RTCA, Inc.
1150 18th Street NW, Suite 910
Washington, DC 20036
USA

Airworthiness Security Process Specification

RTCA DO-326B
September 26, 2024

Prepared by: SC-216
© 2024 RTCA, Inc.

Copies of this document may be obtained from
RTCA, Inc.
Telephone: 202-833-9339
Facsimile: 202-833-9434
Internet: www.rtca.org
Please visit the RTCA Online Store for document pricing and ordering information.

FOREWORD

This document was prepared by Special Committee 216 (SC-216) Aeronautical Systems Security jointly with EUROCAE Working Group 72 (WG-72) Aeronautical Systems Security and approved by the RTCA Program Management Committee (PMC) and the EUROCAE Council on September 26, 2024.

RTCA, Incorporated is a not-for-profit corporation formed to advance the art and science of aviation and aviation electronic systems for the benefit of the public. The organization develops consensus-based recommendations on contemporary aviation issues. RTCA's objectives include, but are not limited to:

- coalescing aviation system user and provider technical requirements in a manner that helps government and industry meet their mutual objectives and responsibilities.
- analyzing and recommending solutions to the system technical issues that aviation faces as it continues to pursue increased safety, system capacity and efficiency.
- developing consensus on the application of pertinent technology to fulfill user and provider requirements, including development of minimum operational performance standards for electronic systems and equipment that support aviation.
- assisting in developing the appropriate technical material upon which positions for the International Civil Aviation Organization and the International Telecommunication Union and other appropriate international organizations can be based.

The organization's recommendations are often the basis for government and private sector decisions as well as the foundation for many Federal Aviation Administration Technical Standard Orders and several advisory circulars.

All URLs referenced in this document are current as of the document publication date.

Since RTCA is not an official agency of the United States Government, its recommendations may not be regarded as statements of official government policy unless so enunciated by the U.S. government organization or agency having statutory jurisdiction over any matters to which the recommendations relate.

DISCLAIMER

This publication is based on material submitted by various participants during the SC approval process. Neither the SC nor RTCA has made any determination whether these materials could be subject to valid claims of patent, copyright, or other proprietary rights by third parties, and no representation or warranty, expressed or implied is made in this regard. Any use of or reliance on this document shall constitute an acceptance thereof "as is" and be subject to this disclaimer.

This Page Intentionally Left Blank

EXECUTIVE SUMMARY

The guidance of this document adds to current guidance for aircraft certification to handle the threat of Intentional Unauthorized Electronic Interaction (IUEI) to aircraft safety. It adds data requirements and compliance objectives, as organized by generic activities for aircraft development and certification, to handle the threat of IUEI to aircraft safety. It can be used to support aircraft and system certification for aircraft information security considerations under EASA AMC 20-42 for CS-E 50, CS-P 230 and CS 25.1319 and the upcoming FAA rules for 14 CFR 25.1319, 33.28 and 35.23. The FAA's Notice of Proposed Rulemaking is expected by the end of 2024 with issuance of rules technically equivalent to EASA's rules in 2025. It is intended to be used in conjunction with related guidance material, including ED-203/DO-356, ED-204/DO-355 and ED-206/DO-392. It is also intended to be used with other applicable guidance material, including ED-79/SAE ARP 4754, ED-135/SAE ARP4761, ED-12/DO-178, and ED-80/DO-254, in the context of Part 25 for Transport Category Aircraft which include an approved passenger seating configuration of more than 19 passenger seats. Tailoring of this guidance may allow it to be applicable in other contexts, such as CS-23, CS-27, CS-29, CS-E, Part 23, Part 27, Part 29, and Part 33.

For a discussion of the history of ED-202B/DO-326B and the differences from the previous versions, please see Appendix F: Background of the ED-202/DO-326 Document.

RTCA/EUROCAE documents on Aeronautical Systems Security will address information security for the overall Aeronautical Information System Security (AISS) of airborne systems with related ground systems and environment. This guidance material is intended for Design Approval Holders including aircraft manufacturers who are applying for an initial Type Certificate (TC) and for later changes including Amended Type Certificates (ATC) and Supplemental Type Certificates (STC). The guidance also applies to the suppliers of systems and equipment being certified under these Type Certificates. The Guidance is derived from understood best practices.

Compliance may be accomplished through a differentiated security process that interacts with the safety process. To sustain this principle, overall consistency between both processes should be maintained, by ensuring that the security assessment process considers the outputs of the safety assessment process. As an alternative, when considered practicable, compliance may be accomplished through a blended process – documented by the applicant – that would integrate safety and security, including suitable evidence that security and safety requirements are met.

The process outlined in this document is not intended to address the physical security of the aircraft or aircraft systems. Physical and procedural protective measures may be used as a mitigation for defined threats within the process to reduce the scope of the assessment (set the trust boundary) or provide supplementary or complete protection of a threat condition.

This document and the process within is not meant to address Airport, Airline, or Air Traffic Service Provider security for the protection against IUEI unrelated to the assets within the aircraft security boundary. While the risk identification and remediation process contained within is sound, a different risk acceptability table would need to be used for determining the hazard classification of threat conditions.

