at the ARAC meeting.

Participation in the Working Group

The ASISP Working Group will be comprised of technical experts having an interest in the assigned task. A working group member need not be a member representative of the ARAC. The FAA would like a wide range of members to ensure all aspects of the tasks are considered in development of the recommendations. The provisions of the August 13, 2014 Office of Management and Budget guidance, ''Revised Guidance on Appointment of Lobbyists to Federal Advisory Committees, Boards, and Commissions'' (79 FR 47482), continues the ban on registered lobbyists participating on Agency Boards and Commissions if participating in their ''individual capacity.'' The revised guidance now allows registered lobbyists to participate on Agency Boards and Commissions in a ''representative capacity'' for the ''express purpose of providing a committee with the views of a nongovernmental entity, a recognizable group of persons or nongovernmental entities (an industry, sector, labor unions, or environmental groups, etc.) or state or local government.'' (For further information see Lobbying Disclosure Act of 1995 (LDA) as amended, 2 U.S.C. 1603, 1604, and 1605.)

If you wish to become a member of the ASISP Working Group, write the person listed under the caption **FOR FURTHER INFORMATION CONTACT** expressing that desire. Describe your interest in the task and state the expertise you would bring to the working group. The FAA must receive all requests by March 5, 2015. The ARAC and the FAA will review the requests and advise you whether or not your request is approved.

If you are chosen for membership on the working group, you must actively participate in the working group, attend all meetings, and provide written comments when requested. The member must devote the resources necessary to support the working group in meeting any assigned deadlines. The member must keep management and those represented advised of the working group activities and decisions to ensure the proposed technical solutions do not conflict with the position of those represented. Once the working group

has begun deliberations, members will not be added or substituted without the approval of the ARAC Chair, the FAA, including the Designated Federal Officer, and the Working Group Chair.

The Secretary of Transportation determined the formation and use of the ARAC is necessary and in the public interest in connection with the performance of duties imposed on the FAA by law.

The ARAC meetings are open to the public. However, meetings of the ASISP Working Group are not open to the public, except to the extent individuals with an interest and expertise are selected to participate. The FAA will make no public announcement of working group meetings.

Issued in Washington, DC, on January 28, 2015.

Lirio Liu,

Designated Federal Officer, Aviation Rulemaking Advisory Committee.

[FR Doc. 2015–01918 Filed 2–2–15; 8:45 am]

BILLING CODE 4910–13–P

DEPARTMENT OF TRANSPORTATION

Federal Highway Administration

[Docket No. FHWA–2015–0002]

Agency Information Collection Activities: Request for Comments for New Information Collection

AGENCY: Federal Highway Administration (FHWA), DOT.

ACTION: Notice and request for comments.

SUMMARY: The FHWA has forwarded the information collection request described in this notice to the Office of Management and Budget (OMB) for approval of a new information collection. We published a **Federal Register** Notice with a 60-day public comment period on this information collection on November 12, 2014. We are required to publish this notice in the **Federal Register** by the Paperwork Reduction Act of 1995.

DATES: Please submit comments by March 5, 2015.

ADDRESSES: You may send comments within 30 days to the Office of Information and Regulatory Affairs, Office of Management and Budget, 725 17th Street NW., Washington, DC 20503, Attention DOT Desk Officer. You are asked to comment on any aspect of this information collection, including: (1) Whether the proposed collection is necessary for the FHWA's performance; (2) the accuracy of the estimated burden; (3) ways for the FHWA to enhance the quality, usefulness, and clarity of the collected information; and (4) ways that the burden could be minimized, including the use of electronic technology, without reducing the quality of the collected information. All comments should include the Docket number FHWA–2015–0002.

FOR FURTHER INFORMATION CONTACT: Keith Williams, 202–366–9212, Highway Safety Specialist, Strategic Integration Team, Office of Safety Programs, Federal Highway Administration, Department of Transportation, 1200 New Jersey Avenue SE., Room E71–119, Washington, DC 20590, Monday through Friday, except Federal holidays.

SUPPLEMENTARY INFORMATION:

Title: Inventory of State Police Accident Reports (PAR) and Serious Injury Reporting.

Background: The Federal Highway Administration (FHWA) Office of Safety's mission is to exercise leadership throughout the highway community to make the Nation's roadways safer by developing, evaluating, and deploying life-saving countermeasures; advancing the use of scientific methods and data-driven decisions, fostering a safety culture, and promoting an integrated, multidisciplinary 4 E's (Engineering, Education, Enforcement, Education) approach to safety. The mission is carried out through the Highway Safety Improvement Program (HSIP), a data driven strategic approach to improving highway safety on all public roads that focuses on performance. The goal of the program is to achieve a significant reduction in traffic fatalities and serious injuries on all public roads, including non-State-owned public roads and roads on tribal lands.

In keeping with that mission, the United States Congress on June 29, 2012 passed the Moving Ahead for Progress in the 21st Century Act (MAP–21), which was signed into law (Pub. L. 112–141) on July 6, 2012 by President Barrack Obama. MAP–21 is a milestone for the U.S. economy and the Nation's surface transportation program as it transformed the policy and programmatic framework for investments to guide the system's growth and development and created a streamlined performance-based surface transportation program. The Federal Highway Administration defines Transportation Performance Management as a strategic approach that uses system information to make investment and policy decisions to achieve national performance goals.

MAP–21 requires the Secretary of Transportation to establish performance measures for States to use to assess serious injuries and fatalities per vehicle mile traveled; and the number of serious injuries and fatalities, for the purposes of carrying out the HSIP under 23 U.S.C. 148. The HSIP is applicable to all public roads and therefore requires crash reporting by law enforcement agencies that have jurisdiction over them.

In defining performance measures for serious injuries, FHWA seeks to define serious injuries in a manner that would provide for a uniform definition for national reporting in this performance area, as required by MAP–21. An established standard for defining serious injuries as a result of highway crashes has been developed in the 4th edition of the Model Minimum Uniform Crash Criteria (MMUCC). MMUCC represents a voluntary and collaborative effort to generate uniform crash data that are accurate, reliable and credible for data-driven highway safety decisions within a State, between States, and at the national level. The MMUCC defines a serious injuries resulting from traffic crashes as "Suspected Serious Injury (A)" whose attributes are: Any injury, other than fatal, which results in one or more of the following: Severe laceration resulting in exposure of underlying tissues, muscle, organs, or resulting in significant loss of blood, broken or distorted extremity (arm or leg), crush injuries, suspected skull, chest, or abdominal injury other than bruises or minor lacerations, significant burns (second and third degree burns over 10 percent or more of the body), unconsciousness when taken from the crash scene, or paralysis.

As part of the effort to understand current reporting levels for serious injuries to support the MAP–21 performance measures, the FHWA seeks to determine at what level law enforcement agencies have adopted the MMUCC definition, attribute and coding convention. FHWA is aware that not all States have adopted the MMUCC definition, attribute and coding convention for serious injuries while other States have only partially adopted the definition. It is also known that some jurisdictions do not use the State Police Accident Report (PAR) form to report on crashes. It is not known if these PARs are MMUCC compliant.

The purpose of the information collection is to conduct an assessment of each Federal, tribal, State and non-State PAR to determine if the definition and coding convention used for reporting on serious injuries is or is not compliant with MMUCC, and if not

The Boeing Company
P.O. Box 3707, MC 09-76
Seattle, WA 98124-2207

October 3, 2016

B-H020-REG-16-TLM-66

Ms. Lirio Liu
Director, Office of Rulemaking, ARM-1
Federal Aviation Administration
800 Independence Avenue, SW
Washington, D.C. 20591

Lirio.liu@faa.gov

Subject: ARAC Report, Aircraft System Information Security/Protection

Reference: Tasking Notice, Federal Register Doc 2015-01918 (80 FR 5880-5882, February 3, 2015)

Dear Ms. Liu,

On behalf of the Aviation Rulemaking Advisory Committee (ARAC), I'm pleased to submit the attached Aircraft System Information Security/Protection (ASISP) report. The ARAC accepted the referenced tasking on December 18, 2014. The report, including recommendations, was submitted to ARAC on August 22, 2016.

The ASISP working group was comprised of members and subject matter experts representing a cross-section of the industry: airframe and avionics manufacturers, industry standards groups, operators, regulators and other stakeholders. The report contains 30 recommendations, including FAA action to initiate rulemaking, update policy and guidance materials and leverage industry standards and adopt best practices.

The details within the report were agreed to by full consensus of the working group members and the report was approved by ARAC during its September 15, 2016 meeting. I want to thank the members of the Aircraft System Information Security/Protection Working Group for their hard work and responsiveness to the FAA's request.

Sincerely yours,

Todd Sigler
ARAC Chair

Enclosure

A Report from the

Aviation Rulemaking Advisory Committee (ARAC)
Aircraft System Information Security / Protection (ASISP)
working group to the
Federal Aviation Administration

Recommendations regarding ASISP rulemaking, policy, and guidance on best practices for airplanes and rotorcraft including both certification and continued airworthiness.

Submitted to the FAA: August 22, 2016

This page intentionally left blank.

Table of Contents

Executive Summary

The Aviation Rulemaking Advisory Committee (ARAC) established the working group on Aircraft System Information Security / Protection (ASISP) to provide information, advice and recommendations on aviation related ASISP issues to the Federal Aviation Administration (FAA) Administrator, through the Associate Administrator of Aviation Safety. The ARAC is comprised of a wide range of domestic and international industry and government experts to ensure that relevant design, airworthiness, and international harmonization aspects of ASISP are considered in the recommendations.

There are many different types of aircraft operating in the United States National Airspace System (NAS), including transport category airplanes, small airplanes, and rotorcraft. The regulations, system architectures, and vulnerabilities are different across these aircraft types. The current regulations do not specifically address ASISP for any aircraft operating in the NAS. The FAA instead publishes Special Conditions for particular make and model aircraft systems. The FAA issues Special Conditions when the current airworthiness regulations for an aircraft do not contain adequate or appropriate safety standards for certain novel or unusual design features. The ARAC working group is tasked to review the Special Conditions and companion issues papers and to make any recommendations deemed necessary to ensure safety equivalent to that established by existing airworthiness standards. .

The ARAC working group has proposed which ASISP related policies and/or guidance materials needed for certain categories of airplanes and rotorcraft, as well as recommendations on the use of existing industry standards including best practices.

Without updates to regulations, policy, and guidance to address ASISP, aircraft vulnerabilities may not be identified and mitigated, thus increasing exposure to security threats. 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. 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.

In summary, the charter of the ARAC ASISP working group required publication of this report, development of recommendations on whether ASISP-related rulemaking, policy and/or guidance on best practices are needed, and, if rulemaking is recommended, specify proposals for where in the current regulatory framework such rulemaking should be placed for both initial certification and continued airworthiness.

This report was written with the intent of being made public. It is also intended for use by other working groups currently undertaking technical work to update specific standards.

The ASISP report is structured into five sections:

- Section 1 provides an overview of how the FAA, and other regulators, have addressed cybersecurity requirements for aircraft and systems without a stand-alone rule. This section also provides background about how the ASISP working group was established.
- Section 2 provides recommended regulations for different types of aircraft, engines, and propellers. This section also identifies areas that warrant specific guidance from the FAA and other regulators including references to industry standards, best practices, and appropriate

means of compliance based on the type of aircraft. This includes recommendations from the ASISP working group for how industry standards and best practices should be updated or developed to provide for a harmonized and proportional approach to addressing cybersecurity for new and legacy aircraft and systems.

- Section 3 provides additional guidance about the operational environment including how ASISP should be addressed as part of Continued Operational Safety. This section also discusses work that is underway in parallel to provide guidance to operators.
- Section 4 provides technical background to support the development of guidance material for specific technologies (e.g., Portable Electronic Devices, Field Loadable Software, and the use of Commercial Off the Shelf Technology). This section also provides a recommended process for how the FAA should review existing Technical Standards Orders (TSO) for Communications, Navigation, and Surveillance (CNS).
- Section 5 provides some general recommendations about data sharing for ASISP, training for FAA personnel and designees, and research opportunities.

List of Recommendations

The ASISP working group provides the FAA with 30 detailed recommendations. These 30 recommendations address eight areas:

- Recommendations for rulemaking for airworthiness standards to address ASISP: 01, 02, 10, 12, 14 and 15.

- Recommendations about other rulemaking to address ASISP: 17 and 18.

- Recommendations to adopt existing standards, update existing standards, or develop best practices and / or means of compliance to support ASISP regulation: 03, 04, 05, 06, 07, 08, 09, 11, 13, 16, 19, 22, and 23.

- A recommendation to update the FAA's existing policy for cybersecurity: 20.

- Recommendations about continued operational safety and data: 21, 22 (also part of standards), and 28.

- Recommendations about specific technologies including Technical Standards Orders: 24, 25, 26, 27.

- A recommendation for how to establish standards for designees: 29

- A recommendation for future research to further address ASISP: R1

Recommendation 01: The ASISP Working group recommends that the FAA work closely with the primary certifying authorities (i.e., ANAC, EASA, TCCA) to achieve harmonization for the airworthiness standards and guidance for Aircraft System Information Security / Protection. (Section 2.1)

Recommendation 02: The ASISP working group recommends that the FAA undertake rulemaking to update 14 CFR 25, Subpart F, to address ASISP based on the regulatory structure developed by the working group. (Section 2.2)

Recommendation 03: ASISP working group recommends FAA consider RTCA standards DO-326, DO-356 and DO-355 and EUROCAE standards ED-201, ED-202, ED-203, ED-204 as acceptable guidance materials to comply with the security rule 25.13xx for large transport aircraft for new Type type certifications or new significant major changes or when the applicant elects to use them on a voluntary basis.

Recommendation 04: The ASISP working group recommends that the FAA establish guidance for Minor or lower equipment that has connectivity with other systems which should be protected. (Section 2.2.4.3.4)

Recommendation 05: The ASISP working group recommends the FAA task SC-216 to create harmonized standards with WG 72 around the Risk Acceptability and Assurance Framework based on the guidance material outlined in sections 2.2.3.4.1 – 2.2.3.4.8 of this report. This harmonized standards material should be incorporated into the appropriate RTCA documents such as DO-356, and the equivalent EUROCAE documents.

Recommendation 06: The ASISP working group recommends that the FAA establish guidance to show compliance with the rule requiring an applicant to define a security environment as required input of any security analysis. Defining the security environment should be done in accordance with industry standards, such as DO-356 or EUROCAE ED-203 at the latest version or equivalent guidance material. Defining a security environment may include a set of trustworthiness assumptions (as illustrated in Table 2.2-4). This security environment should be submitted to the airworthiness authority for agreement. This agreement remains granted for any further security risk analysis on a dedicated aircraft model, as long as the security environment remains unchanged. The example given in section 2.2.4.5 can be considered as an acceptable method for defining a security environment.

Recommendation 07: In accordance with SC-216 TOR (approved in March 2016), ARAC ASISP WG recommends to both RTCA SC-216 and EUROCAE WG-72 the following additional tasks:

- Carry out an exhaustive review of ED-202A/DO-326A, DO-356/ED-203 and DO-355/ED-204 to identify missing continuing airworthiness objectives and to identify existing continuing airworthiness objectives without guidance and/or compliance criteria,

- Complete or add, when relevant, continuing airworthiness objectives allocated to DAH in DO-356/ED-203,

- Complete or add, when relevant, guidance to meet these continuing airworthiness objectives and compliance criteria such as correctness, completeness, consistency, validation and verification, evidences, …,

- If Continuing Airworthiness considerations applicable to the Operators are missing in DO-355/ED-204, assess the relevance and the consequences for updating DO-355/ED-204,

- If RTCA SC-216 and EUROCAE WG-72 decide to update DO-355/ED-204:

- Assess the need to reactivate the former ED-204/DO-355 working group (SG-4)

- Assess the opportunity to transfer the existing DAH-related continuing airworthiness considerations from DO-355/ED-204 to DO-356/ED-203, in order that Continuing Airworthiness considerations of DO-356/ED-203 be limited to DAH only and the Continuing Airworthiness considerations of DO-355/ED-204 be limited to Operator only,

- Complete or add, when relevant, continuing airworthiness objectives allocated to the Operators,

- Complete or add, when relevant, guidance to meet these continuing airworthiness objectives and compliance criteria such as correctness, completeness, consistency, validation and verification, evidences, …

- DO-355 and ED-204 should remain harmonized as far as practicable

Recommendation 08: The ARAC WG recommends the FAA task SC-216 to work on Guidance Materials topics GM#1 – GM#9 in accordance with paragraphs 2.2.4.1 to 2.2.4.8.

Recommendation 09: The working group recommends that the FAA consider the results of the SC-216 tasking (which is due in December 2017) as part of the agency's development of guidance for the regulation for the topics listed in section 2.2.4.

Recommendation 10: The ASISP working group recommends that the FAA develop airworthiness regulations for rotorcraft in 14 CFR 27 and 29 and bounded the regulation to only require consideration of catastrophic and hazardous/severe major effects on safety as caused by intentional unauthorized electronic interaction. (Section 2.3)

Recommendation 11: The ASISP working group notes that DO-356 and ED-202, ED-203, and ED-204 are currently not aligned with respect to their applicability to rotorcraft and recommends that the documents should be updated and tailored to better address rotorcraft. (Section 2.3)

Recommendation 12: The ASISP working group recommends that the FAA, as part of its guidance for 14 CFR 23.1315, include in the definition for IUEI that the applicant when showing compliance to "airplane system or equipment… abnormal operation… [that] has not been specifically addressed by another requirement in this part" also consider cybersecurity threats as an abnormal operation. (Section 2.4)

Recommendation 13: The ASISP working group recommends that the FAA – in coordination with other regulators – work with industry in F44 (in a manner similar to how the ASISP has provided recommendations for tasks to be assigned to RTCA SC-216) to finalize and ballot for approval the best practices that support 14 CFR 23.1315 and addresses the following topics identified in Section 2.4.3.1 for small airplanes. (Section 2.4)

Recommendation 14: The ASISP working group recommends that the FAA undertake rulemaking to update 14 CFR 33.28 to establish information security protection for engines. (Section 2.5.2)

Recommendation 15: The ASISP working group recommends that the FAA undertake rulemaking to update 14 CFR 35.23 to establish information security protection for propellers. (Section 2.5.2)

Recommendation 16: The ASISP working group encourages the IFE and connectivity industry to participate in information sharing partnerships. (Section 2.6)

Recommendation 17: The ASISP working group recommends that the FAA sets a legal basis for prohibiting tampering with aircraft systems. (Section 2.6)

Recommendation 18: The ASISP working group recommends that the FAA not establish additional security requirements for IFE systems – other than those which would result from the recommendations of section 2.2 through 2.4 (e.g., the security assessment process for airworthiness for Minor systems) in this report and the existing standards for IFE identified in section 2.6 – because additional regulatory requirements could negatively affect the security posture when IFE software has to be upgraded. (Section 2.6)

Recommendation 19: The ASISP working group recommends that existing policies for type design changes, such as the establishment of certification basis, for existing safety regulations and means of compliance are also applicable to ASISP considerations and a phased adoption of industry standards should be anticipated. (Section 2.7)

Recommendation 20: The ASISP working group recommends that the FAA update the policy statement PS-AIR-21.16-02, Establishment of Special Conditions for Cyber Security, based on the input provided by the working group. (Section 3.1)

Recommendation 21: The ASISP working group recommends that the FAA establish policy to leverage existing COS programs for reporting security events affecting safety. (Section 3.2.1)

Recommendation 22: The ASISP working group recommends that DO-356/ED-203 be updated to include guidance for logging for large transport category airplanes. (Section 3.2.2)

Recommendation 23: The ASISP working group recommends that the FAA encourage adoption of General Aviation/ASTM Security Best Practices Section 7.9 for logging considerations. (Section 3.2.2)

Recommendation 24: The FAA should develop guidance to address:

> Development of equipment intended for direct connections to PEDs should include considerations to protect against intentional corruption due to intentional unauthorized electronic interaction from the PED. Development of Aircraft Installed Equipment which supports PEDS direct connections should consider the following security threats:
>
> - unauthorized interaction with the direct connection
> - intentional corruption of the PED (in particular, this includes support for portable media), and
> - unauthorized access to the PED by sources external to the aircraft and PED. (Section 4.1)

Recommendation 25: The ASISP working group recommends that the FAA establish guidance for Field Loadable Software (FLS) including Aircraft Databases as identified in Sections 4.2.1 through 4.2.7 of the report.

Recommendation 26: The ASISP working group recommends that the FAA establish guidance for the Use of Commercial Off the Shelf (COTS) and Previously Certified Products as identified in Section 4.2 of the report.

Recommendation 27: The ASISP recommends that the FAA undertake a review of the existing CNS/ATM TSOs, in coordination with industry, and determine if targeted risk mitigations should be integrated into future revisions to specific standards. Some of this work is already underway (e.g., RTCA SC-159 and SC-186, as well as ICAO CP), but a comprehensive table top review of the CNS avionics standards would help to mitigate risk and address concerns. (Section 4.4)

Recommendation 28: The ASISP working group recommends that both the A-ISAC and US-CERT should continue to develop capabilities to address ASISP specific threats and issues in support of ensuring a safe and secure aviation industry. (Section 5.1)

Recommendation 29: The ASISP working group recommends that the FAA develop and provide clear standards for security designations for designees. (Section 5.2)

Recommendation Research R1: The ASISP recommends that the FAA consider the following topics as part of future agency research to address cybersecurity (Section 5.3):

- The FAA should undertake research to determine how threat and vulnerability sharing can be most effectively done for ASISP including in coordination with international partners and regulators.
- The FAA should fund the development of tools that can facilitate event log analysis.
- Study means of detecting and preventing vulnerabilities from PED's connectivity to Avionic Interface Devices.
- Study means of detecting vulnerabilities in receiving transponder and ADS-B Data in aircraft.

The associated section provides detailed information to the FAA about how to move forward with the recommendation.

1 ASISP Working Group Task

The Aviation Rulemaking Advisory Committee (ARAC) established the Aircraft System Information Security / Protection (ASISP) working group at its December 18, 2014 meeting. The FAA published the assignment of a new task in the Federal Register[1] on February 3, 2015; with a deadline for requests for membership on March 5, 2015.

This new task requires the working group to provide recommendations regarding ASISP rulemaking, policies, and guidance on best practices for airplanes and rotorcraft, including both certification and continued airworthiness. Without updates to regulations, policies, and guidance to address ASISP, aircraft vulnerabilities may not be identified and mitigated, thus increasing exposure to security threats. In addition, a lack of ASISP-specific regulations, policies, 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.

Specifically, the ASISP Working Group was 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.

[1] 80 FR 5880-5882

1.1 Background and History

There are many different types of aircraft operating in the United States National Air Space (NAS), including transport category airplanes, small airplanes, and rotorcraft. The regulations, system architectures, and security vulnerabilities are different across these aircraft types.

The current Federal aviation regulations do not specifically address ASISP for any aircraft type operating in the NAS. To address this issue, the FAA has published special conditions for particular make and model aircraft designs. The FAA issues Special Conditions when the current airworthiness regulations for an aircraft do not contain adequate or appropriate safety standards for certain novel or unusual design features including e-enabled connectivity.

Even though the FAA has issued special conditions to address ASISP, an update to the current regulations, policies and guidance should be considered for the reasons discussed above. International civil aviation authorities are also considering rulemaking for ASISP, and the ASISP Working Group is using its input to facilitate global harmonization of these standards.

The FAA has issued policy statement, PS–AIR–21.16–02, Establishment of Special Conditions for Cybersecurity, to describe when the issuance of special conditions is required for certain aircraft systems and network designs and modifications. This policy statement provides general guidance and requires an update to address the ever evolving security threat environment.

A companion issue paper is published with each FAA ASISP Special Condition. The issue paper provides guidance for specific aircraft models and contains proprietary industry information which is not publically available. With industry input, these issue papers, could provide additional guidance and best practices recommendations and could be used as input into the development of national policy and guidance (e.g., advisory circular). The FAA has not published guidance on the use of security controls and best practices for ASISP, thus ARAC recommendations in this area are highly desirable.

There are many industry standards addressing various security topics, such as Aeronautical Radio Incorporated (ARINC), Federal Information Processing Standards (FIPS), International Standards Organization (ISO), and National Institute of Standards and Technology (NIST) standards. There are also industry standards addressing processes for requirements development, validation, and verification, such as Society of Automotive Engineers (SAE) Aerospace Recommended Practices (ARP) 4754a and SAE ARP 4761.

In addition, RTCA, Inc. and the European Organisation for Civil Aviation Equipment (EUROCAE) – have collaborated on several related standards, including the following as:

(1) RTCA DO–326A ‘‘Airworthiness Security Process Specification,’’ published August 6, 2014 and associated EUROCAE documents. This document provides process assurance guidance and requirements for the aircraft design regarding systems information security. (EUROCAE ED-202A.)

(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. (EUROCAE ED-204.)

(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. (EUROCAE ED-203)

The FAA specifically requested the ASISP Working Group make recommendations as to the usability of these standards in ASISP policy and/or guidance.

The working group is specifically tasked with providing recommendations about how and where to establish initial and continued airworthiness requirements in the existing regulations (e.g., Part 23, 25, 27, 29 33, or 35). A long-standing point of discussion is whether Security Risk Assessment is a parallel process to system Safety Assessment Processes, or whether the two are part of one integrated process as well as their degree of independence. Additionally, the working group has agreed that security for the purpose of aircraft systems should be considered a contributor to safety and airworthiness requirements; and the working group recommendations align with this principle. In addition to reviewing the existing standards the working group identified best practices where appropriate.

1.2 ASISP Tasking Overview

As discussed above, the February 3, 2015 Federal Register notice identified seven specific tasks for the working group. The following table maps these tasks to the sections in this report that provide the ASISP working group’s response.

Table 1.2-1 – ASISP Tasking Overview

ASISP Task	Primary ASISP Report Section(s)
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.	2.1; 2.2; 2.3; 2.4; 2.5 and 2.6
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.	2.0 and 3.1;
3. If it is recommended that ASISP-related policy and / or guidance on best practices are needed, specify (i) Which categories or airplanes and rotorcraft such policy and / or guidance should address, and (ii) Which airworthiness standards such policy and / or guidance should reference.	2.2; 2.3; 2.4
4. If it is recommended that ASISP-related policy and / or guidance on best practices is needed, recommend whether security-related industry standards from ARINC, FIPS, ISO, RTCA, NIST, SAE ARP 4754a and / or SAE ARP 4761 would be appropriate for use in such ASISP-related policy and / or guidance. *Note: The Federal Register did not include RTCA and EUROCAE in the list of industry standards.*	2.2.3; 2.3.4; 2.4.3; 4.1; 4.2; 4.3; 4.4
5. Consider EASA requirements and guidance material for regulatory harmonization.	2.1
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	This report section 1 through 5 No dissenting opinions were provided.

rationale for each position. b. Any disagreements should be documented, including the rationale for each position and the reason 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.	2.8

1.3 Issues Not Addressed by Working Group

The FAA tasked the ARAC working group with developing recommendations about airplanes and rotorcraft and their associated systems, but specifically directed the working group not to address Unmanned Aircraft Systems (UAS) security issues.

The FAA tasking also excluded ground, satellite, and other Air Traffic Services (ATS) infrastructure from its scope and requested that the working group focuses on the systems that support the physical aircraft. FAA is undertaking other work to address non-airborne infrastructure. The ARAC working group, however, makes recommendation in Section 4.4 about conducting desk top reviews related to FAA Technical Standard Orders that invoke minimum performance standards for safety, performance, and interoperability connectivity to the ATS services (e.g., GPS, aeronautical databases).

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, fuel contamination, cutting wire bundles) are not addressed by the ASISP working group. Physical aircraft security is addressed by various Federal agencies, including the FAA, the Department of Homeland Security (DHS), and the Transportation Security Administration (TSA).

The working group also did not specifically address aircraft operations, but reviewed existing guidance (e.g., AC 119-1) for commercial operators. The working group does provide recommendations about Type Certificate Holder (TCH) responsibilities to produce certain information for operators to ensure the continued security of aircraft systems. These instructions are typically part of the aircraft's Instructions for Continued Airworthiness (ICA), which commercial operators (i.e., Part 121 / 135) must follow and private operators (i.e., Part 91) should follow to ensure the security of their aircraft.

2 Recommendations for Rulemaking

The working group prioritized the development of an amendment to Subpart F of the airworthiness standards for transport category airplanes to support harmonization between rulemaking projects underway by the FAA and other international civil aviation authorities such as the European Aviation Safety Agency (EASA), Transport Canada Civil Aviation (TCCA) and Agência Nacional de Aviação Civil – Brasil (ANAC).

The working group then reviewed the draft regulatory amendment to ensure that guidance and industry standards appropriate to ensure the safety of aircraft systems exist or are developed to support compliance with the new ASISP regulation. The working group also reviewed the transport category airplane regulatory framework or its applicability to other aircraft categories (e.g., small airplanes and rotorcraft) and engines. The regulatory text for different categories of aircraft achieves a consistent objective, but the regulatory structure is adapted to each section of the airworthiness standards and the means of compliance differ based on a consideration of the security threat and an understanding of the safety continuum.

The following sections provides the working group's recommendations for how FAA, in coordination with international partners, should move forward on ASISP rulemaking and the associated development of standards, policies, guidance material and best practices. The sections specifically address:

- 2.1 Importance of harmonization of regulatory standards.
- 2.2 Rulemaking Recommendations: Transport Category and Large Airplanes. This section also provides working group recommendations about how standards should be updated including with considerations for other aircraft types (i.e., rotorcraft and small airplanes) as applicable.
- 2.3 Rulemaking Recommendations: Rotorcraft
- 2.4 Rulemaking Recommendations: Small Airplanes
- 2.5 Rulemaking Recommendations: Engines and Propellers
- 2.6 Additional Direction Provided by U.S. Congress: This section provides a detailed analysis and review of In-Flight Entertainment systems based on direction provided by Congress as part of the FAA extension.
- 2.7 Phased Adoption of Standards

Chapter 2 of the report closes out with considerations for periodic reviews of the existing standards and the importance that any updates of the standards be based on data in 2.8.

2.1 Importance of Harmonization of Regulatory Standards

The FAA specifically included harmonization with other certifying authorities as a task given to the working group. To achieve this objective, the FAA invited representatives from the ANAC, EASA, and TCCA to participate as members of the working group. EASA, in support of global harmonization, also took steps to align its rulemaking schedule for cybersecurity[2] with the work of the ARAC ASISP Working Group.

Aircraft and their systems are certified and subject to validation of the certification in every country in which they operate. Significant efforts have been undertaken to ensure that the airworthiness standards for aircraft are harmonized to the greatest extent possible.

The three primary tasks given to the ASISP Working Group involve framing a way forward for potential agency rulemaking. The FAA tasked[3] the ASISP to:

1. Provide recommendation 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 should 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 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.

The working group prioritized the development of a proposed regulatory framework to address the FAA's tasks and to facilitate harmonization with other regulators, specifically EASA.[4] The EASA rulemaking programme includes the publication of a Notice of Proposed Amendment (NPA) in the third quarter of 2016 and a final amendment to Certification Specification (CS) 25 by the summer of 2017. (The FAA has not identified a schedule for possible agency rulemaking for ASISP.)

The working group views harmonization of the regulatory framework for aircraft system information security and protection as a priority for the manufacturer community. For transport category aircraft, the existing airworthiness standards and associated guidance material have to a great extent been harmonized among the primary certifying authorities (i.e., ANAC, EASA, FAA, and TCCA) to facilitate product development and certification. For these aircraft, the recommendation of the working group is to pursue similarly harmonized airworthiness standards for ASISP. Additionally, in an emerging field such as system security, there are benefits gained from cooperation among authorities and industry experts in establishing the new standards.

---

[2] RMT.0648 Aircraft Cyber Security. Available on EASA's website at: https://www.easa.europa.eu/document-library/terms-of-reference-and-group-compositions/tor-rmt0648 (Uploaded May 17, 2016).

[3] 80 FR 5881

[4] EASA published a preliminary regulatory impact assessment (RIA) in June 2014 titled RMT.0648 Aircraft cyber security for review by the agency's stakeholder bodies. EASA presented its rulemaking schedule for RMT.0648 at the September 2015 ASISP WG meeting. See, https://www.easa.europa.eu/document-library/rulemaking-programmes/2016-2020-rulemaking-programme

<u>Recommendation 01:</u> The ASISP working group recommends that the FAA work closely with the primary certifying authorities (i.e., ANAC, EASA, TCCA) to achieve harmonization for the airworthiness standards and guidance for Aircraft System Information Security / Protection.

2.2 Rulemaking Recommendations: Transport Category and Large Airplanes

The ASISP working group began its regulatory development work with transport category airplanes. The airworthiness standards for these airplanes are contained in 14 CFR Part 25,[5] Subpart F, Equipment. The ASISP WG proposes that the airworthiness standards for aircraft system information security protection be established as a separate requirement in Subpart F. Although sections 2X.1301 Function and installation and 2X.1309 Equipment, systems, and installations could be used for the purpose of addressing ASISP, experience gained by industry and authorities in recent airplane certification activities in combination with in-depth discussions among stakeholders has made it clear that there are benefits gained from establishing the requirements for security within a separate regulation against which the applicant must show compliance.

Key to the opposition against using 2X.1309 regulation to address security hinges on the fact that "intentional failure" is excluded from the 1309-regulation. Although aircraft security controls are planned, designed, implemented, and tested under the system umbrella, adding security within this framework was seen as difficult, if for no other reason than the expected very long time that amending the 1309-regulation is expected to take due to the large number and varying viewpoints of stakeholders. The addition of illicit acts (i.e., terrorism) to the 1309-regulation would also set an undesirable precedent in case future security concerns emerge. The current national emphasis on protection against cybersecurity threats resulted in industry and government stakeholders concluding that a new regulation specifically with that concern in mind appropriate.

The working group discussed addressing security as a particular risk (e.g., similar to High-intensity radiated field (HIRF) and lightning are addressed) and include security as just another set of requirements for aircraft system safety. There were strong and divergent opinions on the appropriateness of this, from both within the ASISP working group and from outside groups of other stakeholders in the aviation industry.

Given these implications, the conclusion of the ASISP work group was that a separate regulation from 2X.1309 was the best path forward, but that security can be addressed in a manner substantially similar to a specific risk.

2.2.1 Parallel versus Integrated Safety and Security Assessment

Establishing a separate regulatory requirement for ASISP does not prevent an applicant from complying by establishing security as integrated sub-activities within other established activities such as the safety process. On the other hand, establishing a single airworthiness standard which incorporates ASISP does not prevent an applicant from complying by establishing security as a parallel activity separate from the safety activity within the overall development process. The ASISP WG has concluded that there are advantages and disadvantages to both the integrated and parallel approaches, and that different applicants will find it to their advantage to make different choices, irrespective of whether the ASISP requirement is separate or incorporated with other regulatory requirements. Guidance material on ASISP includes guidance on shared interests between security and safety objectives which can be used either to implement integrated sub-activities, or to define required data exchanges for parallel activities (see section 2.2.4 for transport category airplanes).

[5] Other certifying authorities have issued airworthiness standards for transport category airplanes similar and to a great extent harmonized with FAA 14 CFR Part 25 Airworthiness Standards: Transport Category Airplanes including EASA Certification Specification (CS) 25 Large Aeroplanes.

2.2.2 Assumptions and Justification – Transport Category Airplanes

As discussed, currently, the FAA and other regulators rely on special conditions, issue papers, and associated policies to address ASISP.[6] The FAA Transport Directorate has been using research and applying Special Conditions (rule basis) with companion issue papers (means of compliance to the Special Condition rule basis) to address aircraft system information security protection since 2005.

The two main topics addressed in Special Conditions / Issue Papers are:

1. **Aircraft Electronic Systems Security Protection from unauthorized external access** "Addresses threats from external connectivity to aircraft systems from public networks such as the internet"

2. **Isolation of Aircraft Electronic System Security Protection from Unauthorized Internal Access** "Addresses threats across aircraft systems domains such as potential hacking of entertainment systems "

FAA special conditions are airplane model specific rules and are not general public rules. When required, an 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 that established by the existing airworthiness standards. The first Special Condition was applied to the B787 airplane program during 2005. During the last ten years the FAA has issued over 20 Special Conditions.[7]

When the issuance of a Special Condition is required, the proposed rule is published in the Federal Register for public comment. A companion issue paper (i.e., project specific policy or guidance on meeting the regulatory standard) that describes the FAA's expectations for compliance to address cybersecurity vulnerabilities and ASISP is also issued to the applicant. The ASISP Special Condition and companion issue paper cover the regulations, policies, and guidance material used to address cybersecurity threats.

Currently, the FAA's airworthiness standards do not specifically define how to address electronic cybersecurity vulnerabilities, whether operated in the NAS or world-wide. To address this issue in the near-term, the FAA issued policy statement PS-AIR-21.16-02 "Establishment of Special Conditions for Aircraft Systems Information Security Protection" in March 2014. This policy describes when the issuance of Special Conditions is required for aircraft systems that directly connect to external services or networks under specific conditions. The FAA has asked the ASISP working group to review this existing policy statement and provide recommendations for how to improve the agency policy for cybersecurity. The current policy statement, including any revisions issued by the FAA, will address cybersecurity and provide guidance to the applicants on when special conditions are required for particular aircraft designs until the FAA amends the existing airworthiness regulations. The aircraft

[6] The overview of the FAA's issuance of special conditions and associated policy was adapted from the 2015 Integrated Communications Navigation and Surveillance (ICNS) conference paper presented by Mr. Peter Skaves, Chief Scientific & Technical Advisor for Advanced Avionics, FAA, April 21-23, 2015, titled FAA Aircraft Systems Information Security Protection Overview.

[7] The following is a partial list of special condition issued on the following airplane programs. Airbus A350; Boeing B747-8, B767-2C, B787, and ONS equipped B737 and B777; ATR42-500 and ATR72-212A; Bombardier BD-500-1A ("C-Series") and Learjet 40/45; Cessna CE-680, CE-680A and CE-750; Gulfstream G280, GIV-X, and G650; and the Embraer EMB-550.

certification basis and date of application for new aircraft or modifications will determine the applicability of any amendment of the airworthiness standards incorporating the new ASISP certification requirements. (Detailed recommendations about the revision to the FAA policy statement on ASISP "PS-AIR-21.16-02" are contained in Section 3.1 of this report.)

The ASISP WG supports the FAA establishing airworthiness standards and means of compliance for ASISP. There are a number of principle objectives to a regulatory framework for ASISP including:

- (1) The objective of the airworthiness standards and associated guidance for ASISP is to ensure the safety of the aircraft.
- (2) The regulation should be objectives-oriented, succinct, and agnostic to the type of equipment, system, technology, or solution, because IT technology changes rapidly.
- (3) The requirement should not require specific security skills to be understood by the applicant.
- (4) The regulatory requirements should be outcome-based and acceptable means of compliance for ASISP should be identified in associated guidance (e.g., EASA Acceptable Means of Compliance and Guidance Material (AMC / GM), FAA Advisory Circulars (AC), Transport Canada Civil Aviation AC, and ANAC AC.
- (5) The airworthiness standards and associated guidance should be proportional to the assumed threat and risk based on the type of aircraft.
- (6) The airworthiness standards and associated guidance should be proportional to the assumed threat and risk based on the type of system architecture.
- (7) The regulation and, to the extent practicable, associated advisory and guidance material should be harmonized.

To address the difference in risk and incorporate regulatory concepts such as the "safety continuum" that is adhered to by both the FAA and EASA, the ASISP Working Group developed its recommendations for rulemaking in response to Task 1-3, along two paths: transport category (section 2.2.2 of the report) airplanes and all other aircraft types (section 2.3 and 2.4 of the report).

While the technology adoption and implementation that exposes aircraft system information security protection threats may be addressed at varying stages of implementation across the aviation sector categories (i.e., 14 CFR Parts 25, 23, 27, 29, 33 and 35) the fundamental threats and potential vulnerabilities are the same. The variation in the risk acceptance level is based on differences in exposure environments, the collective safety impact and the general perception that certain transport category airplanes may represent more attractive targets in terms or, for example, economic disruption.

The working group also separately looked at standards for engines (section 2.5) and provides a detailed overview of In-Flight Entertainment system (section 2.6).

2.2.3 Proposed Rule Text – Transport Category Airplanes

The ASISP has drafted a proposed amendment to 14 CFR Part 25, Subpart F. This proposed regulatory framework establishes a single set of objective airworthiness standards for all transport category airplanes. The proposed regulation is structured to be a clear set of discrete requirements that simplify the effort of the applicant providing evidence of compliance. The proposal does not provide specific threshold recommendations based on the size of the airplane (as does, for example RTCA DO-326A, which is applicable to Transport Category airplanes with more than 19 passenger seats), the complexity of the system, or the type of service or network with which the equipment or aircraft interacts. The proposed regulatory framework is instead general in nature. The intent is that the FAA (in coordination

with other regulators) establish appropriate means of compliance, based on the type of transport category airplane, and / or the type of system and interface, in associated guidance material published in coordination with issuance of the rule. For example, the working group supports tailoring these requirements through means of compliance and appropriate guidance for small transport category airplanes (e.g., 19 passenger seats or less).

In addition, the working group recommends not using terminology that differentiates governmental and non-government al services because of institutional differences in different regions; i.e., services that may be provided by the U.S. government or the FAA in the United States may be provided by non-government entities in other countries in which the aircraft operate. For example, although the United States government is the Air Navigation Service Provider in the United States, in Europe the regulator (i.e., EASA and individual civil aviation agencies) establishes the requirements for the Air Navigation Service Provider, but the services may be provided by entities that are stand-alone corporations or affiliated government entities.

ASISP proposed regulation amending 14 CFR 25, Subpart F, Equipment

> 14 CFR Part 25 – Airworthiness Standards: Transport Category Airplanes
> […]
>
> Subpart F – Equipment (§25.1301through 25.1461)
> […]
>
> $25.13XX Equipment, Systems, and Network Security Protection
>
> (a) Airplane equipment, systems and networks, considered separately and in relation to other systems, must be protected from intentional unauthorized electronic interactions that may result in an adverse effect on the safety of the airplane by showing that the security risks have been identified, assessed, and mitigated as necessary.
>
> (b) When required by paragraph (a), applicants must make available procedures and instructions for continued airworthiness to ensure security protections are maintained.

This proposed regulatory text builds on several key concepts:

- The term “intentional unauthorized electronic interaction” (or “IUEI”) was developed by way of joint work between RTCA and EUROCAE (see, section 2.2.4.1 for additional context and examples of what is intended by IUEI).
- The working group placed specific emphasis on addressing propagation (i.e., threat vectors) between systems which resulted in the set of terms “considered separately and in relation to other systems…” in the final draft of the text.
- The term “adverse effect on safety of the aircraft” limits the scope of this regulation to security breaches that impacts the safety and airworthiness of the aircraft and its operation versus security breaches that may impact non-safety systems on the aircraft. As an example, while the manufacturer and operator may have a real concern about protecting a device used to process passenger credit cards and securing the passenger’s information, the working group does not see this as being subject to FAA review and approval as part of the certification of the system,

but instead something that the operator or manufacturer would address as part of its business practices and responsibilities to the customer.

- The term "mitigated as necessary" clarifies that the applicant has discretion, as the applicant has for all risks, to establish appropriate mitigations against security risks. This is further laid out in the guidance to this regulation.
- The term "procedures and instructions for continued airworthiness" clarifies that – while the ICA may be one mechanism for providing the necessary instructions to maintain airworthiness – the security protections may go beyond traditional ICA material and also include other procedures provided to the operator. This aligns with existing practices among those applicants that have been issued Special Conditions to address ANSP.

Recommendation 02: The ASISP working group recommends that the FAA undertake rulemaking to update 14 CFR 25, Subpart F, to address ASISP based on the regulatory structure developed by the working group.

2.2.4 Guidance Material Supporting Implementation of Regulation

The working group recommends that the FAA, in coordination with other regulators, promulgate the proposed regulation for ASISP for large transport category airplanes. The propose regulations builds on close to a decade's work between airworthiness authorities and industry during certification projects, experience gained with special conditions and associated issue papers, and cooperative work in various industry standards groups. This section provides additional background for guidance needed in support of the regulation and select areas where work needs to continue to further refine the standards. Specifically the ARAC ASISP working group has identified the following 10 key areas that guidance materials should cover:

- GM1 – Definition of assets to be protected (2.2.4.3)
- GM2 – Definition of "intentional unauthorized electronic interaction" (2.2.4.1)
- GM3 – Guidance for how to identify security risk (2.2.4.4) and Security Environment (2.2.4.5)
- GM4 – Risk acceptability (2.2.4.4)
- GM5 – Security assurance and security effectiveness requirements (2.2.4.4)
- GM6 – Guidance for Type Design Changes, more particularly STCs (including those without access to OEM data) (2.2.4.2)
- GM7 – Acceptable certification evidence (2.2.4.6)
- GM8 – Scope of Security ICA (2.2.4.7)
- GM9 – Event logging and compliance with 14 CFR 21.3 (2.2.4.8)
- GM10 – Secure data sharing between applicant and authority (2.2.4.10)

Each of these topics will be discussed in the subsequent sections of this document. While there is industry consensus around the majority of these topics, several areas require additional industry standards development. As such, the ASISP working group recommended the FAA task RTCA SC-216 to further develop and harmonize around these topics. The result was a new TOR for SC-216 (see Appendix F) tasking them to update DO-356 to address these topics and harmonize with updates to EUROCAE WG 72 ED-203. Additional information is provided in section 2.2.4.9 below.

At the conclusion of the harmonization activities, and in conjunction with the guidance below, the ARAC ASISP working group recommends FAA to consider RTCA standards DO-326, DO-356 and DO-355 and

EUROCAE standards ED-201, ED-202, ED-203, ED-204 as acceptable guidance materials to comply with the security rule 25.13XX for large transport aircraft for new type certifications or new significant major changes or when the applicant elects to use them on a voluntary basis.

