Civil Aviation Cybersecurity Change Impact Assessment and Affected areas Recommendations Report

AIA Civil Aviation Cybersecurity Subcommittee

Stefan Schwindt – WG Chair (GE Aviation)

Sean Sullivan – WG Vice Chair (The Boeing Company)

Working Group Membership:

Sarah Stern	Boeing
Stefan Schwindt	GE Aviation

EASA has introduced cybersecurity into certification with ED Decision 2020/006/R. With effect from January 2021, the following certification specifications include cybersecurity rules:

- CS-23 Small airplanes
- CS-25 Large airplanes
- CS-27 Small rotorcraft
- CS-29 Large rotorcraft
- CS-E Engines
- CS-P Propellers
- CS-APU Auxiliary Power Units
- CS-ETSO European Technical Standard Orders

In addition to amending the certification specifications, Part 21 was updated with an amendment to Appendix A to GM 21.A.91 "Classification of changes to type certificate" declaring that changes that introduce a potential for unauthorized electronic access should be considered a major change. As an effect, a change to any type certificate – regardless of previous cybersecurity inclusion in the certification basis – would need to be analyzed for such impacts on information security.

The FAA is currently pursuing equivalent rulemaking with the Notice of Proposed Rulemaking anticipated for May 2023 and final rule to be issued in 2024. In the interim, the FAA is using Special Conditions to the same effect as EASA's published rules.

With these regulations for cybersecurity in certification in effect, it is necessary when assessing changes to type certificates ("product change rule") to additionally consider cybersecurity. Well established processes exist for performing a Change Impact Analysis for various technical domains such as Systems, Software and Airborne Electronic Hardware. However, a review of guidance for Change Impact Analysis for security in DO-326A "Airworthiness Security Process Specification" has shown that it does not harmonize with the existing processes.

The preferred approach for a Change Impact Analysis is to establish a scope of direct changes to a product as well as areas not proposed for change but may be affected ("affected areas"). The relative risk of

changes is used to classify the change into minor, major/non-significant, major/significant or major/substantial (as defined by 21.A.101 or 14 CFR 21.101). In addition, the nature of the changes is used to determine what activities should be performed as part of the change development and re-verification to obtain approval for the change. This approach ensures that appropriate level of effort and scrutiny is applied for each change.

In DO-326A, the current guidance does not follow this generic template. Instead, it uses the threat condition classification of the product being changed to determine which data submittals should be provided. This is a divergence from the generic template as it requires knowledge of the system's threat condition before the change and, as such, does not tailor submittals to the actual change. For legacy aircraft which have not (yet) included cybersecurity in the certification basis, the threat condition for the aircraft systems may not be known *a priori* and a more extensive risk assessment may have to be performed. This may extend beyond the system being changed but upstream systems which could be impacted through propagation. The value of following the template is to identify the correct amount of analysis, design, and verification is conducted in a system to ensure any risk created by the change is fully mitigated. To ensure the correct balance is achieved better guidance is needed.

As a consequence, the AIA Cybersecurity Subcommittee has stood up a subgroup to analyze Change Impact Analysis processes and to propose how to establish guidance for security Change Impact Analysis that is compatible with all other analyses performed for 14 Part 21.93 "Classification of changes in type design". The subcommittee has collected guidance for other technical domains and discussed how to use these as a starting point for cybersecurity.

Discussions over the last year within AIA have helped identify the need for more aligned guidance resulting in EUROCAE WG-72 and RTCA SC-216 accepting an update to DO-326 Revision B into their Terms of Reference based on the recommendations from AIA. As a result, the activities of the AIA subgroup will be transferred to and continue as the SC-216 / WG-72 work statement to be completed in 2024. The update of the standard is supported by AIA and it is expected that SC-216 / WG-72 will satisfy the aim of having:

- Change Impact Analysis guidance that is compatible with other change analyses under 14 CFR 21.93
- Change Impact Analysis identifies scope of security impact of changes
- Change Impact Analysis classifies the change
- Change Impact Analysis identifies areas of security risk related to change so that appropriate activities can be captured in certification, development and verification plans
- Change Impact Analysis guidance will be suitable for changes to aircraft that previously have not considered security as well as aircraft with previous security activities
- Change Impact Analysis provides tailoring based on the nature and magnitude of the change