Aircraft and Propulsion Type Certificates – Case for Separate Cybersecurity Regulation

AIA Civil Aviation Cybersecurity Subcommittee

Dan Diessner – Chair (The Boeing Company)
Hank Wynsma – Vice-Chair (GE Aviation)

Membership:

Bill Lamberti	Pratt & Whitney
Bret Lynch	Pratt & Whitney
Siobvan Nyikos	Boeing
Stefan Schwindt	GE
Brittany Skelton	Boeing

Executive Summary

Current Issue Papers and associated Special Conditions applied on e-enabled aircraft have been focused only on Part 25. However, propulsion – engines and propellers – have independent Type Certificates and may have their own external interfaces that need to be considered from a cybersecurity perspective. This paper analyzes the current rulemaking environment and the recent rules issued by EASA on their equivalents to Part 25, 33 and 35. Recommendations have been issued to adopt a similar rulemaking scheme and to apply appropriate Issue Papers until rules have been published.

Scope

Aircraft as a whole are increasingly connected internally and externally. The higher degree of connectivity provides numerous benefits ranging from passenger experience – such as improved In-Flight Entertainment, internet and phone access in flight, etc. – to operational improvements – such as better diagnostic capabilities and collection and distribution of maintenance data. The higher revenue potential and reduction of operating costs suggest that connectivity is unlikely to decrease to earlier levels and instead the trend may be for even more connectivity. However, the new connectivity also introduces risks into aviation – entry points for attackers can be established as well as providing access to many more systems. The regulatory authorities have recognized this trend and early established Special Conditions to cover a lack dedicated rules for cybersecurity. The authorities have also identified the trend of continuing connectivity and set forth motions to provide appropriate regulations, and industry has reacted by releasing a suite of standards to provide Acceptable Means of Compliance to the anticipated regulations. The industry standards released are:

- DO-326A/ED-202A "Airworthiness Security Process Specification" providing process guidance for initial airworthiness
- DO-356A/ED-203A "Airworthiness Security Methods and Considerations" providing detailed methods to comply with the process and a set of objectives to be used for demonstrating compliance for initial airworthiness
- DO-355/ED-204 "Information Security Guidance for Continuing Airworthiness" providing guidance to operators and design approval holders to ensure continuing airworthiness[1]

DO-326A indicates that the standard addresses Part 25 developments only whereas the – otherwise – identical ED-202A states that it may be applicable for all other design parts with potential tailoring. Both DO-356A and ED-203A state that the standard was developed for use with Part 25 but that they may be used for other design parts including Part 33 and 35.

Problem Statement

The text of the Special Conditions that have been developed for e-enabled or connected aircraft have been similar over the various applicable aircraft with a minor evolution as experience has been gained. For reference, some relevant Special Conditions relating to aviation cyber-safety are included showing the evolution of the definition and the split of Special Conditions into threats internal and external to the aircraft.

- Airbus A350-900
    - *Accordingly, pursuant to the authority delegated to me by the Administrator, the following special conditions are issued as part of the type-certification basis for Airbus Model A350–900 series airplanes.*
        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.*

[1] DO-355A/ED-204A has been recommended for publication by RTCA SC-216 and EUROCAE WG-72. The publication is expected end of September 2020. As the document has not been published, the EASA AMC could not reference Revision A. In discussion with EASA, AMC 20-42 will be updated to include DO-355A/ED-204A after publication at the next suitable instance. EASA will accept Revision A as a Means of Compliance even if it is not listed in AMC 20-42.

Civil Aviation Cybersecurity Subcommittee
Aerospace Industries Association of America, Inc.
1000 Wilson Boulevard, Suite 1700 | Arlington, VA 22209-3928 | 703.358.1000 | www.aia-aerospace.org

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 allow the operator to ensure that continued airworthiness of the airplane is maintained, including all post-type-certification modifications that may have an impact on the approved electronic system-security safeguards.* [79 FR 43239]

- Accordingly, the Federal Aviation Administration (FAA) proposes the following special conditions as part of the type certification basis for Airbus Model A350-900 series airplanes. Isolation of the Airplane Electronic System Security Protection from Unauthorized Internal Access.
  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*
  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 safeguards. [78 FR 76252]*

- Boeing B787-8
  - *Accordingly, pursuant to the authority delegated to me by the Administrator, the following special conditions are issued as part of the type certification basis for the Boeing Model 787-8 airplane.*