Recommendation 03: ASISP working group recommends FAA consider RTCA standards DO-326, DO-356 and DO-355 and EUROCAE standards ED-201, ED-202, ED-203, ED-204 as acceptable guidance materials to comply with the security rule 25.13XX for large transport aircraft for new Type type certifications or new significant major changes or when the applicant elects to use them on a voluntary basis.

2.2.4.1 Intentional Unauthorized Electronic Interaction (GM#2)

In the development of standards and regulations within the aerospace community, much discussion has formed around cyberattacks[8] -- what are they, and how they should they be addressed. Although the primary focus of mitigating the risk is still protecting the safe operation of the aircraft, cybersecurity events (cyber-attacks) are different than safety events and likewise are often mitigated differently in design and operation. To help create a distinction between the two types of events DO-326A has introduced the term Intentional Unauthorized Electronic Interaction (IUEI). This section provides a detailed definition and scope for what is and is not considered IUEI.

2.2.4.1.1 Intentional Unauthorized Electronic Interaction – Definition and Meaning

Intentional Unauthorized Electronic Interaction (IUEI) is defined as "[a] circumstance or event with the potential to affect the aircraft due to human action resulting from unauthorized access, use, disclosure, denial, disruption, modification, or destruction of information and/or aircraft system interfaces. Note that this includes malware and the effects of external systems, but does not include physical attacks such as electromagnetic jamming."[9]

To fully understand the term, the reader should consider the meaning of its individual parts in the context of a typical cyber-event:

- The word “intention” clarifies that the event originates with an intentional act from a human to separate it from other adverse events covered under ARP 4754A and ARP 4761, such as equipment failures, software logic errors, or human input or decision errors. To clarify, a person who writes a piece of malware defines the intention, not a person who unintentionally installs the malware, for example by inserting an infected USB device into a system.
- The word “unauthorized” specifies that the event is not defined as permitted within the system definition / function. Referring back to the example above, malware operating on a system conducts unauthorized activity that was not planned by the original system designer.
- The word “electronic” differentiates the interaction from physical attacks and is more easily thought of in the context of being digital in nature. Malware which results in a failed function is an electronic interaction whereas a hammer is not.

[8] Cyberattack in the context of aircraft systems is unauthorized access to aircraft electronic control or communications systems or maintenance or ground support systems for aircraft, either wirelessly or through a wired connection. (from https://www.congress.gov/crec/2016/04/06/CREC-2016-04-06-pt1-PgS1717.pdf)
[9] RTCA DO-356, Appendix B.2 , Glossary

2.2.4.1.2 Intentional Unauthorized Electronic Interaction – Some Principles

The distinction between what is and what is not an unauthorized interaction can seem complicated in the scope of DO-326A, but is perhaps easier to conceptualize with the understanding that the ultimate purpose is to cover malicious attacks that occur through digital means. Below are some principles to consider in determining whether an event falls within the scope of IUEI.

- The event is not the result of a purely physical attack, human error, or equipment failure.
- Analog attacks on digital hardware are not electronic interaction, but digital attacks through analog connections are ("electronic means digital, not electrical").
- The event can include digital read (unauthorized access to private data) or write operations (unauthorized modification of system configuration or function).
- The location of the origin of the attack is not important. Cyberattacks can originate from anywhere in the world.
- The event originates with a human actor's intentional act, such as a programmer writing malware, or a malicious hacker trying to gain access to connected aircraft systems.
- The attack isn't necessarily restricted to physically or wirelessly connected systems. (USB flash drives are a common means for attacking isolated networks.)
- Any and all events attributed to malware[10].
- The event is not the result of an accidental introduction of a vulnerability though configuration or a software defect does not constitute IUEI.
- An attempt to utilize a system vulnerability to modify the availability, integrity, or confidentiality of a system is IUEI.

2.2.4.1.3 Intentional Unauthorized Electronic Interaction – Some Examples

To assist in developing a comprehensive understanding of IUEI some specific examples are provided below.

- Misuse of designed system functionality to avert change or modify system operation to cause harm or danger.
- Personnel with privileged access accidentally introducing malware into a system which alters the system behavior or inhibits its function.
- A person compromising a system in light an unintentional reduction or deactivation of security controls.
- Use of a communication device to corrupt data communication (by interception, insertion or destruction, etc.) or test the access possibilities until a way of corruption is found.
- Capturing user information in an undetected manner (passively), to subsequently use them for malicious purpose.
- Rate-based attacks which saturate the systems resources or communication buses to inhibit function.
- Unauthorized use of another user's identification characteristics to obtain access rights and privileges.
- Execution of forbidden operations that damage system functions, or corrupt the data handled by the functions, causing misuses and unrecoverable reactions.
- Misuse of a provided functionality so as to damage or alter data in a manner to impact normal operation.

[10] **Malware** is broad term used to refer to many types of hostile or intrusive software including: viruses, worms, trojans, ransomware, spyware, adware, scareware, and other malicious programs.

- System delivery or installation in a manner that intentionally undermines security.
- Unauthorized use of rights to access systems to gain more privileges or to organize privileges so as to illegally grant or remove access privileges to others.
- Hidden software installed by a malicious person, including trojans, viruses, worms, bots, etc.
- Malware that waits for a specific event (often referred to as a time-bomb) after which it executes its payload.
- Mimicking the behavior of a real system (referred to as spoofing) to deceive an authorized user.
- Gaining access to a system by encroaching on someone else's privilege or identity for bypassing access controls (a form of man-in-the-middle attack).
- Gaining access to a system from outside a protected domain by impersonating or spoofing a trusted machine inside the protected domain. Once accepted as a trusted machine, the user may be able to corrupt function or data.
- Port scans and other interrogation techniques which identify networked systems for the purpose of identifying available services and possible system vulnerabilities.
- A memory resident virus which is incorporated into operational software code in order to corrupt a function.
- Malware on a maintenance computer developed by a non-aviation party that ends up on the computer because the user of the computer has access to the internet and downloads an inappropriate executable (.exe) file. The "intent" is captured in the development of the malware.
- An Electro Magnetic Pulse event is outside the scope of IUEI and ASISP.

2.2.4.2 Type Design Changes (GM#6)

The Supplemental Type Certificate (STC) applicant can find the applicable aircraft certification basis in the TCDS (Type-Certificate Data Sheet). TCDS are publically available on aviation authority web sites.

Every change to the Type Design (post-TC modification), initiated or not by STC, must comply with the applicable certification basis described in the relevant TCDS.

If security considerations are part of the certification basis (e.g., through a new security paragraph to be incorporated in CS-25 / 14 CFR 25 or a Security Special Condition), then the STC applicant shall produce evidence that the security level of the aircraft is not compromised.

This principle excludes any security demonstration during the STC approval process on a legacy aircraft for which security is not part of its certification basis, except if the Authority raises a new security Special Condition/CRI/IP or applies a generic CRI/IP or refers to guidance material giving security considerations for the system/function addressed by the change to the Type Design (e.g., FAA Policy Statement PS-AIR-21.16-02, FAA AC 120-76 or EASA AMC 20-25 for EFB).

2.2.4.2.1 Applicant responsibility to protect the aircraft systems

Prior to installation of a modification, the applicant must determine that the interrelationships between this modification and any other previously installed modification and/ or technical adaptations will not introduce any adverse effect upon the security and airworthiness of the product.

Four cases should be considered:

1) The STC applicant justifies that the system/function is completely isolated from the aircraft systems (no dataflow) or only able to receive data from the aircraft systems (unidirectional dataflow) and cannot interfere with aircraft systems.
2) The STC applicant justifies that the change remains outside the security perimeter [11] already certified by the TC holder with unchanged logical and physical interface. Examples include adding connectivity or other passenger systems outside the security perimeter.
3) If not covered by 1) or 2), e.g., the STC applicant installs or modifies a system/function which is able to send data to the aircraft system, or changes the aircraft systems interfaces (logical or physical), or creates a new access point (e.g., new or increased connectivity, new Field Loadable Software (FLS) importation means):
    a. On a case-by-case basis, the STC applicant obtains a data package from the OEM or an involvement of the OEM through a specific arrangement. Based on this data package or outcomes of the OEM involvement, the STC applicant should provide evidence using an acceptable process (such as those described in DO-326A/ED-202A) that the aircraft security level is or remains acceptable when embodying the STC change.
    b. Without OEM (TC holder) involvement or without OEM data, the STC applicant justifies that the aircraft systems are protected (including from threats propagation) via a security risk assessment to be approved by the relevant airworthiness authority. The security risk assessment should be completed using acceptable processes and methods (such as those methods in ED-203 or DO-356). Additional guidance for the comparability of risk assessments can be found in ED-201.

2.2.4.2.2 STC applicant responsibility to protect the NEW system installed by the STC change

The required level of security depends on the criticality of the new or modified system, subject to the STC change. Beyond the level of security required to assure that the system can properly perform its intended functions (if a required, essential or a critical system), the level of security ultimately required depends on the abilities, the integration level and the connectivity level of the system and is defined by the security risk assessment. For instance, depending on the outcomes of the security risk assessment, a system installed by STC, which has the ability to send data to critical aircraft systems, could be required to have a higher level of security than a system that only receives data.

In order to protect the new or modified system to be approved by STC, the STC applicant should carry out a security risk assessment at system level to be approved by the relevant airworthiness authority. The security risk assessment should be completed using acceptable methods compatible with existing

[11] The security perimeter catalogs the parts of the aircraft or system that contact external systems or users including passengers. These are the parts that support the interfaces and processes by which a system can be affected or interacted with from external sources or from unauthorized internal access. These dependencies are considered to be avenues for threats, such as threats from airline business information systems or in-flight entertainment systems. It includes the equipment that support physical links (e.g., ethernet ports, wireless transceivers), logical links (e.g., IP stack), network protocols (e.g., DNS, ICMP, gateways, packet filters), network services and clients (e.g., HTML server, FTP client/server, IPSEC server), security controls (e.g., packet filtering, encryption/decryption), and remote applications (e.g., file transfer services, remote monitoring, and web applications). When there is an addition or modification of connectivity and interfaces that can add new opportunities for security threats to adversely affect aircraft systems, then those interfaces should be included in the security perimeter.

aircraft security analysis of the aircraft (such as those the methods in ED-203 or DO-356). Additional guidance for the comparability of risk assessments can be found in ED-201. The security risk assessment should consider the possible threats from the aircraft systems in addition to the security environment (refer to the considerations of the security environment in paragraph 2.2.4.5 of this report).

2.2.4.3 Defining Assets to be Protected (GM#1)

The ARAC ASISP discussions have included the topic of what assets should be protected. This is from a safety hazard classification viewpoint. Within the working group, it was generally agreed that assets with a safety hazard classification of Major and above should be protected and that guidance being developed should be used to address those assets appropriately. However, there are some differences of opinion when discussing assets with safety hazard classification of Minor or lower (some disagreement on whether to use lower or simply state No Effect). Protecting an asset with a safety hazard classification of No Effect or even Minor is considered by some to be an unnecessary expense in implementation and certification. It is generally agreed that these assets do not need protection for themselves based on their potential impact to the aircraft. However, even for these systems an initial security assessment is needed to determine:

- The effect to hazard classification considering Safety Effect Caused by Security Events (SECSE)
- The potential impact on surrounding systems, no matter the hazard classification
- The mitigations and corresponding developmental assurance levels

This paragraph addresses the current discussion for determining when an asset must be protected, and also provides criteria to reify those concepts. A list of equipment is not provided, as it would become outdated before it could be published. Considerations for security controls at safety hazard classification of Minor and No Effect are also addressed.

2.2.4.3.1 Determination of Hazard Classification

It would be impossible to determine the hazard classification of an asset without some level of assessment of the asset and its security environment. The ASISP working group discussions have centered on what connectivity a Minor or No Effect asset would have and therefore what vulnerabilities might be introduced. This must consider assets that are part of the Type Certificate (TC), Supplemental TCs (STCs), amended TCs, or amended STCs.

The initial assessment can be very brief; it is dependent on the level of connectivity required by the asset under assessment. If the asset is part of the Aircraft Control Domain (ACD) or Airline Information Service Domain (AISD)[12], connectivity needs to be assessed in the context of the installed domain. If the asset has connectivity in one or more ways with other systems on the aircraft and/or off the aircraft, this needs further examination to determine the type of connectivity. Some regulators will exclude connectivity with governmental systems as those systems have a level of security that is accepted through other means. The connectivity can be important even in non-flight modes since during maintenance it could be used to update other systems. In the trivial case, the asset has no internal

[12] The Aircraft Control Domain (ACD) or Airline Information Service Domain (AISD) are defined in ARINC 811 and ARINC 664.

connectivity, it is not used in the ACD or AISD, and it is a Minor or No Effect hazard classification, then the assessment ends here.

The initial assessment can be brief but should answer the following questions at a minimum:

- What aircraft domain is the asset employed in?
- What electrical and RF interfaces exist between the asset and the remainder of the aircraft (internal connectivity)?
- What electrical and RF interfaces exist between the asset and governmental systems outside the aircraft (external governmental connectivity)?
- What electrical and RF interfaces exist between the asset and non-governmental systems outside the aircraft (external non-governmental connectivity)?
- In what phases of development, operations, and maintenance is the asset and its interfaces used?
- If connectivity defined by the above questions is positive, is digital data exchanged and in what directions?

The answers to these and any similar questions should be documented and used for discussion between regulator and applicant. The result of this assessment is to define the potential for unexpected SECSE on the asset in its intended environment and the potential for SECSE on other systems on the aircraft.

2.2.4.3.2 Potential Impact on Surrounding Systems

In the case that an asset has connectivity with another aircraft system, the level of connectivity with other systems and the possible interactions must be examined. The ASISP working group generally agreed that simple connectivity such as power is not the same concern as a bidirectional connection exchanging digital data. However, the domain in which the asset is employed can raise this level of concern.

A bidirectional connection to a Major or higher asset is a significant concern, but even connection to another Minor or No Effect asset will require assessment since it may not be designed to protect itself and may itself have connectivity to other systems. With a Minor or lower asset, the connectivity and propagation of SECSE is a genuine concern. Additionally, assets that have external connectivity utilized during non-flight modes can create SECSE through Field Loadable Software (FLS). Assets of Minor or lower already have safety provisions about connectivity to power busses common to other equipment so additional comments are not needed here.

Some questions that may help to identify assets that require closer examination to determine potential impacts include:

- Does the asset have write access internal connectivity to one or more onboard systems?
- Does the asset have external non-governmental connectivity, including airline operations centers, maintenance equipment, or wireless connectivity?
- Does the asset have bidirectional internal connectivity to other Minor or lower systems?
- Does the asset have write access internal connectivity during modes other than flight?

With additional connectivity comes the requirement to understand the operation of connected systems. The connectivity must be understood well enough to determine the behavior of the connected systems under SECSE occurring in the asset under assessment. This is more difficult when the asset is being deployed under an STC but does not relieve the applicant of the burden of proof when there is connectivity present with capability to interfere with the connected systems.

2.2.4.3.4 Defining Assets to be Protected – Summary

Recommendation 04: The ASISP working group recommends that the FAA establish guidance for Minor or lower equipment that has connectivity with other systems which should be protected.

The following statements summarize the position of the ARAC ASISP on protection of assets. These bullets summarize the concerns with Minor or lower equipment that has connectivity with other systems and may propagate SECSE to other systems. These statements form the suggested guidance that can be implemented by a regulator, such as in an FAA Advisory Circular, or in guidance produced by RTCA SC216, or some other means. This list does not direct the applicant how to protect the asset, but only identifies when protection may be needed. The applicant must perform an initial security assessment for assets with Minor or lower hazard classification to determine connectivity and possible impact to other aircraft systems.

Assets with hazard classification of Major or higher need protection based on their security assessments.

Protection is not needed when assets with hazard classification of Minor or lower have no internal connectivity to systems with Major or higher, including if having external connections.

Minor and lower hazard classification systems have the following exceptions to the above:

- **Protection is not needed when assets with hazard classification of Minor or lower have internal connectivity that can be shown to be read only and the read only enforcement is resistant to attack, such as hardware enforced.**
- **Assets with hazard classification of Major or higher need protection at the aircraft level (by design or by procedure) when systems of Minor or lower have internal connectivity (write access) to the Major or higher asset(s) based on the security assessment of the asset and the asset they are connecting to.**
- **Assets with hazard classification of Major or higher need protection at the aircraft level (by design or by procedure) when systems of Minor or lower have connectivity to the Major or higher asset(s), through one or more other systems no matter the hazard classification of those intermediate systems, based on the security assessment of the asset and the asset they are connecting to.**
- **Assets with hazard classification of Major or higher need protection at the aircraft level (by design or by procedure) when systems of Minor or lower have external non-governmental connectivity and have connectivity to Major or higher assets.**

Note: These are the scenarios that the working group reviewed, but others may exist and may be possible to identify in guidance material.

2.2.4.4 Security risk identification (GM#3), Risk Acceptability (GM#4) and Assurance Framework (GM#5)

The purpose of section 2.2.4.4 is to present a risk acceptability framework that will provide for:

- Regulatory requirements for security risk acceptability in airworthiness security type certification;
- Harmonization with risk management criteria in ISO 27005 and ED-201;
- Acceptability of currently recognized risk acceptability matrices; and
- Framework for regulatory authorities and applicants to negotiate alternate risk acceptability criteria.

The recommended approach is to tailor the requirements for risk communication and risk sharing as defined in ED-201 to meet the requirements of risk acceptability for security-related flight safety in TC, STC, and ATC.

This document also discusses considerations for using qualitative event likelihood to measure scale of threat.

2.2.4.4.1 Risk Acceptability Process (GM#3)

The purpose of the risk acceptability process is to demonstrate to authorities that the residual security risks are acceptable according to the criteria in the negotiated basis of certification. The figure below (2.2-1), taken from ED-201, shows the elements of the risk assessment as elaborated in ISO 27005. ED-201 also defines four areas of agreement for criteria for communicating risk. In this case, the risk communication is from the applicant to the regulatory authority.

FIGURE 2.2-1: ED-201 RISK ASSESSMENT STAGES

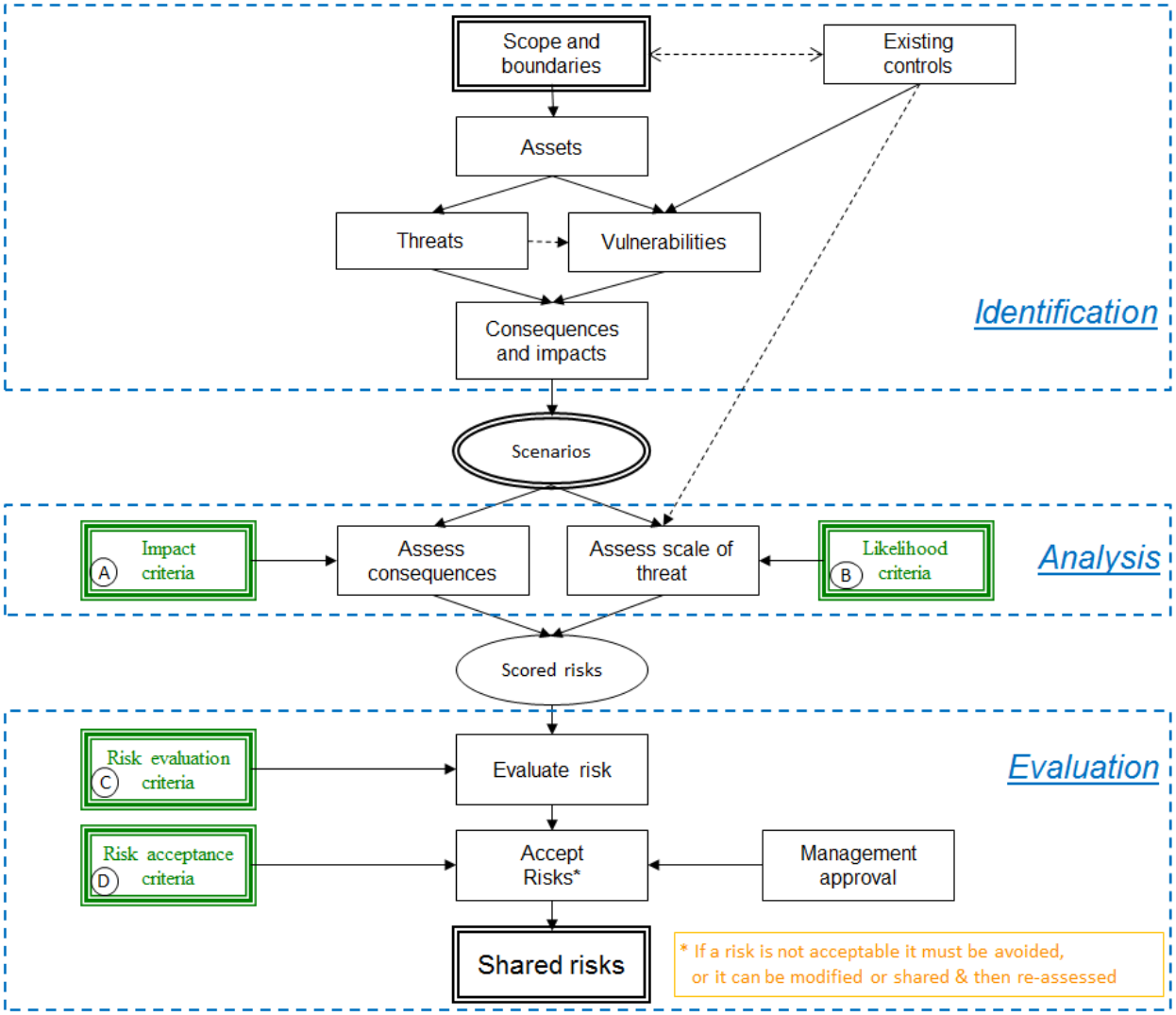


TABLE 2.2-1: RISK MANAGEMENT STAGES

ISO 27005 Stage	DO-326A Compliance	Shared Criteria
Risk Identification	Security Risk Assessment / Threat Scenario Identification	Risk Evaluation Criteria
Risk Estimation / Analysis	Security Risk Assessment / Evaluation of Severity and level of Threat	Impact Criteria and Level of Threat Criteria
Risk Evaluation	Risk Acceptability	Risk Acceptance Criteria

2.2.4.4.2 Risk evaluation criteria (GM#3)

Risk evaluation criteria establish what classes of risks are being evaluated, including classes of assets and classes of threats.

This paragraph is specifically concerned about the airworthiness of the aircraft with respect to intentional unauthorized electronic interaction. The scope of what equipment and systems are being assessed, and the scope of the security environment and issues of trust, are negotiated as part of the basis of certification.

Compliance is through the Plan for Security Aspects of Certification, and/or (in the case of modifications) the security aspects of the Change Impact Analysis.

2.2.4.4.3 Impact criteria (GM#3)

Impact criteria defines how the degree of damage or costs to the organization caused by an information security event will be communicated.

This document defines the impact criteria to be measured according to the standard safety effects of Catastrophic, Severe/Hazardous, Major, and Minor, as caused by Intentional Unauthorized Electronic Interaction.

2.2.4.4.4 Scale of threat criteria (GM#3)

Scale of threat criteria defines how to measure the expectation that the threat will materialize, or in ISO 27005 terms, the chance of the threat happening.

Different organizations and standards have defined different measures. Possible candidates have included qualitative event likelihood, difficulty of attack, and effectiveness of protection.

This document requires that the scale of threat criteria should be compatible with the impact criteria by negotiating a table showing the different severity levels with the acceptable scale of threat for each severity level. See tables below for examples from both the security domain and the pure safety domain.

2.2.4.4.5 Risk acceptance criteria (GM#4)

The risk acceptance criteria is based on the regulatory requirements expressed in the risk evaluation criteria and the impact criteria. Table 2.2-2 shows related examples from the area of safety assessment for the evaluation of risk due to failure and the risk due to software defect.

The applicant should negotiate an acceptable scale of threat for each level of severity with the regulatory authority. Table 2.2-3 shows two possible candidates for acceptability of risk for security-related safety risk.

TABLE 2.2-2: EXAMPLES OF ACCEPTABLE RISK FOR SAFETY FOR NON-SECURITY APPLICATIONS

	Safety Effect of Failure	Safety Effect of Software Defect
Impact Severity	**Reliability Failure Rate per fl-hr**	**Software Design Assurance Level**
Catastrophic	< 10**-9	Level A + more
Hazardous	< 10**-7	Level B
Major	< 10**-5	Level C
Minor	<10**-3	Level D
No Effect		Level E

TABLE 2.2-3: TWO EXAMPLES OF ACCEPTABLE RISK CRITERIA FOR SAFETY EFFECT OF SECURITY EVENT

Impact Severity	**DO-356 Security Level of Threat Likelihood Scale**
Catastrophic	Extremely Remote + more
Hazardous	Extremely Remote
Major	Remote
Minor	Likely
No Effect	Frequent

Impact Severity	**ED-203 Level of Threat Security Effectiveness Level**
Catastrophic	Very High + more
Hazardous	High
Major	Moderate
Minor	Basic
No Effect	None

2.2.4.4.6 Considerations for use of Qualitative Event Likelihood (GM#3)

DO-356 uses a qualitative event likelihood to measure the scale of threat, expressed in terms of number of incidents that could happen for a fleet as it operates.

It can distinguish between a threat that can reasonably be expected to occur daily, from one that should only happen at most yearly, or only once in the life of an aircraft type. It cannot be used usefully to distinguish between monthly and weekly. Roughly speaking, the qualitative event likelihood only cares about two orders of magnitude; e.g., the difference between 10 and 1000.

It is not a predictive measure. It is based on currently known factors and trends ("if this goes on…"). Future unpredicted events are managed through monitoring and changes to maintain continuing airworthiness. Trends in increasing computer power and connectivity provide a known factor that should be considered in the scale of threat and will help drive robustness and margin in design and controls will aid in limiting the need for future changes.

Reductions in the qualitative event likelihood should be conservative and based on factors that are under control or can be verified. Reducing the qualitative event likelihood of GPS spoofing by expecting passengers to not carry on a GPS pseudolite because historically they haven't is not conservative unless its presence is monitored so that in the future it could be forbidden in carry-on luggage. Reducing the qualitative event likelihood of GPS spoofing because multiply-redundant navigation systems provide

cross-checks that will detect GPS errors is legitimate, because the cross-check is part of the type design basis (although the performance of such cross-checks should be taken in consideration).

Similarly, taking credit for a likelihood reduction due to software features that aren't known to attackers should only be done if there are also measures in place to ensure the confidentiality of the software features and design.

The major determinants of the qualitative event likelihood are:

- External Access: The ability of relevant security controls (including, if not primarily, organizational) in place to control or prevent access to each external access point. This is generally expressed in terms of the organization and access role that is involved (e.g., "cabin crew", "maintenance technician", "general public", "passengers"). DO-356 defines "trustworthiness" to be the level of assurance that the security is adequate for the external access point.

- Security Controls: The ability of the security controls "as-is" (as designed and implemented, including the presence of known vulnerabilities and defects) to control or prevent access by unauthorized elements. Note that these access roles defined in "External Access" include unauthorized access as well as intended access (e.g., distinguishing authorized users of a ground connection from unauthorized (e.g., cleaning crew) personnel as "authorized support" vs. "general public".)

- Operations: The operational profile of the aircraft equipment, including all phases of operation including maintenance.

Other factors can be considered as well, but will not be discussed further here.

2.2.4.4.7 Considerations for use of Difficulty of Successful Attack / Effectiveness of Protection (GM#3)

ED-203 uses the effectiveness of protection to measure the scale of threat. This section 2.2.4.4.7 is an excerpt from ED-203, used with permission from EUROCAE, and presents the following considerations:

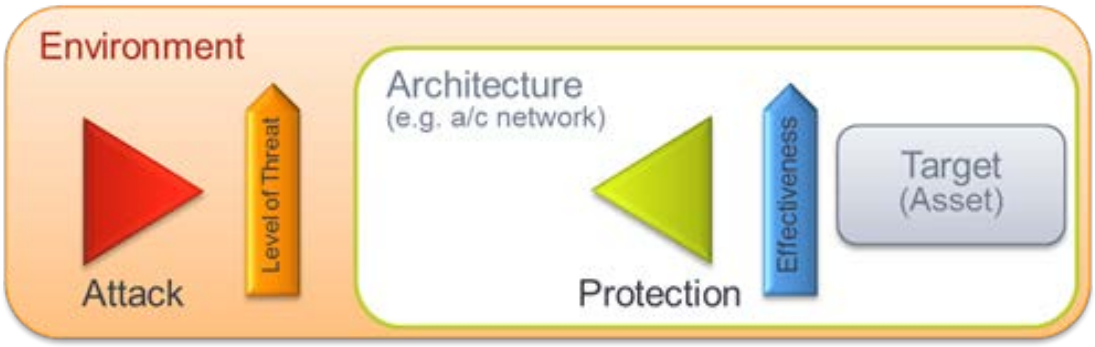
Relation of Effectiveness and Level of Threat

In ED-202A / DO-326A, the term "Effectiveness" (of security protection) has been used and is formally defined as "the ability of a security measure to protect an asset against the threat scenarios identified during Security Risk Assessment". Its notion is described as "the concept and term that describes how well the aircraft is protected against unauthorized interactions". Thus effectiveness could be interpreted as the "protection-centric" perspective or defender perspective.

The term "Level of Threat" is defined in ED-202A / DO-326A as "A qualitative evaluation of the possibility that a Threat Condition might occur." It can be expressed in at least two ways: as the likelihood that a threat scenario can be successfully completed, or the difficulty of attack that security measures, the target (asset) and security properties of other elements of the threat scenario expose to the attack. Thus level of threat could be interpreted as the "attack-centric" perspective (though **not** the one of an individual attacker, as this would be subjective!).

In summary, the evaluation of likelihood depends on attack properties and relies on what is known now about threat incidents rather than predictions, whereas the evaluation of effectiveness depends on protection properties about which assurance statements can be made. Figure 2.2-2 illustrates these two different perspectives showing how the attack-centric perspectives relies on what is known of the security environment while the protection-centric perspective is based on assurances accomplished by security mechanisms.

FIGURE 2.2-2 RELATION OF EFFECTIVENESS AND LEVEL OF THREAT (FIGURE 2-11 FROM ED-203)



Hence, effectiveness and level of threat can be interpreted as two perspectives of the same subject.

Level of Threat Evaluation considerations

The level of threat will be evaluated using multiple criteria. The evaluation that is applied to determine the level of threat based on its criteria should be specified in the method used to evaluate the Level of Threat of a given attack. The method needs to express without ambiguity when and where human expert knowledge / engineering judgment is applied (and when and where it should not be applied). The level of threat can be expressed by the effectiveness of security measures against an attack or by the exposure[13] of the target to an attack due to its vulnerabilities (summation of effectiveness or reduction of exposure).

Methods should at least evaluate the following criteria or be able to translate their criteria to these criteria in order to be comparable with the framework within this document. The mandatory criteria are defined as follows:

- **Elapsed time to prepare the attack** is the minimum amount of time taken by an attacker to identify the potential vulnerabilities that may exist in the target and the security measures, to identify potential attack vectors and attack paths, to acquire and/or build equipment and to develop and test potential attacks.
- **Elapsed time to perform the attack** is the minimum amount of time taken by an attacker to conduct an attack against the target.
- **Expertise required to prepare the attack** is the level of knowledge of a general topic needed for attack preparation. Examples include a specific technology, product, procedure or vulnerability identification method.

[13] Some methods may express exposure as likelihood

- **Expertise required to perform the attack** is the level of knowledge of a general topic needed to conduct the attack. Examples include a specific technology, product, procedure or attack method.
- **Knowledge of the target** is the specific level of knowledge or information about the target and attack path that is required to prepare and conduct the attack.
- **Window of opportunity** is the consideration that an attack is only possible at certain times (for example only during maintenance of the target) or under certain circumstances (for example an attack is only possible during other failure or attack events or an attack attempt that has to be sustained for an extended amount of time or repeated multiple times).
- **Equipment required to prepare the attack** is the kind and amount of equipment, tools and resources needed to prepare and test the attack. Examples include samples of the target, software analysis tools, software and hardware attack tools, computing power (e.g., a server cluster to compute specific rainbow tables).
- **Equipment required to perform the attack** is the kind and amount of equipment, tools and resources needed to conduct the attack. Examples include use of specific technologies or products, software and hardware attack tools, botnets.

These criteria are not independent, but some of them may be substituted for each other in varying degrees. A method should include these criteria in such a way as to compensate for any dependence between criteria.

A method should define useful combinations of the mandatory criteria and possibly additional optional criteria for the Level of Threat Evaluation.

These criteria are based on the factors given in CEM [Common Criteria Evaluation Methodology V3.1] (see, ED-203 section B.4.2.2) to support comparability with Common Criteria Methodology where needed. In contrast to the 5 factors used in CEM, criteria for the attack preparation and those for attack execution are separate so that the same underlying considerations result in 8 criteria. This allows for a more accurate evaluation of threat scenarios in which attack preparation and attack execution are separated by a significant amount of time or distinct roles and persons.

2.2.4.4.8 Security Assurance in non-DO-178 certified systems (GM#5)

The current DO-356 document discusses systems that have robust security requirements and defines a correlation between the DO-178/DO-254 design assurance process that implements the systems security requirements and the security assurance of the system. While this provides a clear methodology for taking certification credit for systems with DAL D and higher assurance, minimal consideration is paid to DAL E systems. In other words, based only on a DO-178/DO-254 design assurance process, DAL E systems could be assumed as to not provide any security assurance. In practice, DAL E systems with security controls that have been implemented and verified to function as intended, in accordance with an additional security assurance process, can provide a meaningful layer of security protection. Certification credit can be taken provided that the security assurance, as part of the security assurance process, is demonstrated as commensurate with the level of threat. Additional work is needed by SC-216 and WG-72 to further define and harmonize this concept as part of the update to DO-356.

2.2.4.4.9 Risk Acceptability and Assurance Framework (GM#4 - GM#5) - Recommendation

Recommendation 05: The ASISP working group recommends the FAA task SC-216 to create harmonized standards with WG 72 around the Risk Acceptability and Assurance Framework based on

the guidance material outlined in sections 2.2.4.4.1 – 2.2.4.4.8 of this report. This harmonized standards material should be incorporated into the appropriate RTCA documents such as DO-356, and the equivalent EUROCAE documents.

2.2.4.5 Defining the Security Environment – An Example (GM#3)

The ASISP Working Group reviewed one example methodology for defining the Security Environment for an aircraft. This methodology has been deemed acceptable by several regulators and is the practice of at least one major OEM. The following is a summary of the considerations made by one OEM, but it is only one example of how an applicant may approach the exercise of defining the security environment for their project. It is essential that each applicant undertake an exercise to appropriately define a security environment for its products.

The process of defining the security environment for an aircraft requires that the applicant make determinations about accessibility of aircraft zones; the expected organization of the aircraft operator; mechanism for data communications; identifies external and remote access points The output of the definition of the Security Environment becomes an input into the applicant's risk assessment activities for identifying relevant potential threats.

The review of the Security Environment requires that the applicant identify relevant "domains" based on the aircraft architecture (e.g., on-board, ground, and air-ground communications). The applicant should also identify the major interfaces of the aircraft, such as with Air Navigation Service Provider and its navigation aid (e.g., VOR, DME, ILS, and GPS); airline operations centers; passengers; the aircraft OEM including continued operational safety activities; the OEM's suppliers; and maintenance repair and overhaul functions.

Having defined the Security Environment, the applicant then considers the trustworthiness of the elements of the Security Environment.

There are two recognized approaches in existing guidance for defining trustworthiness.
One approach described in RTCA DO-356 paragraph 2.1.4.1 considers the trustworthiness of the threat source with different possible levels according to the severity of misuse of the asset under assessment (e.g., the highest trustworthiness level is assigned to an entity using and managing assets of catastrophic safety impact).

Another approach considers "trustworthiness" as binary, where an entity is either considered "trustworthy" or "not trustworthy" for the purpose of the analysis. The procedures in place within an organization are part of the consideration whether an entity is trustworthy, or not. A zone can be considered a "trusted zone" if only authorized persons have access to that area. When something is considered "trustworthy" or within a "trusted zone", there are no requirements for additional threat consideration as part of the system architecture analysis.

TABLE 2.2-4 AN EXAMPLE SET OF ASSUMPTIONS TO SUPPORT THE BINARY DETERMINATION OF "TRUSTWORTHINESS" AS PART OF THE SECURITY ENVIRONMENT REVIEW USED BY ONE OEM ON ONE PROJECT

Assumptions about Aircraft Zones	
Trusted – Aircraft vicinity (i.e., physical access) – Flight deck – Nose / main landing gear – Forward E-bay – Cargo compartment – Aft bay – Flight Crew Rest Compartment – Cabin Crew Rest Compartment	Not Trusted – Cabin (including lavatories)
Assumptions about External Interfaces	
Trusted – Plugs, connectors, cables and any piece of equipment (even in the cabin) that are not readily accessible to unauthorized persons (i.e. located behind structure or interior panels and/or that require removal or tampering of aircraft parts).	Not Trusted – E-tools and media[14]
Assumptions about External Entities[15]	
Trusted: – Airports – Airlines – Aircraft manufacturers – Aircraft manufacturer suppliers – Air Navigation Service Providers – Maintenance Repair and Overhaul	Not Trusted: – Passengers
Assumptions about Data and Other ANSP Communications	
Trusted – ADS-B – ATC – ATN – GPS – ILS – VOR – TCAS	Not Trusted – AOC – GSM – Any IP data communications (e.g., SATCOM, WiFi and wired)

Recommendation 06: The ASISP working group recommends that the FAA establish guidance to show compliance with the rule requiring an applicant to define a security environment as required input of

[14] E-tools and E-media are mobile devices and media that can be connected to the aircraft to store data (e.g., USB mass storage devices, flash cards), maintenance equipment including GSE (e.g., PMAT, PDL, laptops) and remote access points, equipment to operate the aircraft by flight crew and cabin crew (e.g., Class II EFB and cabin crew PDA) and any other mobile devices including those brought onboard the aircraft by passengers.

[15] External entities include staff and infrastructure.

any security analysis. Defining the security environment should be done in accordance with industry standards, such as DO-356 or EUROCAE ED-203 at the latest version or equivalent guidance material. Defining a security environment may include a set of trustworthiness assumptions (as illustrated in Table 2.2-4). This security environment should be submitted to the airworthiness authority for agreement. This agreement remains granted for any further security risk analysis on a dedicated aircraft model, as long as the security environment remains unchanged. The example given in section 2.2.4.5 above can be considered as an acceptable method for defining a security environment.

It must be pointed out that a STC applicant, applying for a change of the Type design, should define a security environment as consistent as practicable with the one defined by the OEM, to not compromise the aircraft security level demonstrated by the OEM. Indeed, wrong assumptions in the security environment could unduly exclude some threats from the security risk analysis whereas they were considered as relevant by the OEM. This consistency can be validated by the airworthiness authority when reviewing the security environment descriptive document.

2.2.4.6 Acceptable Certification Evidence (GM#7)

Appropriate guidance for certification evidence is contained in RTCA/EUROCAE documents. This statement is supported by involvement of OEM, regulators, and suppliers in the development of DO-326A/ED-202A, helping assure that a comprehensive set of certification evidence was defined. DO-326A/ED-202A define the required content for certification evidence, however they do not define specific documents and there are multiple options on how to package this content into certification documents. One such packaging of the data, as outlined below, has been found acceptable by the FAA and EASA in previous certification projects and shown the below table as an example.

TABLE 2.2-5 ACCEPTABLE CERTIFICATION EVIDENCE (FROM DO-326A, TABLE 4.1)

Data Content (DO-326A Table 4-1)	Corresponding Applicant Data
Plan for Security Aspects of Certification (PSecAC)	Certification Plan Preliminary Analysis Final Analysis
Aircraft Security Scope Definition (ASSD)	Preliminary Analysis
Preliminary Aircraft Security Risk Assessment (PASRA)	Preliminary Analysis
Aircraft Security Risk Assessment (ASRA)	Final Analysis
System Security Scope Definition (SSSD)	Preliminary Analysis Final Analysis
Preliminary System Security Risk Assessment (PSSRA)	Preliminary Analysis
System Security Risk Assessment (SSRA)	Final Analysis
PSecAC Summary	Accomplishment Summary
Aircraft Security Operator Guidance (ASOG)*	Operator Guidance
Aircraft Security Verification (ASV)*	Test Plan and Test Cases Test Report

*Not listed in DO-326A Table 4-1, not required but proposed by one applicant.

Data that will be submitted to the regulator should be identified in the agreed upon certification plan. The scope of certification evidence will be different between an aircraft derivative versus a simple modification.

As illustrated above, there is no requirement to create ten separate documents from the DO-326A list or to define document structure in RTCA/EUROCAE documents. This list of required content can be grouped into 5-6 documents depending on the scope of the certification project, for example: Preliminary Analysis, Final Analysis, Test Plan and Test Cases, Test Report, Accomplishment Summary, and Operator Guidance. Additional options for grouping the data may exist, and the matrix above is intended to provide a sample of one possible method.

The certification evidence defined in DO-326A/ED-202A is not new and has been successfully implemented in past certification projects. Therefore, the certification evidence and guidance defined in RTCA/EUROCAE documents is appropriate and acceptable.

2.2.4.7 Scope of Security ICA (GM#8)

In order to interpret and comply with the proposed security rule 25.13XX (b) (see section 2.2.3) a guidance material has been considered as necessary by the ASISP working group to support the Design Approval Holder (DAH) and aircraft operators in ensuring continuous airworthiness. This encompasses the DAH providing procedures for the operator and maintenance instructions to ensure the aircraft equipment, systems, and network security protection are maintained, and it encompasses as well aircraft operators establishing a process to ensure security in their continuing airworthiness process.

This guidance material could be adopted by the FAA through an Advisory Circular (AC) and by EASA through an Acceptable Means of Compliance (AMC).

The ASISP working group has decided not to develop a new guidance material by itself, but to consider and to revisit existing relevant industry standards such as RTCA DO-355 and EUROCAE ED-204 and to identify recommendations for improvement/completeness as necessary.

DO-355 and ED-204 “Information Security Guidance for Continuing Airworthiness”, both released in June 2014, had been prepared jointly by respectively RTCA SC-216 and EUROCAE WG-72.

DO-355 and ED-204 are technically identical and provide guidance for the operation and maintenance of aircraft and for organizations and personnel involved in these tasks. They are intended to support the responsibilities of the Design Approval Holder (DAH) to obtain a valid airworthiness certificate and aircraft operators to maintain their aircraft to demonstrate that the effects on the safety of the aircraft of information security threats are confined within acceptable levels.

These documents are built on a principle of allocation of responsibilities between the DAH and the Operator.

As one example to illustrate this principle, DO-355/ED-204 recommends that:

- The DAH should provide guidance to the operators to establish policies and associated procedures for the handling and managing of airborne software.

- The operator should document and implement policies and procedures for handling and managing of airborne software regarding information security.

DO-355/ ED-204 is a companion document to ED-202A / DO-326A ("*Airworthiness Security Process Specification")* which addresses security aspects of aircraft certification and to DO-356/ED-203 ("*Airworthiness Security Methods and Considerations*") which provides a set of methods and guidelines that may be used within the airworthiness security process defined in ED-202A / DO-326A.

ED-202A / DO-326A and DO-356 / ED-203 are guidance for the DAH, notably to define security objectives, security requirements and security activities in order to define security measures for an adequate level of protection at type certification and when embodying a change to the type design. Those security measures can be security functions as part of the aircraft design, but as well, operational or maintenance procedures to be carried out by the Operator.

However, the adequate level of protection established at type certification has to be maintained during the whole life cycle of the aircraft. It is the reason why ED-202A / DO-326A and DO-356/ED-203 give recommendations to the DAH about procedures and instructions to ensure the aircraft equipment, systems, and network security protection are maintained.

However, an analysis of ED-202A/DO-326A and DO-356/ED-203 has shown a completeness issue that is not addressed by DO-355/ED-204 either.

Indeed, ED-202A / DO-326A and DO-356/ED-203 may give objectives or best practices for Continuing Airworthiness but without explaining how to meet these objectives. Such objectives should be completed by guidance and/or by pass/fail criteria.

In addition, Continuing Airworthiness considerations may be spread between different documents (ED-202 /DO-326A, DO-356/ED-203 and DO-355/ED-204) with a mix of responsibilities between DAH and operators and a risk of inconsistency or completeness between all those documents.

2.2.4.7.1 Scope of ICA – Recommendations

Upon ASISP working group's request, the RTCA PMC has asked the SC-216 to revise DO-356 in accordance with the Terms of Reference (TOR) released on March 17, 2016. Those TOR specify that the DO-356 changes should be limited to and informed by the ARAC ASISP Final Report and should be harmonized with ED-203. However, those TOR exclude revision of DO-355.