    The applicant shall ensure system security protection for the Aircraft Control Domain and Airline Information Domain from access by unauthorized sources external to the airplane, including those possibly caused by maintenance activity. The applicant shall ensure that security threats are identified and assessed, and that risk mitigation strategies are implemented to protect the airplane from all adverse impacts on safety, functionality, and continued airworthiness. [72 FR 73582]
  - *Accordingly, pursuant to the authority delegated to me by the Administrator, the following special conditions are issued as part of the type certification basis for the Boeing Model 787-8 airplane.*

    The design shall prevent all inadvertent or malicious changes to, and all adverse impacts upon, all systems, networks, hardware, software, and data in the Aircraft Control Domain and in the Airline Information Domain from all points within the Passenger Information and Entertainment Domain. [73 FR 27]

From the referenced text, it is evident that engines have not been considered in the text of the Special Conditions; instead there is only the discussion of the type certificate basis of the airplane. This is a reference to the 14 CFR 25 ("Part 25") regulation which is separate to the 14 CFR 33 ("Part 33") regulation of engines. While earlier engines did not have external connectivity, this state will be changing as health, maintenance and other data will be streamed from engines either through aircraft interfaces or dedicated interfaces installed on the engines. The aircraft listed above do not

have propellers, but as propellers are regulated separately as 14 CFR 35 ("Part 35"), all parts of the propulsion units need to be considered separately and separate from the airplane.

By not providing a separate Special Condition for propulsion nor including propulsion parts as a sub-item of the airplane Special Conditions, complexities arise in demonstrating compliance. Due to the separation of Type Certificates, the airplane Design Approval Holder does not have any authority over the propulsion Design Approval Holder(s) and is limited to setting interface requirements on the airplane/propulsion interface. Any information not available as part of the interface definition becomes the subject of difficult contractual negotiations.

The recommendation of AIA is to issue Special Conditions for both airplane and propulsion until the relevant regulations are updated to include provisions for aircraft cybersecurity. When the regulatory update is performed, AIA suggests full harmonization with EASA's proposed amendments such that Part 25, Part 33 and Part 35 are updated, and the responsibilities are separated and clarified. By defining responsibilities for Part 25, Part 33 and Part 35 to each secure all interfaces where attacks can occur – the domains will not need to cross check each other unless specified in the interface specifications. This recommendation is consistent with the 27th September 2017 FAA internal memos on regulation and certification requesting alignment in airplane and engine requirements.

The approach of aligning airplane and propulsion requirements has been adopted by EASA in their NPA 2019-01 to introduce Initial Airworthiness requirements. AIA and ASD have provided comments on the NPA 2019-01 proposal to strengthen the individual responsibilities of the Design Approval Holders and this has been accepted and adopted by EASA in the rules issued on 1 July 2020.

Comments 212, 213 and 244 in the Comment Response Document to NPA 2019-01 describe the industry request for the clear separation of TC responsibilities and EASA's acceptance of the text:

Comment 244 *(nature of comments and responses equivalent for 212 and 213)*
Commented text "[…] with special consideration given to the interfaces between the aircraft and the engine, if applicable. In particular, specific cases of intentional unauthorised electronic interactions that could potentially have similar effects on all the engine control systems of an aircraft should be taken into account in the security risk assessment, rather than any interactions that could only have an adverse effect on a single engine." **Proposed modification** Modify to "[...] with special consideration given to any external interfaces of the engine and to the interfaces between [...]" **Justification** Engines and propellers are separate Type Certificates from the rest of the aircraft. Sharing of risk and responsibilities is necessary to simply certification processes for all involved - the aircraft TC applicant needs to be able to rely on engines/propellers not introducing risks via common interfaces and vice versa as neither will have insight into design of other TC applicant. Current Special Conditions required aircraft TC holders to make statements on security of entire aircraft including powerplants without the easy insight and oversight of any external connections that the powerplants may have. By adding appropriate text, this can be simplified in the future - the aircraft TC applicant no longer needs to make statements on behalf of the powerplants and only needs to check that the aircraft systems do not create a risk to the powerplant. Similarly, the

Civil Aviation Cybersecurity Subcommittee
Aerospace Industries Association of America, Inc.
1000 Wilson Boulevard, Suite 1700 │ Arlington, VA 22209-3928 │ 703.358.1000 │ www.aia-aerospace.org

powerplant TC applicants need to ensure that any external interfaces are secured and that no risks are being introduced to that aircraft via the interface.
Response **Accepted**

The following text has been issued for large airplanes, engines and propellers:

- CE-E 50 amended as following:
  CE-E 50 Engine Control System
  […]
  (l) Information System Security Protection.
  Engine Control Systems, including networks, software and data, must be designed and installed so that they are protected from intentional unauthorised electronic interactions (IUEIs) that may result in adverse effects on the safety of the aircraft. The security risks and vulnerabilities must be identified, assessed, and mitigated as necessary. The applicant must make procedures and Instructions for Continued Airworthiness (ICA) available that ensure that the security protections of the Engine controls are maintained.