Recommendation 07: In accordance with SC-216 TOR (approved in March 2016), ARAC ASISP WG recommends to both RTCA SC-216 and EUROCAE WG-72 the following additional tasks:

- **Carry out an exhaustive review of ED-202A/DO-326A, DO-356/ED-203 and DO-355/ED-204 to identify missing continuing airworthiness objectives and to identify existing continuing airworthiness objectives without guidance and/or compliance criteria,**

- **Complete or add, when relevant, continuing airworthiness objectives allocated to DAH in DO-356/ED-203,**

- **Complete or add, when relevant, guidance to meet these continuing airworthiness objectives and compliance criteria such as correctness, completeness, consistency, validation and verification, evidences, …,**

- **If Continuing Airworthiness considerations applicable to the Operators are missing in DO-355/ED-204, assess the relevance and the consequences for updating DO-355/ED-204,**

- **If RTCA SC-216 and EUROCAE WG-72 decide to update DO-355/ED-204:**

    - **Assess the need to reactivate the former ED-204/DO-355 working group (SG-4)**

    - **Assess the opportunity to transfer the existing DAH-related continuing airworthiness considerations from DO-355/ED-204 to DO-356/ED-203, in order that Continuing Airworthiness considerations of DO-356/ED-203 be limited to DAH only and the Continuing Airworthiness considerations of DO-355/ED-204 be limited to Operator only,**

    - **Complete or add, when relevant, continuing airworthiness objectives allocated to the Operators,**

    - **Complete or add, when relevant, guidance to meet these continuing airworthiness objectives and compliance criteria such as correctness, completeness, consistency, validation and verification, evidences, …**

    - **DO-355 and ED-204 should remain harmonized as far as practicable**

Note: RTCA SC-216 was tasked in the March 2016 update to its TOR to use the preliminary analysis of ED-202A/DO-326A and ED-203 carried out in the frame of the ARAC ASISP activities as part of its joint work with EUROCAE WG-72. It is important that the ASISP working group report be provided to the standards committees to allow them to complete which has already identified some gaps to be addressed and allow the standards committees to complete the analysis as part of its update of the DO and ED material.

2.2.4.8 Event logging and compliance with 14 CFR 21.3 (GM#9)

Considerations and recommendations about Event logging and compliance with 14 CFR 21.3 for large transport airplanes are given in section 3.2.

2.2.4.9 New Tasks Assigned to SC-216 to Address Harmonization Issues

The FAA, based on discussions at the ASISP Working Group, presented a new task as part of the revision of the Terms of Reference (TOR) of RTCA Special Committee (SC) 216 at the March 2016 Program Management Committee (PMC) meeting. The tasking was intentionally narrow in scope, given a timeline that would support the FAA's development of guidance material, and builds on a detailed review and gap analysis between existing RTCA documents (i.e., DO-326A, DO-355, and DO-356) and the associated

EUROCAE documents (i.e., ED-202A, ED-204, and ED-203). Key to the TOR is an update to DO-356 to harmonize with EUROCAE ED-203 on the following topics[16]:

1. A definition of what assets have to be protected based on Safety Effect, determined by security assessment. (GM#1)
2. A definition of "intentional unauthorized electronic interaction" in the guidance. (GM#2)
3. Guidance on how to identify security risk, including guidance on what is trusted in the security environment. (GM#3)
4. A harmonized risk acceptability matrix, taking credit from previously accepted matrices as appropriate. (GM#4)
5. Guidance on how to demonstrate that residual risk is acceptable. (GM#5)
6. Guidance on how type design changes should be considered (such as STCs), including those without access to OEM data. (GM#6)
7. A definition of what constitutes acceptable certification evidence. (GM#7)
8. A definition of the scope of security Instructions for Continuing Airworthiness, including additional Design Approval Holder (DAH) guidance as appropriate. (GM#8)
9. Guidance for event logging and compliance with 14 CFR 21.3. (GM#9)
10. A definition of the role of trust in the security environment, including which service providers may or may not be trusted. (GM#3)

The Special Committee was directed to adopt the final recommendations of the ASISP Working Group about several key policy issues that had previously been debated in the standards group, but was determined to be more appropriately resolved in the ASISP Working Group. These policy decisions are described in this document in sections 2.2.4.

Recommendation 08: The ARAC WG recommends the FAA task SC-216 to work on Guidance Materials topics GM#1 – GM#9 in accordance with paragraphs 2.2.4.1 to 2.2.4.8.[17]

Recommendation 09: The working group recommends that the FAA consider the results of the SC-216 tasking (which is due in December 2017) as part of the agency's development of guidance for the regulation for the topics listed in section 2.2.4.

2.2.4.10 Process for Secure Data Sharing between Applicant and Authority (GM#10)

Due to the sensitive nature of security information, care should be taken to ensure that information is handled appropriately and only shared with authorized personnel, both within the applicant's organization and between the applicant and regulatory authorities. In the United States, the Transportation Security Administration has a data classification called "Sensitive Security Information" (SSI), which is defined as information that, if publicly released, would be detrimental to transportation security, as defined by Federal Regulation 49 CFR Part 1520. Applicants should review 49 CFR Part 1520

[16] This list of harmonization topics were identified by the working group during initial meetings and included the SC-216 TOR. The working group discussions further refined this list which is now found in section 2.2.4 of this report. The SC-216 TOR directs the Special Committee to consider the final ASISP working group report.

[17] The FAA updated the terms of reference of SC-216 at the March 2015 meeting of the PMC to allow the technical work to update the RTCA standards to begin in parallel to the completion of the ASISP working group report and to allow the work to be conducted in coordination with EUROCAE WG-72.

and take steps to assure they comply with it. Similar regulatory requirements may exist in other countries and be reviewed and complied with as well where applicable.

Applicants should make it clear that data submitted to the regulatory authorities is to be considered proprietary and should be returned to the applicant immediately following the completion of use by the authority. In addition, applicants should work with their regulatory authority to understand any specific information handling procedures for SSI information.

2.2.4.11 Supply Chain Control and Considerations

The working group reviewed several industry standards about methods for controlling the supply chain to address cyber security. The working group determined that no additional guidance was needed, because existing regulatory requirements for controlling supply chain are sufficient.

2.3 Rulemaking Recommendations: Rotorcraft

Special conditions have not been applied to rotorcraft as result of the FAA policy. Nevertheless rotorcraft are also candidates for issuance of cybersecurity special conditions when rotorcraft onboard system connects to untrusted services.

2.3.1 Assumptions and Justification: Rotorcraft

The ASISP working group proposes that the airworthiness standards for aircraft system information security and protection be established as a separate requirement in Subpart F of 14 CFR part 29 and 14 CFR Part 27 Rotorcrafts. The two regulations provide for a mechanism to address cybersecurity for rotorcraft through proportional safety/security requirements. The proposed regulation for small airplanes (see section 2.4) in a single regulation 14 CFR 23.1315 was considered by the group, but – because the rotorcraft airworthiness standards have not yet been updated[18] – the working group recommends instead including the proportionality by tailoring specific rules for 29 and 27 respectively to address cybersecurity. (The rotorcraft community also considered using the 1301/1309-regulations, but – as explained in section 2.2 of this report – similarly concluded that a stand-alone regulation would be more appropriate.)

Principles to a regulatory framework for ASISP are identified in the principles list in section 2.2.1 for transport category airplanes, and are also applicable to rotorcraft for the purpose of a regulation.

2.3.2 Proposed Rule Text – Transport Category Rotorcraft

Security issues and cyber threats are comparable with large airplanes. Today transport rotorcraft include more and more complex safety critical systems which could lead to catastrophic effects in case of successful cyberattacks on these systems. Airworthiness authorities should address transport category rotorcraft and transport category airplanes with similar security objectives. As an example, Part 29 is closer to Part 25, containing similar specific airworthiness requirements:

- Instrument systems,
- Operation with normal electrical power generating system inoperative,
- Safety critical equipment/systems.

The working group recommends that the regulation for transport category rotorcraft, however, be bounded to only require consideration of catastrophic and hazardous/severe major effects on safety as caused by intentional unauthorized electronic interaction. The working group has proposed this difference in regulation for transport category rotorcraft due the reduced exposure to threats of most rotorcraft operators in relation to part 25 large transport category airplanes.

ASISP proposed regulation amending 14 CFR 29, Subpart F, Equipment

> 14 CFR Part 29 – Airworthiness Standards: Transport Category Rotorcraft
> […]
>
> Subpart F – Equipment

[18] The FAA, in coordination with other regulators, is in the process of updating all regulation in 14 CFR Part 23 into a modernized regulatory structure. The FAA NPRM and EASA NPA were published in spring 2016. The work to modernize the rotorcraft regulatory structure, however, has just recently started.

[…]

$29.13XX Equipment, Systems, and Network Security Protection

(a) Rotorcraft equipment, systems and networks, considered separately and in relation to other systems, must be protected from intentional unauthorized electronic interactions that may result in catastrophic or hazardous/severe major effect on the safety of the rotorcraft. Protection must be ensured by showing that the security risks have been identified, assessed, and mitigated as necessary.

(b) When required by paragraph (a), applicants must make available procedures and instructions for continued airworthiness to ensure security protections are maintained.

Appendix A to Part 29 – Instructions for Continued Airworthiness
The applicant must prepare Instructions for Continued Airworthiness (ICA) applicable to security protection as defined by §29.13XX.

2.3.3 Proposed Rule Text – Normal Category Rotorcraft

The working group reviewed the draft policy statement and the history of the use of special conditions for rotorcraft. The working group concluded that Part 27 single engine rotorcraft are exempted from special conditions and that neither FAA or EASA have issued special conditions / CRIs against normal category rotorcraft as of today.

Part 27 rotorcraft, however, have operating capabilities, such as multiple engines, Cat A, and IFR capability, that are similar to Part 29 rotorcraft and may need to demonstrate security compliance, if critical systems are installed for similar operating capabilities.

The working group recommends that the regulation for normal category rotorcraft similarly be bounded to only require consideration of catastrophic and hazardous/severe major effects on safety as caused by intentional unauthorized electronic interaction. The working group has proposed this regulation for normal category rotorcraft to say:

ASISP proposed regulation amending 14 CFR 27, Subpart F, Equipment

14 CFR Part 27 – Airworthiness Standards: Normal Category Rotorcraft
[…]

Subpart F – Equipment
[…]

$27.13XX Equipment, Systems, and Network Security Protection

(a) Rotorcraft equipment, systems and networks, considered separately and in relation to other systems, must be protected from intentional unauthorized electronic interactions that may result in catastrophic or hazardous/severe major effect on the safety of the rotorcraft. Protection must be ensured by showing that the security risks have been identified, assessed, and mitigated as necessary.

(b) When required by paragraph (a), applicants must make available procedures and instructions for continued airworthiness to ensure security protections are maintained.

Appendix A to Part 27 – Instructions for Continued Airworthiness
The applicant must prepare Instructions for Continued Airworthiness (ICA) applicable to security protection as defined by §27.13XX.

Recommendation 10: The ASISP working group recommends that the FAA develop airworthiness regulations for rotorcraft in 14 CFR 27 and 29 and bounded the regulation to only require consideration of catastrophic and hazardous/severe major effects on safety as caused by intentional unauthorized electronic interaction.

2.3.4 Guidance Material Supporting Implementation of the Regulation: Rotorcraft

ASISP working group sees a need to tailor the compliance methods for transport category airplanes to be more suitable to proportional security needs in rotorcraft. This can be done by tailoring the existing RTCA/EUROCAE standards (DO-326A and ED202A) or by tailoring the GA Recommended Practices and Guidance for ASISP document (see section 2.4) as an acceptable method for rotorcraft. It should be noted that the RTCA and EUROCAE standards have the same content, but the RTCA documents are not applicable to rotorcraft yet, while EUROCAE documents are allowed to be applicable if tailored.

The rotorcraft industry believes that experience must be developed with both GA and RTCA/EUROCAE standards before they can be used for compliance with the regulation. The working group recommends that standards and / or best practices be reviewed and tailored for applicability to ensure the specific issues to rotorcraft for:

- The global airworthiness security process
- Airworthiness authority liaison process
- The security risk assessment related activities
- The security development related activities
- The security compliance means
- The security effectiveness and security assurance
- Security instructions for continued airworthiness
- CTSO / ETSO / TSO installation security requirements
- Post certification activities: e.g., vulnerability monitoring, forensic activity, Logs topics.

The ASISP working group recommends that AC 29-2C and AC 27-1B be updated in order to propose possible means for complying with new 2X.13XX security requirements.

Rotorcraft warrant specific consideration about security which should be identified in guidance to the regulation. The rotorcraft security scope has to take care of specificities in addition of the normal scope definition as provided in standards such as ED-202A/DO-326A. The GA Recommended Practices and Guidance (see, Section 2.4) have considered some of the same unique differences compared to non-air-carrier operations including:

- Cockpit and cabin not separated (except on very high lift helicopters),

- Specialized approval like emergency medical systems, hoisting, Very Important Person (VIP) transportation, or specialized operation like training, and offshore transport,
- Size of Operators.

The rotorcraft community notes that these differences identified for GA airplanes are in most ways also applicable to rotorcraft.

2.3.4.1 Best Practices: Rotorcraft

New guidance should be derived from DO-326A / ED-202A standards or GA Recommended Practices and Guidance (see, Section 2.4) since these standards add to current guidance for aircraft certification to handle the threat of intentional unauthorized electronic interaction to aircraft safety. They add data requirements and compliance objectives, as organized by generic activities for aircraft development and certification, to handle the threat of unauthorized interaction to aircraft safety and is intended to be used in conjunction with other applicable guidance material.

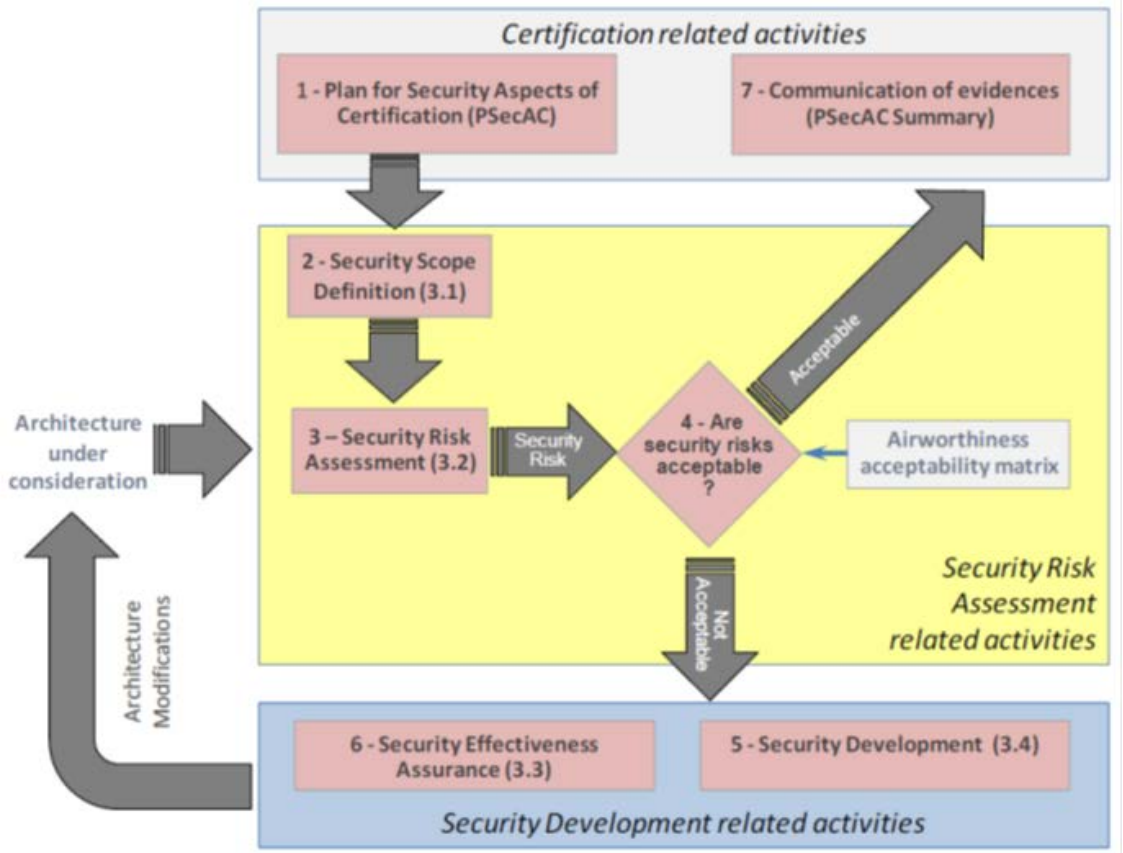
Tailoring by the applicant of these guidance documents may allow them to be applicable in other contexts such as Part 27 and Part 29.

These guidance material are for equipment manufacturers, aircraft manufacturers, and anyone else who is applying for an initial Type Certificate (TC), and afterwards (e.g., for Design Approval Holders (DAH)), Supplemental Type Certificate (STC), Amended Type Certificate (ATC) or changes to Type Certification for installation and continued airworthiness for aircraft systems.

The above standards address all the security activities requested to aircraft certification and give related objectives. They notably define:

- The global airworthiness security process
- The security risk assessment related activities
- The security development related activities
- The security compliance means
- The security effectiveness and security assurance
- Security instructions for continued airworthiness
- CTSO / ETSO / TSO installation security requirements

FIGURE 2.3-1 SECURITY PROCESS OVERVIEW EXAMPLE FROM EUROCAE ED-202A



2.3.4.2 Security related industry Standards

There are existing industry standards developed by EUROCAE/RTCA – in coordination with airworthiness authorities – that can be made applicable to rotorcraft including DO-326A / ED-202A, Airworthiness Security Process Specification, and be the basis for an update of AC 29-2C and AC 27-1B to address security. The GA Recommended Practices and Guidance (see, Section 2.4) can also be made applicable to rotorcraft.

Similarly, the rotorcraft industry notes that DO-356, Airworthiness Security Methods and Considerations, should be updated to state in the pre-amble that these Methods and Considerations may be tailored to make the standards more applicable to rotorcraft. The rotorcraft industry also notes that ED-203, Airworthiness Security Methods and Considerations, may become an acceptable means of compliance for rotorcraft, but that ED-203 should not be the only method for managing security risk assessment and security assurance.

Recommendation 11: The ASISP working group notes that DO-356 and ED-202, ED-203, and ED-204 are currently not aligned with respect to their applicability to rotorcraft and recommends that the documents should be updated and tailored to better address rotorcraft.

ED-203 provides methods and considerations for airworthiness security for the aircraft life cycle. The current version of ED-203 addresses activities for security risk management and security assurance. (ED-203 is a companion document to ED-202A / DO-326A.)

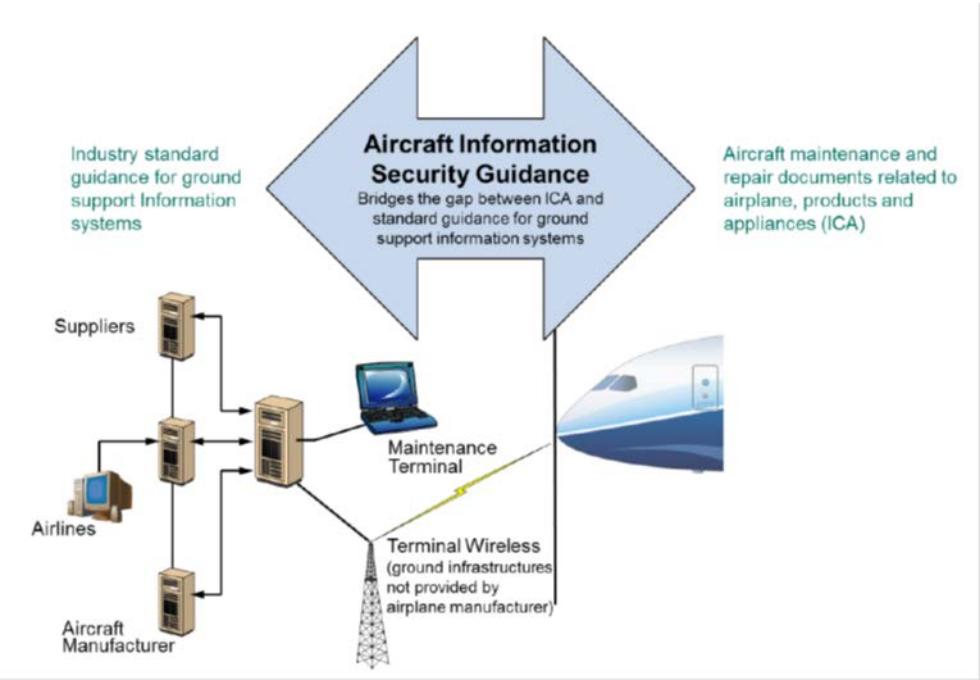
The ED-203 document is not mature and is not a complete means of compliance for certification at this time. As noted by WG-72, the document is incomplete and includes topics that warrant further deliberations. The document, however, provides an initial set of methods and considerations for security aspects for an aircraft and starting point for industry to assess their applicability to different aircraft types and systems.

Work is underway to update ED-203 to address Threat Condition Identification and Evaluation, Adequate Level of Protection, and Assurance Level.

The rotorcraft industry notes that ED-203, in its current version, cannot be considered mature enough to be used as an applicable standard for rotorcraft.

ED-204 / DO-355 address activities that need to be performed in operation and maintenance of the aircraft to address information security threats. (ED-204 / DO-355 are companion documents to ED-202A / DO-326A to address the product life cycle including operations, support, maintenance, and administration.) The current structure of ED-204 / DO-355 is focused on Large Transport Category aircraft, but do not make any assumptions about their applicability to other aircraft types. The rotorcraft industry believes that ED-204 / DO-355 can be tailored to become applicable to Part 27 and Part 29

FIGURE 2.3-2 AIRCRAFT INFORMATION SECURITY GUIDANCE EXAMPLE FROM ED-204 / DO-355



2.3.4.3 Other Standards that May be Applicable to Rotorcraft

The rotorcraft industry also reviewed other existing standards for their applicability to rotorcraft in context of ASISP. This review included from ISO / IEC (2700X: Information Security Management), NIST (SP 800-53: Security and Privacy Controls for Federal Information Systems and Organizations), ATA (Specification 42: Aviation industry standards for digital information security), and ARINC (ARINC-822:

Aircraft / Ground IP Communication; ARINC-823: Data-Link Security, ACARS Message Security; ARINC-827: Electronic Distribution of Software by Crate; ARINC-835: Guidance for Security of Loadable Software Parts Using Digital Signatures; and ARINC-852: Guidance for Security Event Logging in an IP Environment). The following sections 2.3.4.3.1 through 2.3.4.3.8 provide the results of the rotorcraft working group members' review of these standards for their applicability to rotorcraft.

The working group notes that the specific standards used will be negotiated between the applicant and the regulator per common practices on a project-specific basis.

2.3.4.3.1 Applicability of ISO 2700X: Information Security Management

Applicability to rotorcraft: Acceptable means, but not the only means for managing aeronautical security risks

The ISO/IEC 27000-series comprises information security standards published jointly by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC).
The series provides best practice recommendations on information security management, risks and controls within the context of an overall information security management system (ISMS), similar in design to management systems for quality assurance (the ISO 9000 series) and environmental protection (the ISO 14000 series).

The series is deliberately broad in scope and it is applicable to organizations of all shapes and sizes. All organizations are encouraged to assess their information security risks, then implement appropriate information security controls according to their needs, using the guidance and suggestions where relevant. Given the dynamic nature of information security, the ISMS concept incorporates continuous feedback and improvement activities, summarized by Deming's "plan-do-check-act" approach, that seek to address changes in the threats, vulnerabilities or impacts of information security incidents.
The main published standards related to "information technology - security techniques" are:

- ISO/IEC 27000 — Information security management systems — Overview
- ISO/IEC 27001 — Information technology - Security Techniques - Information security management systems — Requirements.
- ISO/IEC 27002 — Code of practice for information security management
- ISO/IEC 27003 — Information security management system implementation guidance
- ISO/IEC 27004 — Information security management — Measurement
- ISO/IEC 27005 — Information security risk management
- ISO/IEC 27031 — Guidelines for information and communication technology readiness for business continuity
- ISO/IEC 27035 — Information security incident management
- ISO/IEC 27036-3 — Information security for supplier relationships - Part 3: Guidelines for information and communication technology supply chain security
- ISO/IEC 27037 — Guidelines for identification, collection, acquisition and preservation of digital evidence

2.3.4.3.2 Applicability of NIST SP 800-53: Security and Privacy Controls for Federal Information Systems and Organizations

Applicability to rotorcraft: Acceptable means, but not the only means for managing security risks

Many organizations (including within aerospace industry) use well-known international information security standards as the basis or as a supplemental source of security controls for risk management.

To aid in selection and comparison, SP 800-53 Rev. 4 provides mapping tables to provide organizations with a general indication of security control coverage with respect to ISO/IEC 27001, Information technology– Security techniques–Information security management systems–Requirements and ISO/IEC 15408, Information technology -- Security techniques -- Evaluation criteria for IT security.

2.3.4.3.3 Applicability of ATA Spec42: Aviation industry standards for digital information security

Applicability to rotorcraft: Fully applicable

The purpose of this specification is to provide guidance for deployment of identity management solutions based on regulatory guidance such as FAA Advisory Circular 120-78A (Acceptance and Use of Electronic Signatures, Electronic Recordkeeping Systems, and Electronic Manuals)

Spec 42 provides recommendations on standardized methods to achieve the appropriate level of security for an application primarily relying on Public Key Infrastructures

Spec 42 includes policies for aviation-specific digital credentials called PIV-AV, which is based on the Personal Identity Verification – Interoperable (PIV-I) credential standard. PIV-AV will be recognized for use in the global aviation industry as a secure and reliable standard for enabling electronic user verification. Using PIV-AV, a single identity badge using standard certificate profiles can be used across companies to perform a variety of functions independent of the application provider or system owner; such as employees of other airlines or a third party MRO performing maintenance for another airline.

2.3.4.3.4 Applicability of ARINC-822: Aircraft/Ground IP Communication

Applicability to rotorcraft: Acceptable guidance for technical implementation of wireless connectivity.

This specification provides the functional and protocol interface definition based on IEEE 802.11 technologies. Other wireless technologies are possible for this link, but the minimum standard for aircraft to airport wireless communication is based on IEEE 802.11.

This document neither advocates, nor does it preclude, the use of other technologies. They may be added in future versions of this standard as the airlines deem them viable.

It is not the intent of this document specify a systems implementation, define components, or even imply an approach to such an implementation. However, given the availability of commonly available off the-shelf technology to implement Local Area Network (LAN) functions, it would be fairly easy to reach

such a conclusion. Ultimately, it is up to suppliers, manufacturers, and end customers (i.e., airlines) to determine the acceptance of products that comply with this specification.

2.3.4.3.5 Applicability of ARINC-823: Data-Link Security, ACARS Message Security

Applicability to rotorcraft: Acceptable guidance for technical implementation. Update could be required for rotorcraft purpose (TBD)

The purpose of this document is to provide an industry standard for ACARS Message Security (AMS), which permits ACARS datalink messages to be exchanged between aircraft and ground systems in a secure, authenticated manner using a uniform security framework. The security framework described herein is based on open international standards that are adapted to the ACARS datalink communications environment.

ARINC 823 Part 1 – ACARS Message Security, which is the first part of a two part specification, sets forth the provisions available to airlines and Datalink Service Providers (DSPs) to protect ACARS messages that are exchanged over traditional ACARS air-ground datalinks (VHF, HF, and SATCOM) and ground-ground communication networks.

The guidance includes the specification of:

- Technical security controls (i.e., security mechanisms that are implemented primarily in hardware, software, and firmware), including encryption, message authentication, and data integrity algorithms.

- Operational requirements for ACARS Message Security and specification of applications that may require ACARS Message Security are beyond the scope of this document. However, Part 2 of this specification provides important provisions and guidance for life cycle management of the cryptographic keys that are necessary for proper and secure operation of AMS.

2.3.4.3.6 Applicability of ARINC-827: Electronic Distribution of Software by Crate

Applicability to rotorcraft: Fully Applicable

EDS describes the format for the exchange of aircraft software parts and other digital contents between business partners without requiring the use of physical media. These business partners include airlines, airframe manufacturers, avionics suppliers, modification sites, and simulation.

Analogous to the practices of packaging and distribution of physical parts, this standard applies the concept of a "crate" to offer secure packaging features for software parts and related digital content. The EDS standard is intended to promote consistent, secure distribution of EDS content to any appropriate destination.

2.3.4.3.7 Applicability of ARINC-835: Guidance for Security of Loadable Software Parts Using Digital Signatures

Applicability to rotorcraft: Fully Applicable

This document provides background and detailed technical information on existing methods to secure loadable software parts. The solutions in this document use digital signatures attached to a file that is distributed with a software part to achieve the objectives of integrity and guarantee of origin.

The signature(s) of a signed software part can be checked at various points, including:

- Distribution: Signature(s) can be verified by any receiver of a software part to authenticate that it came from a valid source.
- Storage: Signature(s) can be verified during or after a software storage process to ensure software was not corrupted.
- Data Loader: Signature(s) can be verified prior to data loading to assure the software was not corrupted during distribution to the data loader.

2.3.4.3.8 Applicability of ARINC-852: Guidance for Security Event Logging in an IP Environment

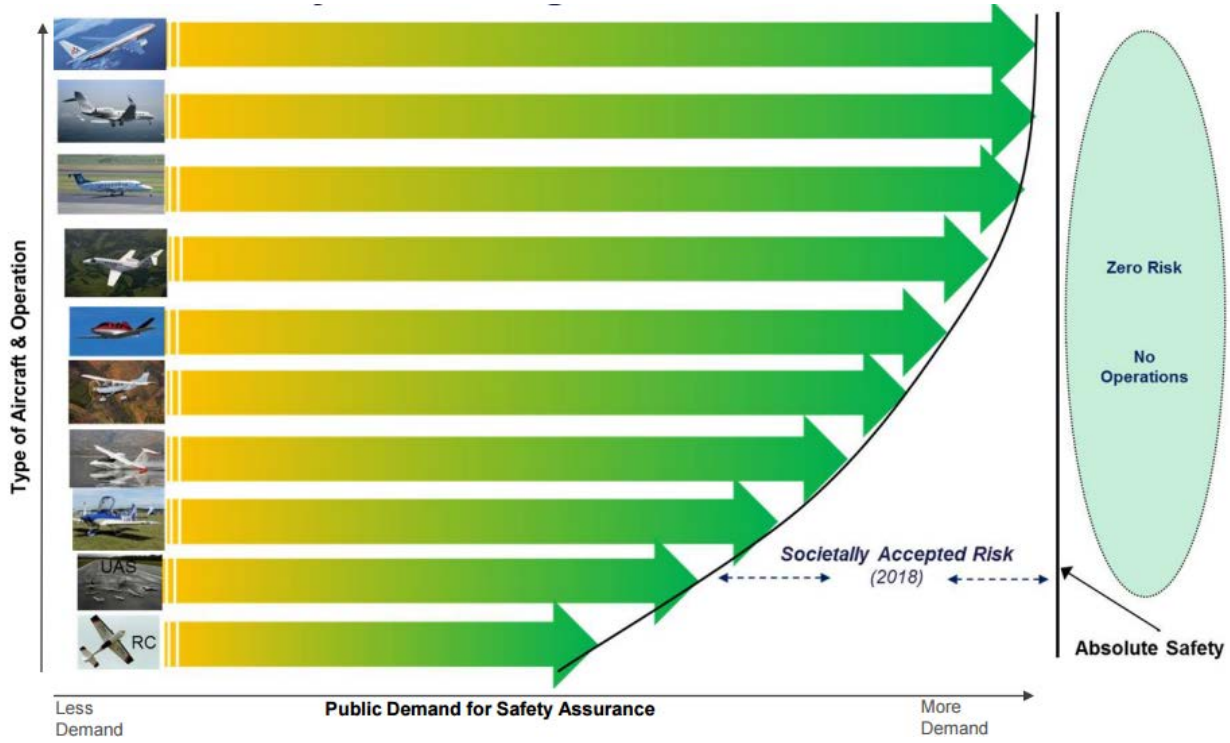
Applicability to rotorcraft: Draft Version; to be assessed when final version is published.

2.4 Rulemaking Recommendations: Small Airplanes

The airworthiness standards for small airplane design and certification are currently under review with parallel rulemaking projects by both FAA and EASA. The FAA issued a Notice of Proposed Rulemaking (NPRM) in March 2016[19] and EASA issued a Notice of Proposed Amendment (NPA) in June 2016[20] to address the same changes.

The primary changes underway shift from prescriptive airworthiness standards to industry-managed standards or best practices, making the regulatory requirements higher level and performance-based regulations. The restructuring also recognizes the benefits of implementing a "safety continuum" where appropriate airworthiness standards are established based on a recognition of risk acceptance for different types of airplanes.

FIGURE 2.4-1 FAA SAFETY CONTINUUM AND PUBLIC DEMAND FOR SAFETY ASSURANCE



The recommendations of the ASISP working group are structured to fit within the new regulatory framework for small airplane certification.

2.4.1 Proposed Rule Text – Small Airplanes

The FAA, in coordination with EASA, has proposed a comprehensive rewrite of Subpart F – Equipment for small airplanes. This includes a new performance-based regulation that addresses system or equipment failures in "23.1315, Equipment, systems, and Installations" which states:

[19] 81 FR 13452, 14 CFR Part 21, 23, 25, et al., Revision of Airworthiness Standards for Normal, Utility, Acrobatic, and Commuter Category Airplanes; Proposed Rule.
[20] NPA 2016-05, Reorganisation of CS-23

§23.1315, Equipment, systems, and Installation.
For any airplane system or equipment **whose failure or abnormal operation** has not been specifically addressed by another requirement in this part, the applicant must:

(a) Examine the design and installation of airplane systems and equipment, separately and in relation to other airplane systems and equipment to determine—

(1) If a failure [condition] would prevent continued safe flight and landing; and

(2) If any other failure would significantly reduce the capability of the airplane or the ability of the flightcrew to cope with adverse operating conditions.

(b) Design and install each system and equipment, **examined separately and in relation** to other airplane systems and equipment, such that—

(1) Each catastrophic failure condition is extremely improbable;

(2) Each hazardous failure condition is extremely remote; and

(3) Each major failure condition is remote.

The ASISP WG discussed whether the 23.1315 regulation could lend itself to also address ASISP requirements and supersede the need for a stand-alone regulation in a manner which the working group is proposing for transport category airplanes and rotorcraft. The working group – in coordination with the FAA – determined that the Part 23 rulemaking was too far along to include ASISP as part of the considerations of the on-going rulemaking as a specific topic at the time of the proposal.

2.4.2 Assumptions and Justifications – Small Airplanes

The ASISP reviewed the FAA's policy statement, the history of the agency's use of the policy statement, and whether any special conditions had been issued against Part 23 airplanes. . The ASISP concluded that the March 2014 policy statement and the ASISP revised policy statement (see, Appendix J) provide a mechanism to exclude small airplanes from special conditions. It is specifically noted that in the revised policy statement special conditions are not required for Part 23 Class 1, 2 and 3 airplanes as defined in AC 23.1309-1E "System Safety Analysis and Assessment for Part 23" and FAR Part 27 Single Engine Rotorcraft. (The ASISP working group also supports inclusion of Part 23 Class 4 as presented by ACE-100.) This does not mean that applicants do not consider security for aircraft systems and equipment as part of the certification of a small airplane.

This working group, as a result, concluded that the proposed 23.1315 is an appropriate regulatory vehicle by which airplane systems and equipment standards for Aircraft System Information Security / Protection to address airworthiness can be addressed. The easiest mechanism for the FAA, in coordination with other regulators, to address system security concerns is by establishing guidance that "abnormal operation" in the proposed 23.1315 also includes the applicant addressing Intentional Unauthorized Electronic Interaction (IUEI).

The revised Part 23 regulation also includes requirements to provide Instructions for Continued Airworthiness in the proposed regulation 23.1525. The working group views the proposed regulation for small airplane ICA to be sufficient to also address ASISP.

2.4.3 Guidance Material for Small Airplanes

Recommendation 12: The ASISP working group recommends that the FAA, as part of its guidance for 14 CFR 23.1315, include in the definition for IUEI that the applicant when showing compliance to "airplane system or equipment… abnormal operation… [that] has not been specifically addressed by another requirement in this part" also consider cybersecurity threats as an abnormal operation.

2.4.4 Best Practices for Small Airplanes to Meet ASISP

The ASISP working group recommends that the FAA ensure that proportionate processes are established for small airplanes with consideration of both the existing safety continuum and where small airplanes fall with respect to the overall threat of a security attack. The ASISP working group, building on prior work by a General Aviation Manufacturers Association (GAMA) working group, has developed a draft set of best practices that build on the standards developed by RTCA and EUROCAE. Work is underway to have this set of best practices further matured and issued by ASTM International.

The ASISP has supported the development of the best practice document.

Recommendation 13: The ASISP working group recommends that the FAA – in coordination with other regulators – work with industry in F44 (in a manner similar to how the ASISP has provided recommendations for tasks to be assigned to RTCA SC-216) to finalize and ballot for approval the best practices that support 14 CFR 23.1315 and addresses the topics identified in Section 2.4.4.1 for small airplanes.

In order to most expeditiously implement the security best practices, a phased approach (building on evolving industry consensus) should be implemented.

2.4.4.1 Topics to be addressed In GA Aircraft Best Practice Document (Initial and Secondary Phases)

Initial Phase:

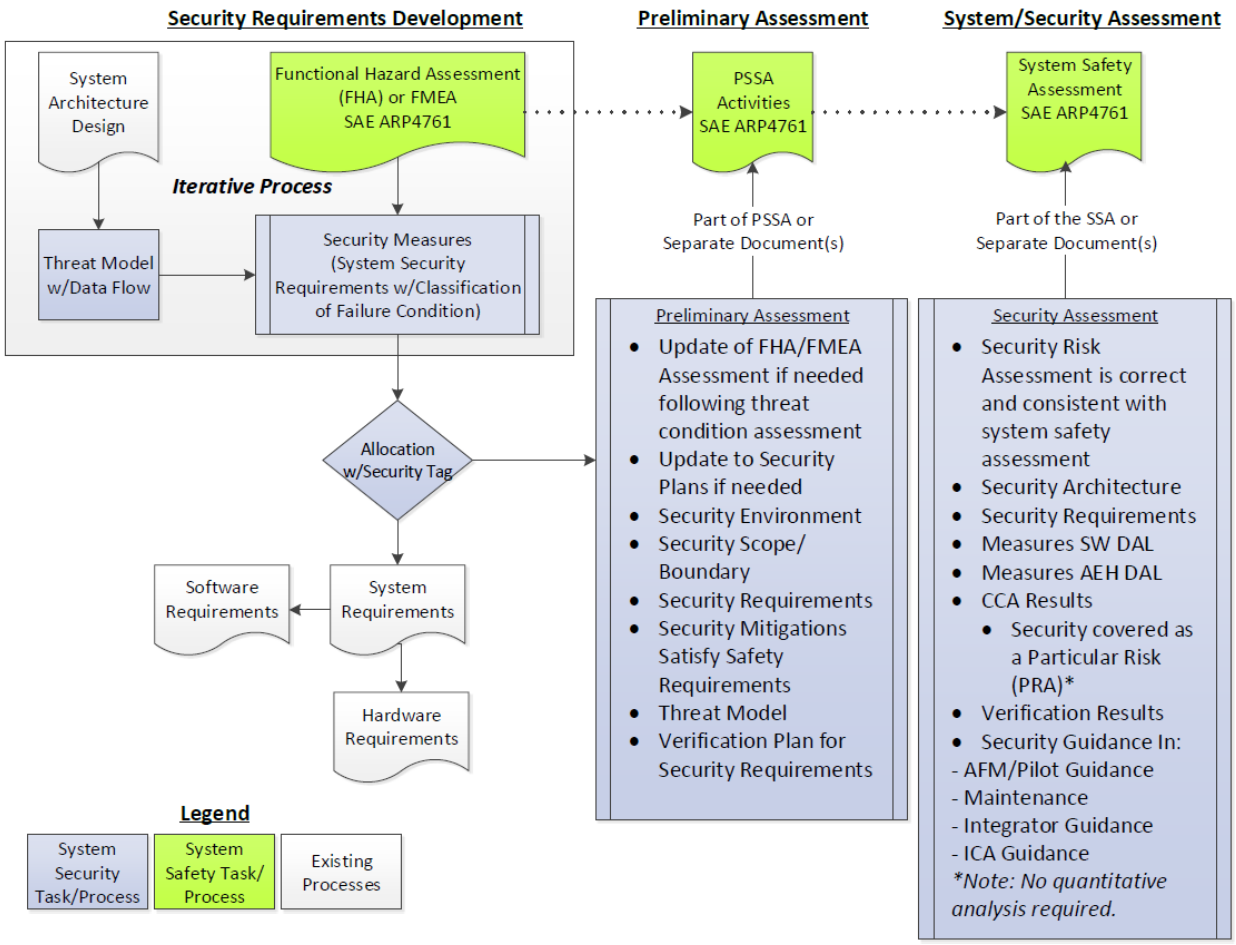
- System Concept of Operations including:
  - How to Define the Security Environment
    - Defining Trusted and Untrusted Actors
    - Setting the Security Scope / Boundary
    - Defining System Assets
  - How to Perform Preliminary Security Risk Assessment
    - Develop / Analyze Threat Model
  - How to Develop Security Requirements
- System Detailed Design including:
  - How to Perform Security Risk Assessment
  - How to Decompose Security Requirements
- System Implementation including:
  - Review of Input Handling and Validation
  - COTS Analysis
  - Static Code Analysis
- System Verification including:
  - Functional Security Testing

  - Application Fuzzing
  - Penetration Testing
  - Security Risk Assessment
- Operational Security Support including
  - Operational Guidance
  - Continued Vulnerability Assessment
- List of recommended certification evidence (e.g., objective tables)
- Considerations for Security Logging

Topics to be addressed – Secondary Phase

  - Definition of Security assurance
  - Definition of a risk acceptability matrix
  - Demonstration that the residual risks are acceptable
  - Considerations for Continuing Airworthiness

FIGURE 2.4-2 PROCESS DIAGRAM OF THE GENERAL AVIATION AIRCRAFT BEST PRACTICE DOCUMENT



The draft best practice document that will be matured by F44-50 also includes how to conduct a risk assessment using threat modeling.

The final draft version of the GA Best Practice document, which is still subject to balloting and additional work within the standards committee, is included in Appendix G. The task was accepted by ASTM F44 at its June 2016 meeting and the activity is on a schedule to be completed by early 2017.

2.5 Rulemaking Recommendations: Engines and Propellers

2.5.1 Assumptions and Justifications – Engines and Propeller Systems

The working group recommends that all rules, policies, and guidance applicable for avionics systems containing digital processing under 14 CFR Parts 23 and 25 be similarly applied to engines and propeller systems containing digital processing under 14 CFR Parts 33 and 35, with appropriate tailoring, in accordance with the guidance provided in DO-326A/ED-202A, DO-355/ED-204, and DO-356/ED-203.

A separate type certificate is issued for engines and propeller systems. At the same time they are connected to aircraft systems that receive a separate type certificate. Consequently, some tailoring may be made for engines and propeller systems. For digital communication networks, protection measures that apply to the engine or propeller system as a member of such a network and are demonstrated under 14 CFR Part 23 or 14 CFR Part 25 may be referenced. However, data connections, including hard-wired and wireless, to the engine or propeller system and unique to the engine or propeller system should be addressed separately under 14 CFR Part 33 or 14 CFR Part 35. The intent is that the engine or propeller system should be shown to be safe and secure (protected) when considered separately, but should not be required to re-certify protection mechanisms that are outside the scope of the engine or propeller system.

For example, if an engine or propeller system is a member of a particular trust domain within a secure aircraft network architecture, proper operation and security of the trust domains is a part of the aircraft systems requirements and is covered under 14 CFR Part 23 or 14 CFR Part 25. It is the responsibility of the engine or propeller system applicant to demonstrate compliance to network security requirements for membership within that trust domain, such as protection of the aircraft system against propagation of threats directed to the engine or propeller system.

Field-loadable software for engines or propeller systems that is directly loadable using ground support equipment should contain authentication mechanisms for off-aircraft handling that are separately demonstrated under 14 CFR Part 33 or 14 CFR Part 35. Field-loadable airborne software loaded onto ground support equipment for installation should be authenticated using measures that provide an adequate level of security (such as a digital signature). When not prevented by existing system hardware or architecture, on-aircraft handling of software loaded from ground support equipment onto the engine or propeller system should be similarly authenticated using measures that provide an adequate level of security.

Field-loadable software installed onto the engine or propeller system using another aircraft system (such as a cockpit data loader) may be treated as originating from a trusted source, as authentication for off-aircraft handling of field-loadable software entering such a system is covered under 14 CFR Part 23 or 14 CFR Part 25. However, the requirement for authentication during on-aircraft handling of field-loadable software for the engine or propeller system is the same regardless of the source of the data.

The 14 CFR Part 33 or 14 CFR Part 35 applicant needs to demonstrate compliance to all system requirements, including on-aircraft authentication of loads originating from inside the aircraft.

2.5.2 Proposed Rule Text

The ASISP has drafted a proposed amendment to 14 CFR Part 33, Subpart B and 14 CFR Part 35, Subpart B. The proposed regulatory text is intended to parallel the language proposed for 14 CFR Part 25, combining the provisions to a single item for information security protection and an update to the Instructions for Continued Airworthiness for each Part.

ASISP proposed regulation amending 14 CFR 33, subpart B – Design and Construction; General

§33.28 Engine control systems.

n) *Information security protection.* Engine control systems, including networks, software, and data, must be designed and installed so that they are protected from intentional unauthorized electronic interactions that may result in an adverse effect on the safety of the aircraft. The security risks and vulnerabilities must be identified, assessed, and mitigated as necessary. Applicants must provide procedures for the operator and maintenance instructions to ensure the engine equipment, systems, and network security protection are maintained.

Appendix A to Part 33 – Instructions for Continued Airworthiness

A33.1 d) The applicant must prepare Instructions for Continued Airworthiness (ICA) applicable to information security protection as defined by §33.28(n).

ASISP proposed regulation amending 14 CFR 35, subpart B – Design and Construction

§ 35.23 Propeller control system.

f) *Information security protection.* The propeller control system, including networks, software, and data, must be designed and installed so that they are protected from intentional unauthorized electronic interactions that may result in an adverse effect on the safety of the aircraft. The security risks and vulnerabilities must be identified, assessed, and mitigated as necessary. Applicants must provide procedures for the operator and maintenance instructions to ensure the propeller control system equipment, systems, and network security protection are maintained.

Appendix A to Part 35 – Instructions for Continued Airworthiness

A35.1 d) The applicant must prepare Instructions for Continued Airworthiness (ICA) applicable to information security protection as defined by §35.23(f).

Recommendation 14: The ASISP working group recommends that the FAA undertake rulemaking to update 14 CFR 33.28 to establish information security protection for engines. (Section 2.5.2)

Recommendation 15: The ASISP working group recommends that the FAA undertake rulemaking to update 14 CFR 35.23 to establish information security protection for propellers. (Section 2.5.2)

2.5.3 Guidance Material – Engines and Propeller Systems

Off-aircraft handling of data loads intended for direct loading to the engine or propeller system via GSE should be conducted with the same physical and organization security measures implemented for off-aircraft handling of data to be loaded via aircraft systems (such as a flight deck data loader).

Artifacts pertaining to the authentication of load images intended for loading onto engine or propeller systems should originate from the engine or propeller type certificate applicant (or a supplier of equipment to the applicant).

For guidance on authentication methods refer to the standards referenced in section 4.2, Field Loadable Data.

2.6 Additional Direction Provided by U.S. Congress

The FAA's prior Congressional authorization expired in 2015. Several recent security events have resulted in a specific focus on aviation security by Congress, including specific considerations about cybersecurity. On July 15, 2016, the U.S. Congress passed and the President signed into law the reauthorization. The bill specifically directs the FAA to address cybersecurity[21] and provides direction to the ASISP working group. The bill is mostly aligned with the charter provided for the ASISP working group by the ARAC, but places specific emphasis on In-Flight Entertainment systems. The working group took note of direction provided in the Senate during spring 2016 and elected to include a review of In-Flight Entertainment systems as part of its final report without returning to the ARAC to amend its charter, since IFE equipment is a system already within the scope of ASISP.

The specific direction given in the bill for In-Flight Entertainment system states:

> SEC. 2111 AVIATION CYBERSECURITY
> (a) COMPREHENSIVE AND STRATEGIC AVIATION FRAMEWORK. --
>
> (1) IN GENERAL. – Not later than 240 days after the date of enactment of this Act, the Administrator of the Federal Aviation Administration shall facilitate and support the development of a comprehensive and strategic framework of principles and policies to reduce cybersecurity risks to the national airspace system, civil aviation, and agency information systems using a total systems approach that takes into consideration the interactions and interdependence of different component of the aircraft systems and the national airspace system.
>
> (2) SCOPE.—In carrying out paragraph (1), the Administrator shall—
>
> (A) identify and address the cybersecurity risks associated with—
>
> (i) the modernization of the national airspace system;
>
> (ii) the automation of aircraft, equipment, and technology, and
>
> (iii) aircraft systems, including by—
>
> (I) directing the Aircraft Systems Information Security Protection Working Group—
>
> (aa) to assess cybersecurity risks to aircraft systems;
>
> (bb) to review the extent to which existing rulemaking, policy, and guidance to promote safety also promote aircraft systems information security protection; and
>
> (cc) to provide the appropriate recommendations to the Administrator if separate or additional rulemaking,

[21] Section 2111, Aircraft Cybersecurity

policy, or guidance is needed to address cybersecurity risks to aircraft systems; and

(II) identifying and addressing—

(aa) cybersecurity risks associated with in-flight entertainment systems; and

(bb) whether in-flight entertainment systems can and should be isolated and separate, such as through an air gap, under existing rulemaking, policy and guidance;

The following section 2.6.1 provides the results of the ASISP working group's In-Flight Entertainment Systems Review with appropriate references to earlier sections of this report including specifically section 2.2.4.2 (Type Design Changes including Defining Assets to be Protected).

2.6.1 Specific Considerations for In-Flight Entertainment Systems

This section provides a framework for a more thorough understanding the implications of aircraft information system information protection (cybersecurity) and potential for aircraft safety effects associated with installed miscellaneous non-required systems; more specifically in-flight entertainment and cabin connectivity systems installed in large transport category airplanes. The document provides the general context under which said systems are installed, the fundamental design principles associated with airplane safety, the general cyber resiliency of these systems, typical cyber protection measures, and additional non-airplane safety regulatory or industry compliance requirements. Lastly a discussion of the implications of imposing additional regulatory requirements onto said systems and the unique position these systems currently retain that enables a more rapid deployment of software updates to counter any cyber concerns.

2.6.1.1 Existing Regulatory References for IFE Certification and Security

The certification, installations, and security considerations of IFE are subject to a number of existing regulatory requirements and standards. The following is a summary list and references as used later in this section:

[A]. Title 14 Code of Federal Regulation [14 CFR] Part 25

[B]. EASA CS-25 Certification Specifications for Large Aeroplanes

[C]. AC 25.1309-1A System Design and Analysis, Advisory Circular

[D]. AMC 25.1309 Equipment, Systems and Installations EASA Acceptable Means of Compliance

[E]. FAA Order 8110.49 Chg. 1 Incorporated Software Approval Guidelines

[F]. AC 20-115B RTCA, Inc. Document RTCA/DO 178B

[G]. AC 20-115C Airborne Software Assurance

[H]. AC 20-174 Development of Civil Aircraft and Systems

[I]. AC20-168 Certification Guidance for Installation of Non-Essential, Non-Required Aircraft Cabin Systems & Equipment (CS&E)

[J]. PS-AIR-21.16-02, Establishment of Special Conditions for Cyber Security

[K]. Interim Policy Guidance for Certification of In-Flight Entertainment Systems on Title 14 CFR Part 25 Aircraft ANM 00-111-160

[L]. EASA AMC 20-115B Recognition of EUROCAE ED-12B / RTCA DO-178B

[M]. EASA AMC 20-115C Software Considerations for Certification of Airborne Systems and Equipment

[N]. EASA CM-SWCEH-002 Issue 01 Rev 01 Software Aspects of Certification

[O]. EASA Proposed CM - SWCEH – 002 Issue: 01 Issue Date: 10th of February 2011

[P]. JAA TGL 17 PASSENGER SERVICE AND IN-FLIGHT ENTERTAINMENT (IFE) SYSTEMS

[Q]. RTCA DO-178C Software Considerations in Airborne Systems and Equipment Certification

[R]. RTCA DO-178B Software Considerations in Airborne Systems and Equipment Certification

[S]. EUROCAE ED-12B Software Considerations in Airborne Systems and Equipment Certification

[T]. EUROCAE ED-12C Software Considerations in Airborne Systems and Equipment Certification

[U]. RTCA DO-313 Certification Guidance for Installation of Non-Essential, Non-Required Aircraft Cabin Systems & Equipment

[V]. RTCA DO-326A Airworthiness Security Process Specification

[W]. EUROCAE ED-203 AIRWORTHINESS SECURITY METHODS AND CONSIDERATIONS

[X]. SAE ARP4761 GUIDELINES AND METHODS FOR CONDUCTING THE SAFETY ASSESSMENT PROCESS ON CIVIL AIRBORNE SYSTEMS AND EQUIPMENT

[Y]. SAE ARP 4754 Guidelines for Development of Civil Aircraft and Systems

[Z]. Payment Card Industry (PCI) Data Security Standard, Requirements and Security Assessment Procedures, Version 3.2 April 2016

[AA]. APEX Specification 0403: MPEG-4 Content Specification & Content Security Requirements For Airline In-Flight Entertainment And Connectivity Systems

[BB]. Payment Card Industry (PCI) Data Security Standard (DSS): Requirements and Security Assessment Procedures (Version 3.2 of April 2016)

[CC]. Payment Card Industry (PCI) Payment Application Data Security Standard (PA DSS): Requirements and Security Assessment Procedures (Version 3.2 of May 2016)

[DD]. Payment Card Industry (PCI) PIN Transaction Security (PTS) Point of Interaction (POI): Modular Security Requirements (Version 4.1c of October 2015)

2.6.1.2 Identification of the Core Issue

Political, social media, and mainstream media driven concerns regarding the potential for cyber vulnerabilities in in-flight entertainment and cabin connectivity systems causing an airplane safety effect. Simply put perception becomes reality. This section intends to show the framework and

foundation that already exists for safety effect assessment and compliance is sufficient, capable and proven. A summary response is provided below.

1. Large Transport Category Airplane regulatory rules are safety driven and provide a solid foundation for any loss of function or anomalous function.
2. The process around which airplanes are determined to be compliant to the rules is robust, standards based, practiced and audited continually.
3. The existing FAA special conditions for security require assessment of physical and logical interfaces across the varying airplane systems.
4. A simple means to remove all power from these systems already exists for the flight and cabin crew.
5. There exist non-airplane security considerations in place for business needs that further buttress this foundation.
6. Most, if not all, suppliers are in the business of protecting their and their customers' brand names and reputation and as such have instituted security measures without regulatory requirements.
7. Most suppliers are participating or soon will do so in information sharing forums so that security collaboration happens at an ever-quickening pace.
8. There should be a legal framework for prosecuting attempts of intentional unauthorized electronic interaction.
9. Additional regulation would negatively affect the security posture of deployed systems.
10. IFE and Cabin Connectivity Systems leverage airport and aircraft physical security that contribute to overall security.

2.6.1.3 Certification Requirements, Industry Standards, and Implementations

This section provides a discussion of fundamental regulatory requirements associated with the installation of the subject systems, industry standards and typical security implementations. It also provides a reference to the associated requirements of the FAA regulations, Orders and policy as needed.

2.6.1.3.1 The Fail Safe Design Concept

Summary Point 1: Aircraft Systems do not get installed without rigorous safety assessments. Any system interconnection effects are integral to the safety assessment process (specific highlights below). The fail-safe design concept is inherent to approved designs.

Borrowing from AC 25.1309-1A published in June of 1988 [C]:

> "THE FAA FAIL-SAFE DESIGN CONCEPT. The Part 25 airworthiness standards are based on, and incorporate, the objectives, and principles or techniques, of the fail-safe design concept, which considers the effects of failures and combinations of failures in defining a safe design".

Furthermore the following 11 constructs from AC 25.1309-1A [C] have guided modern transport category aircraft design for almost three decades.

"The fail-safe design concept uses the following design principles or techniques in order to ensure a safe design. The use of only one of these principles or techniques is seldom adequate. A combination of two or more is usually needed to provide a fail-safe design; i.e., to ensure that major failure conditions are improbable and that catastrophic failure conditions are extremely improbable.
(1) Designed Integrity and Quality, including Life Limits, to ensure intended function and prevent failures.
(2) Redundancy or Backup Systems to enable continued function after any single (or other defined number of) failure(s); e.g., two or more engines, hydraulic systems, flight control systems, etc.
(3) Isolation of Systems, Components, and Elements so that the failure of one does not cause the failure of another. Isolation is also termed independence.
(4) Proven Reliability so that multiple, independent failures are unlikely to occur during the same flight.
(5) Failure warning or Indication to provide detection.
(6) Flightcrew Procedures for use after failure detection, to enable continued safe flight and landing by specifying crew corrective action.
(7) Checkability: the capability to check a component's condition.
(8) Designed Failure Effect Limits, including the capability to sustain damage, to limit the safety impact or effects of a failure.
(9) Designed Failure Path to control and direct the effects of a failure in a way that limits its safety impact.
(10) Margins or Factors of Safety to allow for any undefined or unforeseeable adverse conditions.
(11) Error-Tolerance that considers adverse effects of foreseeable errors during the airplane's design, test, manufacture, operation"

Summary Point 2: Aircraft Systems and system interconnection effects are integral to the safety assessment process. Highlights added to reflect system interconnection effect considerations.

AC20-174 Development of Civil Aircraft and Systems [H] prescribes ARP4754A Guidelines for Development of Civil Aircraft and Systems as an acceptable method for said systems. This document along with its predecessor ARP4754 [Y], and ARP4761 Guidelines and methods for conducting the safety assessment process on civil airborne systems and equipment [X] prescribe the need for functional hazard assessments at both the aircraft and system levels.

From ARP4754A:

"5.1.1 Functional Hazard Assessments
The functional hazard assessments (FHAs) should be carried out at both the aircraft and system levels. They should provide the following information relative to each function (aircraft or system level accordingly):
a. Identification of related Failure Condition(s).
b. Identification of the effects of the Failure Condition(s).
c. Classification of each Failure Condition based on the identified effects (i.e., Catastrophic, Hazardous/Severe-Major, Major, Minor, or No Safety Effect) and assignment of the necessary safety objectives, as defined in e.g., AC 25.1309-1A, AC23.1309-1D and AMC 25.1309 extended to include the No Safety Effect classification.

d. A statement outlining what was considered and what assumptions were made when evaluating each Failure Condition (e.g., adverse operational or environmental conditions and phase of flight). The goal in conducting this step is to clearly identify the circumstances and severity of each Failure Condition along with the rationale for its classification.

Since it is possible that use of common architectures or complex components in separate systems could introduce additional aircraft-level Failure Conditions involving multiple functions, the FHA should identify and classify these new Failure Conditions. When aircraft-level functions are integrated by a system or combination of systems, the FHA should be re-evaluated to identify and classify Failure Conditions involving multiple functions. If the FHA is constructed in system-oriented sections, traceability of hazards and Failure Conditions between the aircraft-level and system-level is necessary.

Implementation choices made during development may introduce common causes for multiple aircraft-level Failure Conditions or interactions between systems resulting in failure. These common causes could cross system or function boundaries. A review of the implementations of systems should be performed to determine if there are such conditions and if they should be added to the aircraft-level FHA."

2.6.1.3.2 The Nutshell Chart

Summary Point 3: There is structure, taxonomy and methods to the aircraft safety assessment process (see Appendix H).

The robustness of the design process, the assurance process and the necessary safety mitigations are driven by the safety effect categorization. Appendix H provides a simple summary of these effects, the effect categorization nomenclature, the assurance method categorization, the probabilistic categorization nomenclature, the quantitative probabilistic range and the system validation methods.

2.6.1.3.3 IFE and Cabin Connectivity Safety Requirements

Summary Point 4: These systems do not have a safety effect from loss of function. However, there are extensive qualification /certification efforts are undertaken to assure fail-safe and demonstrate non-interference with other systems.

These systems from a certification and safety perspective can be summed up in three statements

1. They don't have to work. These systems are not required by regulation and the failure to function has no impact to airplane safety.
2. When they fail they must fail nicely, e.g., no arc, no spark, no smoke.
3. They must "play nicely" with their "friends" on the airplane. In other words they cannot interfere electronically or electrically with other systems

FAA AC 20-168 [I] provides guidance for the installation of these systems.

2.6.1.3.4 FAA Special Conditions for Security

Summary Point 5: The existing FAA Special Condition for cybersecurity requires that interconnection of systems must address security protections.

> "1. The applicant must ensure airplane electronic system security protection from access by unauthorized sources external to the airplane, including those possibly caused by maintenance activity.
>
> 2. The applicant must ensure that electronic system security threats are identified and assessed, and that effective electronic system security protection strategies are implemented to protect the airplane from all adverse impacts on safety, functionality, and continued airworthiness.
>
> 3. The applicant must establish appropriate procedures to enable the operator to ensure that continued airworthiness of the aircraft is maintained, including all post Type Certification modifications that may have an impact on the approved electronic system security safeguards."[22]

The applicants including the original equipment manufacturers are of a general consensus that boundaries of trust must be established for the purposes of compliance to the special conditions. For simplicity and sustainment purposes the trust boundary generally does not include areas exposed to the general public. This typically defaults to not trusting sources, access points, or interface points exposed in the cabin. To show compliance the applicant will deploy multiple layers of protections between the cabin and other airplane systems.

Additionally, in large transport category airplanes the software loading processes for IFE and Connectivity Systems are distinct and separate from the other airplane systems. Frequency, size of software files and the technology pace for the IFE and Connectivity systems have driven this segregation and will continue to do so.

2.6.1.3.5 Security requirements outside of FAA regulatory purview already exist

Summary Point 6: Security assessments to comply with payment card industry data security standard (PCI DSS) and security standards for media protection.

IFE or Connectivity Systems which process credit card information are required to be compliant with the PCI DSS standards [BB] [CC] [DD] and must undergo schedule auditing. PCI DSS includes regular vulnerability assessment and penetration testing. IFE and Connectivity systems also provide digital rights management (DRM) protected content, the media providers typically assess the security measures or means in place to protect such content.[AA]

2.6.1.3.6 Security protections already exist within these systems

Summary Point 7: Suppliers of these systems already employ security measures for the aforementioned requirements as well as brand name protection, theirs and the operators.

[22] FAA Special Conditions for the 777-200/-300/-300ER Docket No. FAA–2013–0959; Special Conditions No. 25–504

In general IFE and Connectivity systems consist of three distinct architectural elements, a head end network, the distribution networks (wired or wireless) and the seat network. Providers of these systems already employ best practices security measures such as firewalls, gateway traffic direction, virtual local area networks (VLANs), traffic restrictions and network separation/segmentation and segregation. In addition most suppliers provide for logging functionality and regular offload and review, Intrusion Prevention/Detection Systems, Software Package integrity. Most of them deploy prevention and correction measures such as security processes to fix vulnerabilities (vulnerability and patch management) and deliver in the shortest time possible and in a secure manner in order to prevent any early exploitation.

On top of these best practices flowed down in IFEC systems from International and National recognised security standards, protection of confidentiality, integrity and availability of its assets (premium content, payment data, sensitive information) is increased. For example, the use of appropriate cryptographic measure enhances integrity and confidentiality of IFEC systems.

2.6.1.3.7 IFE and Cabin Connectivity Power Removal Requirements

Summary Point 8: There are existing means for IFE and Cabin Connectivity Systems in modern transport category airplanes that separately remove power from these systems.

FAA policy memo Interim Policy Guidance for Certification of In-Flight Entertainment Systems on Title 14 CFR Part 25 Aircraft ANM 00-111-160 [K] requires that "A means should be provided for the crew to disconnect the IFE system from its source of power." In Part 25 aircraft this requirement has been met by either providing a power removal switch in either, the flight deck, cabin area or both. Additionally this concept has been extended to cabin connectivity systems and may be incorporated as a separate switch or integral. The flight crew or cabin crew has a means to remove power and cease all system functions should they need to do so. Refer to Appendix I for a typical example.

2.6.1.3.8 IFE and Cabin Connectivity Systems physical security

Summary Point 9: IFE and Cabin Connectivity Systems leverage airport and aircraft physical security that contribute to overall security.

Airport Security: Airport physical security safeguards/measures (e.g., access control, security perimeter, passenger check) is a part of aircraft protection and especially, protect from anyone bringing physical tools to access IFE and Cabin connectivity systems. Aircraft Security: Physical access to IFE and Cabin connectivity systems is reserved to authorized personnel only. During flight time, cabin crew could identify suspect behaviors and prevent **malicious acts on IFE and Cabin connectivity systems when detected.**

2.6.1.4 IFE Recommendations

Recommendation 16: The ASISP working group encourages the IFE and connectivity industry to participate in information sharing partnerships.
It is increasingly common for suppliers of IFE to be engaged in information sharing partnerships to manage security. As an example, the Aviation ISAC has a growing number of participants from the IFE and connectivity equipment sector and they are working to maintain awareness of threat information by activity sharing information.

Recommendation 17 – The ASISP working group recommends that the FAA sets a legal basis prohibiting tampering with aircraft systems.

Tampering with an aircraft is prohibited today by U.S. statute and in the Code of Federal Aviation Regulations. One of the most commonly known prohibitions is against tampering with an airplane smoke detector[23] which is communicated to persons onboard the aircraft through both placards and as part of the pre-flight briefing.

While the working group understands that existing statute (e.g., 18 U.S.C §32 - Destruction of aircraft or aircraft facilities and 18 U.S.C §1030 (A)(5)) provides the U.S. Government sufficient legal basis to pursue action against any person or entity found to have attempted to tamper with an electronic system on an aircraft, the working group recommends that the FAA take the opportunity to further clarify this prohibition and make tampering with electronic aircraft systems an explicit prohibition.

The working group recognizes that regulatory prohibitions are adhered to by law-abiding persons and those persons with ill intent are not necessarily discouraged by a regulatory prohibition. The working group still believes that there is benefit gained from establishing a clear prohibition because:

(1) The number of nuisance events should be reduced.

(2) If any intentional interference is identified, then there will be a clearer basis to pursue legal action against the person(s) involved in the activity.

The working group recommends that the FAA consider amending either Part 121 for commercial operations or – alternatively – make the prohibition broadly applicable by amending Part 91. The working group has drafted the following proposed addition to the operational regulation.

> 14 CFR XX1 Prohibition Against Tampering with Electronic Systems
>
> No person may intentionally tamper with or alter an aircraft or aircraft system without authorization from the operator. This prohibition includes unauthorized access to aircraft systems, networks and data bases to alter, collect information, or deny service.

The working group also reviewed the existing United States Code (U.S.C.) to make the prohibition against tampering with an electronic system clear, but concluded that amending existing statutes that prohibit Aircraft Piracy (49 U.S.C. §46502) or those that pertain to interference with flight crew and flight attendants (49 U.S. Code § 46504) is not necessary.

This message is reinforced as part of the airplane pre-flight safety briefing; **similar announcements should be made for intentional tampering with any other airplane system.**

IFE systems are typically minor under 14 CFR 21.93. The manufacturer of IFE systems must be in a position to upload new software without the cumbersome type design change process or the IFE-provider's ability to manage security in real-time could be reduced. Software revisions may be done by the IFE manufacturer without involvement by the regulator as long as the security perimeter is not changed.

[23] 14 CFR 121.317 (i) No person may tamper with, disable, or destroy any smoke detector installed in any airplane lavatory.

Recommendation 18: The ASISP working group recommends that the FAA not establish additional security requirements for IFE systems – other than those which would result from the recommendations of section 2.2 through 2.4 (e.g., the security assessment process for airworthiness for Minor systems) in this report and the existing standards for IFE identified in section 2.6 – because additional regulatory requirements could negatively affect the security posture when IFE software has to be upgraded.

Note: The specific requirements applied to an IFE system will be established between the IFE equipment manufacturer and the organization installing the equipment, as an applicant, and the regulator.

2.7 Phased Adoption of Industry Standards

Industry standards for ASISP are relatively new, DO-326A/ED-202A was published in late 2014. While these documents provide overall guidance and are harmonized across standards groups, work remains to harmonize the methods documents DO-356 and ED-203, as outlined in Section 2.2.4 Guidance Material. RTCA SC-216 and EUROCAE WG-72, at the request of the ARAC ASISP WG are moving towards harmonization, with the goal to complete by the end of 2017.

As the industry standards mature, aircraft production, operation and development activities progress leading to the practical need to phase in the adoption of those industry standards. One such way this phasing may progress is based on the certification basis of the airplanes, as described below.

1. Legacy Aircraft – Aircraft developed and certified without the increased network connectivity of newer airplanes did not require, and therefore do not have, ASISP Special Conditions as part of the certification basis for the airplane. These airplanes will likely continue as before unless a design change drives the need for Special Conditions from the Regulatory Authorities.

2. ASISP Special Conditions Aircraft - Aircraft developed and certified to comply with Special Conditions already have a methodology and process that has been approved by the Regulatory Authorities. As such, they will likely continue to use those approved methods and processes for the remaining life of the aircraft program. The Applicant may choose to adopt the new RTCA and/or EUROCAE methods and processes if deemed beneficial and in coordination with the Regulatory Authorities.

3. Future Aircraft – For new aircraft programs developed and certified after the harmonization of ASISP methods and processes, Regulatory Authorities will likely adopt these new industry standards through an AC/AMC as a method of the compliance to either Special Conditions or the new ASISP rule as described in Section 2.2, the Applicant may choose to adopt them or propose and negotiate alternate methods.

A number of aspects will prevent the immediate adoption of the new standards, including training, resources and the potential for evolution of the standards as they are implemented, tested, and updated. In summary, the harmonization of industry standards for ASISP and ensuing adoption time frame will depend on many factors, with the practical effect of phasing in over a number of years.

Recommendation 19: The ASISP working group recommends that existing policies for type design changes, such as the establishment of certification basis, for existing safety regulations and means of compliance are also applicable to ASISP considerations and a phased adoption of industry standards should be anticipated.

2.8 Period Review of Regulation and Industry Standards

The regulations and especially the standards referenced throughout section 2 of this report are not intended to become stale, but instead provide a dynamic framework through which regulators in cooperation with industry can update the requirements, standards, and industry best-practices to respond to new threats in the cybersecurity field. The strong reliance on industry standards (i.e., RTCA and EUROCAE) and best practices (i.e., ASTM) allows for timely responses that do not require the regulators to go through the cumbersome process of updating the airworthiness standards.

It is essential that any updates to the standards are based on a data-driven process. The strong safety record in aviation relies on data-driven review of existing regulations and standards. The ASISP regulations for cybersecurity and the associated policies, standards, and best practices should also base its changes on lessons learned and data collected by individual companies and shared through cooperative mechanisms (i.e., see separate sections 3.2.1 for data reporting and 5.1 about A-ISAC and CERT.)

3 Other Rulemaking and Policy Considerations

3.1 Revision of Policy Statement for Cybersecurity Special Conditions

The FAA published policy statement PS-AIR-21.16-02, *Establishment of Special Conditions for Cyber Security*, on March 6, 2014. The FAA's authority for issuing special conditions is contained in 14 CFR 11.19 and states that:

> "A special condition is a regulation that applies to a particular aircraft design. The FAA issues special conditions when we find that the airworthiness regulations for an aircraft, aircraft engine, or propeller design do not contain adequate or appropriate safety standards, because of a novel or unusual design feature."

The FAA 2014 policy statement identified several criteria for the agency issuing a special condition on an initial Type Certificate (TC) and Supplemental Type Certificates (STC) as well as amended TC and STC including an aircraft system that:

- Directly connect to external services and network where the external service or network is non-governmental;
- The aircraft system receives information from non-governmental services or network; and
- The failure effect classification of the aircraft system is "major" or higher.

The FAA has issued Special Conditions for a number of transport category airplanes[24] over the past decade. The special condition contains requirements for both the aircraft design and its continued airworthiness. Specifically, the special condition:

> Special Condition 25-509-SC – Isolation or Security Protection of the Aircraft Control Domain and the Information Service Domain from the Passenger Service Domain
>
> 1. The applicant must ensure that the design provides isolation from, or airplane electronic system security protection against, access by unauthorized sources internal to the airplane. The design must prevent inadvertent and malicious changes to, and all adverse impacts upon, airplane equipment, systems, networks, or other assets required for safe flight and operations.
> 2. The applicant must establish appropriate procedures to allow the operator to ensure that continued airworthiness of the aircraft is maintained, including all post-type-certification modifications that may have an impact on the approved electronic system security safe guards.

The FAA provides additional guidance about how to maintain the continued airworthiness of the aircraft systems in AC 119-1, Airworthiness and Operational Authorization of Aircraft Network Security Program (ANSP) (see, Section 3.2.3 for additional background).

[24] Airbus A350; Boeing B747-8, B767-2C, B787, and ONS equipped B737 and B777; ATR42-500 and ATR72-212A; Bombardier BD-500-1A and Learjet 40 / 45; Cessna CE-680, CE-680A and CE-750; Gulfstream G280, GIV-X, and G650; and the Embraer EMB-550.

The FAA will rely on agency policy to manage cybersecurity risk until completing the rulemaking recommended by the ASISP working group unless the aircraft certification basis excludes the amendment of the airworthiness standards incorporating the new security certification requirements.

The FAA asked the working group to review and provide feedback to the FAA about revising the agency's cybersecurity policy to ensure that it is aligned with the recommendations for rulemaking.

The working group completed its review of the FAA's policy statement at its June 2016 meeting. A copy of the revised draft policy statement is included in Appendix J for reference.

The changes to the revised policy statement were undertaken to make it reflect current practice for issuing special condition based on the type of aircraft and design changes. The changes include:

- A shift away from the term "non-governmental services" which generated confusion outside the United States since many air traffic services are non-government services. The policy statement instead uses the term "non-trusted" and includes a set of examples of services that should not be trusted including public network (e.g., the Internet), Portable Electronic Devices, and airport gate link networks.
- Adding specific guidance for considerations that should be made about field loadable software (FLS), aeronautical data bases (ADB), and the Aircraft Communications Addressing and Reporting System (ACARS).
- Considerations for non-transport category airplanes (i.e., small airplanes defined as Class 1, 2, and 3 [and 4] in AC 23.1309-1E and Part 27 Single Engine rotorcraft

The FAA is finalizing the updated policy statement in parallel to the work of the ASISP WG and its recommendations for rulemaking.

Recommendation 20: The ASISP working group recommends that the FAA update the policy statement PS-AIR-21.16-02, Establishment of Special Conditions for Cyber Security, based on the input provided by the working group.

3.2 Continued Operational Safety

3.2.1 Continued Operational Safety Considerations

The existing Special Conditions and draft 2X.13XX regulation contain requirements for the manufacturer to develop Instructions for Continued Airworthiness (ICA). Manufacturers also provide non-ICA information to operators to support the security of the aircraft electronic systems.

Manufacturers support the safe operation of aircraft through Continued Operational Safety (COS) activities. These COS programs involve the on-going monitoring of the safety of the fleet including regulated reporting under 14 CFR 21.3 (and equivalent regulatory requirements such as EASA Part 21A.3) reporting of failure, malfunctions, and defects.

Reporting requirements in 14 CFR 21.3 that associated with Aircraft System Information Security Protection include those that relate to the following conditions:

(C)(11) Any structural or flight control system malfunction, defect, or failure which causes an interference with normal control of the aircraft for which derogates the flying qualities.
(C)(12) A complete loss of more than one electrical power generating system or hydraulic power system during a given operation of the aircraft.
(C)(13) A failure or malfunction of more than one attitude, airspeed, or altitude instrument during a given operation of the aircraft.

However, these reporting requirements do not apply to situations that result from improper maintenance or improper usage as described in 14 CFR 21.3 (D), and excerpt of which is shown below:

(D) The requirements of paragraph (a) of this section do not apply to—
(1) Failures, malfunctions, or defects that the holder of a Type Certificate (including a Supplemental Type Certificate), Parts Manufacturer Approval (PMA), or TSO authorization, or the licensee of a Type Certificate—
(i) Determines were caused by improper maintenance, or improper usage

While the potential exists for interpretation of the ”improper usage” text to include malicious intent and security events, the ASISP working group believes that it should be interpreted in the traditional context of not using a system or function for its intended purpose.

Recommendation 21: The ASISP working group recommends that the FAA establish policy to leverage existing COS programs for reporting security events affecting safety.

Current COS criteria provide reporting requirements for failures, malfunctions and defects that result in an unsafe condition as outlined above. System failure or malfunction as a result of a security attack fall within the existing criteria, and no ASISP specific criteria needs to be added to 14 CFR 21.3 (C).

The FAA should consider whether clarifying language is needed to assure security events are not excluded from reporting as defined in 14 CFR 21.3 (D)(1)(i). Specifically, there are some that may attempt to categorize security attacks and compromises as ‘improper usage’ however it is the intent of the ASISP working group that these types of issues are not included in the exclusions defined in (D)(1)(i).

3.2.2 Security Event Logging

Special Condition Issue Papers contain requirements for event logging in those aircraft electronic systems for which security requirements have been issued. For context, a partial list of those requirements is included here:

1. In order to support the investigation and analysis of any possible inadvertent or malicious attack, and monitor the occurrences and frequency of such attempts, <Applicant> should establish security requirements that provide an information system security audit capability for the Aircraft Control Domain and Airline Information Services Domain such that:
   a. All access attempts should be **automatically** recorded in a security audit log.
   b. The time, date, and entity identifier of all access attempts are recorded in a security audit log.
   c. The Instructions for Continued Airworthiness include the requirement that the security audit log is preserved for a minimum of 90 days.
   d. Modification of the security audit log is **automatically** prevented.

e. If provided, malicious code detections should be **automatically** recorded in the security audit log, as well as the identification of the entity introducing the malicious code, if possible.
f. All attempts to violate system security rules (i.e., security policies enforced by the system) should **automatically** be recorded in the security audit log, including identification of the entity attempting to violate the security rules.

Currently, manufacturers use these event logs to conduct forensic analysis when a system failure has occurred to attempt to determine whether an intentional unauthorized access into the avionics system was causal to or a factor that resulted in the failure. There are, however, not the necessary tool-set in place to proactively monitor the event logs to determine if security-related events are occurring in a real-time basis in the fleet or to conduct predictive analysis of security events that may result in a system failure. Simply stated, while security logs provide an important use in 'post-event' investigations, they are not an appropriate source of data for determining airworthiness of an aircraft.

In addition, security logging is only one component of the larger "Security Event Management" activity which may include other processes, procedures and information to manage security events. Further, "Security Events Management" is a sub component of a larger activity to "Maintain Product Security" which may include activities such as technical and procedural change management, vulnerability management and others.

ARINC 852 is being developed by industry to provide guidance to help define interoperability requirements as well as minimum log file contents to support security monitoring by airlines and operators.

In addition to traditional uses by operators, the security logs may provide added value in identifying and documenting unauthorized access to aircraft systems and are therefore may be of interest to additional government agencies aside from the FAA to support law enforcement activities such as those proposed in Section 2.6.

Recommendation 22: The ASISP working group recommends that DO-356/ED-203 be updated to include guidance for logging for large transport category airplanes.

The security standards such as DO-356 and ED-203 need to include top level objectives for security logging, as well as a concept of operations for their practical use in the aviation industry. While not directly linked to supporting airworthiness, security log files provide critical information in determining if security attacks have taken place, and to what extent they impacted aircraft systems. Once the objectives have been agreed to, ARINC 852 and other standards should be reviewed for applicability and updated if necessary to include industry consensus on security logging standards, guidance and considerations.

Manufacturers should provide guidance to operators on security logging. In addition, FAA AC 119-1 item 13 identifies steps operators should take to address security logs generated by the aircraft systems, and expected actions to assess their contents. Existing industry standards, such as DO-355, ARINC 811 and NIST 800-92, also contain guidance for how an operator should manage maintenance computers and associated devices, such as SD cards and USB drives, that are used for airworthiness functions including software updates, databases, and accessing maintenance logs. This guidance, however, is focus on air

transport airplanes and commercial operators and not necessarily appropriate or tailored to the general aviation community.

Recommendation 23: The ASISP working group recommends that the FAA encourage adoption of General Aviation/ASTM Security Best Practices Section 7.9 for logging considerations.

General Aviation Airplanes and Rotorcraft operations are significantly different from those in the commercial transport category operations, such that there is no practical solution to regularly retrieve and monitor security logs for cyber threats in general aviation. While ARINC 852, DO-355, ED-203 and DO-356 and other standards may not be directly applicable, those standards in conjunction with the GA/ASTM Best Practices document include potential best practices for security logging, such as generating and storing a defined set of logs in the onboard equipment to support later forensic investigations by the equipment manufacturer.

3.2.3 Advisory Circular for ANSP

The FAA issued Advisory Circular (AC) 119-1, Airworthiness and Operational Authorization of Aircraft Network Security Program (ANSP), on September 30, 2015. The AC describes how commercial operators obtain operational authorization for an aircraft certified with a special condition related to security of the onboard computer network (see, Section 3.1 for additional background about Special Conditions).

4 Security Considerations for Specific Systems and Technologies

The primary work of the ASISP working group focused on the requirements established for applicants that certificate aircraft and systems as well as the operation of these aircraft. The FAA, however, also invited input from the working group about other policy areas including aircraft databases, field loadable software, portable electronic devices (PED), and the use of Commercial Off-The Shelf (COTS) equipment onboard aircraft. Additionally, the FAA invited the working group's recommendation about how existing Technical Standards Orders (TSO) be managed for security, specifically those TSOs that support Communication, Navigation, and Surveillance (CNS) functions.

The following set of considerations for COTS, FLS, and PEDS are specifically focused on those aircraft, systems and network for which, per Section 2 above, have identified the need for specific requirements. If not specifically addressed in Section 2, the following technical content should be considered best practices.

4.1 Considerations for Aircraft Systems Intended to Connect to PEDS

4.1.1 Considerations of PEDs by ASISP WG

During the ASISP working group deliberations, the working group raised the issue of security of portable electronic devices (PEDs). The ASISP working group determined that cybersecurity aspects of PEDs are considered outside the scope of the FAA's ARAC ASISP tasking, however the security aspects of installed systems intended to connect to PEDs is not considered out of scope.

This section describes existing FAA policy on PEDs used to support flight operations (section 4.1.2, 4.1.3, and 4.1.5) and maintenance functions in (section 4.1.4). Section 4.1.6 contains the security aspects of installed systems intended to connect to PEDs.

4.1.2 PEDS Used by Part 121 Certificate Holders

The following examples Section4.1.3of a portable EFB and 4.1.4 maintenance PEDs are the only cases FAA regulations and policy allow a PED to connect to an aircraft system to support flight operations or maintenance functions. The ASISP working group understands that these two examples do not apply to general aviation operations under 14 CFR Part 91 or any other PED (e.g., passenger use of PEDs).

For all other PEDs intended to connect to an aircraft system (e.g., passenger PEDs connecting to an aircraft's installed onboard broadband network commonly referred to as inflight entertainment (IFE)), aircraft operators must comply with the requirements in 14 CFR 91.21, 121.306, 125.204, and 135.144 governing the use of PEDs onboard aircraft. These regulations require the aircraft operator to make a determination ensuring the use of certain PEDs will not adversely affect the installed avionics systems (e.g., communication or navigation systems). The FAA's current guidance to aircraft operators on allowing the use of PEDs is in AC 91.21-1C and 8900.1, Volume 3, Chapter 66, Section 1 - Expanded Use of Passenger PEDs for Aircraft Operations Conducted Under Parts 91 Subpart K (Part 91K), 121, 125 (including A125 LODA holders), and 135. Future guidance on the subject of PEDs is being developed by RTCA SC-234 and is set to be published by the end of 2016.

4.1.3 PEDS Used in Flight Operations

The FAA uses operations specifications (OpSpecs), management specifications (MSpecs), or letter of authorization (LOA) to place certain controls on PEDs intended to connect to an aircraft system and that are used to support flight operations.

For aircraft operated under 14 CFR part 91K, 121, 125, and 135, the only PEDs permitted for use to support flight operations are FAA-authorized by issuance of OpSpec/MSpec/LOA A061 – Use of Electronic Flight Bag (EFB). First, the operator submits an application to obtain FAA OpSpec/MSpec/LOA A061 in accordance with the guidance in the current version of FAA Advisory Circular (AC) 120-76 - Guidelines for the Certification, Airworthiness, and Operational Use of Electronic Flight Bags. The FAA evaluates the operator's application for a portable EFB program by following the aviation inspector (ASI) guidance in FAA Order 8900.1, Volume 4, Chapter 15, Section 1 - Electronic Flight Bag Operational Authorization Process. If the FAA issues OpSpec/MSpec/LOA A061 as applicable, then the aircraft operator is authorized to use certain PEDs as an electronic flight bag (EFB) to support its flight operations.

Note: The FAA is currently working with other agencies and industry stakeholders to develop aviation centric PED cybersecurity risk assessment guidance and associated mitigation strategies for aircraft

operations conducted under 14 CFR part 121, 125, 135, or 91 subpart F (part 91F) and part 91 subpart K (part 91K) related to the operational use of PEDs. The ASISP working group strongly supports this work to develop best practices/guidance for the use and management of PEDS intended for use for flight operations or maintenance operations.

4.1.4 PEDs used in Maintenance Operations

The FAA uses OpSpecs to place certain controls on PEDs intended to connect to an aircraft system which was certified with an electronic security special condition and that are used to support maintenance functions.

For aircraft certified with a security special condition and operated under 14 CFR 121, 121/135, 125, and 129, the only PEDs permitted for use to support maintenance functions and connect to an aircraft system are FAA-authorized by issuance of OpSpec D301. First, the operator submits an application to the FAA to obtain OpSpec D301 by following the guidance in the current revision of AC 119-1 - Airworthiness and Operational Approval of Aircraft Network Security Program (ANSP). The FAA evaluates the operator's application for an ANSP by following the ASI guidance in FAA Order 8900.1, Volume 3, Chapter 61, Section 1 - Evaluate the Operator's 14 CFR Parts 121, 121/135, 125, and 129 Aircraft Network Security Program. If the FAA issues OpSpec D301, then the aircraft operator is authorized to use certain designated maintenance PEDs as part of its ANSP. The FAA verifies compliance with program requirements by conducting routine Safety Assurance System (SAS) surveillance, activity 4.6.1 - (AW) Avionics Special Emphasis Programs.

Aircraft certified with a security special condition and not subject to an authorization under OpSpec D301 are required to use the equipment and procedure requirements of the manufacturer. This approach is identical to any other type of special equipment or procedures. Any deviations to procedures or equipment must be evaluated for equivalency and included in the maintenance program.

4.1.5 PEDS Used in Part 91 General Aviation Operations

Part 91 operators have a wide variety of options regarding PEDs. Phones, tablets and other general-purpose devices running the popular Android or iOS operating systems offer a variety of aviation-focused apps for use by operators. Additionally, purpose-built aviation PEDs provide aviation-specific functionality with better sunlight readability.

Portable receivers for services such as ADS-B or SiriusXM weather are also popular with Part 91 operators. These portable receivers, when coupled with a general-purpose or aviation-specific display PED, enable the in-flight display of traffic and weather information that operators can use to make better strategic decisions.

The phone and tablet platforms, as well as the aviation-specific PEDs, provide pre-flight functionality such as flight planning, weather briefing, fuel planning, and flight plan filing. Additionally, the PEDs can be used in flight for enhanced situational awareness. In-flight features include a moving map, indication of terrain and obstacles, display of traffic and weather, and display of charts and approach plates.
A typical use case may include the operator checking the weather on their tablet the before a flight. The operator can input a route in to their app and look at current weather conditions and weather forecasts, and adjust their flight plan accordingly. They can then file or amend their flight plan and view preferred routes to help ensure the planned route is accepted by ATC.

Once in the aircraft, the operator can use a portable GPS sensor, or connect to the aircraft's position source (if the aircraft is properly equipped). The PED can also be connected to a portable ADS-B receiver to view in-flight traffic and weather. "What if" flight plan changes can be "previewed" on the PED before any changes are made to active navigation. This could include routing around weather or making a fuel stop due to stronger than expected headwinds.

4.1.6 Summary ASISP Considerations of PEDs

The purpose of section 4.1.6 is to present policy and guidance recommendations for aircraft systems designed to connect to portable electronic devices (PEDs). This includes:

1. PEDS not authorized for use for flight operations or maintenance operations, including but not limited to Passenger-Owned Devices (POD);

2. PEDs intended for use for flight operations or maintenance operations such as portable Electronic Flight Bags (EFB), Ground Support Equipment (GSE), and portable media.

Recommendations are made for 1) the development and certification of the installed equipment, 2) general guidance.

A PED not authorized for use for flight operations or maintenance operations can only have a direct connection to non-essential and non-required CS&E that is intended for that function. (Note that in this case, interaction does not include the RF negotiation necessary to accept or reject a WiFi connection.)

A PED not authorized for use for flight operations or maintenance operations can be logically connected to an essential or required CS&E only if the CS&E is certified for that intended use.

A PED not authorized for use for flight operations or maintenance operations is not allowed to have a logical connection to installed equipment in the AISD or the ACD.

In aircraft in which direct connections are allowed to PED not authorized for use for flight operations or maintenance operations, the aircraft design and installation should prevent non-essential non-required CS&E from intentional unauthorized electronic interaction with systems, networks, and data in the ACD and AISD.

An essential or required aircraft function is allowed to have a transmit-only unidirectional connection to PEDs intended for use for flight operations or maintenance operations.

PEDs intended for use for flight operations or maintenance operations can be directly connected to installed airline operations equipment (e.g. AISD) only if the equipment is certified for that intended use. In addition, authentication of the PED and use by an authorized user are recommended.
PEDs intended for use for flight operations or maintenance operations can be logically connected to installed aircraft control equipment or airline operations equipment (e.g. ACD or AISD) only if the equipment is certified for that intended use.

Any direct physical connection (with the possible exception of transmit-only connections, see above) from installed aircraft control equipment to PEDS or portable USB devices is allowed only if it is

accounted for in the security assessment and has appropriate security controls. In particular, this includes USB slots which should consider the threat of connection with a non-standard PEDS or portable USB device which includes unintended function.

Recommendation 24: The FAA should develop guidance to address:

> **Development of equipment intended for direct connections to PEDs should include considerations to protect against intentional corruption due to intentional unauthorized electronic interaction from the PED. Development of Aircraft Installed Equipment which supports PEDS direct connections should consider the following security threats:**
> - **unauthorized interaction with the direct connection**
> - **intentional corruption of the PED (in particular, this includes support for portable media), and**
> - **unauthorized access to the PED by sources external to the aircraft and PED.**

ASTM F44 (see Section 2.4) is authoring a document "Operational Requirements" which includes recommended practices for handling PEDS. This material should be made available to the industry as guidance.

Appendix K contains reference guidance and applicable regulations for PEDs.

4.2 Security Considerations for Field Loadable Software including Aircraft Data Bases

The purpose of section 4.2 is to present policy and guidance recommendations for the data security of Field Loadable Data (FLD) through their aeronautical life cycle up to the point where they become part of the aircraft configuration. FLD is considered to be any type of persistently stored data which determines or modifies the intended behavior of the equipment. This includes:

1. Executable object code including software and firmware;
2. Data for re-programming an item after manufacture, such as FPGA code;
3. Persistent data sets that influence the behavior of avionics and is managed as a separate configuration item, such as aeronautical data bases, parameter data items, or firewall rules;
4. Dynamically interpreted, but persistently stored, executable scripts.

This overview of FLS excludes data, stored or not, whose update and modification is intended as part of the intended function of the installed equipment, such as flight plans and flight plan updates.

Section 4.2.1 discusses the aeronautical data life cycle, the Data Chain for FLD.