  AMC to CS-E 50(l) Information system security protection
  For Engine Control Systems, AMC 20-42 provides acceptable means, guidance and methods to address CS-E 50(l), with special consideration given to any external interfaces of the Engine and the interfaces between the aircraft and the Engine, if applicable. In particular, specific cases of intentional unauthorised electronic interactions (IUEIs) that could potentially have similar effects on all the Engine Control Systems of an aircraft should be taken into account in the security risk assessment, and not just any interactions that could only have an adverse effect on a single Engine.

- CS-E 25 amended as following:
  CS-E 25 Instructions for Continued Airworthiness
  […]
  (c) The following information must be considered, as appropriate, for inclusion into the manual(s) required by CS-E 25(a).
  […]
  (13) Instructions applicable to information system security protection as required by CS-E 50(l).

- CS-P 230 amended as following:
  CS-P 230 Propeller Control System
  […]
  (g) Information system security protection. Propeller control systems, including their networks, software and data, must be designed and installed so that they are protected from intentional unauthorised electronic interactions (IUEIs) that may result in adverse effects on the safety of the aircraft. The security risks and vulnerabilities must be identified, assessed and mitigated as necessary. The applicant must make procedures and Instructions for Continued Airworthiness (ICA) available that ensure that the security protections of the propeller control systems are maintained.

  AMC P 230 Propeller Control System

[…]
(5) Information System Security Protection
For electronic Propeller control systems, AMC 20-42 provides acceptable means, guidance and methods to address CS-P 230(g), with special consideration given to any external interfaces of the Propeller and the interfaces between the aircraft and the propeller, if applicable. In particular, specific cases of intentional unauthorised electronic interactions (IUEIs) that could potentially have similar effects on all the Propeller control systems of an aircraft in a relatively short period of time, and the resulting adverse effect on the safety of the aircraft, should be taken into account for the security risk assessment, and not just any interaction that results in an adverse effect on a single Propeller.

- CS-P 40 amended as following:
  CS-P Instructions for Continued Airworthiness
  […]
  (c) The following information must be considered, as appropriate, for inclusion into the manual(s) required by CS-P 40(a).
  […]
  (13) Instructions applicable to information system security protection as required by CS-P 230(g).

- CS-25 additional text:
  CS 25.1319 Equipment, systems and network information protection
  (a) Aeroplane equipment, systems and networks, considered separately and in relation to other systems, must be protected from intentional unauthorised electronic interactions (IUEIs) that may result in adverse effects on the safety of the aeroplane. Protection must be ensured by showing that the security risks have been identified, assessed and mitigated as necessary.
  (b) When required by paragraph (a), the applicant must make procedures and Instructions for Continued Airworthiness (ICA) available that ensure that the security protections of the aeroplane's equipment, systems and networks are maintained.

  H25.6 Information system security Instructions for Continued Airworthiness
  The applicant must prepare Instructions for Continued Airworthiness (ICA) that are applicable to aircraft information system security protection as required by CS 25.1319 (see AMC 20-42 Section 9).

Conclusion and recommendations

The industry stakeholders from both the aircraft design approval holder sector and from the propulsion (engines and propeller) design approval holder sector agree that the current special conditions introduce ambiguity over demonstrating security of the entire aircraft to external threats in light of connectivity in the propulsion units and that the ambiguity leads to a contradiction in current separation of type certificates each for airplane, engine and propeller (if latter is installed).

AIA recommends that the FAA issues cybersecurity rules for engines and propellers at the same time as the update to Part 25 in line with the relevant FAA internal memos. In this joint update, the responsibilities for each of the design approval holders should be clarified that each can trust the connections to the other – on the basis that cybersecurity has been considered in the approval of

Civil Aviation Cybersecurity Subcommittee
Aerospace Industries Association of America, Inc.
1000 Wilson Boulevard, Suite 1700 │ Arlington, VA 22209-3928 │ 703.358.1000 │ www.aia-aerospace.org

their type certificate. If all design parts follow the same process, this mutual trust is acceptable. The current means for sharing requirements on the interface should be extended to include the technical and operational requirements for security. The use of the future ED201A / DO-XXX standard will provide guidance on how organizations share risk including the outputs of each risk assessment and requirements.