Section 4.2.2 discusses policy and guidance recommendations for different types of FLD, classified according to current regulatory practices.

The Appendix L presents informative data on threat modeling for FLD, technical controls for data transmission, and data security for organizations.

4.2.1 Data Chain for Field-Loadable Data Parts

In looking at the various stages in the life cycle of data parts, this section follows DO-200B in distinguishing between the data chain up to the end-user, and the data chain once the data part has been accepted by the end-user. For this section, the end-user is the organization/owner/operator that is responsible for the operation and maintenance of the aircraft equipment which will be using the persistent data part.

Off-Aircraft Handling occurs as the data is transferred and stored on systems belonging to the end-user, when those systems are not part of the installed equipment on the aircraft. It will include the management of data stored on GSE as well as ground support systems.

On-Aircraft Handling occurs as the data is transferred and stored on installed equipment on the aircraft, but not including onboard field loading.

This section considers the following life cycle stages for FLD during which data may be subject to attack (see Figure 4.2-1). Note that not all of these will apply to every type of FLD.

Data Part Origin occurs when the data is initially generated as a coherent set of information.

Data Part Processing occurs as the data is transformed or reformatted for various purposes.

Data Part Transmission occurs as the data moves from system to system, or from responsible entity to responsible entity. This includes the transmission to the end-user.

Data Part Storage occurs as the data rests unchanged and unused within a particular system or responsible entity.

When transmission and storage takes place on systems within the operator organization (e.g., airline or MRO parts storage vaults), it is part of Off-Aircraft Handling, and is known as **Ground Staging**.

- When transmission and storage takes place on installed aircraft equipment, it is part of On-Aircraft Handling, and is known as **Aircraft Staging**.

- When transmission and storage takes place on the ground support equipment for an aircraft, it is part of Off-Aircraft Handling, and will be referred to as **GSE Storage**.

Data Part Loading occurs as the data is transferred to the final aircraft equipment to modify the equipment intended function. There are a number of different options for Data Part Loading, depending on when and how the data loading is performed:

- **Shop Data Loading** occurs when data part loading is done after the equipment is removed from the aircraft and transferred to a facility under the control of the maintainers or operators, and then re-installed on the aircraft. Note that this stage includes any Data Part Storage and Transmission which occurs within the systems and responsibility of the maintainers or operators.

- **GSE Field Loading** occurs when data part loading is done on the aircraft to the installed equipment using Ground Support Equipment (GSE) operated by the maintainers or operators. Note that this stage includes any Data Part Storage and Transmission which occurs on the GSE.

- **Onboard Field Loading** occurs when data part loading is done on the aircraft to the installed equipment using other equipment installed on the aircraft. Note that this stage includes any Data Part Storage and Transmission which occurs on installed aircraft equipment.

- **Factory Data Loading** occurs when data part loading is done as part of the manufacturing process. It is NOT considered part of the scope of this paper since it takes place before the end of manufacturing. However, Field Loadable Software is often initially loaded during manufacture, and Factory-Loading features and requirements can be mentioned in aircraft equipment specifications and guidance material, so it is mentioned here for completeness.

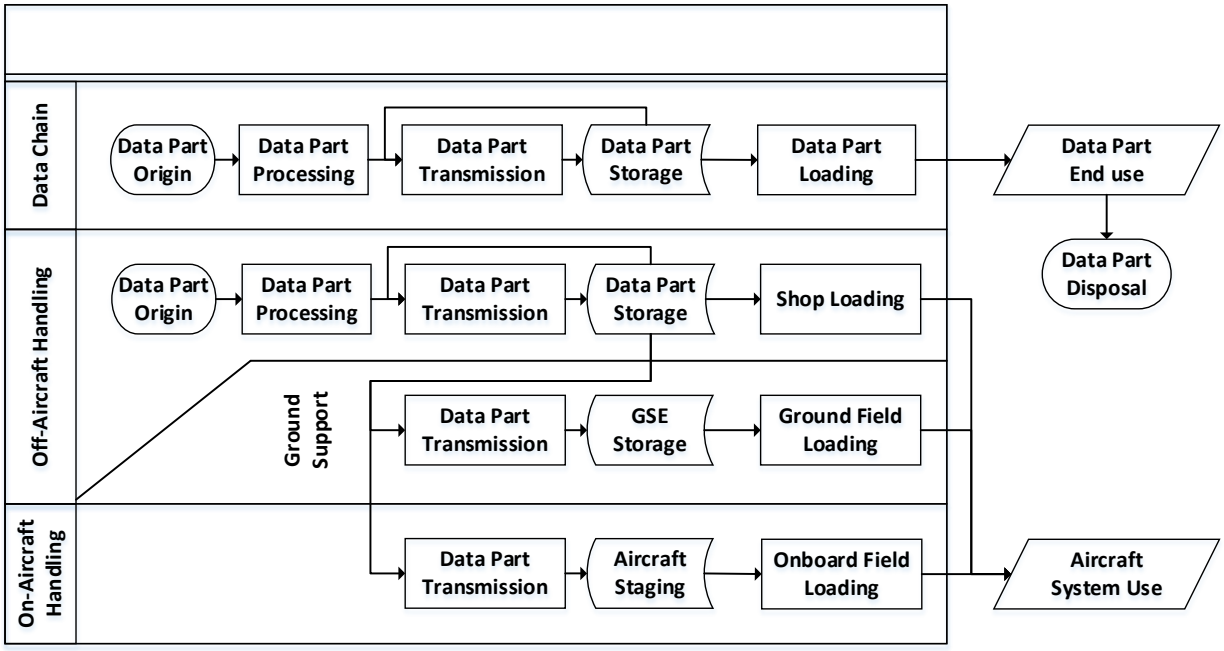
NOTE: ARINC 791P2 Appendix B defines a method for Remote Software Loading which provides for dataloading of multiple SATCOM units from a Network Operations Center. There is at least one fielded implementation and may be considered as an option if it is accounted for in the security assessment and has appropriate security controls.

Data Part End-Use occurs as the equipment exercises its intended function using the persistent data parts. Security issues in this phase are considered to be issues with the equipment and not with the field-loadable data**.**

When a piece of installed aircraft equipment executes a software part or uses a data part during aircraft operation, it is known as **Aircraft System Use**.

Data Part Disposal occurs when the data is removed from the aircraft equipment so as to no longer influence the intended function.

FIGURE 4.2-1 DATA CHAIN FOR FIELD-LOADABLE DATA PARTS



4.2.2 Considerations for Field-Loadable Data

This section presents policy and guidance recommendations for different categories of Field Loadable Data (FLD), classified according to current regulatory practices. These non-exclusive categories include -

- Field Loadable Software and Software Parameter Data Items
    - Includes items which comply with the guidance of DO-178C and excluding items for which DO-178C provides no guidance (e.g., DAL E)
- Aeronautical Databases
- User Modifiable Software (Or Data)
- User Modifiable Security Data
- Field Loadable Software Not Covered by DO-178C
- Aircraft Controlled Software (ARINC 667)
- Remote Software Loading of SATCOM (ARINC 791 P2 App B)

4.2.2.1 Field Loadable Software and Software Parameter Data Items higher

Policy Recommendation 25A: For Field Loadable Software, or Parameter Data Items which are already subject to DO-178C[25] objectives:

In general, in addition to the existing policies in Order 8110.49 Chg 1, policy should add requirements to:

- Protect data parts from intentional corruption during transmission, storage, off-aircraft handling, and on-aircraft handling;
- Confirm that received and stored data parts are uncorrupted in all stages;
- Protect the system and its configuration information from intentional corruption of the data parts during field loading;

More specifically, developers should:

- Protect data parts from intentional corruption during development, storage, and;
- Protect the system and its configuration information from intentional corruption of the data parts during field loading;

And operators (e.g. airlines and MROs) should:

- Protect data parts from intentional corruption during transmission, storage, off-aircraft handling, and on-aircraft handling;
- Confirm that received data parts are authentic (come from a trusted source) and uncorrupted (not corrupted during transmission from the source).

Guidance Recommendation 25B: For Field Loadable Software, or Parameter Data Items which are already subject to DO-178C objectives -

In addition to the existing guidance in DO-178C, and, if applicable based on aircraft type, ARINC 666, and ARINC 667:

- Add the considerations from DO-356 on Security Assurance for development[26]:
  - Qualification of security testing tools
  - Protection from contamination by malicious code
  - Verification of security guidance
  - Secure configuration management
  - Security review of problem reports and derived requirements

[25] While this report points to DO-178C, regulators (i.e., FAA and EASA) have agreed that any organization with an existing DO-178B compliant process can keep using it indefinitely. The FAA guidance is AC20-115C and FAA cooperating with EASA are harmonizing on a new A(M)C20-115D which will provide further guidance on the use of any earlier version than 178C.
[26] The DO-356 guidance may not be applicable based on aircraft type.

  - Security-specific content in design and review standards
  - Independence of design and code reviews

- Add considerations for monitoring for vulnerabilities in commercially-available software/hardware from authoritative sources;
- Add considerations to protect the data parts from exposure during transmission, storage, and loading if the data part includes sensitive security data;
- Add considerations for secure disposal if the data part includes sensitive security data.

Discussion: DO-178C provides relevant requirements for two classes of Field Loadable Data: Field-Loadable Software (FLS) and Parameter Data Items (PDI). It also has special provisions for a third class-User Modifiable Data, which will be discussed below. FAA Order 8110.49 Chg1 "Software Approval Guidelines" also adds Option Selectable Software.

For DAL E software items, DO-178C provides no guidance or objectives. For purposes of this discussion, such software is not considered as being subject to DO-178C, and is not included in this discussion. Field-Loadable Software is field loadable data which consists of executable object code, Parameter Data Items are "data sets that influence the behavior of the software without modifying the Executable Object Code and are managed as a separate configuration item".

Most of the DO-178C requirements apply to the Data Part Origin phase: they are required as part of the development process to ensure that the original developed data part is correct and has been verified. This includes requirements for the robustness of the code under incorrect inputs, and the absence of unintended function as would be represented by the presence of malicious code in the original software part.

In addition, DO-178C includes requirements that the system design considers the whole of the life cycle for the FLS or PDI from Data Origin, through Data Storage and Transmission, including Data Loading, and through Data Part End Use (but excluding Data Disposal). This includes:

- 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

Many standards, notably ARINC 615A and ARINC 665, include means of meeting these requirements. ARINC 666 includes additional requirements about the distribution aspects of data, while ARINC 667 addresses questions about how airlines control the FLDs they have received from suppliers.

As a result, basic configuration control of FLS and PDI is extremely strong, stronger that most Security Configuration Controls in related sectors, such as NIST 800-53V3.

There are gaps in the current practices for Data Origin. DO-356 defines the following additional considerations for FLD intended for security measures:

- Qualification of security testing tools
- Protection from contamination by malicious code
- Verification of security guidance
- Secure configuration management
- Security review of problem reports and derived requirements
- Security-specific content in design and review standards
- Independence of design, test, and code reviews

There are gaps in the current practices for Data Transmission and Storage for FLS. To see how to cover these gaps, DO-200B defines the following additional provisions for Aeronautical Data to cover the issues of security threats, which can be applied to the case of FLS:

- Provide means to confirm that the data has been received without intentional corruption;
- Provide means to ensure that stored data is protected from intentional corruption;
- Provide users with the ability to verify that the data received by the user has not been intentionally corrupted.

There are existing standards that define means to meet these requirements, notable ARINC 827 and ARINC 835.
There are gaps in monitoring for security issues from sources other than the aircraft operators, for which there are authoritative sources such as the common security vulnerabilities cataloged by CERT and current attacks as reported to the various security ISACs.

4.2.3 Aeronautical Databases

Policy Recommendation 25C: For Field-Loadable Data (FLD) classified as Aeronautical Databases which are already subject to DO-200B objectives -

In addition to the existing policies in Order 8110.55B, policy should add requirements to:

- Validate that data is free from intentional corruption when accepting data originated from non-authoritative sources;
- Protect the system and its configuration information from intentional corruption of the data parts during field loading;

More specifically, developers should:

- Validate that data is free from intentional corruption when accepting data originated from non-authoritative sources;

And operators (e.g., airlines and MROs) should:

- Protect data from intentional corruption during transmission, storage, off-aircraft handling, and on-aircraft handling;

- Confirm that received data is authentic (comes from a trusted source) and uncorrupted (not corrupted during transmission from the source).

Guidance Recommendation 25D: For Aeronautical Databases which are already subject to DO-200B objectives:

In addition to the existing guidance in DO-200B:

- Add considerations to protect the data parts from exposure during transmission, storage, and loading if the data part includes sensitive security data;

- Add considerations for secure disposal if the data part includes sensitive security data.

Discussion: For Aeronautical Data, DO-200B provides relevant requirements to protect against intentional corruption during Data Transmission and Storage. For Data Origin, it requires either that data originate at an Authoritative Source, or else the data must be validated by the first recipient in the Data Chain, and protected thereafter.

FAA Order 8110.55B and AC 20-153B invokes DO-200B for any TSO, TC, STC, or LOA project databases with a safety effect.

DO-200B states that "The objective of data security is to ensure that data is received from a known source and that there is no intentional corruption during processing and exchange of data" and defines the following additional provisions to cover the issues of security threats:

- Provide means to confirm that the data has been received without intentional corruption;

- Provide means to ensure that stored data is protected from intentional corruption;

- Provide users with the ability to verify that the data received by the user has not been intentionally corrupted.

In addition, DO-200B provides material on current practices used to meet these requirements. See Appendix for an early draft version of this material.

DO-200B does not cover Data Loading, or Disposal. Nor does it include intentional corruption during validation of the data as part of Data Origin.

DO-178C provides requirements that could be applied to Data Loading. This would include:

- Detection of corrupted or partially loaded software

- System/Data compatibility
- Loss or corruption of the configuration identification

4.2.4 User Modifiable Software (Or Data)

Policy Recommendation 25E: For Field-Loadable Data (FLD) classified as User Modifiable Software (UMS) (or Data) and for the products certified to use the UMS -

In addition to the existing policies in Order 8110.49 Chg1, policy should add requirements to:

- In establishing the mitigation and isolation of the effects of corrupted UMS:
    - Should include the consideration of Safety Effects Caused by Security Events;
    - Should include the consideration of intentional corruption in the UMS;
- Protect data parts from intentional corruption during transmission, storage, off-aircraft handling, and on-aircraft handling;
- Confirm that received and stored data parts are uncorrupted in all stages;

More specifically, developers should:

- Develop mitigations for the possibility of intentional corruption in the UMS;

And operators (e.g. airlines and MROs) should:

- Protect data parts from intentional corruption during transmission, storage, off-aircraft handling, and on-aircraft handling;

Guidance Recommendation 25F: For User Modifiable Software (or Data) and for the products certified to use the UMS -

In addition to the existing guidance in DO-178C, ARINC 666, and ARINC 667 for User Modifiable Software:

- If qualified tools are used for modification, add the following provisions
    - Add considerations to confirm data parts were generated by an authorized qualified tool;
    - Add considerations to protect the tool from intentional corruption;
- Add considerations to protect the data parts from exposure during transmission, storage, and loading if the data part includes sensitive security data;
- Add considerations for secure disposal if the data part includes sensitive security data.

Discussion: DO-178C provides for a third class of data parts, User Modifiable Data, which has much more relaxed requirements for Data Transmission and Storage.

User Modifiable Software (UMS) is field loadable data which may be changed by the "user", which in this case may include the operator, owner, or duly appointed support organizations such as the AOC or MRO. More importantly, UMS is allowed for use in n systems of DAL D or higher provided the system (and systems software/firmware) properly mitigates the potential safety effects of defects in the UMS.

In order to allow the use of UMS, DO-178C requires that any adverse effect of the UMS must be prevented by the system and aircraft affected the UMS, so that the UMS will not adversely affect safety, operational capabilities, flight crew workload, safety-related information display, or non-modifiable data parts. In addition, once the UMS is originated or modified, then the user should assume responsibility for protecting the UMS from corruption or loss.

Under FAA Order 8110.49 Chg1, it is allowable to prevent adverse effects by using qualified tools to modify the UMS. The user then assumes responsibility for managing the modifications so as to meet the system requirements.

There are gaps in the current practices for systems that intend to use UMS, largely to ensure that any protection against the adverse effects of the UMS includes the effects of intentional corruption and any adverse effects on airworthiness security.

There are gaps in the current practices for Data Transmission and Storage. DO-200B defines the following additional provisions to cover the issues of security threats:

- Provide means to confirm that the data has been received without intentional corruption;
- Provide means to ensure that stored data is protected from intentional corruption;
- Provide users with the ability to verify that the data received by the user has not been intentionally corrupted.

4.2.5 User Modifiable Security Data

Policy Recommendation 25G: For Field-Loadable Data (FLD) that is classified as User Modifiable Data, and contains User Modifiable Security Data that is required to be validated during Data Origin and Processing for its security properties -

In addition to the existing policies in Order 8110.49 Chg1 for User Modifiable Software, policy should add requirements to:

- Validate as part of Data Origin and Processing that the data part is free from intentional corruption and satisfies its security requirements;
- Protect data parts from intentional corruption during transmission, storage, off-aircraft handling, and on-aircraft handling;
- Confirm that received and stored data parts are uncorrupted in all stages;
- Protect the system and its configuration information from intentional corruption of the data parts during field loading;

More specifically, developers should:

- Develop mitigations for the possibility of intentional corruption in the UMS;

And operators (e.g., airlines and MROs) should:

- Protect data parts from intentional corruption during transmission, storage, off-aircraft handling, and on-aircraft handling;

- Confirm that received data parts are authentic (come from a trusted source) and uncorrupted (not corrupted during transmission from the source).

Guidance Recommendation 25H: For User Modifiable Security Data which is validated during Data Origin and Processing for its security properties -

In addition to the existing guidance in DO-178C, ARINC 666, and ARINC 667 for User Modifiable Software:

- Add considerations to protect the data parts from exposure during transmission, storage, and loading if the data part includes sensitive security data;

- Add considerations for secure disposal if the data part includes sensitive security data.

Discussion: For systems with security controls there is a need for field loadable data which may be changed to meet requirements for continuing airworthiness security. Important examples could be security policy updates such as firewall rules or anti-virus signatures which may need to be passed to the field quickly, within days or hours of the initial recognized security need.

Such User Modifiable Security Data (UMSD) may originate from security support organizations which are responsible for the validation of the security properties of the UMSD, but these organizations are not necessarily held responsible for non-security-related safety properties.

UMSD thus falls into the category of traditional UMS parts as discussed in the previous section, with the notable exception that due to the security validation, there is no need for the system to mitigate against the adverse effects of error and corruption on the airworthiness security risk.

4.2.6 Field Loadable Software Not Covered by DO-178C

Policy Recommendation 25I: For Field Loadable Software not covered by DO-178C, but is established as a protected asset by policy or by a security risk analysis -

In addition to the existing policies, policy should add requirements to:

- Identify acceptable security assurance requirements or standard for use during Data Origin and Processing;

- Protect data parts from intentional corruption during transmission, storage, off-aircraft handling, and on-aircraft handling;

- Confirm that received and stored data parts are uncorrupted in all stages;

- Protect the system from error, corruption, and intentional corruption of the data parts during loading ;

- Protect the system and its configuration information from intentional corruption of the data parts during field loading;

More specifically, developers should:

- Apply acceptable security assurance requirements and standards during development;
- Protect data parts from intentional corruption during development, storage, and;
- Protect the system and its configuration information from intentional corruption of the data parts during field loading;

And operators (e.g., airlines and MROs) should:

- Protect data parts from intentional corruption during transmission, storage, off-aircraft handling, and on-aircraft handling;
- Confirm that received data parts are authentic (come from a trusted source) and uncorrupted (not corrupted during transmission from the source).

Guidance Recommendation 25J: For Field Loadable Software not covered by DO-178C, but is established as a protected asset by policy or by a security risk analysis -

In addition to the existing guidance:

- Identify acceptable security assurance guidance for use during Data Origin and Processing, such as DO-356 or ED-203A;
- Add considerations for monitoring for vulnerabilities in commercial software/hardware from authoritative sources;
- Add considerations to protect the data parts from exposure during transmission, storage, and loading if the data part includes sensitive security data;
- Add considerations for secure disposal if the data part includes sensitive security data.

Discussion: Current airworthiness security standards such as ED-203 do not require the use of DO-178C for systems or functions which are assessed with a Severity Caused By Security Event (SECSE) impact that is equivalent to Minor or higher.

DO-326A and DO-356 require that security assurance requirements are directly allocated to the systems. These security assurance requirements apply to the Data Origin phase. This includes requirements for the robustness of the code under incorrect inputs, and the absence of unintended function as would be represented by the presence of malicious code in the original software part. ED-203 provides guidance on this topic without necessarily limiting requirement to only the Data Origin phase.

These security assurance requirements may not govern the whole of the life cycle of the Data Chain. DO-178C and DO-200B provide additional requirements for the life cycle for the FLD after Data Origin, through Data Storage and Transmission, including Data Loading, and through Data Part End Use (but excluding Data Disposal). This include:

- Detection of corrupted or partially loaded software
- System/Data compatibility
- Loss or corruption of the configuration identification
- Confirming that the data has been received without intentional corruption;
- Ensuring that stored data is protected from intentional corruption;
- Providing users with the ability to verify that the data received by the user has not been intentionally corrupted.

4.2.7 Aircraft Controlled Software (ARINC 667)

Policy Recommendation 25K: ARINC 667 should be a recognized means of compliance for the management of Field-Loadable Data (FLD) for airworthiness security. Note that this will involve regulatory requirements for both Type Certification and Operational Approval, and use of ARINC 667 by both developers and operators.

Guidance Recommendation 25L: ARINC 667 is complete with respect to addressing airworthiness security concerns after the software has been developed and approved. It does not provide guidance for software development- applicants must seek other guidance for that. ARINC 667 is also highly dependent on current avionics dataloading practices and requires the presence of an airline operations organization, so applicants which do not meet that criteria or who seek additional flexibility must seek other guidance.

Discussion: ARINC 667 provides a comprehensive set of practices under Part 25 and Part 121 for an airline to manage and distribute Aircraft Controlled Software. Aircraft Controlled Software is defined to be digital data which can be distributed to or from an aircraft that:

- Is included in an aircraft system safety assessment, or
- Requires flight operations approval, or
- Requires maintenance operations approval.

As such, it can include (but is not limited to) Field Loadable Software (FLS), Software Parameter Data Items (SPDI), User Modifiable Software (UMS), User Certified Software (UCS) (including cabin databases), Aeronautical Databases, Flight Operations Software (including flight manuals, airport maps, and Type A and B EFB applications), Maintenance Operations Software, and Aircraft Production Test Software.

The key element of ARINC 667 is the Loadable Software Part (LSP), which is transferred as a whole to the target hardware. A key element of managing an LSP is the Software Part Number which uniquely identifies the bit image of the binary file which resides in the memory of the target hardware, and which is electronically verifiable when as the LSP is resident in the target hardware. For security, it defines security objectives for the process elements, and references the security controls defined in ARINC 827, “Electronic Distribution of Software by Crate”.

ARINC 667 addresses the following operational processes:

- Distribution of LSP from OEM to operator, within operator facilities and from operator facilities to aircraft,
- Development and release of LSPs for UMS,
- Storage of LSPs in ground and onboard storage devices.
- Receipt of a newly delivered aircraft by an airline.
- Management of aircraft software configuration changes.
- Software data loading.
- LSP security during the processes of LSP release, acquisition, distribution, and onboard storage.

4.3 Considerations in the Use of Commercial Off The Shelf (COTS) and Previously Certified Products

This section addresses a range of topics related to, but not necessarily limited to, the use of Commercial Off The Shelf Products (COTS) and Previously Certified Systems in Airworthiness Security Certification. These include the following topics:

- Use of Previously Certified Systems
- Use of Commercial Hardware Parts
- Use of Parts Without Development Assurance Data
- Vulnerability Management of Commercial Software or Hardware Parts

4.3.1 Use of Previously Certified Systems

Recommendation 26A: Existing considerations for the use of legacy aerospace systems for airworthiness in general should be applied to the use of legacy aerospace systems for airworthiness security. This includes the requirement for a change impact analysis which would include airworthiness security considerations.

Discussion: For this section, legacy aerospace systems are those that have been subject to type certification and safety assessment with no change to the functionality. They might or might not have been subject to an airworthiness security assessment process.

What is the difference between aircraft systems and aircraft functions? An aircraft function defines a set of requirements. Aircraft systems may perform part of a function, the complete function, or multiple functions. As an example, a navigation function may require flight crew input, navigation position processing, display of information, etc. This function could be performed by multiple aircraft systems including a control display unit with keyboard, flight management computer system and display. Multiple functions could be hosted on an IMA system and could include display, navigation, and communication functions. Functions are design concepts and systems are the implementations of those concepts in hardware, software, and actions.

Functional Hazard Assessments (FHA), especially at the aircraft-level, can be technology-independent. An FHA considers a functional representation of the aircraft. It starts with a list of aircraft or system functions (e.g., attitude control, communications, navigation, etc.). Failure conditions are identified as being impairments of those functions. Each failure condition's effects and effect severities are described. Reference information is noted. The analysis methods are identified by which the safety requirements for each failure condition will be verified. As the design proceeds to parse functions into component functions (e.g., attitude control = pitch control + roll control + yaw control) with specific relationships, the FHA can be refined to account for this parsing process. As a rule of thumb, FHAs can remain technology-independent as they concentrate on the failure conditions related to functions. From a practical standpoint, however, when the implementation technology is known, i.e. the system components that will provide the function are determined, technology may be considered. A failure condition effect's severity might take on a different nuance between differing technologies, and this can

and should be taken into account in order to most accurately describe a failure condition's effect severity and related requirements.

Applicants proposing to use legacy systems for airworthiness in general are to perform a change impact analysis based on the proposed intended use of the function and how that intended use differs from the original use of the function. That analysis is used to drive the determination of the specific activities needed to show airworthiness. For the security consideration of change impact analysis see DO-326A Section 4.2.1 and GA Best Practices Section 4.2. Software change impact analyses guidance can be found in section 12.1 in DO-178C and chapter 11 in Order 8110.49 change 1. Hardware change impact analysis guidance can be found in section 11.1 in DO-254. Systems change impact guidance can be found in SAE ARP 4754A section 6.3. These considerations also apply to the case of airworthiness security:

- In many cases, previously certified systems were not subject to a security assessment because they did not involve any external dependencies for which airworthiness security is an issue. Initially, the change in the security scope for the installation should be established and analyzed as part of the change impact analysis of the previously certified system. If the change impact analysis shows relevance, then the applicant should conduct a preliminary airworthiness security assessment for the intended use of the item that considers the legacy item's designated role within the aircraft architecture. All airworthiness security risks of the use of the previously certified items should be addressed by the architecture, operator's guidance, and external agreements for the aircraft.
- If the system was previously certified to a particular set of development assurance requirements and the technical security requirements of the previous certification satisfies the requirements of the intended application, that assurance may be used in the assessment. In that case, there must also be activities to verify that the assumptions of the referenced standard match the intended use and environment.
- If the system was previously certified to an assurance level lower than that required by the intended application, or if the security requirements of the previous certification does not satisfy the intended application, the Change Impact Analysis will determine what qualities may be extracted from the existing development life cycle data and applied to the current development in order to show retroactive compliance. Service history may be used to help demonstrate retroactive compliance, but must include a current vulnerability analysis of the item.

Note that hostility environments change largely through the addition and augmentation of threats. As a result, use of the service history is limited to providing evidence of effectiveness against the threats that were in place during the service history. The required additional vulnerability analysis will document the threats that were not in place during the service history.

4.3.2 Use of Commercial Hardware Parts

Recommendation 26B: Existing considerations for the use of commercial hardware parts for airworthiness in general should be applied to the use of commercial hardware parts for airworthiness security with the additional consideration that mitigation and isolation of the effects of airworthiness security events can require properties unique to security for isolating failures. The ECMP should include

the implementation of controls in the supply chain and development processes to monitor, control, and protect the integrity of commercial parts.[27]

Discussion: Mature commercial parts produced in very high quantities or as commercially available for multiple fields of computing have been used in commercial aviation for well over forty years. Such content on a typical modern system is often well above eighty-five percent. Several years ago, there was a large “Mil Spec” manufacturing base and parts made under that process had far greater scrutiny, process control and additional environmental qualification for the harsher military environments. Consequently, changes to products were very tightly controlled and manufacturers were required to inform users of any changes to their product. Today the environment has changed. The military dropped its “Mil Spec” requirement mainly because of cost reasons and switched to commercial parts.

The techniques discussed here have been used successfully over the last several years and should be used to mitigate the security risks associated with commercial hardware items. However, as threats evolve, the methods and techniques should evolve too. They should be flexible enough to allow change.

OEMs have typically used architectural mitigation on many critical and hazardous systems to protect against a common cause failure. Such as using similar parts from different manufacturers or dissimilar parts to perform the same function, or adding asynchronous clock mechanisms to further mitigate the common mode or common cause effect.

Multiple techniques and mitigation strategies should be used to achieve an acceptable level of protection with the additional consideration that mitigation and isolation of the effects of airworthiness security events can require properties unique to security for isolating failures.

Most large OEMs have the equivalent of an Electronic Component Management Plan (ECMP). This plan identifies each commercial hardware part. It can identify multiple trusted suppliers/sources for the part. It can also specify alternate equivalent parts and their sources should the procurement form the primary sources cease. There is an ANSI standard for preparing ECMPs. Its title is “Standard for Preparing an Electronic Components Management Plan”, EIA-STD-4899-A. The document defines the requirements for developing an Electronic Components Management Plan (ECMP).

Over the last several years there have instances of counterfeit/spurious/recycled parts entering the electronics market. OEMs have countered that by buying parts from qualified sources and known reputable suppliers. Buying on the internet and the open market brings with it certain risks. Recent news reports indicated certain Field Programmable Gate Arrays with changed date codes being sold on the open market. This becomes more of an issue as some critical parts become obsolete. Most OEMs execute last time buys to try and mitigate the impact.

Manufacturers routinely announce changes to their product and errata information via their web pages on the internet. As a result, OEMs have had to put into place a process whereby they would on a fixed frequency, visit all the required websites to look for product changes or problems.

[27] For additional discussion and guidance, see FAA CAST 31 "Technical Clarifications Identified for RTCA DO-254 / EUROCAE ED-80" and EASA CM - SWCEH - 001 Issue: 01 Revision: 01, "Development Assurance of Airborne Electronic Hardware".

4.3.3 Use of Parts Without Development Assurance Data

Recommendation 26C: Existing guidance for the use of products-without-development-assurance-data addresses airworthiness in general. This same guidance should be applied to the use of products-without-development-assurance-data for airworthiness security, with the additional consideration that mitigation and isolation of the effects of airworthiness security events can require properties unique to security for isolating failures.[28] (Note that products developed under DO-178B/C without additional security considerations would be covered under Section 4.3.1 above.)

Discussion: By definition, products without development assurance data are systems or functions, (including but not limited to COTS parts, COTS sub-assemblies, and COTS software) which will not be brought into compliance with the assurance objectives of airworthiness security.

In some cases the necessary design documentation can be lacking or insufficient from either a safety or a security perspective. In other cases, the design data can be proprietary or sensitive information which the vendor or developer will not provide (so as to ensure protection of its intellectual property and competitive advantage, or prevent theft by its competitors or unscrupulous persons). In other cases, this can include partially compliant systems which the developer, for whatever reason, will not bring into complete compliance.

Because the design details are not available, it can be very challenging to determine if and how much unknown functionality the product can contain or what anomalous behaviors it can exhibit.

The use of products without development assurance data should be very limited in aircraft applications. From a security perspective:

- All airworthiness security risks of the use of the products without development assurance should be addressed outside the product, by those airplane or system elements which are in contact with the product, including architecture and the operator's guidance and external agreements,

- The aircraft or system design should prevent any potential adverse impact of products without development assurance on the aircraft applications.

The use of products with security-related development assurance should include consideration of the existing security product guidance. These include:

- The use of applicable validated Protection Profiles (ref. Common Criteria) for standard security products to define requirements, and

- The use of published Security Product Configuration Guides for installation, administration, and user guidelines.

[28] Id.

The use of such products should include the monitoring of the use of the products in other uses and applications, Security events reported by other users, e.g., problem reports submitted to the vendor by other users, can require analysis to determine if those reported vulnerabilities can impact the product use on the airplane.

In these cases, the activities must also verify that the referenced standard matches the intended use and environment of the function within the system.

4.3.4 Vulnerability Management of Commercial Software or Hardware Parts

Recommendation 26D: Considerations for commercial software or hardware parts for airworthiness security should include the consideration of vulnerability management to monitor their use in other products and sectors for security vulnerabilities and events, which can affect their airworthiness security, including continued airworthiness security.

Discussion: COTS or previously certified systems are exposed to attack in all their uses, and so may have vulnerabilities in one application that can be exploited in other applications. In addition, as targets exposed to a variety of threat environments not controllable by any particular regulator or user, software packages and hardware parts can themselves be attacked within the supply chain, and may have malware injected into them.

As a result, it is important to monitor the use of the previously developed products in other uses and applications for potential security events reported by other users, and to monitor publicly available sources of known security vulnerabilities in commercial products, such as the US NIST National Vulnerability Database, and to control the supply chain so as to detect and prevent corruption of commercial parts.

A comprehensive program would include:

1. Maintaining a database of commercial parts and their versions that are installed in currently fielded products, or are being used in current development programs,
2. Using a comprehensive source of publicly-released security vulnerabilities to determine reported vulnerabilities for the version of the commercial parts maintained in (1),
3. Performing an analysis to determine if those reported vulnerabilities can impact the product use on the airplane,
4. Reporting the analyzed vulnerabilities with impact into the appropriate problem report system for the impacted product, and
5. Implementing controls into the supply chain and development processes to monitor, control, and protect the integrity of commercial parts.

4.4 Existing Industry Equipment Standards and Technical Standards Orders

The equipment standards for Communication, Navigation, and Surveillance (CNS) are contained in Technical Standards Orders (TSO), or European TSOs (ETSO) for EASA and typically reference industry standards held by organizations such as RTCA and EUROCAE. There are other TSO/ETSO that non-CNS technologies (e.g., APUs and smoke detectors), but this overview addresses only CNS. The CNS standards are typically developed and maintained by joint Special Committees (SC) and Working Groups (WG) between RTCA and EUROCAE as well as SAE.

The FAA requested that the working group specifically provide the agency feedback about the existing TSOs for CNS/ATM. The FAA communicated to the ASISP WG that:

> "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, RTCA / TSO standards and ATS / flight crew procedures."
>
> "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 provider services"

In April 2015, the U.S. Government Accountability Office issued a report about cybersecurity and NextGen[29]. The GAO had previously reported that the FAA has taken steps to protect its ATC system from cyber-based threats. The GAO specifically pointed to a concern that "Modern aircraft are increasingly connected to the Internet." The GAO noted that "As part of the aircraft certification process, FAA's Office of Safety (AVS) currently certifies new interconnected systems through rules for specific aircraft and has started reviewing rules for certifying cybersecurity of all new aircraft."

While the focus of existing FAA policy and the task given to the ASISP is interfacing with non-government networks, the FAA has invited input from the ASISP WG about existing TSOs.

> "ARAC should provide a recommendation on whether an ASISP assessment is required for existing RTCA MOPS / TSO standards used for connectivity to ATS service providers and address continued airworthiness and maintenance of these documents"[30]

4.4.1 Review of Communications Equipment Standards and Security

The deployment of data communications capabilities is underway across several key regions including Europe (enroute), the United States (tower), and in oceanic airspace.

[29] U.S. Government Accountability Office; Air Traffic Control; FAA needs a More Comprehensive Approach to Address Cyber Security as the Agency Transitions to NextGen; GAO-15-370; Published: Apr. 14, 2015
[30] Aircraft Systems Information Security Protection (ASISP) Strategic Working Plan, Peter Skaves, FAA CSTA for Advanced Avionics, June 23, 2015

In June 2015, the U.S. aviation industry, through the NextGen Advisory Committee requested an overview of the security of data communications.[31] The FAA provided industry an SSI-level overview of the data communications security features. The FAA also provided a non-SSI set of "take away points", based on the August 2015 meeting, to be shared more broadly. The FAA noted that:

- The FAA addresses [Information System Security] (ISS)throughout the development of the design of all our acquisitions, including Data Comm, through robust Systems Engineering and ISS processes
- The FAA is leveraging existing avionics and aviation technologies which are well understood and in use across large parts of the globe – a choice supported by industry
- The Data Comm design architecture results in some inherent security features (e.g., no persistent storage of flight information, is not connected to the Internet)
- Data Comm does not interfere with or diminish other NAS protective measures (i.e., collision avoidance, conflict alert)
- Data Comm does not allow machine/override control of aircraft through the data comm link – Human always in the loop on both ends
- Augments voice communications – can fall back to voice
- The FAA continues to move forward with the Data Comm program and continues to gain momentum in implementing the capability

VDL Mode 2, which serves ACARS and ATN, is covered by TSO-C160(). (ACARS on its own is not covered by a TSO (see section 5.3 for additional consideration of ACARS).

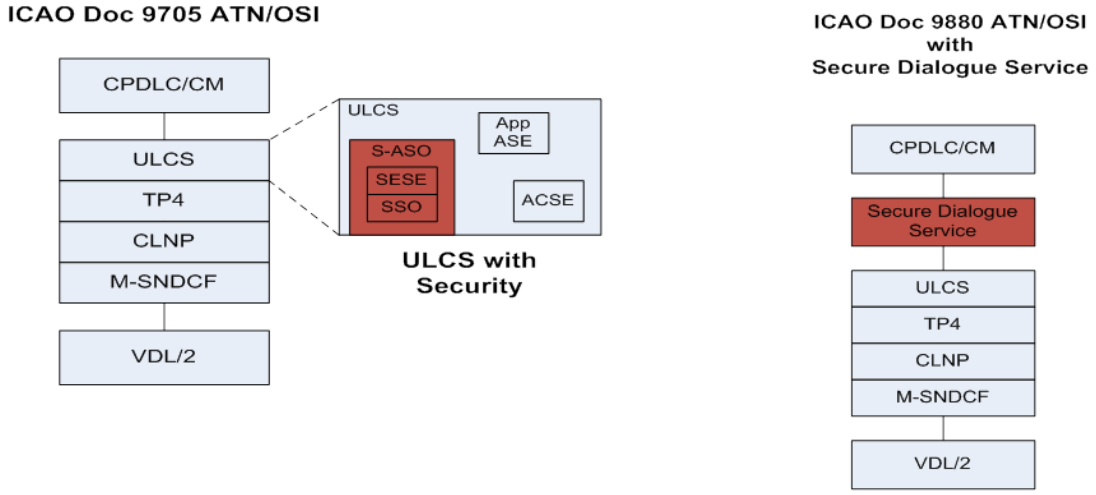
The FAA provided the ASISP working group an overview of on-going work at ICAO, specifically the Secure Dialogue Service Sub Working Group (SDS SWG) of the Communications Panel to enhance security of data communications standards to update DOC 9880[32] and DOC 9896[33].

The SDS is an alternative to implementing security in the OSI Upper Layer Communication Service (ULCS). SDS, besides reducing ULCS complexity, permits security to be done in one sub-layer rather than involving the Context Management (CM) application for key exchange. The SDS facilitates the implementation of security on an application-by-application basis to protect CPDLC or ADS-C.

The ICAO SDS SWG work addresses both ATN using ISO/OSI and ATN using IPS. Figure 4.4-1 shows the notional integration of SDS in the ISO/OSI as proposed.

[31] "The FAA's Aviation Safety Organization will also communicate with airline chief information officers on steps taken to ensure the communication process and procedures for the DataComm program are secure and subject to appropriate steps to ensure safety against cyber attacks." Letter from NextGen Advisory Committee (NAC) Chairman, Richard Anderson to FAA Deputy Administrator Michael Whitaker, July 2015.
[32] ICAO Doc 9880, Manual on Detailed Technical Specifications for the Aeronautical Telecommunication Network (ATN) using ISO/OSI standards and protocols.
[33] ICAO Doc 9896, Manual on the Aeronautical Telecommunication Network (ATN) using Internet Protocol Suite (IPS) Standards and Protocols.

FIGURE 4.4-1 COMPARISON OF EXISTING ICAO DOC 9705 ATN/OSI AND PROPOSED ICAO DOC 9880 ATN/OSI WITH SECURE DIALOGUE SERVICE (SOURCE: FAA BRIEFING TO ASISP WORKING GROUP)



The original Doc 9705, Edition 3, approach to ATN security is a validated standard, but has the disadvantage that its implementation in the ULCS introduces significant complexity to the ULCS and requires the complete ULCS to be replaced. The proposed SDS approach would simplify the implementation of ATN security.

ICAO Doc 9880 is also being updated to operate with stronger cryptography domain parameters. The current proposal is to use Elliptic Curve Cryptography over a 256-bit curve. (ECC using a 256-bit prime curve is one of the selections recommended by the National Security Agency.) As an example, Doc 9880 will:

- Use Elliptic Curve Digital Signature Algorithm (ECDSA) for signatures
- Use Elliptic Curve Diffie-Hellman (ECDH) for key agreement
- Use keyed-has message authentication code (HMAC) as the message authentication code
- Use Secure Hash Algorithm 256 (SHA-256) as the hash algorithm.

The FAA expects the work on Doc 9880 to be completed by December 2016 and validation to occur during 2017 based on the existing workplan.

Operators today also use ACARS (Aircraft Communications Addressing and Reporting System) for purpose of certain operational communications. ACARS, originally deployed in 1978, is a digital data link system for transmission of messages between aircraft and ground stations. The ASISP working group did not specifically review ACARS, but notes that the FAA has launched a research effort to evaluate the security of ACARS based on its role in the NAS.

4.4.2 Review of Navigation Equipment Standards and Security

The FAA began revising the agency's Roadmap for Performance-Based Navigation, originally issued in 2006, as a project under the Performance-based Aviation Rulemaking Committee. The revised document was provided to the FAA in early 2016. The strategy states that there is also a need to provide cybersecurity that ensures that the PBN-centric NAS remains safe and secure. In the near-term the FAA will promote the development of a digital data communications authentication standard, to be

implemented in the mid- [2021] and far-term [2026-2030], to ensure that navigation, position data, information/requests from the cockpit, and direction/clearances from ATC can be authenticated.[34]"

This strategy points to a long-term vision for enhancing cybersecurity in the CNS/ATM environment through a coordinated set of government efforts. Aircraft and equipment manufacturers are not expected to address security aspects of the CNS/ATM system on an ad hoc basis for each certification. Instead, when CNS/ATM interoperability standards are updated, specific consideration should be given to include security-specific requirements within the appropriate standards to ensure that all stakeholders can update their systems pursuant to the new security requirements.

Efforts, however, are already underway to update specific MOPS that support CNS/ATM equipment standards. The ASISP WG reviewed the content of the existing TSO/ETSO including the status of activities underway to update these standards by discipline.

As an example, the FAA in March 2015 requested that the RTCA Program Management Committee (PMC) amend the Terms of Reference for SC-159 Global Positioning Systems to address security threats. The FAA proposed, and the PMC accepted, that the SC-159 TOR be expanded to require an update to address specific cybersecurity concerns stating "New MOPS should address, to the extent practicable, the threats of intentional interference and spoofing."[35] The task given to SC-159 is targeted in nature and focused on jamming / denial of service, and spoofing.

The work underway by SC-159 builds on the knowledge that GNSS is vulnerable to intentional interference and spoofing. The FAA's navigation program in October 2012 established a study team to examine existing threat assessments, studies and data and develop specific actionable recommendations. The importance of resilience to GNSS issues is not a new issue but has been reviewed before in U.S. government sponsored studies[36]. There are a number of threat scenarios explored by the special committee including low-power mobile interference (e.g., personal privacy devices in vehicles on nearby roads), high-power interference (e.g., unplanned use of military equipment that causes GNSS jamming); and spoofing attacks – each of these vary in whether they have been experienced in real-world operations or are known to be possible by a capable actor. Their impact on aircraft avionics also vary greatly including short-time loss of GPS tracking to loss of continuity and availability.

The work in SC-159 is being conducted in the context of existing operational mitigations such as reversion to backup navigation (e.g., DME/DME, VOR MON) and ATC intervention to address loss of GPS and the use of TCAS to mitigate spoofing.

There are both policy and technology mitigations to GNSS vulnerabilities under consideration including GNSS system cross checking against independent position sources and the possible implementation of

[34] Performance-Based Navigation (PBN) NAS Navigation Strategy – 2016, January 19, 2016
[35] RTCA Paper No. 077-15/PMC-1317, March 24, 2015, Terms of Reference, Special Committee SC-159, Navigation Equipment Using the Global Navigation Satellite System (GNSS), (Version 6)
[36] Johns Hopkins University Applied Physics Lab (APL) Risk Assessment Study (1999); Department of Transportation Vulnerability Assessment (2001)

digital signatures within future satellite-based augmentation system (SBAS) messages as well as GPS L5 navigation data. [37]

The FAA, at the June 2015 PMC, requested a further expansion to SC-159 TOR to include a more general tasking of "cybersecurity" without the specificity of the March amendment to the TOR. Industry rejected this broad tasking in favor of focusing on the two areas for which GNSS is susceptible to external interference; i.e., intentional interference (jamming) and spoofing, per the March TOR.

The ASISP endorses this targeted approach to amending specific MOPS, based on the risk that its specific function exposes, and encourages the FAA to work in cooperation with industry and other regulators to identify targeted security risk mitigations that can feasibly be included within the scope of specific CNS/ATM standards.

4.4.3 Review of Surveillance Equipment Standards and Security

Today's on-board equipment used for aircraft surveillance is based on transponder beacon technology standards first developed in 1975. The primary transponder technology is based on Mode S. The Mode S standard has gone through recent changes to its supporting standards through the development of 1090ES and Automatic Dependent Surveillance Broadcast (ADS-B). Aircraft equipped with Mode S transponder broadcast their "Mode S" code which is a 24-bit address code assigned to each aircraft. The code is sometimes referred to as the aircraft's ICAO address. For civil aircraft registered in the United States, the ICAO 24-bit aircraft address is established as a function of the aircraft's registration number.

The development of ADS-B started in 1995 and uses the same frequency, 1090MHz, as the aircraft's Mode S transponder. Aircraft upgrading with ADS-B capability typically swap their existing transponder for one that also meets the ADS-B equipment standard. (Deployment of ADS-B in the United States also permits use of equipment that transmits on 978MHz if the aircraft has a separate Mode A/C or S transponder.)

Concerns have been raised about ADS-B security issues [38] since the start of the deployment of the technology in the mid-2000s. Critique of the system includes the ability to jam (denial of service) and spoof (introducing ghost targets) as well as the ability to track aircraft positions in real-time and that the signal is not encrypted.

ICAO in 2011 provided its perspectives about ADS-B security. ICAO notes that ADS-B, like other civil aviation CNS technologies, "are currently defined as "open systems"." which includes the standards being available to the public. ICAO notes that "the development of a receiver or emitter does not require exceptional expertise or very expensive hardware." And that "Emitting false traffic information from ground location is also feasible." ICAO makes several recommendations including awareness that ADS-B security specific issues exist; the importance of considering ADS-B in context of the overall surveillance infrastructure, and that:

[37] Federal Aviation Administration; GNSS Intentional Interference and Spoofing [power point slides]; Ken Alexander and Deborah Lawrence; RTCA SC-159; October 2015.
[38] ADS-B Is Insecure and Easily Spoofed, Says Hacker, Matt Thurber, Aviation International News, September 3, 2012

> "2.4 Future development of ADS-B technology, as planned in the SESAR master plan for example, should address security issues. Studies should be made to identify potential encryption and authentication techniques, taking into consideration the operational need of air to ground and air to air surveillance application. Distribution of encryption keys to a large number of ADS-B receivers is likely to be problematic and solutions in the near and medium term are not considered likely to be deployed worldwide."[39]

More recently, the FAA chartered the Equip 2020 program to support the implementation of ADS-B technology in the United States. One item reviewed specifically by Equip 2020 is whether the deployment of ADS-B created privacy or security implications for the persons onboard the aircraft. Equip 2020 concluded that "for the purpose of determining the aircraft's identify or location in the airspace, adding ADS-B data does not significantly impact the privacy or security of the aircraft since the ICAO address and FLT ID were previously located in the basic Mode S message."[40] Equip 2020 reviewed how the aircraft's real-time position data is transmitted and used by different types of transponder technologies, Secondary Surveillance Radars, and TCAS II (ACAS).

While the deployment of ADS-B does not materially change the ability to track an aircraft in real time, the FAA and industry agreed that the long-standing security and privacy implications arising from the ability to track and aircraft's transponder signal warrant further review. Equip 2020 concludes that:

> "Since the privacy and security risks are driven by the basic 1090 –link concept of operations and not ADS-B, the mitigation of these risks must be developed in the context of the broader operation of the National Airspace System and aircraft surveillance not just ADS-B."

Equip 2020 recommends that two activities should be launched to address these real concerns over privacy and security caused by the ability of tracking aircraft transponder IDs in real time. First, the FAA should review whether the agency can change how the 24-bit address assignment is done and whether a concept like Dynamic Mode S can be leveraged for civil aviation. Second, the FAA should task RTCA to undertake "an assessment to determine if it is feasible, and would support the objective of mitigating the ability to track aircraft on a real time basis, to add encryption to the transponder interrogation response, or other means to mitigate privacy and security risk, as part of a future change" the applicable standards.

The FAA has requested feedback from industry, by way of SC-186, on the feasibility and practicality of encrypting ADS-B information transmitted on the 1090MHz frequency.[41] The FAA specifically requested that "RTCA, utilizing the expertise of SC-186, provide responses to the FAA in response to the following two questions:

(1) Is it technically feasible to encrypt the ADS-B and transponder signal? As part of the review, consideration should be given to identifying what part of the ADS-B and transponder message

[39] Guidance Material: Security Issues Associated with ADS-B, International Civil Aviation Organization, Asia and Pacific Office

[40] Aircraft and Operator Privacy – Implications from Mode S Transponders and ADS-B for Civil Aircraft, Equip 2020, June 22, 2015

[41] Feasibility of Encrypting ADS-B information on the 1090MHz Frequency, RTCA Special Committee SC-186, Presented to Automatic Dependent Surveillance-Broadcast (ADS-B) Plenary, Meeting #64, Washington, D.C., October 30, 2015 by Alejandro Rodriguez, FAA

would be required to be encrypted to achieve a degree of risk mitigation against the real-time tracking of an aircraft's identify (i.e., aircraft 24-bit address code).

(2) Is it technically practical to encrypt the ADS-B and transponder signal? As part of this review, consideration should be given to what systems currently rely on the ADS-B and transponder signal in the National Airspace System. The response should also identify harmonization issues that may result from signal encryption. The FAA only views those solutions as practical that would not be require retrofit of existing avionics (i.e., the encrypted signal must be backwards compatible with existing avionics including ADS-B OUT and IN MOPS as well as other systems that use the transponder's identity information."[42]

This feasibility review is currently underway and expected to be completed in 2016.

ADS-B relies on GPS position data to provide an accurate transmission of the aircraft's location. As a result, the same vulnerabilities discussed previously about navigation (see, Section 4.1.2) are also risks to ADS-B. The NAS, however, is not exclusively reliant on ADS-B for surveillance. ADS-B denial of service could occur during GPS outages and because of signal jamming. The mitigations against this risk to ADS-B include the retention of secondary surveillance radars as a back-up system through the enroute and high-density terminal airspace. The FAA will also retain all primary radars and can use primary radar to mitigate single-aircraft avionics failures. The FAA also actively monitors the ADS-B signal which would permit any anomalies to be investigated and resolved. ADS-B spoofing (false target attacks) is also possible and has been investigated. Several mitigations are in place to address spoofing including the retention of radar, ranging to a ground based radio station on Universal Access Transceiver (UAT) avionics, and Time Difference of Arrival (TDOA) on 1090-ES. The FAA uses these and other automation capabilities to validate target aircraft and filter out those signals not suitable for tracking or being displayed to ATC. Additional protections are in place for the ground infrastructure which must adhere to FAA's Federal Information Security Management Act (FISMA) compliance.

The work chartered by Equip 2020 and assigned to SC-186 does not currently include consideration of authentication of ADS-B. Proposals have previously been made to embed a digital signature within[43] Mode S Extended Squitter (ES) ADS-B messages through the use of Phase-Shift Keying modulation.

4.4.4 Conclusion – Security Considerations for CNS Technologies

The FAA, as well as other regulators, should continuously work to assess security risks of existing CNS technologies. This work should be targeted, based on how each technology operates by itself, and how each technology operates as part of the broader infrastructure. Proposed risk mitigations are under review for technical feasibility and ability to address the underlying security concern.

<u>Recommendation 27:</u> The ASISP recommends that the FAA undertake a review of the existing CNS/ATM TSOs, in coordination with industry, and determine if targeted risk mitigations should be integrated into future revisions to specific standards. Some of this work is already underway (e.g., RTCA SC-159 and SC-186, as well as ICAO CP), but a comprehensive table top review of the CNS avionics standards would help to mitigate risk and address concerns.

[42] Letter from Richard E. Jennings, Acting Assistant Manager, Design, Manufacturing, & Airworthiness Division, aircraft Certification Service, FAA, to Margaret Jenny, President RTCA; December 14, 2015.

[43] ADS-B Authentication Compliant with Mode-S Extended Squitter Using PSK Modulation; Omar A. Yeste-Ojeda and Rene' Jr. Landry; LASSENA Labs; Ecole de Technologie Superieure, Montreal, Canada.

5 Additional Considerations

5.1 Role of A-ISAC and CERT Activities in Data Sharing for ASISP

One aspect of what makes ASISP different from Aviation Safety is the potential rapid pace that threats evolve and adapt, as witnessed in traditional IT systems and networks. A number of organizations have banded together to form the National Council of Information Sharing and Analysis Centers (ISAC). For each sector (such as Financial, Communications, Defense), members share threat information so that additional protections and mitigations can be put in place, helping to strengthen the overall industry.

In 2014, the Aviation Information Sharing and Analysis Center (A-ISAC) was formed to help share cyber threat information for the aviation industry. As of July 2016, approximately 24 members of the aviation industry have become trusted members of the A-ISAC. As the A-ISAC continues to develop and mature, ASISP related threat information will be shared between trusted members.

US-CERT (United States Computer Emergency Readiness Team), part of the Department of Homeland Security, strives to address cybersecurity by responding to major incidents, analyzing threats, and exchanging critical cybersecurity information with trusted partners. While not specifically focused on ASISP threats, US-CERT is a valuable resource that can help support the Aviation industry.

Recommendation 28: The ASISP working group recommends that both the A-ISAC and US-CERT should continue to develop capabilities to address ASISP specific threats and issues in support of ensuring a safe and secure aviation industry.

5.2 Security Considerations for FAA Designees and Associated Training

For many other aspects of aviation compliance, the FAA has established designees or delegated authority to individuals (Designated Engineering Representatives (DERs) and Authorized Representatives (ARs)) and organizations (Organization Designation Authorization (ODAs)). These individuals and organizations are authorized by law to perform certification tasks on behalf of the FAA, enabling the FAA to focus resources on critical areas while still supporting oversight of ongoing certification activities.

The same need and rationale that applies to other aspects of regulatory compliance delegation, also exist for ASISP activities. While ASISP practices continue to evolve, the FAA, in partnership with industry, should begin now to develop national standards for requirements and training associated with ASISP delegation authorities. These requirements should be commensurate with designee requirements in other aspects of aviation engineering, while being tailored to address ASISP considerations.

Recommendation 29: The ASISP working group recommends that the FAA develop and provide clear standards for security designations for designees.

5.3 Research Activities to Support ASISP

FAA and industry have worked to address system security for over two decades. This report's recommendations build on the experience matured during this work.

The FAA has identified research opportunities to increase understanding and advance the standards for cybersecurity.

- **FAA Security Research Activities Phase 1**: Study to determine feasible method(s) to conduct an **ASISP Vulnerability Assessment** based on a system view perspective. The effort will begin with one system interface which will be used to explore how to conduct a system view vulnerability assessment. The approach(s) if successful will be expanded to include several interfaces (e.g., ACARs, EFB, FLS, maintenance laptops, etc.). The system view means that the vulnerability assessment will be conducted on a system with a black box approach. A **Risk Assessment Methodology** will also be developed to take into account the ASISP threat assessment and asset value assessment.

- **FAA Security Research Activities Phase 2:** In FY18 the risk assessments will be used to develop methodologies for a deeper analysis of the vulnerabilities and risks found in Phase I. Explore ASISP tools and techniques to generate mitigation options. Analysis techniques will include the impact of changing the vulnerability and/or changing the asset values.

- **FAA Security Research Activities Phase 3:** Explore an AVS ASISP safety risk management process and integrate all of the components developed in Phase I & II with all available resources. Propose effective formal strategies which will leverage the efforts from other government agencies and industry stakeholder. Goal: Reduce the associated ASISP risks for aircraft certification, maintenance and continued operational safety.

Recommendation Research R1: The ASISP recommends that the FAA consider the following topics as part of future agency research to address cybersecurity:

- **The FAA should undertake research to determine how threat and vulnerability sharing can be most effectively done for ASISP including in coordination with international partners and regulators.**
- **The FAA should fund the development of tools that can facilitate event log analysis.**
- **Study means of detecting and preventing vulnerabilities from PED's connectivity to Avionic Interface Devices.**
- **Study means of detecting vulnerabilities in receiving transponder and ADS-B Data in aircraft.**

5.4 Cost and Benefit of ASISP Rulemaking

The ASISP working group did not provide a detailed cost-benefit analysis of the FAA undertaking rulemaking to establish airworthiness standards to address cybersecurity. The working group, however, notes the following things to help inform FAA cost-benefit analysis.

The working group notes that industry already expends significant resources to address ASISP when complying with special conditions, but also the work to address cybersecurity when special conditions are not issued by the regulator. The establishment of a consistent and harmonized regulation with associated guidance will help address cost to industry by a establishing a set of clear and standardized approaches to ASISP. A key benefit to the manufacturers is reducing program risk, because uncertainty is a key cost driver.

Industry also note that the cost of the ASISP regulation will not only be conducting the required assessment to support the rule, but primarily driven by the cost of implementing the requirements to address ASISP. The working group notes that cost avoidance may be possible to assess by considering the impact of potential flight delays, but also potential safety issues resulting from lack of standardized and appropriately robust ASISP.

Finally, the working group notes that the FAA should apply lessons-learned from the HIRF-rulemaking where the FAA justified the regulation based on years of having issued special conditions for a number of years and those special conditions, like for ASISP, were then implemented in an amendment to the airworthiness code.

List of Appendices

Appendix A – ARAC Task and Federal Register Notice

DEPARTMENT OF TRANSPORTATION
Federal Aviation Administration
Aviation Rulemaking Advisory Committee - New Task

AGENCY: Federal Aviation Administration (FAA), DOT.

ACTION: Notice of new task assignment for the Aviation Rulemaking Advisory Committee (ARAC).

SUMMARY: The FAA assigned the Aviation Rulemaking Advisory Committee (ARAC) a new task to provide recommendations regarding Aircraft Systems Information Security/Protection (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. This notice informs the public of the new ARAC activity and solicits membership for the new ASISP Working Group.

FOR FURTHER INFORMATION CONTACT:
Steven C. Paasch, Federal Aviation
Administration, 1601 Lind Ave. S.W., Renton, WA 98057-3356,
Email: steven.c.paasch@faa.gov, Phone: (425) 227-2549, Fax (425) 227-1100.

SUPPLEMENTARY INFORMATION:
ARAC Acceptance of Task
As a result of the December 18, 2014, ARAC meeting, the FAA assigned and ARAC accepted this task establishing the ASISP Working Group. The working group will serve as staff to the ARAC and provide advice and recommendations on the assigned task. The ARAC will review and approve the recommendation report and will submit it to the FAA.

Background
The FAA established the ARAC to provide information, advice, and recommendations on aviation related issues that could result in rulemaking to the FAA Administrator, through the Associate Administrator of Aviation Safety.

The ASISP Working Group will provide advice and recommendations to the ARAC on ASISP-related rulemaking, policy, and guidance, including both initial certification and continued airworthiness. 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. 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. 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.

There are many different types of aircraft operating in the United States National Air Space (NAS), including transport category airplanes, small airplanes, and rotorcraft. The regulations, system architectures, and security vulnerabilities are different across these aircraft types. The current regulations do not specifically address ASISP for any aircraft operating in the NAS. To address this issue, the FAA has published special conditions for particular make and model aircraft designs. The FAA issues Special Conditions when the current airworthiness regulations for an aircraft do not contain adequate or appropriate safety standards for certain novel or unusual design features including ASISP. Even though the FAA published special conditions for ASISP, an update to the current regulations should be considered. International civil aviation authorities are also considering rulemaking for ASISP and the ASISP Working Group could be used as input into harmonization of these activities.

The FAA has issued policy statement, PS-AIR-21.16-02, Establishment of Special Conditions for Cyber Security, which describes when the issuance of special conditions is required for certain aircraft designs. This policy statement provides general guidance and requires an update to address the ever evolving security threat environment.

A companion issue paper is published in combination with each FAA ASISP Special Condition. The issue paper provides guidance for specific aircrafts and models and contains proprietary industry information which is not publically available. These issue papers, with industry input, could provide additional guidance and best practices recommendations and could be used as input into the development of national policy and guidance (e.g., advisory circular). The FAA has not published guidance on the use of security controls and best practices for ASISP, thus ARAC recommendations in this area are highly desirable.

There are many industry standards addressing various security topics, such as Aeronautical Radio Incorporated (ARINC), Federal Information Processing Standards (FIPS), International Standards Organization (ISO), and National Institute of Standards and Technology (NIST) standards. There are also industry standards addressing processes for requirements development, validation, and verification, such as Society of Automotive Engineers (SAE) Aerospace Recommended Practices (ARP) 4754a and SAE ARP 4761. In addition, there are standards from RTCA such as (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.

The ASISP Working Group recommendations as to the usability of these standards in ASISP policy and/or guidance are highly desirable.

The Task

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 ARINC, FIPS, International Standards Organization (ISO), NIST, SAE ARP 4754a and/or SAE ARP 4761 would be appropriate for use in such ASISP-related policy and/or guidance.
5. Consider 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.

Working Group Activity
The ASISP Working Group must comply with the procedures adopted by the ARAC, and are as follows:
1. Conduct a review and analysis of the assigned tasks and any other related materials or documents.
2. Draft and submit a work plan for completion of the task, including the rationale supporting such a plan, for consideration by the ARAC.
3. Provide a status report at each ARAC meeting.
4. Draft and submit the recommendation report based on the review and analysis of the assigned tasks.
5. Present the recommendation report at the ARAC meeting.
6. Present the findings in response to the FAA's questions or concerns (if any) about the recommendation report at the ARAC meeting.

Participation in the Working Group
The ASISP Working Group will be comprised of technical experts having an interest in the assigned task. A working group member need not be a member representative of the ARAC. The FAA would like a wide range of members to ensure all aspects of the tasks are considered in development of the recommendations. The provisions of the August 13, 2014 Office of Management and Budget guidance, "Revised Guidance on Appointment of Lobbyists to Federal Advisory Committees, Boards, and Commissions" (79 FR 47482), continues the ban on registered lobbyists participating on Agency Boards and Commissions if participating in their "individual capacity." The revised guidance now allows registered lobbyists to participate on Agency Boards and Commissions in a "representative capacity" for the "express purpose of providing a committee with the views of a nongovernmental entity, a recognizable group of persons or nongovernmental entities (an industry, sector, labor unions, or environmental groups, etc.) or state or local government." (For further information see Lobbying Disclosure Act of 1995 (LDA) as amended, 2 U.S.C 1603, 1604, and 1605.)
If you wish to become a member of the ASISP Working Group, write the person listed under the caption **FOR FURTHER INFORMATION CONTACT** expressing that desire. Describe your interest in the task and state the expertise you would bring to the working group.

The FAA must receive all requests by March 5, 2015. The ARAC and the FAA will review the requests and advise you whether or not your request is approved.

If you are chosen for membership on the working group, you must actively participate in the working group, attend all meetings, and provide written comments when requested. The member must devote the resources necessary to support the working group in meeting any assigned deadlines. The member must keep management and those represented advised of the working group activities and decisions to ensure the proposed technical solutions do not conflict with the position of those represented. Once the working group has begun deliberations, members will not be added or substituted without the approval of the ARAC Chair, the FAA, including the Designated Federal Officer, and the Working Group Chair.

The Secretary of Transportation determined the formation and use of the ARAC is necessary and in the public interest in connection with the performance of duties imposed on the FAA by law.

The ARAC meetings are open to the public. However, meetings of the ASISP Working Group are not open to the public, except to the extent individuals with an interest and expertise are selected to participate. The FAA will make no public announcement of working group meetings.

Issued in Washington, DC, on January 28, 2015.

Lirio Liu,
Designated Federal Officer,
Aviation Rulemaking Advisory Committee.
[FR Doc. 2015–01918 Filed 2–2–15; 8:45 am]
BILLING CODE 4910–13–P

Appendix B – ASISP Working Group Membership and Oberservers / SMEs

Committee Members:

David H. Floyd – Boeing, Commercial Airplanes, Co-Chair
Jens C. Hennig – General Aviation Manufacturers Association (GAMA), Co-Chair
Steve Paasch – Federal Aviation Administration, FAA Representative

Steve Bates, Panasonic Avionics Corporation
Brian Brown, FedEx Express
Frederic Caro, Sagem
Claudio Henrique de Castro, Embraer
Karl Frantz, GoGo
John DeBusk, FreeFlight Systems
Mark Gulick, GE Aviation Systems
Phil Hardy, United Airlines
Dan Johnson, Honeywell
Cyril Marchand, Thales
Philippe Marquis, Dassault Aviation
Kevin Meier, Textron
Patrick Morrissey, Rockwell Collins
Ben A. Morrow, BendixKing by Honeywell
Bernard Newman, Astronautics Corporation of America
Lionel Robin, Sagem
Romuald Salgues, Airbus
Michael Severson, Bell Helicopter
Wendy Sullivan, Gulfstream Aerospace Corporation
Mitchell Trope, Garmin

Subject Matter Experts, Observers, and Government Representatives:

Jonathan Archer, GAMA
Youri Auroque, EASA
Serge Barbagelata, Airbus Helicopters
Alan Blood, Garmin
Matt Brackmann, FAA
Stephane Chopart, Airbus Helicopters
Willer Cruz, ANAC
Christine M. DeJong, ASTM International
Jeffrey Dorwart, U.S. Coast Guard Aviation Forces
Rob Duffer, FAA
Ricardo Hachiya, Embraer
Katie Haley, FAA (Office of Rulemaking)
Mark Hingsbergen, GE
Steven Hofmann, Department of Defense
Karan Hofmann, RTCA
Maruice Ingle, American Airlines
Randall Johnson, Bell Helicopter
Varun Khanna, FAA

Cedric Le May, Thales
Eric Lieberman, Boeing
Marc Lord, Transport Canada Civil Aviation
Les Lyne, FAA
Rodrigo Magalhaes, ANAC
Monica Maher, Department of Homeland Security
Bruce Mahone, SAE
Dinkar Mokadam, Association of Flight Attendants, CWA
Natesh Manikoth, FAA
Dominic Nadarski, Government Accountability Office (GAO)
David Pierce, GE Aviation Systems
Cyrille Rosay, EASA
Peter Skaves, FAA
Michelle Swearingen, FAA
John VanHoudt, FAA
Brian Verna, FAA
Chris Witkowski, Association of Flight Attendants, CWA

Appendix C – Meeting List

Meeting 1: June 23-25, 2015 (Seattle, Washington)

Meeting 2: September 29-October 1, 2015 (Washington, DC)

Meeting 3: November 17-19, 2015 (Seattle, Washington)

Meeting 4: January 20-22, 2016 (Philadelphia, PA)

Meeting 5: March 22-24, 2016 (Seattle, WA)

Meeting 6: June 13-15, 2016 (Washington, DC)

Meeting 7: July 19-22, 2016 (Seattle, WA)

Appendix D – List of Briefings

Aviation Information Sharing and Analysis Center, John Craig, Chief Engineer, Cabin & Network Systems, The Boeing Company

Aircraft Systems Information Security Protection (ASISP) Data Communications Security, Stephen Van Trees, AIR-132, FAA

Aircraft Systems Information Security Protection (ASISP) Strategic Working Plan, Peter Skaves, FAA Chief Technical Advisor for Advanced Avionics, FAA

Cybersecurity in Aviation, Cyrille Rosay, Senior Expert Avionics and Cyber Security, EASA

Current Applicability Example to Non-Part 25 Aircraft, John Van Houdt, ACE-100, FAA

Department of Defense Aviation Cyber Evaluation Discussion, Steve Hofmann, HAF A3 / OSD AT&L, U.S. Air Force

Review of Aircraft Systems Information Security Protection (ASISP) Tasking in Context of Broader CNS-ATM Cyber Issues, Steve Paasch, FAA Representative to Working Group.

SAE International Standards – Counterfeit Avoidance, Detection, Mitigation and Disposition, Bruce Mahone, Director, Washington Operations, SAE International

Updating Databases on Garmin Flight Decks, Mitch Trope, Garmin International, Inc.

Appendix E – List of Relevant Industry and Government Standards

RTCA DO–326A ‘‘Airworthiness Security Process Specification,’’ published August 6, 2014 and associated EUROCAE documents. This document provides process assurance guidance and requirements for the aircraft design regarding systems information security. (EUROCAE ED-202A.)

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. (EUROCAE ED-204.)

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. (EUROCAE ED-203.)

Appendix F Terms of Reference for SC-216

RTCA Paper No. 077-16/PMC-1446
March 17, 2016

TERMS OF REFERENCE
Special Committee (SC) 216
Aeronautical Systems Security
(Revision 6)

REQUESTORS:

Organization	Person
Boeing Commercial Airplanes	Munir Orgun, Electronic Systems Chief Engineer

SC LEADERSHIP:

Position	Name	Affiliation	Telephone	email	Change
Co-Chairs	David Pierce	**General Electric Aviation**	**(616) 241-7507**	dave.pierce3@ge.com	
	Dan Johnson	**Honeywell**	**(763) 954-6548**	**daniel.p.johnson@honeywell.com**	
DFO	Varun Khanna	**FAA, Transport Airplane Directorate**	**(425) 227-1298**	Varun.khanna@faa.gov	
Secretary	Derek Schatz	**Boeing Commercial Aircraft**	**(562) 797-8673**	**derek.p.schatz@boeing.com**	

BACKGROUND:

Prior to 2007, existing aircraft system safety guidance did not specifically address airborne network and data security issues, which results in non-standardized and potentially inequitable agreements between the various applicants and the various regulatory agencies on an acceptable process and means of compliance for ensuring safe, secure and efficient aircraft network design and operations.

This Special Committee is needed to bring together aircraft manufacturers and systems designers, CNS/ATM systems designers and operators, airlines maintenance and operations personnel and government (primarily civil aviation authorities) to form a consensus and document guidance for security of aircraft systems.

The PMC established Special Committee 216 (SC-216) on June 26, 2007, in response to a request by Boeing to provide guidance for compliance with new Special Conditions for airplane systems information

security. SC-216 has produced three documents, DO-326A, DO-355, and DO-356 to address development, certification, and continuing airworthiness processes and methods guidance.

EUROCAE committee WG-72 has produced 3 similar documents; ED-202A which is the same as DO-326A, ED-204 which is the same as DO-355, and ED-203 which contains significant differences from DO-356. The differences in ED-203 and DO-356 are currently not aligned between the two groups and additional work is needed to harmonize the two documents.

The Aviation Rulemaking Advisory Committee (ARAC) Aeronautical Systems Information Security Protection (ASISP) Working Group desires to utilize the work of SC-216 in its recommendations but that requires harmonization of the concepts in DO-356 and ED-203.

DELIVERABLES:

Product	Description	Due Date	Change
Revise DO-356, Airworthiness Security Methods and Considerations	The document should update guidance for systems affected by security considerations. The changes should be limited to and informed by the ARAC ASISP Final Report and should be harmonized with ED-203.	**Dec 2017**	

The revision of DO-356 should be limited to and informed by the ARAC ASISP final report. SC-216 should work with EUROCAE WG-72 to harmonize the following topics within DO-356 and EUROCAE ED-203 as limited to the recommendations of the ARAC ASISP:

1. Provide a definition of what assets have to be protected based on Safety Effect, determined by security assessment.
2. Provide a definition of “intentional unauthorized electronic interaction” in the guidance.
3. Provide guidance on how to identify security risk, including guidance on what is trusted in the security environment.
4. Provide a harmonized risk acceptability matrix, taking credit from previously accepted matrices as appropriate.
5. Provide guidance on how to demonstrate that residual risk is acceptable.
6. Provide guidance on how type design changes should be considered (such as STCs), including those without access to OEM data.
7. Define what constitutes acceptable certification evidence.
8. Define the scope of security Instructions for Continuing Airworthiness, including additional Design Approval Holder (DAH) guidance as appropriate.
9. Provide guidance for event logging and compliance with 14 CFR 21.3.
10. Define the role of trust in the security environment, including which service providers may or may not be trusted.

SCOPE:

The scope of this committee is the type certification for airworthiness, instructions for continued airworthiness (ICA), and operational implementation of the ICA, (hereinafter referred to as continuing airworthiness) of installed aircraft systems connected to an aircraft electronic network. The committee will address conditions, including latent 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 - excluding communication, navigation, and surveillance services managed by US Federal agencies or their international equivalents.

The material developed by this SC will encompass the following:

a. Security threats can be identified as those that impact aircraft safety, operations, and maintenance, and those that have business or privacy implications, but no impact on safety of flight. Operations and maintenance issues may have different security considerations from the traditional safety related analyses. This SC will only develop guidance material that addresses installed aircraft systems when the airworthiness and safety of flight of those systems has been impacted by information security threats from non-installed systems. Business or privacy security concerns will be considered only when they have a safety effect on continuing airworthiness.

b. Aircraft systems and equipment:

i. All aircraft systems electronic equipment.

ii. Electronic networks used for on-board data exchange and for information exchange with systems external to the airplane, and data exchange with portable devices.

c. Assumptions about and considerations for the impact of security on aircraft systems and equipment from aircraft external systems, including, as necessary, means for the evaluation and assessment of such systems in terms useful to airborne security processes. The following systems will be considered, but only the portions that have an effect on aircraft safety, aircraft operations security, or maintenance security:

i. Airline-owned systems

ii. Airport-owned systems

iii. Private network service providers

The SC will not address:

a. Other aspects of safety already addressed in existing guidance material, such as AC/AMJ 25.1309, ARP 4754, DO-178B, DO-278, and DO-254, except to the extent where there is a reliance on those other means of compliance.

b. Physical security or physical attacks on the aircraft (or ground element)

c. Airport, Airline or Air Traffic Service Provider security (e.g., access to airplanes, ground control facilities, data centers, etc.)

d. Communication, navigation, and surveillance services managed by US Federal agencies or their international equivalents (for example; GPS, SBAS, GBAS, ATC data communications, ADS-B, etc.).

e. Business or privacy concerns that have no safety effect on continuing airworthiness.

ENVISIONED USE OF DELIVERABLE(S)

The **Airworthiness Security Process Specification, the Information Security Guidance for Continuing Airworthiness**, and **Airworthiness Security Methods and Considerations** documents are intended to be used by the FAA and other civil aviation authorities (CAAs) as an acceptable means of addressing the security-related safety, operational, and maintenance security aspects of aircraft systems. It is envisioned that the documents would be invoked by an Advisory Circular for applicable aircraft types for certification. The continuing airworthiness document would be invoked by an Advisory Circular for operators responsible for operating and maintaining a secure aircraft system. The ARAC ASISP committee is currently working to determine the appropriate use of these documents.

SPECIFIC GUIDANCE:

The special committee should develop guidance material that, at a minimum:

a. Provides processes and methods for assessing system networks for security threats and to identify specific Aeronautical Networked System Security Issues.
b. Identifies network and data security issues that may impact aircraft safety and those where the impact is more business or privacy related, but has a safety effect on continuing airworthiness.
c. Establishes assurance levels for security that relate to existing safety assurance (e.g., AC/AMJ 25.1309) criteria and levels and provides objectives for evaluating network security implementations
d. Contains acceptable methods of demonstrating system safety when security issues impact aircraft systems.
e. Addresses recording and responding to security "events" and guidelines for operations, continued operational safety and maintenance of security features.
f. Addresses the requirements and guidance for post-response recovery, including identification of affected systems, restoration of system configurations, notification requirements, and other related activities.
g. Will help aircraft manufacturers, system developers, and operators ensure their systems comply with the guidance material and maintain required levels of safety where security vulnerabilities have been identified.
h. Identify attributes and characteristics of architectures and designs that constitute good practice, or which should be considered as basic to aeronautical security implementations.

During preparation of its deliverables, the SC should:

1. Emphasize that security should be considered early in the aircraft and network design and from an aircraft systems perspective.
2. Recognize the international implications of Aeronautical Network System Security and that aircraft operate globally.
3. Consider emerging technologies and systems.
4. Consider establishing a Security Domain Reference Model as a means to classify the effect of Aeronautical Network Systems Security Issues.
5. Develop, to the extent possible, an approach (or approaches) that accommodate changes in technology and that recognizes that aeronautical network system security is an on-going process (continuing airworthiness) and more involved than a single point-in-time analysis (operations, maintenance of security features). The material should focus on security objectives rather than specific solutions that may become obsolete.
6. Consider the unique role that cryptographic technology plays in typical network security architectures. Determine what design and operational compliance methods are appropriate and adequate for the application of this technology to safety-related functions.
7. Recognize that today, the airworthiness of Aeronautical Networked Systems is largely maintained by Airline processes and procedures approved by regulatory agencies, and that Aeronautical Network System Security will likely be maintained in a similar manner by the same people.

ICC Coordination – Complete.

EUROCAE Coordination - RTCA SC-216 will coordinate with EUROCAE WG72 to the extent practical. Specifically, the committee will work to harmonize EUROCAE ED203 with RTCA DO-356 as limited to the recommendations of the ARAC ASISP.

- *Initial Documentation*

Documents	**Intended Use**
FIPS 140-2, "Security Requirements for Cryptographic Modules" FIPS 199, "Standards for Security Categorization of Federal Information and Information Systems" FIPS 200, "Minimum Security Requirements for Federal Information and Information Systems" NIST SP 800-37, "Guide for the Security Certification and Accreditation of Federal Information Systems" NIST SP 800-64, "Security Considerations in the Information System Development Life Cycle" NIST SP 800-30, "Risk Management Guide for Information Technology Systems" NIST SP 800-23, "Guidelines to Federal Organizations on Security Assurance and Acquisition/Use of Tested/Evaluated Products" NIST SP 800-53, "Recommended Security Controls for Federal Information Systems" ARAC ASISP Final Report, " Recommendations regarding ASISP rulemaking, policy, and guidance on best practices for airplanes and rotorcraft including both certification and continued airworthiness" expected to be complete by August 2016	The Special Committee should examine the guidance provided by these documents when developing the committee products.

TERMINATION:
Activities of Special Committee 216 will terminate with approval by the PMC of the committee's final documents listed in the Terms of Reference. Any change/extension of a committee's work program requires prior PMC approval.

Appendix G – Draft General Aviation Best Practice Document

Recommended Practices and Guidelines for Aircraft Systems Information Security Protection (ASISP)

Version 8.0

Date: August 14th, 2016

1.0 PURPOSE

The purpose of this document is to provide equipment manufacturers, aircraft manufacturers, supplemental type certificate (STC) facilities, operators, and aircraft maintenance shops guidelines and best practices to address aircraft systems and information security protections (ASISP) related to cyber intrusion & system security threats. The guidelines and best practices in this document address system security vulnerabilities and exploits that are either not covered, or not adequately covered, by Federal Aviation Administration (FAA) regulations, policy, or guidance. This document is intended to be used as an accepted means to show to certification agencies that system security threats on aircraft installations, defined in the scope section of this document, have been adequately addressed during design, development, certification, and maintenance of the aircraft in an airworthy state (continued airworthiness). This document is meant to be easily revised in the future so that it can include new areas of vulnerabilities and updates covering new threats and mitigation techniques.

2.0 APPLICABILITY

This document may be used by applicants for a new type certificate (TC), changes to an existing TC, or supplemental type certificate (STC) projects when the installation requires the applicant to address ASISP certification requirements. It is also recommended for those applicants where the system certification basis does not require ASISP certification requirements to be addressed; however the system may introduce security vulnerabilities. The guidance in this document supports the showing of compliance for ASISP certification requirements.

3.0 SCOPE

The scope of this document is limited to system security issues related to intentional unauthorized electronic interaction that could cause threats and expose vulnerabilities of aircraft systems and networks.

These guidelines and best practices are intended to provide the applicant means to address the threat of intentional unauthorized electronic interaction to aircraft safety. The occurrence of such an interaction may affect the aircraft safety, which may contribute to a functional failure condition. While an event was not intended to cover sabotage, the act of intentional unauthorized electronic interaction to deliberately cause a failure may be applied as a hazard that ASISP intends to mitigate using both system security and system safety practices.

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

to individuals that could gain physical access to aircraft in order to cause malicious damage (e.g., aircraft fuel contamination, cutting wire bundles, etc.) are not addressed in this document.

This document has been written to provide coverage for aircraft systems and installations not covered by RTCA/DO-326A "Airworthiness Security Process Specification" and its companion documents; RTCA/DO-355 "Information Security Guidance for Continuing Airworthiness" and RTCA/DO-356 "Airworthiness Security Methods and Considerations". This document references RTCA standards and FAA guidance, but recognizes equivalent international standards found in European Organization for Civil Aviation Equipment (EUROCAE) and European Aviation Safety Agency (EASA) documents.

4.0 REFERENCE MATERIAL

List of references to this document:

AC 20-115C	*Airborne Software Assurance*
AC 20-140B	*Guidelines for Design Approval of Aircraft Data Link Communication Systems Supporting Air Traffic Services (ATS)*
AC 20-149A	*Installation Guidance for Domestic Flight Information Services - Broadcast*
AC 20-152	*RTCA, Inc., Document RTCA/DO-254, Design Assurance Guidance For Airborne Electronic Hardware*
AC 20-153A	*Acceptance of Aeronautical Data Processes and Associated Databases*
AC 20-156	*Aviation Databus Assurance*
AC 20-164	*Designing and Demonstrating Aircraft Tolerance to Portable Electronic Devices*
AC 20-168	*Certification Guidance for Installation of Non-Essential, Non-Required Aircraft Cabin Systems & Equipment (CS&E)*
AC 20-172A	*Airworthiness Approval for ADS-B In Systems and Applications*
AC 23-17C	*Systems and Equipment Guide for Certification of Part 23 Airplanes and Airships*
AC 23.1309-1E	*System Safety Analysis and Assessment for Part 23 Airplanes*
AC 25.1309-1A	*System Design and Analysis*
AC 27-1B	*Certification of Normal Category Rotorcraft*
ASTM F3153-15	*Standard Specification for Verification of Avionics Systems*

CM-SWCEH-001 Issue 1	*EASA Certification Memo, Development Assurance of Airborne Electronic Hardware*
FAA Order 8110.49 Chg 1	*Software Approval Guidelines*
FAA Order 8110.54A	*Instructions for Continued Airworthiness Responsibilities, Requirements, and Contents*
PS-AIR-21.16-02	*FAA Policy Statement, Establishment of Special Conditions for Cyber Security*
RTCA/DO-178B	*Software Considerations in Airborne Systems and Equipment Certification*
RTCA/DO-178C	*Software Considerations in Airborne Systems and Equipment Certification*
RTCA/DO-200B	*Standards for Processing Aeronautical Data*
RTCA/DO-254	*Design Assurance Guidance for Airborne Electronic Hardware*
RTCA/DO-313	*Certification Guidance for Installation of Non-Essential, Non-Required Aircraft Cabin Systems & Equipment*
RTCA/DO-326A	*Airworthiness Security Process Specification*
RTCA/DO-355	*Information Security Guidance for Continuing Airworthiness*
RTCA/DO-356	*Airworthiness Security Methods and Considerations*
SAE ARP 4754A	*Guidelines for Development of Civil Aircraft and Systems*
SAE ARP 4761	*Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment*

5.0 BACKGROUND

ASISP concerns cover the protection of aircraft systems that connect to external non-trusted services and networks if:

I. It cannot be shown by either a change impact analysis or by a safety and security risk assessment that no aircraft system with a failure effect classification of major or higher can be adversely affected, either directly or through propagation of security threats to any other system; or

Connectivity, services and networks that are "read only" or do not interface in any manner to aircraft systems essential to safe operations would only require a simple assessment to show that there are no security concerns related to the system installation. For systems and installation where there may be physical or logical interfaces to aircraft systems essential to safe operation a security assessment must show that security vulnerabilities have been mitigated.

In general increased connectivity in aircraft system designs may introduce new risks associated with security vulnerabilities that typically were not assessed during the traditional safety assessment because it excludes intentional unauthorized electronic interaction. The addition of the security methods and system processes which identify security vulnerabilities and mitigations which may flow into the system and installation design should provide acceptable means to address security concerns.

5.1 Government Service Providers

This document assumes Air Traffic Service (ATS) providers, which are managed by the United States federal agencies or their international equivalents, provide secure "authorized services". FAA ATS systems 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 "authorized 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 systems do not require any additional security considerations to ensure that the transmission links are secure. The assumption in this document 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.

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

5.2 Non-trusted Services

Recent designs for aircraft systems have included connectivity to "non-trusted services" such as the internet, portable electronic devices (PEDs), and commercial-off-the-shelf technologies that have not been certified and accredited for secure operations by a government authority. These designs can introduce system security vulnerabilities beyond the scope of current airworthiness regulations and traditional systems safety assessment methods typically used to show compliance with the airworthiness requirements.

FAA Policy Statement PS-AIR-21.16-02 provides guidance on when issuance of special conditions would be required for a certification project. This document is designed to provide guidance that can be used in conjunction with the FAA policy or future regulatory changes.

6.0 DEFINITIONS

List of key terms and definitions used in this document:

Airworthiness	*The condition of an aircraft, aircraft system, or component in which it operates in a safe manner to accomplish its intended function. [ARP 4754A]*
Asset	*Something within a system which has value (ie. needs to be protected), this could be specific data such as an encryption key, a function, or a complete computing system. Assets have properties which are used to help determine what about the asset needs to be protected, these properties are availability, integrity, and confidentiality.*
Assessment	*An evaluation based upon engineering judgement. [AC 23.1309-1E]*
Attack	*An assault on a system that derives from an act that is an attempt to violate the security of a system. Includes intentional and unintentional acts. [RTCA/DO-326A]*
Availability (A)	*A property of an asset which defines that the asset is always available when it is needed.*
Certificate Authority	*A component of the Public Key Infrastructure. Responsible for issuing and verifying digital certificates. [RTCA/DO-355]*
Confidentiality (C)	*A property of an asset which defines that the asset can only be access by authorized actors (processes or users).*
Connectivity	*Capacity for the interconnect of platforms, systems and applications*
Countermeasure	*A technical measure or process which reduces the probably that a threat can successfully compromise a vulnerability.*
Data Link Systems	*Reference AC 20-140A*
Data loading	*The process of moving airborne software and data from a storage source into the active executable memory of aircraft systems. [RTCA/DO-355]*
Development Assurance Level (DAL)	*All those planned systematic actions used to substantiate, to an adequate level of confidence, that errors in requirements, design, and implementation have been identified and corrected such that the system satisfies the applicable certification basis. [AC 23.1309-1E]*
Digital Certificate	*Refers to the Private key and associated Public Key of the digital certificate. The private key is use for signing and decrypting; the public key is used to verify the signature and encrypting. [RTCA/DO-355]*
Effectiveness	*The ability of the security protection to prevent or mitigate misuse of the assets, while preserving use of the assets for normal operation of the system and aircraft.*
External (Aircraft)	*Reference point outside of the aircraft systems, not part of the aircraft type configuration. May include carried on devices.*
Event	*An internal or external occurrence that has its origin distinct from the airplane. [AC 23.1309-1E]*
Failure	*An occurrence that affects the operation of a component, part, or element such that it can no longer function as intended (this includes both loss of a function and malfunction). [AC 23.1309-1E]*
Failure Conditions	*A condition having an effect on either the airplane or its occupants, or both, either direct or consequential, which is caused or contributed to by one or more failures or errors considering flight phase and relevant adverse operational or environmental conditions or external events. [AC 23.1309-1E]*
Field Loadable Software	*From FAA Order 8110.49*
Function	*The lowest defined level of a specified action of a system, equipment, and flight crew performance aboard the airplane that, by itself, provides a completely recognizable operational capability. [AC 23.1309-1E]*

Hazard	*A potentially unsafe condition resulting from failure, malfunctions, external events, error, or combination thereof. This term is intended for single malfunctions or failures that are considered probably based on either past service experience or analysis with similar components in comparable airplane applications, or both. There is no quantitative analysis intended in the application. [AC 23.1309-1E]*
Integrity (I)	*A property of an asset which defines that the asset is only changed or modified through a controlled process.*
Intentional Unauthorized Electronic Interaction	*Circumstance or event with the potential to affect the aircraft due to human action resulting from unauthorized access, use, disclosure, denial, disruption, modification or destruction of information and/or aircraft system interfaces. Does not include physical attacks or electromagnetic jamming. [RTCA/DO-326A]*
Level of Threat	*A qualitative evaluation of the possibility that a threat condition might occur. [RTCA/DO-326A]*
Malware	*Malicious software that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim's data, application, or operating system. [RTCA/DO-326A]*
Misuse (Security)	*Unintended (according to the design intent) actions undertaken by a person or system to interact with systems, interfaces, or data. [RTCA/DO-326A]*
Mitigation	*Reduction of risk either through lessening of severity or lessening of occurrence. [RTCA/DO-326A]*
Non-trusted Services	*Examples of non-trusted services that require assessment in system threat certification: [from FAA Policy PS-AIR-21.16-02]* • *Airport gate link networks* • *Public Networks* • *Wireless aircraft sensors and sensor networks* • *Cellular networks* • *Portable Electronic Devices (PEDs), and portable Electronic Flight Bags (EFBs)*
Requirement	*An identifiable element of a function specification (Technical) or a development assurance standard (Assurance) that can be validated and against which an implementation can be verified. [RTCA/DO-326A]*
Risk	*A measure of the acceptability of the occurrence of a cyber-event (a system contains a vulnerability which enables access to an asset which is accessible by a threat resulting in the violation of the A, I, or C constraints of the asset).*
Security Architecture	*A Security architecture defines architectural elements, together with their roles, responsibilities and interrelationships, which will implement and support security measures. Elements may incorporate hardware, software, algorithms, procedures, and policies. [RTCA/DO-326A]*
Security Effectiveness	*The ability of the security measure to mitigate misuse of the assets by the unauthorized elements of the external population, while permitting and preserving use of the assets by the authorized elements if the external population. [RTCA/DO-326A]*
Security Environment	*A security environment is the external security context in which an asset performs its function. [RTCA/DO-326A]*
Security Event	*An occurrence that has its origins from an Unauthorized Intentional Electronic Interaction.*
Security Measure	*Used to mitigate or control a threat condition. Security measures may be features, functions, or procedures, both onboard or offboard. Security measures can be technical, operational, or management. [RTCA/DO-326A]*
Security Requirements	*Requirements that are related to the implementation of a security measure. [RTCA/DO-326A]*

Severity	*Qualitative indication of the magnitude of the adverse effect of a Threat Condition. [RTCA/DO-326A]*
Threat	*Something with the potential to effect the availability, integrity, or confidentiality of an asset.*
Trust Boundary	*A logical element in a system description which designates where a change occurs in the trust component of a system. This is most often where a countermeasure is implemented. A system may have 1 or more trust boundaries designating different levels of trust. A trust boundary can typically be found at the system boundary but this isn't the only way to view a system. Elements outside a trust boundary are less trusted than elements inside the trust boundary within a system. Threats to a system are always indicated by data flows which cross the trust boundary.*
Threat Source	*Either (1) intent or method targeted at the intentional exploration of vulnerability or (2) a situation and method that can mistakenly trigger vulnerability. The threat source of a threat is intent and method: the attacker and the attack vector. [RTCA/DO-326A]*
Validation	*The determination that the requirement for a product are sufficiently correct and complete. [SAE ARP4761]*
Verification	*The evaluation of an implementation to determine that applicable requirements are met. [SAE ARP4761]*
Vulnerability	*A weakness (system defect or design flaw) which permits an attacker to access and modify the A, I, or C of an asset.*
Vulnerability Assessment	*Generic term encompassing the two existing methods, namely vulnerability analysis or vulnerability testing, used during the evaluation of the development and anticipated operation if the system item that could be exploited by a threat source. [RTCA/DO-326A]*
Vulnerability Testing	*Methods of testing for unintended function and robustness, using exploratory testing methods to detect and probe vulnerabilities that may be present in an implementation attempt to break or to circumvent the security measures. [RTCA/DO-356]*
Whitelist	*A whitelist is a computer file that lists all authorized digital certificates that have permission to access to a certain system or protocol. Any entity that is not included in the Whitelist has its access, to the system or protocol, denied. [RTCA/DO-355]*

7.0 ASISP APPROACH

The following activities provide an acceptable process to address ASISP concerns in system design, installation, documentation and certification:

1. Identify the system(s) to be assessed
2. Identify if trusted or not trusted services
3. Identify the connectivity, communication paths, and interfaces to the aircraft system that need to be evaluated for ASISP concerns.
4. Establish the equipment and systems functional failure conditions; determine criticality of the system(s) involved.
5. ASISP compliance plan should be established to identify security aspects of the certification project.
6. Apply security threat modeling and practices to determine security mitigations.
7. Apply the appropriate validation and verification to each security mitigation.
8. Identify instructions for continued airworthiness aspects related to security mitigation.
9. Document security requirements, test results, and compliance.
10. Maintenance, protection assurance and modifications need to be maintained per the instructions for continued airworthiness.