The rules issued by EASA should be used as a template to ensure harmonized rulemaking and the interpretation of the language in the rule with respect to Type Certificate boundaries confirmed in the Comment Response Document should be adopted. Until such rules are issued, industry recommends issuing separate Special Conditions for each product or updating existing Special Conditions to include all relevant type certificates on the basis of the proposed rule update.

The SAE committee E-36 on Engine Controls is developing proposals for applying the RTCA cybersecurity standards in a propulsion context. This work may be used as the basis for establishing a rule for Part 33 and Part 35 and the corresponding Advisory Circulars describing the Acceptable Means of Compliance.

Referenced documents

Reference	Title
14 CFR Part 25	Airworthiness Standards: Transport Category Airplanes
14 CFR Part 33	Airworthiness Standards: Aircraft Engines
14 CFR Part 35	Airworthiness Standards: Propellers
72 FR 73582	Special Conditions: Boeing Model 787-8 Airplane; Systems and Data Networks Security-Protection of Airplane Systems and Data Networks from Unauthorized External Access (Docket No. NM365 Special Conditions No. 25-357-SC)
73 FR 27	Special Conditions: Boeing Model 787-8 Airplane; Systems and Data Networks Security-Isolation or Protection From Unauthorized Passenger Domain Systems Access (Docket No. NM364 Special Conditions No. 25-356-SC)
78 FR 76252	Special Conditions: Airbus, Model A350-900 Series Airplane; Isolation or Protection of the Aircraft Electronic System Security From Unauthorized Internal Access
79 FR 43239	Special Conditions: Airbus Model A350-900 Airplanes; Isolation or Protection of the Aircraft Electronic System Security From Unauthorized Internal Access (Docket No. FAA-2013-0910 Special Conditions No. 25-534-SC)
CS-25 Amendment 25	Certification Specification and Acceptable Means of Compliance for Large Aeroplanes
CS-E Amendment 6	Certification Specifications for Propellers
CS-P Amendment 2	Certification Specifications for Engines
CRD 2019-01	Comment-Response Document 2019-01 Related NPA: 2019-01 – RMT.0648

Civil Aviation Cybersecurity Subcommittee
Aerospace Industries Association of America, Inc.
1000 Wilson Boulevard, Suite 1700 │ Arlington, VA 22209-3928 │ 703.358.1000 │ www.aia-aerospace.org

EASA NPA 2019-01	Aircraft Cybersecurity
EUROCAE ED-201A (draft)	Aeronautical Information System Security (AISS) Framework Guidance
EUROCAE ED-202A	Airworthiness Security Process Specification
EUROCAE ED-203A	Airworthiness Security Methods and Considerations
EUROCAE ED-204	Information Security Guidance for Continuing Airworthiness
FAA Internal Certification Coordination Memo September 29, 2017	Internally Certification Issues with Engine and Aircraft Interfaces
FAA Internal Regulatory Coordination Memo September 29, 2017	Internally Coordinating Regulatory Changes with Engine and Aircraft Interfaces
RTCA DO-326A	Airworthiness Security Process Specification
RTCA DO-355	Information Security Guidance for Continuing Airworthiness
RTCA DO-356A	Airworthiness Security Methods and Considerations
RTCA DO-XXX (draft, no document number assigned)	Aeronautical Information System Security (AISS) Framework Guidance

Abbreviations

AIA	Aerospace Industries Association
AMC	Acceptable Means of Compliance
ASD	AeroSpace and Defence Industries Association of Europe
CFR	Code of Federal Regulations
CRD	Comment Response Document
CS	Certification Specification
DAH	Design Approval Holder
EASA	European Aviation Safety Agency
FAA	Federal Aviation Administration
FR	Federal Register
ICA	Instructions for Continued Airworthiness
NPA	Notice of Proposed Amendment
RMT	Rulemaking Task
TC	Type Certificate

Civil Aviation Cybersecurity Subcommittee
Aerospace Industries Association of America, Inc.
1000 Wilson Boulevard, Suite 1700 | Arlington, VA 22209-3928 | 703.358.1000 | www.aia-aerospace.org