7.1 Planning

If the initial assessment reveals that the security aspects of the interfacing system:

- Is a government services or trusted interface, or
- Data flow is “read only” from the aircraft systems, or
- Equipment and aircraft systems interfaced with are Minor or No Safety Effect (NSE), and do not propagate security threats to another aircraft system whose failure condition effect classification is “major” or higher.

Then a simple assessment statement may be provided in certification planning documents covering the new installation or change. This would typically be in a Project Specific Certification Plan (PSCP) and should provide the statement and any assessment details to clearly establish agreement that ASISP concerns for the project do not require further showing of compliance.

When the security perimeter identification activity shows that security concerns must be addressed for the project, then the means of compliance for security concerns must be documented and approved by the certification authority. The plan may be included in the PSCP.

It is recommended to define in the PSCP, or other certification documents, the aircraft and aircraft systems which from a security perspective will be defined as assets. These assets are separated from security threats by a defined security trust boundary. The trust boundary is where logical and physical

interactions with asset take place and must be analyzed for security vulnerabilities. For most general aviation aircraft and operations the security environment will be primarily defined by the persons and interfacing equipment that can come into both logical and physical contact with the aircraft and aircraft systems. The PSCP should include information about the security environment, security boundary, personnel that interact with the aircraft, operational and maintenance environments.

The security planning tasks should cover the objectives detailed in *Table A-1 Planning*.

7.2 Preliminary Assessment

The applicant should identify aircraft systems and interfaces that require ASISP assessment. When the connectivity, services and networks are with non-trusted sources then an assessment must be conducted. Reference Sections 5.1 and 5.2 for government and non-trusted services definition. An understanding of the system interfaces, communication paths and system architecture must be known to determine data flow.

System interface details including communication protocols, data flow (read, write, read/write) and possible redundant paths in combination with other aircraft systems should be assessed to determine possible threat conditions.

Use the safety process to determine the equipment and aircraft systems failure conditions following 14 CFR 23.1309 and 27.1309 processes (SAE ARP4761 Section 3.2 and Appendix A). This evaluation is not intended to only cover the initial interfacing equipment and systems. An understanding of the system architecture must be known to determine the highest criticality of a failure condition caused by a security event. In general the safety process failure condition effects of “loss of function” or “misleading failure modes” would be considered. In addition, further understanding and assessment of the effected systems should consider failure conditions caused by security threat conditions related to asset integrity, availability and confidentiality. In some cases the security event may cause a failure condition that might have a higher criticality failure condition than originally determined in the original hazard assessment. When this occurs, the highest level should be adopted to the development of the security measures.

The preliminary security assessment tasks should cover the objectives detailed in *Table A-2 Preliminary Assessment*.

7.3 Threat Analysis

Apply security threat modeling and practices to determine security mitigations required to reduce risks of intentional unauthorized electronic interactions with the aircraft systems. The applicant should define the system, assets, architecture, communication paths and trust boundaries. Section 8 of this documents provides best practices to conduct a security threat analysis using the data flow diagram method. The intent of this process is to identify the security vulnerabilities and the associated affected properties Availability (A), Integrity (I), and Confidentiality (C) of each asset.

The threat analysis tasks should cover the objectives detailed in *Table A-3 Threat Analysis*.

7.4 Security Development

Following the completion of the security threat modeling the system security measures should be identified along with their properties (A, I, C). The best practice document recommends that the security mitigations be considered were identified and where possible a layered protection scheme is implemented to make a more robust security architecture defense.

Once accepted for implementation each security requirement by best practice should be assigned a security tag in the applicant system, similar to a safety requirement tag, to support traceability of validation and verification activities. These security requirements should then be managed and developed with the existing processes used for avionics systems development in software (RTCA/DO-178) and hardware (RTCA/DO-254). The successful implementation of the mitigation(s) will be shown by validation of each requirement, verification of each requirement, and system level testing (during more extensive security testing).

While a security assurance level is not proposed in this best practice, a qualitative evaluation should be conducted to assess the ability of each security mitigation and the security architecture to protect an asset against the threats identified during the threat modeling process. The applicant and the certification authority should assess the acceptability of the security measures early in the program, similar to or included in the preliminary system safety assessment (PSSA).

Current level of threat and therefore security risk is assessed as extremely improbable from government agencies when concerning Part 23, 25 with 19 seats or less, 27 and 29. Incorporation of security measures and mitigations may be incorporated without the assessment efforts trying to establish effectiveness, likelihood, probabilities and assurance metrics. The effort if taking this path of security development will require coordination with certification agencies to reach agreement on security effectiveness objectives when implementing security measures and mitigations alone. This process will support the development of security measures at a reduced level of effort acceptable when considering the safety continuum and level of security level of threat to safety. Possible solutions in conducting a qualitative risk analysis are provided in Section 8.4.4.

The development of the security mitigations and the associated validation processes should cover the objectives detailed in *Table A-4 Security Development*.

7.5 Verification Testing

The verification of the security mitigations and the security architecture will initially be conducted during the standard verification processes which are part of DO-178 and DO-254 processes (Security Functional Requirements Testing). These tests will be used to verify that each security requirement meets its intended function. Specific tests should then be conducted to test the security requirements when submitted to abnormal inputs and conditions (Application Fuzzing, Robustness Tests), and aggressive tests intended in misuse the aircraft systems (Penetration Testing, Vulnerability Tests).

The verification testing coverage should cover the objectives detailed in *Table A-5 Verification Testing*.

7.6 Security Assessment

An assessment of the security requirements implemented to mitigate the threats to the system should be provided in compliance documentation. The assessment should evaluate the security vulnerabilities and that appropriate mitigations were implemented correctly and completely in relations to the system requirements and safety objectives.

Assessment should evaluate verification testing outlined in Section 7.5, and shown complete via inspection of test plans and results reports.

The security assessment, considering all the security mitigations and activities should cover the objectives detailed in *Table A-6 Security Assessment*.

7.7 Compliance Summary - Documentation

The formal documentation of the security requirements, assessments, testing and showing of compliance to guidance, policy or regulations should be completed in a way to provide evidence of the stated tasks. Where required the showing of compliance to applicable regulations must be shown in formal documentation to support the finding of compliance by the certification authorities or its delegates. Documentation supporting ICA activities or installation guidance must also be released and maintained to ensure that security requirements remain effective.

The documentation covering security activities and showing of compliance to system security requirements should cover the objectives detailed in *Table A-7 Compliance Summary - Documentation*.

7.8 System Security Interfacing with System Safety Processes

An acceptable method to handle security concerns is to utilize existing system safety process already in use to support showing of compliance to safety regulations; using ARP 4761 processes. The system security coverage interfacing with existing system safety processes applies only to security events related to the intentional unauthorized electronic interaction, not physical security or other means of tampering with the aircraft and systems.

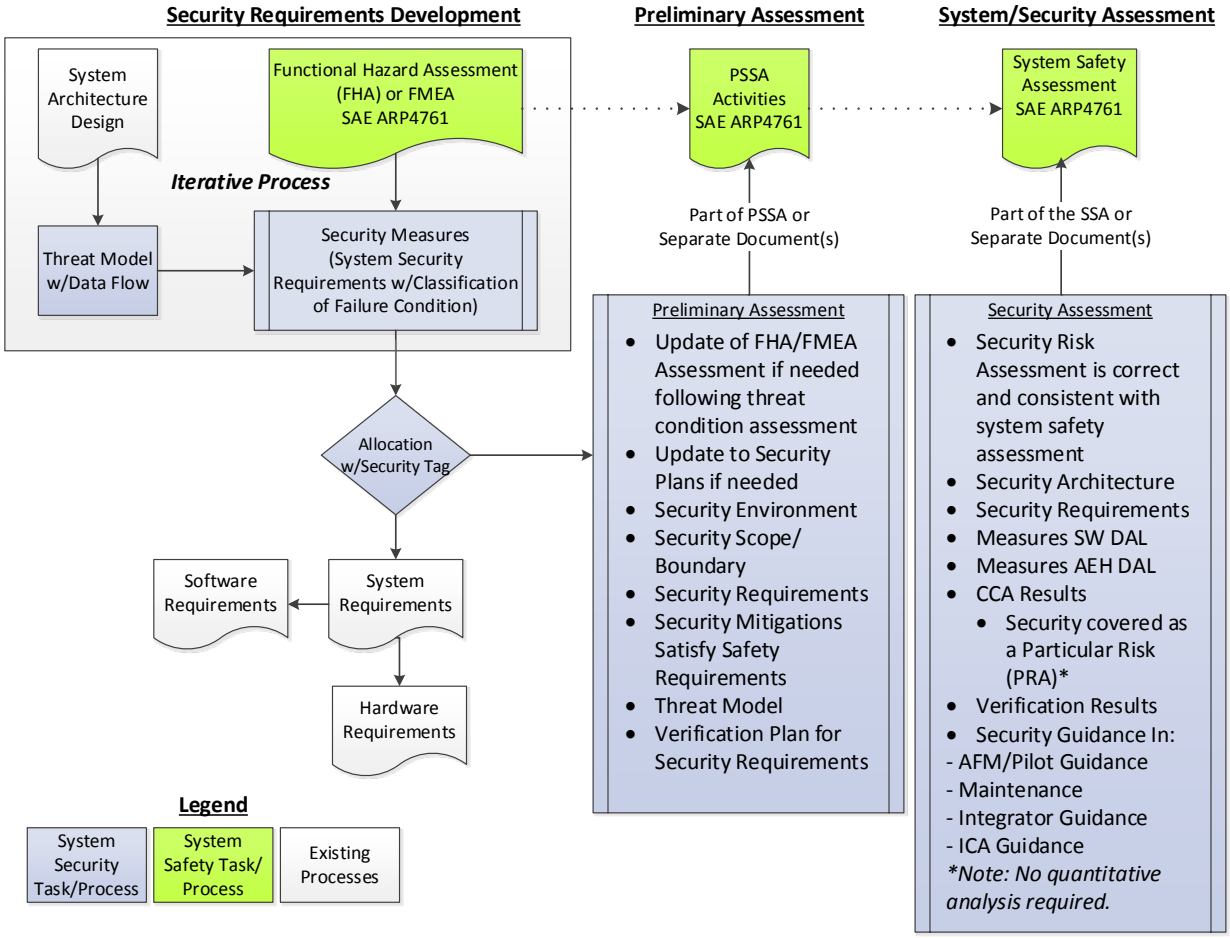


Figure 1– Security and System Safety

Initial system architecture and functionality needs to be defined with enough clarity to identify interfaces, systems, assets, users (Pilot/Crew/Passengers/Maintenance/Public). This is an iterative process with updates to the system definition and architecture through the development of the system and integration into the aircraft.

The creation of the security threat model with data flow diagrams should identify the assets, communication interfaces & types (Data Flow), and security boundary(s). The threat model process and outputs will support the identification of security vulnerabilities, mitigations, severity of the threat condition, and impact to asset properties (Availability, Integrity, and Confidentiality). Reference Section 8 for the system security analysis methods.

Review the hazard assessment (where applicable AFHA, SFHA or FMEA if no FHA conducted) to assess that the functions and failure conditions when applying considerations related to system security are adequately addressed. The expected failure conditions should consider security events that may cause both loss of function and malfunction failures. When considering loss of function in the context of security the vulnerability of the asset is Availability (A), and when considering malfunctions in the context of security the vulnerability of the asset is Integrity (I). Failure conditions of functions in most cases do not address Confidentiality (C) in the FHA or FMEA, these should be considered when reviewing and working the FHA or FMEA. For more information on the security handling of Availability, Integrity and Confidentiality reference Section 8.1.1.3.

- System Requirements from Threat Model (Security Mitigation Requirements)
    - Threats from Threat Model
    - Asset (Aircraft System)
    - Security Measures/Mitigations (Technical Recommendations from this document or other references)
    - Failure Condition Classification by System

Note: Identified security measures that interface to systems with functional hazard assessments that are Minor or lower will stop here, others move on to the PSSA and SSA processes below.

- PSSA or SSA Coverage (Follow AC 23.1309-1E, SAE 4761) – Major & Above
    - Assessment Methods – coverage where Threat Model activities are outputs to the PSSA/SSA tasks using existing processes for SW, HW, Systems objectives and processes
        - Design Appraisal
        - Installation Appraisal
        - Development Assurance Levels (DAL) – Software and AEH
            - System Security requirements should be implemented to the same DAL
        - Qualitative Analysis
            - CCA Common Cause Analysis (SAE 4761)
                - Particular Risk Assessment (PRA) – Major & Above (SAE 4761)
        - Quantitative Analysis – Not part of the assessment method, Security Measures/Mitigations do not feed into the quantitative analysis

.

7.9 Additional Best Practice Recommendation

The following recommendations should be considered in the development of a robust security architecture:

- **Security Event Logging** – Consider security event specific fault log items to aid in the investigation of system faults, failures and malfunctions. Presently there is not a standardized Security Fault Log specification used by industry so implementation presently is not defined. Intent would be for forensic data analysis. Challenges with implementation may be infrastructure for storing and processing of data, capability to retrieve and store logs, and desire of the operators to do any sort of regular periodic review of the logs.

- **Task Drivers to Force Security Reviews** – Implementation of Task Drivers into the sustaining life cycle of a system to ensure review of security updates; such as in Common Vulnerabilities and Exposures (CVEs).

8.0 SECURE SYSTEM DEVELOPMENT

Developing cyber resilient systems cannot be accomplished through the loose application of security measures late in the design process. Nor can it be done without a complete understanding of a systems purpose and function. Security must be designed into the system. That is, it must be considered at every stage of the design process. Developing systems using this approach enables the system designers to consider threats and potential vulnerabilities during the design and manage those risks at a lower cost. This section looks at the standard system development process and how security activities can be incorporated into each stage to ensure a secure product to support the overall security of aircraft operation.

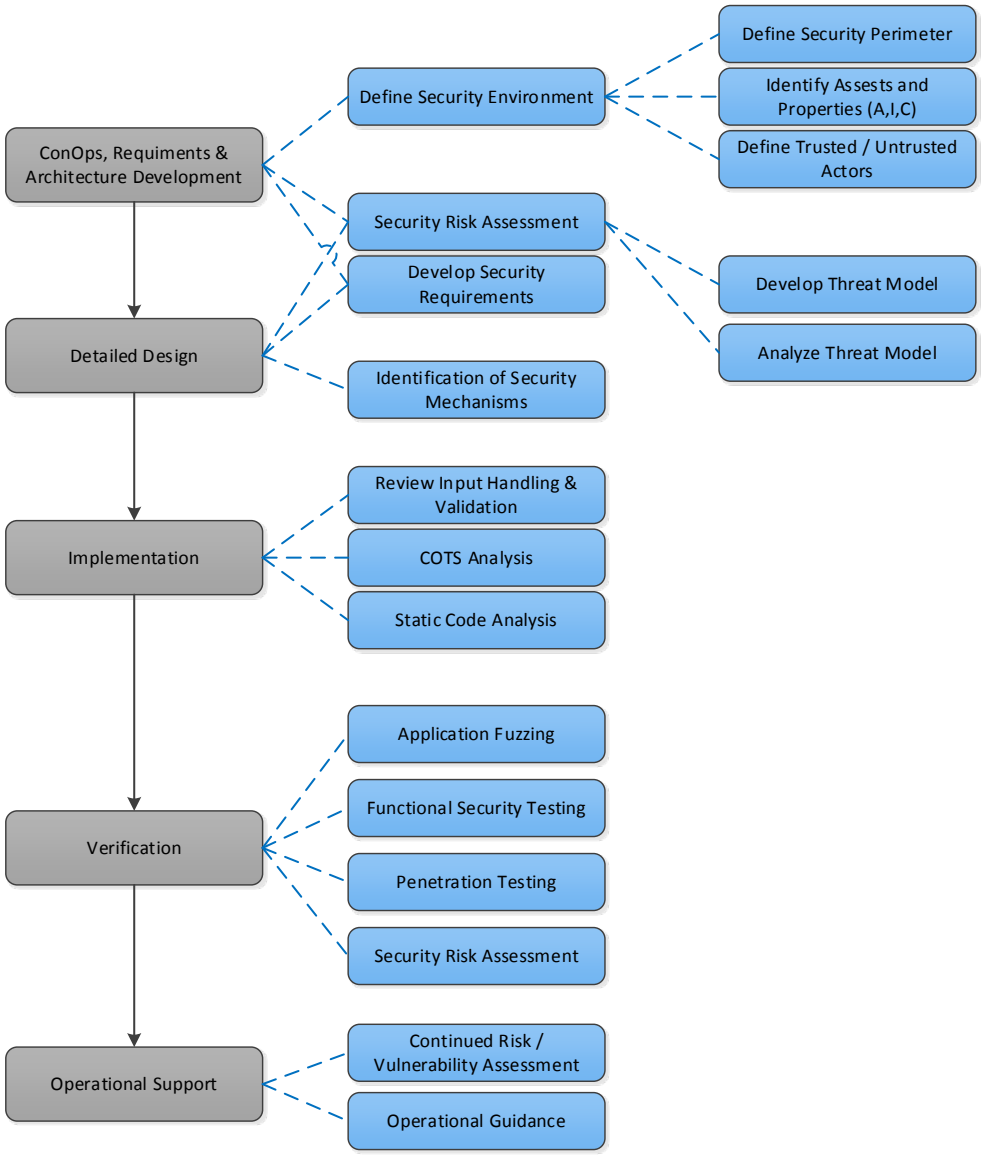


Figure 2 – Secure System Development Process

8.1 Concept of Operations (ConOps), Architecture & Requirements Development

During this phase of the traditional systems development process the operational environment of the system is defined. This includes system-level design activities such as use case development and actor definition. By considering security during this early phase of system development the foundation for the security aspects of the system can be developed alongside the functional aspects. As with other aspects of the system the purpose of considering security early (and throughout) the design helps ensure the end product addresses the correct problem. To address the security aspects the system designer should define the security environment for the systems and develop a system level security assessment.

8.1.1 Define Security Environment

In defining the security environment the system designer should consider the operational environment of the system, where it will be used or installed and what type of security is provided by the operational environment. For instance if the system will be installed in a secure locked area only accessible by trusted personnel, physical access to the hardware will be considered a trusted interaction. Likewise network ports which are only available in the cockpit maybe considered trusted because of their location and only be accessible by the pilots. But the wireless interface, and supported protocols, which broadcast outside of the cockpit and into publicly accessible areas may not. ARINC-811 provides a good reference for consideration and provides an example of how an aircraft might be broken up into multiple trust zones for analysis. Just as each interface on a system has a functional purpose; it also has a trust level associated with the actor(s) affiliated with the interface.

8.1.1.1 Define Trusted and Untrusted Actors

To do this successfully the system designer needs to often look at the actor definition more broadly. A functional system design may define a use case for a maintenance operator to install software but how is it assured the individual accessing the interface is a valid maintenance operator? Do they wear a badge which was checked prior to entry? Likewise a use case might exist for a pilot who uploads a flight plan over a wireless interface. How is it assured the actor was in fact a pilot? It might be necessary to add an authentication function into the system to validate the actor prior to the use case. By considering the actor more broadly the system designer can better define the trust level of each actor and begin to understand where security functions will need to be implemented.

8.1.1.2 Setting the Security Scope / Boundary

By defining actors with the system as trusted or untrusted the interfaces affiliated with the actors can be labeled accordingly and a security boundary can be developed. The system security boundary (or trust boundary) is defined as the location in a system where the level of trust of data handled by the system changes from untrusted to trusted. In system design this is an indicator of where security functions will need to be implemented. At the system level this boundary will typically be drawn at an interface with an untrusted actor but as the system is decomposed the boundary will be pulled inside the system and affiliated with a security function which will mitigate the threat associated with the mis-use case.

8.1.1.3 Define System Assets

To correctly address security in a system it's important to define the system assets and the properties of those assets that are critical to the system. An asset is anything in a system which is important to its primary function. Another way to think of it is a system or component of a system which would have a negative effect if it became unavailable, altered, or accessed, in an unexpected way during operation. The properties are defined as: Availability (A), Integrity (I), and Confidentiality (C) and are defined below and depicted in Figure 3:

- Availability – The condition that a service or function is available when it's needed (this does not necessarily mean all the time.
- Integrity – The condition that data is modified or altered only according to a defined process in an expected manner.
- Confidentiality – The condition that data is only accessible to and read by the intended parties.

It's uncommon for all three of these properties to be considered critical in the implementation of an asset. For example in avionics systems availability and integrity are typically important but the information processed by the system doesn't often have a confidentiality requirement. The exception to this would be passwords or key material used for access control or encryption.

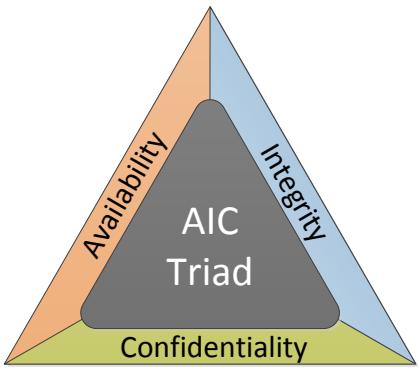


Figure 3 – AIC Triad

8.1.2 Perform Preliminary Security Risk Assessment

Risk management is defined as the process of identifying vulnerabilities and threats to information resources and deciding what countermeasures to take in reducing the risk to an acceptable level[44]. This is the purpose of the Preliminary Security Risk Assessment. During this phase the system designer uses the definition of actors, assets, and security boundary from the previous step to begin assessing and managing the risks in the system. One means of doing this is through threat modeling.

8.1.2.1 Develop / Analyze Threat Model

Threat modeling is a popular technique employed by system designers to think about and document the security threats to their system. A threat model is typically composed of a collection of lists and

[44] Certified Information Systems Auditor Review Manual, 2006

diagrams which provide the reader with an understanding of information flow within the system from multiple views. There are many approaches to threat modeling and the development team should utilize the one that works best within their process to produce a complete analyzable model.

The threat model should not be thought of as a static artifact developed at a singular phase in the program but instead an evolving view of the system which is decomposed as the system is decomposed. As such it can be continually used to re-evaluate the system to identify new potential vulnerabilities and threats as the system is decomposed.

Threat modeling consists 3 distinct steps:

1. Decompose the system
2. Identify and Rank Threats
3. Determine security measures

For further discussions and examples of threat modeling refer to Section 9 of this document.

8.1.3 Develop Security Requirements

Once a threat model of the system has been developed and its analysis completed (for the current system decomposition) the needed security measures for the identified threats are indicated. These security measures can then be refined into security requirements appropriate for the level of the system. Using this process, security requirements should be tagged in some manner to make them easily identifiable during the verification phase.

8.2 Detailed Design

During the detailed design phase, the system-level architecture and requirements are decomposed into the system components. Likewise the threat models, functions, and requirements of the system should be decomposed.

8.2.1 Perform Security Risk Assessment

For each additional decomposition of the system into lower-level design and requirements the threat model should also be decomposed and assessed until a determination has been made that the threats to the system have been mitigated to an acceptable level.

8.2.2 Decompose Security Requirements

With the decomposition of the threat model the system designer is provided a deeper understanding of the systems threats and its component parts. Likewise a view of lower-level threats and attack paths through the system are demonstrated. This will enable the system designer to define lower-level security requirements indicated by the lower-level mitigations.

8.3 Implementation

Because the goal of developing secure systems is to create systems which will hold up to intelligent adversaries it should be considered that simple verification of security requirements may not be

adequate. Cyber-resilient systems should be tested through a variety of means, including: verification of security requirements, and vulnerability testing such as application fuzzing and creative penetration testing.

8.3.1 Review of Input Handling and Validation

It's a good rule of thumb in software development that all untrusted input should be validated. This concept is demonstrated throughout this process beginning with the initial environment definition where the trust level of the interfaces and actors were determined. The threat model developed as part of the security risk assessment shows the data flow from untrusted interfaces into the system. Ultimately until input data has been properly vetted against rules which bound its characteristics (such as length, type, or frequency) the processes and functions which consume the data are considered at risk. For this reason it's important to verify input validation on all untrusted data flows into the system. This should be done as part of a code review process to ensure untrusted data is treated properly within the software design. Application fuzzing may also be designed to exercise input validation.

8.3.2 COTS Analysis

As more airborne systems begin to communicate with broader networks using standard protocols they are employing more commercial software components. This effectively equates to a software supply chain. As with other supply chains it is susceptible to defects. Software supply chain defects are measured in lines of code, not parts per million. So if a software defect exists, it exists in every deployment, not just a percent. . For this reason its recommended OEMs and suppliers monitor published vulnerability databases for defects in the versions of COTS software which they utilize in their products. From this, an analysis can be conducted of the COTS components. Identified vulnerable versions should be assessed within the system context to determine if the vulnerability poses a risk to the system. If a risk is identified then the effected package should be mitigated through patches and upgrades (if available), or the design modified to address the issue.

8.3.3 Code Analysis

Static and Dynamic code analysis tools are considered a common best practice in today's software development process and should be integrated with the software build process to reduce the occurrence of defects in custom code which could result in unexpected system vulnerabilities.

8.4 Verification

Because the goal of developing secure systems is to create systems which will hold up to intelligent adversaries it should be considered that simple verification of security requirements may not be adequate. Cyber-resilient systems should be tested through a variety of means, including: verification of security requirements, application fuzzing, and creative penetration testing.

8.4.1 Functional Security Testing

Once security requirements have been defined for a system many of them can be verified as other functional requirements through inspection, test, demonstration, or analysis. But some requirements,

specifically those which surround validation of untrusted data should consider employing application fuzzing (especially if the data format is expansive and all possible mis-use cases cannot be completely described). These tests are already required by DO-178 and DO-254.

8.4.2 Application Fuzzing

It's common when testing input validation functions in software to test: many successful or positive scenarios, several data point at or adjacent to the boundary, and finally few out of bounds scenarios to complete the coverage. In today's world this often does not prove to be adequate. Often buffer overflows don't occur until large volumes of data are passed, or perhaps there's a particular corner case which creates a particularly bad failure. Application fuzzing (sometimes referred to as robustness testing) seeks to identify more failure cases by using protocol-aware test software which sends high rates of invalid test cases to identify areas or unexpected behaviors in software systems. It's not uncommon for application fuzzing to execute 200,000 or 1,000,000 iterations against a software function over a period of days. Development teams which utilize this type of testing commonly discover bugs which wouldn't have otherwise been found. In the case of security testing it's more important to conduct this testing against applications which receive data which crosses a trust boundary. For more information on this test approach see: https://www.owasp.org/index.php/Fuzzing.

8.4.3 Penetration Testing

The purpose of penetration testing is to expose weaknesses in a systems design or implementation during the development process to reduce the probability of the system being compromised while in operation. This form of testing typically takes a more free-form approach to address the system being tested. By free form it's meant that a strict scope is not typically adhered to (although it's common to define a minimum scope). This enables the tester to change the testing or scope as they see fit. This approach more closely models how a hacker would seek to compromise a system, allowing the tester the flexibility to think differently about accessing the system and to be more creative in their applied methodology. There are tools that provide vulnerability and penetration test automation that may be used to help perform these tests (e.g. Kali Linux).

8.4.4 Security Risk Assessment

With the conclusion of the verification activity a final security risk assessment should be conducted of the system to ensure all the threats identified during the development of the program have been mitigated to an acceptable degree. Any security requirements associated with failed tests should be evaluated for impact to the system as should any vulnerabilities identified during the COTS analysis activity.

Once the system threats have been identified they should be ranked or evaluated in a meaningful way in order to enable system developers or evaluators to prioritize the issues and select the appropriate action. There are many approaches to this problem each with strengths and weaknesses (DO-356 offers a qualitative approach expressed in terms of "likelihood" of occurrence). But they all tend to have a few items in common, a concept of time which expresses the expected frequency of occurrence, and a

measure of impact to the system. For instance in financial risk management the following equation is used:

ARO x SLE = ALE

- ARO – Annual Rate of Occurance
- SLE – Single Loss Expectancy
- ALE – Annualize Loss Expectancy

Using this method multiple risks can be evaluated against each other and prioritized based on the ALE value. This approach works well for risks which can be monetized, but it doesn't necessarily translate well to safety systems such as in the case of avionics.

The important thing to understand in developing (or adopting) a methodology for ranking threats is that it should be meaningful to the system under evaluation. One method of threat evaluation historically used with threat modeling is DREAD.

- **D**amage – what's the impact of the attack?
- **R**eproducibility – how easy is it to reproduce?
- **E**xploitability – how hard is it to execute?
- **A**ffected users – how many people will be impacted?
- **D**iscoverability – how easy is it to discover the threat?

As mentioned previously we see the concepts frequency of occurrence being captured in the Reproducibility, Exploitability, and Discoverability measures while impact is captured in the Damage and Affected users measures. Using these characteristics various scales can be assigned and values applied. Once this is done an equation can be used to calculate a value for each threat.

8.5 Operational Security Support

In the operational support phase of the program there remains a few activities which should be conducted to ensure continued secure operation of the equipment.

8.5.1 Operational Guidance

As with other functional components of the system, the system designer should provide the owner operator or system integrator with information and procedures pertinent to maintaining the operational security of the system. This would include (but not be limited to) procedures for modifying security parameters (such as passwords and certificates), disposal procedures (if needed to remove confidential material), or documentation about unsafe configurations which should be avoided due to unnecessary risk. Typically this content is developed earlier in the program when other support materials are generated. It is included in this section primarily to clarify its relevance.

8.5.2 Continued Vulnerability Assessment

Once a system has been fielded and in use, its possible new vulnerabilities may be discovered which are relevant to the system. The source of this information could be from security researchers, customer penetration testing, or public disclosure through CVEs (Common Vulnerabilities and Exposures) such as from the National Vulnerability Database (NVD)[45]. Newly discovered vulnerabilities should be reviewed in the context of the system for potential impact and a determination made as to where an update is required to resolve the issue.

[45] https://nvd.nist.gov

9.0 RISK ASSESSMENT USING THREAT MODELING

In system security, threat modeling is a process for optimizing network and computing security by identifying objectives and vulnerabilities and then defining security measures to prevent, or mitigate the effects of threats to the system. While this process is new in the development of aircraft systems it is commonly used in the development of networked systems for other industries. This section summarizes how to develop a threat model and how it can be used to ensure the system in development is resilient to cyber-attacks in operation. At a high level the process is described by the following steps:

1. Decompose the system
2. Identify and Rank Threats
3. Determine security measures

In a formal definition of threat modeling *decomposing the system* is the process of: identifying assets, interfaces, actors, and trust levels; defining connectivity and information flow within the system. For our purposes the assets, interfaces, actors, and trust levels were defined as part of the security environment definition so the work left to do is to integrate this information into a model. For this we'll use an information flow diagram common to threat modeling known as a data flow diagram (DFD).

Identifying and ranking threats is an analysis of the resulting model from the previous step in which threats revealed in the model are documented and assessed for potential impact and system effect.

Determining security and mitigations is the process of identifying the type of security measures appropriate to mitigate the threat. This step is a natural precursor to the development of security requirements to support the implementation of security functions.

When the risk assessment activity is complete all the threats to the system should be identified, their individual risk to the system evaluated and appropriate security measures identified. It's important to remember in developing networked systems that threats can also be propagated (or passed through) a system which is under evaluation. This is important to capture in a threat model so it's clear to the system designer there's a potential impact to an upstream system. Once identified, the threat can be communicated to the designer of the upstream system and the threat properly mitigated at the target. An example of this can be seen in the case of the EFB threat to the MFD in the below example. If the wireless gateway were an individual system under evaluation this threat (if unmitigated at the wireless gateway) would be passed through to the MFD where it would then have to be addressed.

9.1 Data Flow Diagrams (DFD)

DFDs get their foundation in software design but their simplicity and ease of use have resulted in expanded utilization for other types of systems from human to electronic systems. For threat modeling the DFD method is often preferred for its advantages in, depicting the relationship between system components and information flows, and support for visual review. The DFD uses simple common shapes to depict typical system elements as shown in Figure 4.

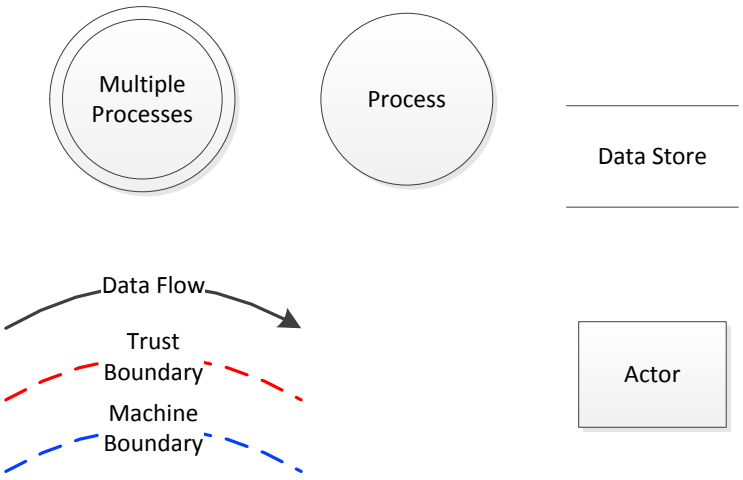


Figure 4 – Data Flow Diagram Nomenclature

DFDs are also hierarchical in structure so they can be used to depict both a high level system as well as a decomposed view of the system. Often times the top-level system view will provide a system context depicting all the external actors while decomposed views of the system will focus primarily on a specific function.

9.2 Sample System

Figure 5 below shows a simple aircraft system block diagram which depicts a multi-function display connected to a wireless gateway to enable interaction with a tablet device which might be carried by the pilot. (Note: this example system is not meant to represent a complete system and all its functions but instead explore the Threat Modeling process). In this block diagram it can be seen that the MFD supports database upload from a USB stick and the Wireless Gateway supports bidirectional communication with the EFB. The two lines between the MFD and the Wireless Gateway indicate that in some configurations for this system the Wireless Gateway only has receive functionality from the MFD while in others it also supports write capability. Both the EFB and USB drives are uncontrolled devices which means they should not be trusted and likewise their communication with the system considered untrusted. The MFD and the functions it hosts are considered an asset with requirements for availability and integrity while the wireless gateway is functionality the aircraft can operate without.

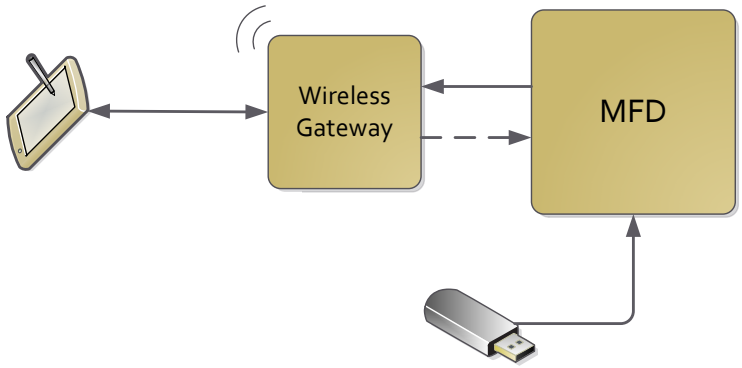


Figure 5 – Example Part 23 System

Based on this information the assets of this system can be tabulated fairly easily as below.

Table 1: Asset Table

Asset ID	Name	A,I,C	Description
1	MFD	A, I	The MFD is used for primary instrumentation and considered critical to aircraft operation.

9.2.1 ARINC 429 RX Only – Example 1

Figure 6 below shows the ARINC 429 receive version of the system depicted in two DFD diagrams. One diagram is a physical view of the system and the other is a logical view. This is done to ensure the complete system is considered with all relevant threats. The diagram shows the MFD and wireless gateway as a set of functions, the two external actors of the system and the directional data flows between them. Because the two actors identified for the system are untrusted a trust boundary has been drawn between the actors and the system. The trust boundary also extends between the MFD and

the wireless gateway to depict that the wireless gateway is not considered trusted by the MFD. But because there is no data flow from this device into the MFD there isn't a threat to be considered.

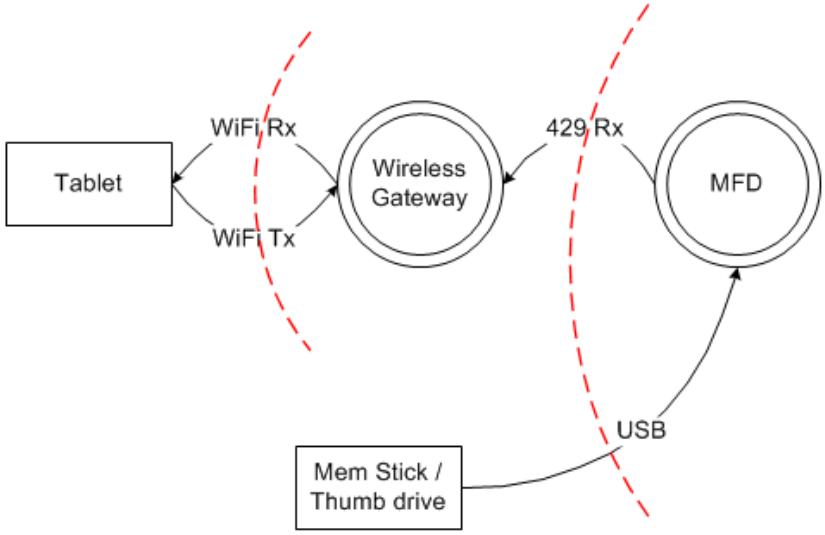


Figure 6 – Physical RX Only Threat Model

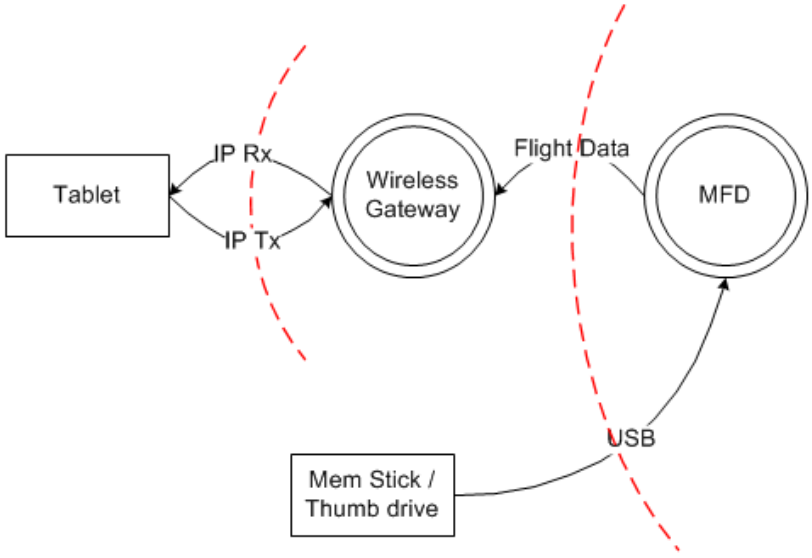


Figure 7 - Logical Rx Only Threat Model

Based on these two diagrams we can quickly see that there's only one information flow into the system's defined asset originating from the USB drive to the MFD. This is then defined as a threat within the system.

Table 2 - Threat Definition

Threat ID	*Source*	*Asset*	*A,I,C Property*	*Description*
1	USB	MFD	A, I	An USB drive hosting malicious software is inserted into the USB port of the MFD.

Based on this threat counter measures are indicated for the USB subsystem and driver. Requirements should be developed for these components to mitigate the associated threats. To completely manage the threat the system needs to be decomposed further into the MFD subsystems and functions to have clarity on what software components are potentially affected and how to best mitigate the threat.

9.2.2 Bi-Directional Communication – Example 2

Figure 8 below shows the bidirectional version of the system depicted in two DFD diagrams. The diagram shows the MFD and wireless gateway as a set of functions, the two external actors of the system and the directional data flows between them. Because the two actors identified for the system are untrusted a trust boundary has been drawn between the actors and the system. The trust boundary also extends between the MFD and the wireless gateway to depict that the wireless gateway is not considered trusted by the MFD. In this second case a threat is indicated from the wireless gateway to the MFD based on the flight plan data transmitted from the wireless gateway to the MFD.

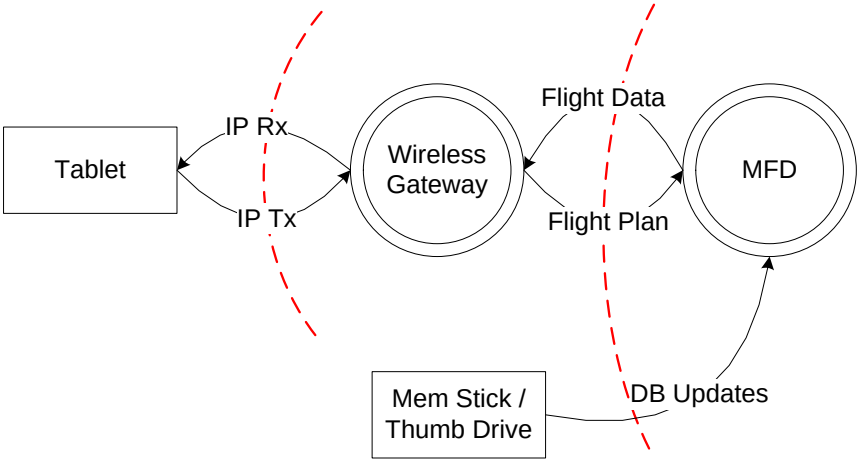


Figure 8– Logical Bi-Directional Threat Model

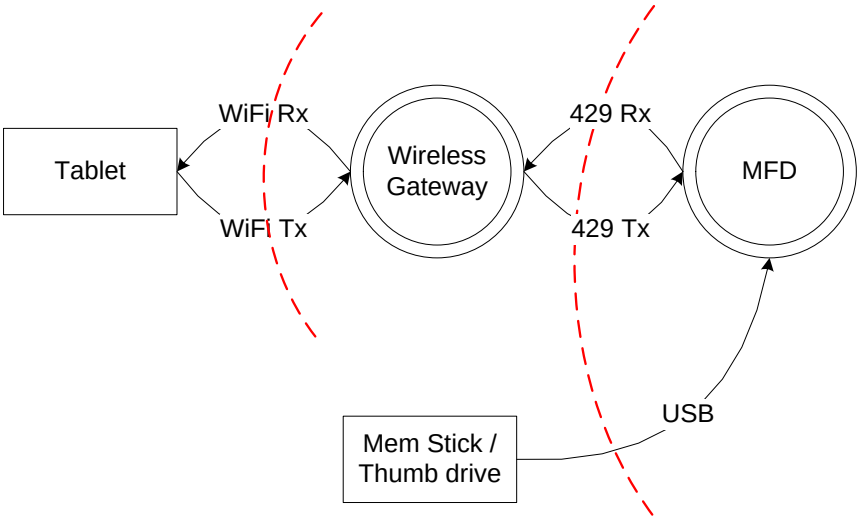


Figure 9 – Physical Bi-Directional Threat Model

Based on these two diagrams we can quickly see that there's two information flows into the system's defined asset originating from the USB and the EFB. These are then defined as threats within the system.

Table 3 - Threat Definition

Threat ID	*Source*	*Asset*	*A,I,C Property*	*Description*
1	USB	MFD	A, I	An USB drive hosting malicious software is inserted into the USB port of the MFD.
2	EFB	MFD	A, I	A malicious user attempts to compromise the MFD through sending malicious data through the wireless gateway or by compromising it and then sending malicious data to the MFD

Based on this threat counter measures are indicated for the USB subsystem as well as the 429 receive and flight plan processing components of the MFD. Note the threat passes through the wireless gateway component which is a part of the system. As such the threat could potentially be mitigated at this first outer layer in the attack sequence. These choices are in the hands of the system designer and will be reflected in the defined requirements. As before, to completely manage these threats the system should be decomposed further into the wireless gateway and MFD subsystems and functions to have clarity on what software components are potentially affected and how to best mitigate the threat.

10.0 MAINTENANCE, PROTECTION ASSURANCE, & MODIFICATIONS

The minimum maintenance required to support system security requirements should be identified in the Instructions for Continued Airworthiness (ICA) as required in 14 CFR 23.1529 and 27.1529. Appropriate maintenance procedures should be defined for these systems, interfaces, and devices to ensure in-service protection integrity. Reference FAA Order 8110.54A for ICA guidance.

System modifications should be assessed for the impact changes may have to the system security protections. The assessment should be based on analysis and follow existing ICA guidance. Reference Appendix B-1, System Security Change Impact Analysis (CIA).

APPENDICES

APPENDIX A – ASISP Process Objectives

References in these tables point to sections in this document that provides additional guidance and background.

Table includes guidance for:

- Objective description and references to the location(s) in this document that provides guidance to address this objective.
- System criticality Catastrophic (CAT), Hazardous (HAZ), Major (MAJ), Minor (MIN) and No Safety Effect (NSE). Applicability of each objective shown by symbology provided in the legend.

LEGEND:	●	The objective to be satisfied
	○	The objective is optional
		Objective is not applicable or required
Appendix:	A-1	Planning
	A-2	Preliminary Assessment
	A-3	Threat Analysis
	A-4	Security Development
	A-5	Verification Testing
	A-6	Security Risk Assessment
	A-7	Compliance Summary - Documentation

Table A-1 Planning

Objective		Ref	Criticality					Comments
No.	Description		CAT	HAZ	MAJ	MIN	NSE	
1a	Security statement and assessment providing evidence that ASISP aspects of certification do not apply. Special Conditions or further compliance activity not required for security aspects.	5.1 5.2 7.2	●	●	●	●	●	Statement that covers the following: • Government or non-trusted service • Read Only • Minor or NSE • Excluded in the FAA Policy by Part or Subset
or								
1b	The regulatory requirements for security aspects are defined.	5.1 5.2 7.1 7.2 7.3	●	●	●	○	○	Applies when 1a is not applicable and ASISP to be covered in the project. Most cases applied by Policy and or Special Conditions, 2X.1301 and 2X.1309.
2	Overview of aircraft and/or system level architecture of selected systems to be covered by security.	7.2 8	●	●	●	○	○	If security threat modeling has been completed, this should be included in certification planning documents.
3	Identification of the certification basis applicable to security aspects	9.0	●	●	●	○	○	Identify in certification planning document(s) the regulations that will include coverage of security aspects: 2X.1301, 2X.1309, 23.1315 (Replaces 23.1309 at Amdt. 23-63)
4	Means of showing compliance to the certification basis related to security.	8.0 9.0	●	●	●	○	○	Recommended to use Security Tags for each security requirement to show tracing to each activity.
5	Aircraft security scope is identified. Includes the definition of the security environment and boundaries. *Note: This is not physical security of the aircraft.*	7.3 8.0	●	●	●	●	●	Define to the security trust boundaries and interactions of aircraft systems with entities outside of the trust boundary. Should cover all systems to show authorities that a complete assessment was performed.
6	Overview of security assessment process to be included in the project.	8.0	●	●	●	○	○	ASISP section in the certification plan or standalone Security documents to cover the Security Methods to be used for the project.
7	Initial development and change management of security artifacts agreed upon with certification authority.	X.X	●	●	●	○	○	Configuration management discussion on how artifacts will be maintained and revised.
8	Identification of the security and safety artifacts that will include security aspects.	9.0	○	○	○	○	○	Identify in the certification plan(s) which security, safety artifacts - if any, will include security aspects of certification.
9	Schedule of interactions with certification authority.	X.X	●	●	●	○	○	Schedule of project milestones typically provided in PSCPs. Include high level security activities.

Table A-2 Preliminary Assessment

Objective	Ref	Criticality	Comments

No.	Description		CAT	HAZ	MAJ	MIN	NSE	
1	Security risk assessment is consistent with functional hazard assessment (AFHA, FHA, SFHA) or FMEA.	8.0 9.0	●	●	●	○	○	Failure condition criticality assignments align between the safety and security assessments.
2	Security environment and perimeter remain consistent with certification plan security scope definition.	7.X 8.0	●	●	●	○	○	Technology and interfaces to the system unchanged from the certification plans. Physical and Logical connections in the original architecture remain unchanged prior to security threat analysis.
3	Identification of threat conditions associated with aircraft and system assets identified.	7.X 8.0	●	●	●	○	○	Preliminary assessment of threat to the system considering interfaces outside of the trust boundary of the system.
4	Identify need for security measures from threat conditions and vulnerabilities preliminary assessments.	7.X 8.X 9.X	●	●	●	○	○	Vulnerabilities with system that support functions with criticalities Major and higher will require security threat analysis; threat modeling.
5	Preliminary assessment that security requirements are acceptable for aircraft and system development efforts.	8.0	●	●	●	○	○	Will the security efforts required to mitigate vulnerabilities to the aircraft and aircraft system be in scope with project expectations?
6	Preliminary system security assessment documentation addresses security risks to identified assets.	9.0	○	○	○	○	○	Documentation includes security preliminary assessment tasks, and results of preliminary assessments.

Table A-3 Threat Analysis

Objective		Ref	Criticality					Comments
No.	Description		CAT	HAZ	MAJ	MIN	NSE	
1	Assets defined.	8.X	●	●	●	●	●	Assets that require protection and what properties of these assets are important. Should include MIN and NSE assets to prevent propagation.
2	Security boundary diagrams complete.	8.X	●	●	●	●	●	Trust boundaries depicted where data sources cross from trusted to untrusted. Diagrams should include MIN and NSE assets to prevent propagation.
3	Data flows identified and complete.	8.X	●	●	●	●	●	Data flow diagrams are complete and accurate with system design and architecture. Diagrams should include MIN and NSE assets to prevent propagation.
4	Properties of the asset identified by Availability, Integrity, and Confidentiality.	8.X	●	●	●	○	○	Assets that have data flow entering assets after crossing a trust boundary.
5	Preliminary System Safety Assessment documentation addresses security risks to identified assets.	9.0	○	○	○			PSSA documentation includes security preliminary assessment tasks, and results of preliminary assessments.

Table A-4 Security Development

Objective		Ref	Criticality					Comments
No.	Description		CAT	HAZ	MAJ	MIN	NSE	
1	Security mitigations to system requirements.	7.X 8.0	●	●	●	○		Mitigations documented in system requirements documentation. Other identified mitigations not implemented should be documented for reason not implemented.
2	Security related system requirements to high-level software requirements.	7.X 8.0	●	●	●	○		RTCA/DO-178 Processes
3	Security related system requirements to high-level hardware requirements.	7.X 8.0	●	●	●	○		RTCA/DO-178 Processes
4	High-level software requirements to low-level requirements.	7.X 8.0	●	●	●	○		RTCA/DO-254 Processes
5	High-level hardware requirements to low-level requirements.	7.X 8.0	●	●	●	○		RTCA/DO-254 Processes
6	Security Tags applied to security requirements to support traceability.	7.X 8.0	○	○	○	○		Use of tags to identify requirements in the system that have security attributes is highly recommended to help in tracing of requirements and actions taken.
7	Preliminary System Safety Assessment documentation addresses security risks to identified assets.	9.0	○	○	○	○		PSSA documentation includes security preliminary assessment tasks, and results of preliminary assessments.

Table A-5 Verification Testing

Objective		Ref	Criticality					Comments
No.	Description		CAT	HAZ	MAJ	MIN	NSE	
1	Security Requirements Test Plans	8.X 9.X	●	●	●	○		Tests plans to test security requirements created to verify security measures functionality – for intended function.
2	Security Robustness Test Plan	8.X 9.X	●	●	●	○		Test plans to test security requirements. Beyond function as intended, this is to verify abnormal inputs and conditions.
3	Security Requirements Test Report	8.X 9.X	●	●	●	○		Tests report.
4	Security Robustness Test Report	8.X 9.X	●	●	●	○		Test report.
5	Vulnerability testing	X.X	●	●	○	○	○	Specific testing activity related to security. Aggressive testing to attempt to break, bypass or tamper with the system being verified.

Table A-6 Security Risk Assessment

Objective		Ref	Criticality					Comments
No.	Description		CAT	HAZ	MAJ	MIN	NSE	
1	Security assessment of assets.	8.0	●	●	●			Currently only addresses measure and mitigations and does not address Effectiveness and Assurance.
2	Criticality of assets consistent with Functional Hazard Assessment.	8.0	●	●	●			Currently only addresses measure and mitigations and does not address Effectiveness and Assurance.
3	Assessment addresses system Availability, Integrity, and Confidentiality.	8.0	●	●	●			
4	Assessment of security threats identified considering system criticality.	8.0	●	●	●			Currently only addresses measure and mitigations and does not address Effectiveness and Assurance.
5	Aircraft security acceptable.	8.0	●	●	●			Currently only addresses measure and mitigations and does not address Effectiveness and Assurance.
6	Systems security acceptable.	8.0	●	●	●			Currently only addresses measure and mitigations and does not address Effectiveness and Assurance.
7	System Safety Assessment documentation summarizes security tasks, substantiating data, test results, qualitative analysis.	9.0	○	○	○	○		SSA documentation covers security tasks under qualitative analysis.

Table A-7 Compliance Summary - Documentation

Objective		Ref	Criticality					Comments
No.	Description		CAT	HAZ	MAJ	MIN	NSE	
1	Security artifacts released and approved per the certification plan(s).	X.X	●	●	●	○		Documents may be delegated for approval, submitted as recommend approve, or available on request.
2	Security summary is complete with respect to the certification plan(s).	X.X	●	●	●	○		Provide evidence that security aspects have been completed per certification plan(s)
3	Regulatory compliance shown where applicable and in accordance with certification plan(s).	X.X	●	●	●	○		Compliance to applicable regulatory requirements has been shown in released and approved artifacts to support finding of compliance.
4	Security verification tasks traced to test results and/or analysis activities.	X.X	●	●	●	○		Tracing of each security requirement should provide tracing to substantiating data and results reports.
5	Deviations to certification plan(s) related to security aspects accepted by the certification authority.	X.X	●	●	●	○		Deviations to the certification plans should be coordinated throughout the project and evidence of agreement to requested deviation should be provided in final certification package.
6	ICA coverage accepted by certification authority.	X.X	●	●	●	○		Requires FAA-AEG acceptance. Covers 2X.1529, reference FAA Order 8110.54A. Recommend that security aspects to be added to the ICA checklists provided in the order.
7	Aircraft and system installation guidance updated to include security requirements.	X.X	●	●	●	○		Where applicable updates to aircraft operating procedures, system installation instructions, maintenance procedures and return to service instructions address security requirements.

APPENDIX B – ASISP System Security Topics

B-1 System Security Change Impact Analysis (CIA)

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.

What is the scope of a system security risk assessment?

The system security risk assessment may be relatively simple or complex depending on the aircraft architecture and intended function of the e-enabled service. As an example, risk assessment of portable electronic devices that have read access only to aircraft systems are less complicated than devices that have read-write access. Wireless aircraft sensors and sensor networks should require a system security risk assessment when they are receiving data from a non-trusted service to ensure that the data is not intercepted or corrupted.

As an example, threat evaluation of portable electronic devices 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 from the threat of unauthorized interaction 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 the threat of unauthorized interaction should have system level, not aircraft level, Security Risk Assessment. In determining the aircraft security scope with a unidirectional bus, only those systems receiving data from non-trusted services would be considered part of the security perimeter. System Security Risk Assessment should show that threats are mitigated by the system(s) to which the threat of unauthorized interaction 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 bus.

When the threat of unauthorized interaction is connected to bi-directional data busses (e.g., 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.

The necessary documentation is strongly affected by the proposed modification, such as whether it connects to a federated system or a highly interconnected aircraft network. Since the Design Approval Holder (DAH) holds all the system interface documentation, interconnected modifications may need data from the DAH. In cases where the applicant cannot obtain sufficient data from either the DAH or publicly available sources to show compliance, the proposed modification might not be possible. In cases where the applicant cannot obtain the necessary data, the applicant can propose an alternate method for compliance.

Data Submittals for Aircraft System Modifications

The Change Impact Analysis will determine if a Security Risk Assessment is necessary. If necessary, data submittals to the regulatory authorities should be documented in the Certification Plan. Packaging of the information is at the discretion of the applicant provided all of the required data is submitted. These activities may be packaged and addressed within the plan for security aspects of certification or distributed into others system, hardware or software documents. The documentation effort can vary greatly from a small task to an extensive effort based on the complexity of the planned modification and the change impact. Simple modifications should require reduced documentation submittals.

System Security Change Impact Analysis – Example Template

Security Change Impact Analysis	*YES/NO*	*Detail Description*	*THREAT SEVERITY*
① *Does certification effort/activity add and/or modify (i.e., WiFi, IR, Bluetooth, etc.) wireless capability?*			
② *Are there any connectivity access point(s) added and/or changed due to this certification effort/activity, (i.e., LAN/WAN accessibility, diagnostics/maintenance port, removable media (non-WiFi or WiFi-enabled), etc.) to Aircraft Systems?*			
③ *Is Field-Loadable Software/Airborne Electronic Hardware (FLS) functionality being added and/or changed due to this certification effort/activity?*			
④ *Are Aeronautical and/or Airborne System Databases uploading being impacted by this by this certification effort/activity?*			
⑤ *Has connectivity to Non-trusted Services to UNI-directional and/or BI-directional Aircraft Networks (Wired/Wireless) been impacted by this certification effort/activity?*			
⑥ *Are COTS parts being utilized in Aircraft Networks and Systems in this certification effort/activity?*			
		NOTE: Any 'YES' response to the questioning above (i.e, items ①-⑥) need to be assessed for its security functional hazard impact; if the classification of the security vulnerability is a "MAJOR or higher" HAZARD from this determination, further analysis and coordination with the ACO is necessary; proceed into the aircraft level and/or system level security risk assessment activities.	

NOTE: THREAT SEVERITY is part of the Airworthiness Security Process, RTCA/SC-216 special committee established in RTCA/DO-326A, section 2.1, "Process Overview"; the process is designed to apply the same model as the safety process in that it allows for the adaptation of the effort needed to establish adequate security as a function of both severity of failure/threat condition effects and the level of threat of the threat scenarios to which the aircraft is exposed.

B-2 Connecting Removable Media to Aircraft Systems Mitigation Techniques

Interface Function Management

For system designers using interfaces (such as USB) it's recommended that the drivers used to support the device limit supported devices to only what is required for the intended function. For example USB interfaces support memory, input (keyboard & mouse), and network devices (bluetooth / Wi-Fi dongle). In the case of an avionics system it's uncommon for these ports to be used for input or network connectivity so it's recommended that the supporting driver for the interface only support memory devices to not provide unintended access to the system.

Media Control Measures

For operators / maintainers the following practices are recommended:

1. In the case of USB memory devices only use FIPS 140-2 Level 3 certified USB devices for interaction with avionics systems as these devices do not allow the firmware of the USB device to be field updated.
2. Purchase a set of memory devices which will be dedicated to the purpose of updating the aircraft. If any of them are used for another purpose, remove them from the pool.
3. Laptops and computers used to read from and write to removable memory devices should be managed consistent with best practices for safe computing. This includes but isn't limited to requiring authentication, regular patching and updating, running antivirus and firewall software. Additionally it's recommended a computer used for this purpose should never be connected to untrusted networks (such as a coffee shop or restaurant).
4. When field loadable software (FLS) and DB update files are downloaded the source of these files should be verified.
5. After download, the file(s) should be verified using a hash comparison against the one provided by the distributor or using a digital signature.
6. All files should be scanned with antivirus software before copying them to the USB drive to be deployed to the avionics system.

B-3 Connectivity Mitigation Techniques

The applicant should consider the integrity and robustness of configuration control measures on the device or service to which the proposed connection is made. Such consideration should additionally consider industry standards and specifications, such as Operational Approval or ARINC standards that address security measures. Such security measures can be described and verified/validated in order to demonstrate some level of threat mitigation outside of the airplane systems. Modifications that include connectivity with devices/services with no such security specifications or standards, such as the Internet, should be considered a larger threat of unauthorized interaction than devices/services that do have security standards/specifications.

Installing New Aircraft Systems and Networks

Installing new aircraft systems and networks with connectivity to the threat of unauthorized interaction should include Security Risk Assessment. The interfaces with other networks and systems should be clearly defined during the Change Impact Analysis.

Replacing Aircraft Systems and Networks

Replacing aircraft systems and networks with connectivity to the threat of unauthorized interaction should include Security Risk Assessment. Examples of replacing systems and networks include parts obsolescence, supplier change, and replacing security measures with improved security measures. The interfaces with other networks and systems should be clearly defined during the Change Impact Analysis.

Modifying Existing Aircraft Systems and Networks

Modifying existing aircraft systems and networks with connectivity to the threat of unauthorized interaction should include Security Risk Assessment. The interfaces with other networks and systems should be clearly defined during the Change Impact Analysis.

Interconnectivities of New or Modified Aircraft Systems

The applicant should address the integration issues between their proposed modification and the connectivity to existing aircraft networks and systems. The applicant should consider the use of the guidance contained in this document during the modification process. The following provides additional clarification:

1. Aircraft System baseline.
2. New or modified System(s): includes new, modified, or removed Networks and Systems.
3. Internal / External the threat of Unauthorized Interaction including onboard uncontrolled PED
4. Define data flow from the existing aircraft systems to the new or modified system(s)
5. Define data flow from the new or modified system(s) to existing aircraft systems
6. Define data flow from internal / external Service or Devices to the new or modified system(s)
7. Define data flow from the new or modified System(s) to Internal or External Services or Devices

B-4 Certification Considerations for Certificates and Keys

In aviation, aircraft-level configuration management requirements typically lead to the fact that a wide variety of software revisions must be supported for a given set of hardware. Updating to the "latest" software may involve a significant expenditure of resources for the owner or owners of a given STC.

In security, one common security measure is to prevent "downgrading" the configuration (e.g. software, settings or other data) of an environment to an insecure state. This is at odds with the aircraft-level configuration management requirement, as hardware may be manufactured under one configuration and then field loaded to an older configuration in support of a given aircraft installation.

To make use of digitally signed deliverables, an up-to-date collection of certificates or keys is necessary. This ensures that any revoked certificates or keys are not used, as revocation is an essential element of a functioning digital signature process. Therefore, a particular, possibly out of date, set of certificates or keys should not be mandated by aircraft configuration control requirements.

Airworthiness authorities, equipment manufacturers and operators must recognize the unique nature of certificates and keys used for signing deliverables intended for the aircraft. Aircraft configuration information should specify the presence of any required certificates or keys, and may specify a minimum version identifier (if available) for compatibility purposes. Newer sets of certificates or keys must also be acceptable from a configuration control standpoint.

The necessary approach is philosophically similar to the treatment of aeronautical databases. The presence of a given database or set of databases may be necessary for a given system, and can be verified, but a particular database cycle is not necessary for the aircraft to be under configuration control.

APPENDIX C – Acronyms & Abbreviations

ADS-B	*Automatic Dependent Surveillance - Broadcast*
AEG	*Aircraft Evaluation Group*
AFHA	*Aircraft Functional Hazard Assessment*
ASISP	*Aircraft Systems and Information Security Protections*
ATC	*Air Traffic Control*
ATS	*Air Traffic Service*
CAT	*Catastrophic*
CIA	*Change Impact Analysis*
COTS	*Commercial Off the Shelf*
CPDLC	*Controller Pilot Data Link Communication*
CVE	*Common Vulnerabilities and Exposures*
DAH	*Design Approval Holder*
DAL	*Development Assurance Level*
DB	*Database*
DFD	*Data Flow Diagram*
EASA	*European Aviation Safety Agency*
EFB	*Electronic Flight Bag*
EUROCAE	*European Organization for Civil Aviation Equipment*
FAA	*Federal Aviation Administration*
FHA	*Functional Hazard Assessment*
FISMA	*Federal Information Security Management Act*
FLS	*Field Loadable Software*
FMEA	*Failure Modes and Effects Analysis*
GBAS	*Global Positioning Augmentation System*
GPS	*Global Positioning System*
HAZ	*Hazardous*
ICA	*Instructions for Continued Airworthiness*
MAJ	*Major*
MFD	*Multi-Function Display*
MIN	*Minor*
NSE	*No Safety Effect*
NVD	*National Vulnerability Database*
OEM	*Original Equipment Manufacturer*
PED	*Portable Electronic Device*

PKI	*Public Key Infrastructure*
PSCP	*Project Specific Certification Plan*
PSSA	*Preliminary System Safety Assessment*
RX	*Receive*
SBAS	*Satellite Based Augmentation System*
SFHA	*System Functional Hazard Assessment*
SSA	*System Safety Assessment*
STC	*Supplemental Type Certificate*
TC	*Type Certificate*
T-PEDS	*Transmitting Portable Electronic Devices*
TSO	*Technical Standard Order*
TX	*Transmit*
USB	*Universal Serial Bus*
WiFi	*Wireless Fidelity, IEEE 802.11( ) standard*

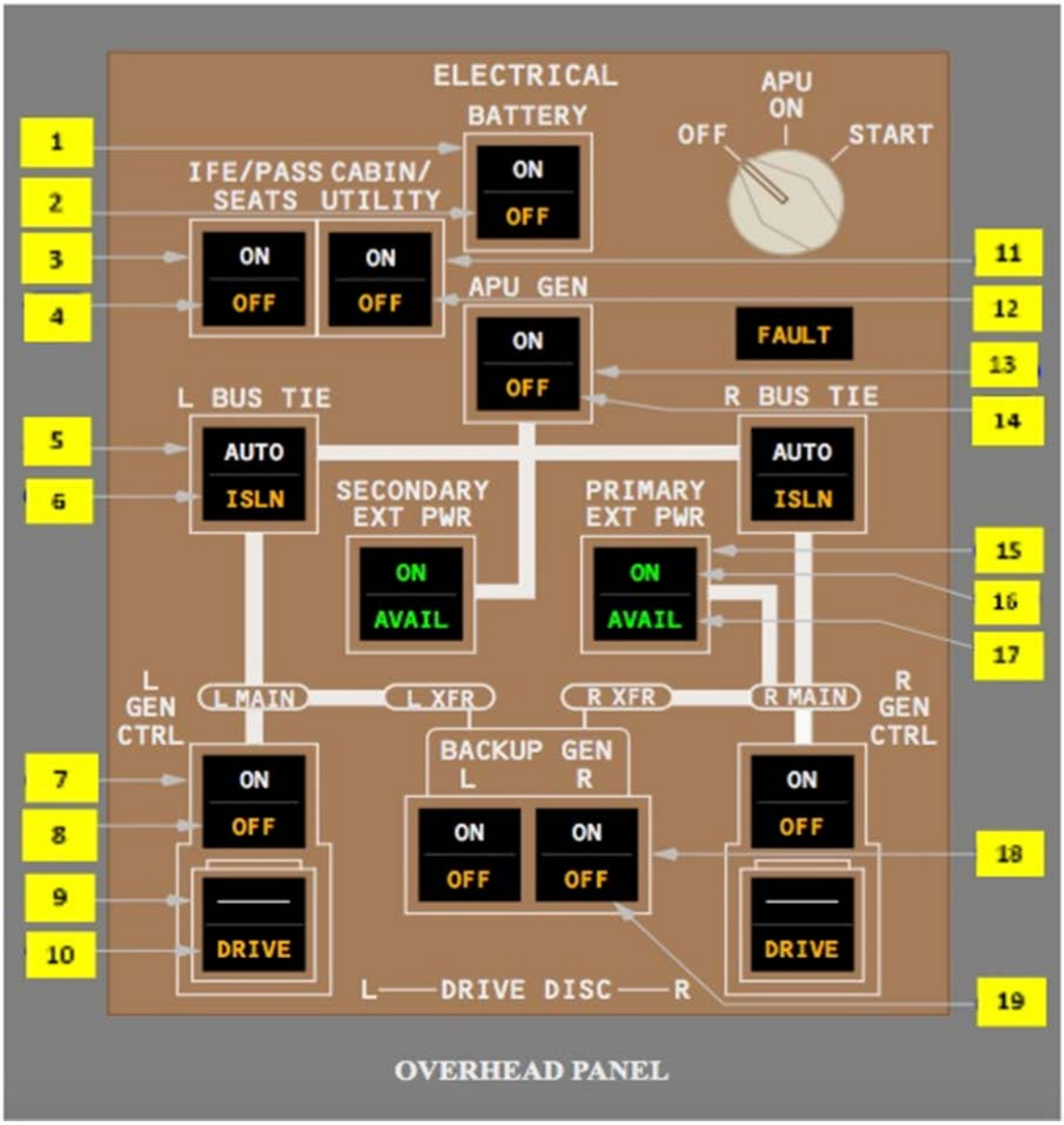
Appendix H – AC / AMJ 25.1309 Criteria "In a Nutshell" Figure

AC/AMJ 25.1309 Criteria "in a Nutshell"

Effects on aircraft and occupants of the identified failure condition.	FAR - AC 25.1309-1A definitions.	No significant degradation of aircraft capability. Crew actions well within their capabilities.	Reduction of the aircraft capability or of the crew ability to cope with adverse operating conditions.		Prevention of continued safe flight and landing of the airplane.
	AMJ of JAR 25.1309 definitions.	Slight reduction of safety margins, slight increase in workload, (e.g. routine changes in flight plan), or physical effects but no injury to occupants.	Significant reduction in safety margins, reduction in the ability of the flight crew to cope with adverse operating conditions impairing their efficiency, or injury to occupants.	Large reduction in safety margins, physical distress or workload such that the flight crew cannot be relied upon to perform their tasks accurately or completely, or serious injury to or death of a relatively small portion of the occupants.	Loss of the airplane and/or fatalities.
FAR effect category AC 25.1309-1A.		Minor	Major		Catastrophic
Effect category AMJ of JAR 25.1309 and Eurocae DO-178A version.		Minor	Major	Hazardous	Catastrophic
Criticality category RTCA DO-178A for system functions.		Non-essential	Essential		Critical
DO-178A Software Levels		Level 3	Level 2		Level 1
DO-178B Software Levels (Level E - No Effect)		Level D	Level C	Level B	Level A
FAR quantitative probability terms.		Probable	Improbable		Extremely Improbable
JAR quantitative probability terms.		Frequent / Reasonably Probable	Remote	Extremely Remote	Extremely Improbable
FAR and JAR quantitative probability ranges.		10-3	10-5	10-7	10-9
		Probability of Failure Condition (for one flight hour or flight if less than one hour).			
System Validation Method (Common cause hazards not conducive to numerical analysis, such as foreign object collision, human error, etc. may be analyzed primarily by Design Review.)		Design Review: Design, functional separation, and implementation reviewed to ensure failures will only produce Minor effect.	FMEA Review: Failure modes & effects analysis reviewed to ensure that failure effects of components involved in the function and failure rates are appropriate for Major category.	Fault Tree Anal.: FMEA & FHA data combined in detailed fault tree analysis to validate that the system probability of hazard is Extremely Remote.	Fault Tree Anal.: FMEA & FHA data combined in detailed fault tree analysis to validate that the system probability of hazard is Extremely Improbable
Effect Category Validation		Where functions are the same as previous airplanes, past experience should be reviewed. Other conditions should be evaluated in lab and simulation tests. Failures affecting handling qualities will be evaluated in piloted simulation and/or flight test.			Specific failures may be evaluated by piloted simulation as necessary.

Appendix I – In-Flight System / Passenger Seat (IFE/PASS SEATS) Power Switch Example

ON – powers IFE, passenger seat, ground maneuver camera, and flight deck entry video surveillance systems when AC power is available.
OFF – removes power from IFE, passenger seat, ground maneuver camera, and flight deck entry video surveillance systems.
IFE/PASS SEATS OFF Light
Illuminated (amber) – the IFE/PASS SEATS Power switch is OFF.



Appendix J – Copy of Final Draft Policy Statement

NOTE: This copy of the draft policy statement was developed by the ASISP Working Group and does not contain the results of the FAA's internal review. The revised policy statement is expected to be published by the FAA during fall 2016.

U.S. Department of Transportation
Federal Aviation Administration

Policy Statement

Subject: Establishment of Special Conditions for Aircraft Systems Information Security Protection

Date: March 15, 2016

Policy No: PS-AIR-21-Draft

Initiated By: AIR-130

Summary

This policy statement is intended to provide guidance to the Aircraft Certification Offices regarding the application of special conditions to address Aircraft Systems Information Security Protection (ASISP) vulnerabilities in aircraft certification programs.

Definition of Key Terms

In the text below the terms "must," "should," and "recommend" have a specific meaning that is explained in Appendix 1.

Current Regulatory and Advisory Material

Recent designs for aircraft systems have included connectivity to "non-governmental services" such as the internet, portable electronic devices, and commercial-off-the-shelf technologies that have not been certified and accredited for secure operations by a government authority. These designs can introduce ASISP vulnerabilities beyond the scope of current airworthiness regulations and traditional systems safety assessment methods typically used to show compliance with the airworthiness requirements located in Title 14 Code of Federal Regulations §§ 23.1301, 25.1301, 27.1301, 29.1301, 23.1309, 25.1309, 27.1309, 29.1309, 33.28, 35.15.

Policy

The Federal Aviation Administration (FAA) will issue special conditions for initial type certificate (TC), supplemental type certificate (STC), amended TC, or amended STC applications for aircraft systems that connect to non-trusted services (e.g., non-governmental) and networks if:

1. It cannot be shown by either a change impact analysis or by a safety and security risk assessment that no aircraft system with a failure effect classification of major or higher can be adversely affected, either directly or through propagation of security threats to or from any other system.

Non- governmental services that receive (read only such as ARINC 429) and do not transmit to aircraft systems do not require issuance of special conditions.

The following are examples of non- governmental services or networks connecting to aircraft systems:

- Airport gate link networks (e.g., Gatelink);
- Public Networks (e.g., Internet);
- Wireless aircraft sensors and sensor networks;
- Cellular networks;
- Portable Electronic Devices (PEDs) and/or portable Electronic Flight Bags (EFBs

This policy statement does not require the issuance of special conditions for airworthiness and operational approval of field loadable software (FLS), aeronautical data bases (ADBs), and the Aircraft Communications Addressing and Reporting System (ACARS). Other policies, standards, and guidance apply to FLS, aeronautical databases, and ACARS, such as FAA Order 8110.49 Software Approval Guidelines, AC 20-153B Acceptance of Aeronautical Data Processes and Associated Databases, ARINC 835 Guidance for Security of Loadable Software Parts Using Digital Signatures, ARINC 842 Guidance for Usage of Digital Certificates, and Spec 42 Aviation Industry Standards for Digital Information Security.

Special conditions are not required for FAR Part 23 Class “1”, “2” and “3” airplanes as defined in AC 23.1309-1E “System Safety Analysis and Assessment for Part 23” and FAR Part 27 Single Engine Rotorcraft.

[Industry support inclusion of Part 23 Class 4 as proposed by ACE-100. Industry is discussing single versus twin Part 27 and input pending from Rotorcraft Directorate, so TBD for now.]

Effect of Policy

The general policy stated in this document does not constitute a new regulation. Coordination is needed between the policy-issuing office and the responsible certification office for using a method of compliance outside of this established policy.

Please contact Mr. Steven C. Paasch, AIR-130, at (425) 227-2549 if you have any questions on the information contained in this policy memorandum.

Implementation

This policy statement applies to those programs with an application date that is on or after the effective date of the final policy statement. If the date of application precedes the effective date of the final policy statement, and the methods of compliance have already been coordinated with and approved by the FAA or its designee, the applicant may choose to either follow the previously acceptable methods of compliance or follow the guidance contained in this policy statement.

Conclusion

The FAA will consider revising the intent and content of this policy statement if other data are presented which are contrary to the guidance contained in this document.

SIGNATURE BLOCK

Appendix K – Reference Current Guidance and Regulations for PEDs

ARINC 664P5, "Aircraft Data Network Part 5, Network Domain Characteristics And Interconnection"

EASA-2014-EFB-Rules-Annex-II-AMC-20-25. "Airworthiness and Operational Consideration for Electronic Flight Bags"

FAA AC-119-1, "Airworthiness and Operational Approval of Aircraft Network Security Program (ANSP)"

FAA AC-120-76D, "Guidelines for the Certification, Airworthiness, and Operational Approval of Electronic Flight Bag Computing Devices"

FAA AC-20-168, " Certification Guidance for Installation of Non-Essential, Non-Required Aircraft Cabin Systems & Equipment (CS&E)"

FAA AC 20-173 , "Installation of Electronic Flight Bag Components"

FAA AC 91.21-1C, "Use of Portable Electronic Devices Aboard Aircraft"

RTCA DO-313, "Certification Guidance for Installation of Non-Essential, Non-Required Aircraft Cabin Systems and Equipment"

RTCA/EUROCAE DO-326A/ED-202A, "Airworthiness Security Process Specification"

Skaves, Peter, DASC30 8-15-2011_White Paper, "Information for cyber security issues related to aircraft systems"

FAA ANM-111 Issue Paper "Use of Portable Electronic Devices (PEDs) to Control Installed Airplane Systems"

Appendix L – Data Security

Data security requires a combination of technical controls and organizational procedures and policies. This section discusses data security practices in common use for protecting data transmission, and data processing systems.

Transmission of data via electronic/digital means (e.g., ftp sites, web downloads, or e-mail) may be subject to malicious attack that can corrupt the integrity of data for its intended use. Provision of means to mitigate the intentional corruption of digitally transmitted data may already exist within the organizational construct and operating procedures of participating entities. The section provides considerations, guidelines, and suggestions to address data security.

The objective of data security is to ensure that data is received from a known source, and that there is no intentional corruption during processing and exchange of data.

Provisions supporting this objective may include:

- Implementation of technical data security measures to provide authentication and prevent intentional corruption during exchange of data, e.g., secure hashes, secure transmissions, digital signatures.
- Implementation of organizational data security measures to protect processing resources and prevent intentional corruption during processing of data.

A-L.1 Security Threat Analysis for Field Loadable Data

A-L.1.1 Data Part Threat Conditions

We are concerned here for Safety Effect Caused by Security Events (SECSE). Note that this is a characterization of the effects on a data part of an attack, rather than any attributes of the attack itself.

TC.ERROR when the data part has data which is missing or wrong.

TC.CORRUPT intentional corruption when the data part has data which has been maliciously removed or modified. Note that in general for security threat conditions, a violation of integrity will be intentional corruption, in which standard protections such as checksums or CRCs will not detect the loss of integrity.

TC.LOSS when the data part is not available for the end-use.

TC.EXPOSE when the contents of the data part have been exposed to an unauthorized party.

However, there are several interesting sub-classes of T.CORRUPT, based on the actual effect of the end-use of the corrupted data part in the installed equipment:

TC. CORRUPT.DENIAL when there is loss of an intended function.

TC. CORRUPT.ERROR when there is partial loss or error in an intended function.

TC. CORRUPT.MISLEAD when there is error in an intended function which will be misleading to the flight crew if the flight crew does not detect the error.

TC. CORRUPT.HIJACK when the corrupted data part has introduced unintended function into the installed equipment. This is the case for corrupted software or firmware parts which include malicious

code, but is also the case for software security vulnerabilities which exploit operating system features, such as buffer overflow attacks which result in the execution of attacker code.

A-L.1.2 Data Part Attack Vectors By Phase

We will organize the directions of attack by phase. Each phase represents a different group of stakeholders, systems, and security policies, so this also helps organize the security controls.

The actual attack vectors and attack sources depend on the specific systems, policies, tools, and access control groups of the responsible organization, but we can present common examples.

AT.ERROR is the introduction of error or unintentional corruption into the data part.

AT.CORRUPT is the intentional introduction of corruption into the data part.

AT.CONTAMINATE is the addition of invalid data to an otherwise valid data part, e.g. through a virus.

AT.COUNTERFEIT is the introduction of a counterfeit part, an invalid data part with the appearance of a valid data part.

AT.CONFIGURATION is an attack which does not change the data parts themselves, but changes the configuration information which is used to determine which part is valid for a particular installation at a particular time.

AT.EXPOSURE is the transfer of knowledge of a data part to an unauthorized party.

TABLE A-L-4-1-2-1: DATA PART ATTACK VECTORS

Phase	Attack	Vectors	Attack Populations
Data Origin	Error Intentional Corruption Contamination Configuration Exposure	Tools Processing systems	Tool Support System Support Developers Unauthorized Public
Data Transmission and Storage	Error Intentional Corruption Contamination Counterfeit Exposure	Transmission systems Storage systems	System Support Maintenance Unauthorized Public
Data Loading	Error Intentional Corruption Configuration Exposure	Loading systems End system	System Support Maintenance Unauthorized Public
Data End-Use	Error Intentional Corruption Exposure	End systems	Crew Unauthorized Public

Data Part Disposal	Exposure	Loading systems End system	Maintenance Unauthorized Public

A-L.2 Technical Controls for Data Transmission

This section addresses technical security controls which can protect the integrity and confidentiality of data transmissions. Many of these controls are based on the use of cryptographic technologies such as hash functions, message authentication codes, symmetric and asymmetric encryption, and digital certificates,

A-L.2.1 Data Integrity and Message Authentication

Hash functions are generalizations of check sums in that they map arbitrary-length files into fixed length fields. Classic forms of aviation check sums such as CRCs are unsuitable for data security because they are easy to invert, so that an attacker can intentionally corrupt data so that the corrupted data still has a valid CRC.

Cryptographic hash functions are designed to be irreversible- i.e., it is computationally infeasible for an attacker who knows the hash of a file to create a corrupted file so as to match the hash of the original file. As a result, the hash of a file can be used to establish the integrity of the original file.
Good cryptographic hash functions are difficult to design, even more so when they become the target of "blackhat" security researchers seeking ways to compromise their protection. Examples include the once popular MD4 and MD5 hash functions. **Standard cryptographic hash functions** have been designed, vetted, and documented in standards such as NIST 800-57, "Recommendation for Key Management: Part 1: General (Revision 3)" and updated in NIST 800-131A, "Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths". Examples include e.g., Secure Hash Algorithm 256 (SHA256) and related hash functions.

Keyed-Hash Message Authentication Codes (HMAC) use a standard cryptographic hash function and a shared secret key to compute a Message Authentication Code (MAC), which is appended to and transmitted with the file being protected. The recipient computes a MAC on the received file using the same shared secret key and hash function. If the computed and received MAC values are equal, then the file has been received correctly (data integrity) from a verified source (message authentication). NIST FIPS 198-1 describes a keyed-HMAC algorithm.

A-L.2.2 Data Confidentiality

Encryption algorithms provide the most basic means for protecting the confidentiality of a file from unauthorized disclosure. It is difficult to design an effective encryption algorithm because full validation that it is secure from attack generally requires the resources and expertise of a national security organization such as the NSA. However, there are effective encryption standards that have undergone such validation and are defined in industrial standards and available in standard implementations.

Symmetric-key encryption uses efficient encryption methods and relies on a shared secret key for both encryption and decryption. The entities that share the key must protect the privacy of the key. As with hash functions, good encryption algorithms are carefully designed and vetted and are the continual targets of attackers. See NIST 800-57 for recommended algorithms, e.g., Advanced Encryption Standard (AES).

Public-key (or asymmetric-key) cryptography employs complex mathematical problems (e.g., discrete logarithm, elliptic curve) and different keys for encryption and decryption. The result is that it is possible to release a decryption key, the public key, while keeping the encryption key, the private key, confidential. As a result, anyone with the public key who successfully decrypts a message can be assured that the file is from the owner of the private key- provided that there is assurance that the private key was kept private, and assurance that the public key really corresponds to the private key and to the entity to which the public key is associated. The management of these assurances leads to the requirements for Public Key Infrastructure (PKI). Unfortunately, not only are public key algorithms also subject to the same continual attacks as hash functions and other encryption algorithms, they are also usually much more computation-intensive.

Mixed Encryption Protocols. Most modern encryption protocols use a mix of asymmetric and symmetric methods. In order to have efficient secure communication for large messages, security protocols use public key cryptography to exchange authentication information and to generate unique secret keys which are then used with more efficient symmetric-key encryption algorithms to protect the data. Of course, secure protocols themselves are subject to attacks and need to be vetted and researched. Examples of modern mixed protocols that have been vetted for good security properties include e.g., Hypertext Transfer Protocol Secure (HTTPS), Transport Layer Security (TLS), Internet Protocol Security (IPSEC), and Wi-Fi Protected Access 2 (WPA2) (for wireless).

A-L.2.3 Digital Certificates

Digital certificates are a means to package and manage a public key, the identity of the entity to which the public key is associated, the operational period of the public key, and other certificate management information. Digital Certificates can be obtained as part of the information security services which are available from a commercial Certificate Authority (CA), not to be confused with the certification authorities that regulate aeronautical information. A trusted CA takes responsibility for verifying the identity information embedded in the certificate, digitally signing the public key certificate, and issuing the certificate for use. If the entity using a certificate also trusts the CA and the certificate's digital signature is valid, then the entity relying on the certificate can trust that the public key is associated with the identity claimed in the certificate.

There are different levels of Certificate Polices which correspond to the degree of identity assurance for the digital certificate. ATA Spec 42, "Aviation Industry Standards for Digital Information Security," specifies a digital identity management framework and digital certificate profiles recommended for use across the air transport industry, as well as standard policies governing the issuance and use of these certificates and the levels of assurance that may be conveyed in a digital identity. ARINC 842-1, "Guidance for Usage of Digital Certificates," serves as a companion to ATA Spec 42 and provides additional guidance for the use of digital certificates in an aircraft environment. The resulting structure of certificates, certificate distribution, certification policies, and the associated assurances is referred to as the Public Key Infrastructure (PKI).

A-L.3 Protecting Data, Tools, and Resources within the Organization

This section discusses organizational security controls in common use to protect the integrity and confidentiality of data processing resources and systems. Many of these controls are based on the management of information security under a data security program.

A-L.3.1 Information Security Management

It is a significantly complex problem to protect data along with the tools and applications used to create, modify, and package the data, and the computational and network resources that support the applications and data. The total process is known as **Information Security Management**. See ISO 27002, "Information technology - Security techniques - Code of practice for information security management" or NIST 800-39, "Managing Information Security Risk: Organization, Mission, and Information System View", for further information.

A-L.3.2 Organizational Controls

The following broad classification of organizational security measures is provided for informational purposes and is based on the PCI_DSS, "Payment Card Industry Data Security Standard" of the payment card industry. Catalogs of controls include e.g., ISO 27005, "Information technology - Security techniques - Information security risk management", and NIST 800-53, "Security and Privacy Controls for Federal Information Systems and Organizations". See those references for further information.

1. Network configuration

   Routers, firewalls, and other network domain control mechanism are configured to partition sensitive data, tools, and resources from unauthorized access, untrusted networks, and untrusted resources.

2. Manage defaults

   Change, remove, or control vendor-supplied default passwords, configurations, accounts, and services, especially those provided for administration and maintenance.

3. Protect data

   Protect confidentially-sensitive data (e.g. digital certificates, private keys, and confidential data) from exposure and intentional corruption, and setup data review policies to minimize the amount of retained sensitive data.

4. Protect transmissions

   Encrypt transmission of data across untrusted networks or mediums (e.g. open, public networks, wireless protocols).

5. Anti-malware

   Deploy anti-malware services to protect tools and resources.

6. Vulnerability management

   Monitor tools and resources for exposure to publicly known vulnerabilities, and implement configuration control to reduce exposure to the identified threats. Include security assurance requirements in tool development.

7. Restrict access by need-to-know

   Restrict access to data, tools, and resources by business role. Consider segregation/separation/rotation of duties.

8. Identify and authenticate access

Deploy user identification, authentication mechanisms, and access control for data, tools, and resources.

9. Restrict physical access and control physical media

Access polices include consideration of physical access, including control of physical media and access to media ports.

10. Track and monitor access

Implement audit trails for administration changes and access to sensitive data, tools, and resources.

11. Regularly test

Periodically conduct vulnerability scans. Monitor for intrusion detection. Audit logs for detection of security events.

12. Maintain policy

Establish, deploy, review, and maintain security policies. Assure that product and service suppliers have implemented necessary security policies.

13. Compensating controls

Compensating controls are alternatives to standard security controls which are sufficiently effective to replace the standard controls without adding security risk. They may be specific to the industry or organization. The security policies may include justification for the compensating control, and information about how the compensating control is to be implemented, tested, validated, and maintained.

A-L.3.3 Objectives for the Data Security Program

A. A Data Security Program accomplishes the following:

1. Ensure that security protection is sufficient to prevent intentional corruption during process and exchange of data..
2. Ensure that security threats specific to the organization's operations are identified and assessed, and that risk mitigation strategies are implemented.
3. Prevent unauthorized access to data or tools.

B. Detailed instructions for the Data Security Program may include:

- Roles and responsibilities, including persons with authority and responsibility;
- Training/qualifications;
- Control of access and use of data tools;
- Control of access to processing and exchange networks;
- Control and transfer of physical media;
- Control of access to resources;
- Secure signing process when digital signatures are used;
- Control of access to private keys and distribution of digital certificates, when used;

- Security event recognition and response; and
- Security event evaluation process with considerations for program improvements.