This Page Intentionally Left Blank

TABLE OF CONTENTS

1 INTRODUCTION 1

1.1 PURPOSE 1
1.2 SCOPE 1
1.3 HOW TO USE THIS DOCUMENT 2
1.4 CONVENTIONS OF THIS DOCUMENT 4
1.5 RELATIONSHIP TO OTHER DOCUMENTS 4

2 AIRWORTHINESS SECURITY PROCESS 5

2.1 PROCESS OVERVIEW 5
2.1.1 The Security Risk Assessment Related Activities 7
2.1.2 The Security Development Related Activities 8
2.1.3 Compliance 8
2.2 SECURITY RISK ASSESSMENT ACTIVITIES IN THE DEVELOPMENT PROCESS 9
2.2.1 Interactions with the Integral Processes of ED-79/ARP 4754 10
2.2.2 Integration of Security Development Activities in the Development Process 12

3 FUNDAMENTAL CONCEPTS 15

3.1 CIA AND INFORMATION FLOW CONTROL 15
3.2 SECURITY DEFINITIONS AND RISK MANAGEMENT 16
3.3 ESTABLISHING THE SECURITY SCOPE 16
3.3.1 Security Perimeter 17
3.3.2 Security Environment 18
3.4 SECURITY RISK ASSESSMENT 19
3.4.1 Threat Condition Identification and Evaluation 20
3.4.2 Threat Scenario Identification 21
3.4.3 Security Measure Characterization 22
3.4.4 Level of Threat Evaluation 22
3.5 SECURITY EFFECTIVENESS 22
3.5.1 Introduction 22
3.5.2 Implementation of Security Effectiveness 24
3.6 SECURITY DEVELOPMENT ACTIVITIES 26
3.6.1 Security Architecture 27
3.6.2 Security Measures 27
3.6.3 Security Guidance 28
3.6.4 Security Verification 29

4 AIRCRAFT MODIFICATIONS 31

4.1 AIRCRAFT LEVEL VERSUS SYSTEM LEVEL SECURITY RISK ASSESSMENT DETERMINATION 31
4.1.1 Aircraft Related Services 32
4.2 MODIFICATION PROCESS ACTIVITIES 34
4.2.1 Change Impact Analysis 35
4.2.2 Service History 36
4.2.3 Interconnectivities of New or Modified Aircraft Systems 36
4.2.4 Installing New Aircraft Systems and Networks 37

4.2.5 Replacing Aircraft Systems and Networks 37
4.2.6 Modifying Existing Aircraft Systems and Networks 37
4.2.7 CTSO/ETSO/TSO Installation Requirements 37
4.3 AIRWORTHINESS SECURITY PROCESS AND SECURITY RISK ASSESSMENT CRITERIA 38
4.3.1 Instructions for Continued Airworthiness 38
4.4 DATA SUBMITTALS FOR AIRCRAFT SYSTEM MODIFICATIONS 38
4.4.1 Plan For Security Aspects of Certification Summary (PSecAC Summary) 39

APPENDIX A DEFINITION OF THE AIRWORTHINESS SECURITY ACTIVITIES A-1

A.1 SECURITY ASPECTS OF CERTIFICATION A-3
A.1.2 Plan for Security Aspects of Certification Summary (PSecAC Summary) A-4
A.2 SECURITY RISK ASSESSMENT RELATED ACTIVITIES A-5
A.2.1 Aircraft Security Scope Definition (ASSD) A-5
A.2.2 Preliminary Aircraft Security Risk Assessment (PASRA) A-6
A.2.3 Aircraft Security Risk Assessment (ASRA) A-7
A.2.4 System Security Scope Definition (SSSD) A-8
A.2.5 Preliminary System Security Risk Assessment (PSSRA) A-9
A.2.6 System Security Risk Assessment (SSRA) A-10
A.3 Security Development Activities A-11
A.3.1 Aircraft Security Architecture and Measures (ASAM) A-11
A.3.2 Aircraft Security Operator Guidance (ASOG) A-12
A.3.3 Aircraft Security Verification (ASV) A-13
A.3.4 System Security Architecture and Measures (SSAM) A-14
A.3.5 System Security Integrator Guidance (SSIG) A-15
A.3.6 System Security Verification (SSV) A-16

APPENDIX B CHANGE IMPACT ANALYSIS QUESTIONNAIRE B-1

B.1 Example Questionnaire B-1
B.2 Threat Models B-5
B.3 Example 1: Adding Pilot EFB to Cockpit Without Aircraft Digital Interfaces. B-8
B.4 Example 2. Adding Wireless Interface to Single Aircraft System. B-13
B.5 Example 3. Adding Modular Avionics to Aircraft Systems. B-18
B.6 Example 4. Adding Seat Actuation System to Aircraft. B-23
B.7 Example 5. Adding Electronic Data Path Between Differing Levels of Trust. B-29
B.8 Example 6. Centralized Data Loading. B-33
B.9 Example 7. New Dataload Connectivity. B-38

APPENDIX C GLOSSARY C-1

APPENDIX D ACRONYMS AND ABBREVIATIONS D-1

APPENDIX E REFERENCES E-1

APPENDIX F BACKGROUND OF THE ED-202/DO-326 DOCUMENT F-1

F.1 HISTORY OF DOCUMENT AND VERSIONS F-1
F.2 RATIONALE FOR AN AIRWORTHINESS SECURITY PROCESS F-1
F.3 INFORMATION ON THE CHANGES BETWEEN ED-202/DO-326 AND ED-202A/DO-326A F-2
F.4 INFORMATION ON THE CHANGES BETWEEN ED-202A/DO-326A AND ED-202B/DO-326B F-3

APPENDIX G COMMITTEE MEMBERSHIP G-1

LIST OF FIGURES

FIGURE 2-1: AIRWORTHINESS SECURITY RISK MANAGEMENT FRAMEWORK 6
FIGURE 2-2: SECURITY RISK ASSESSMENT RELATED ACTIVITIES IN THE DEVELOPMENT PROCESS V-MODEL 9
FIGURE 2-3: AWSP AS PART OF AIRCRAFT CERTIFICATION PROCESS 11
FIGURE 2-4: SECURITY DEVELOPMENT AS PART OF AIRCRAFT CERTIFICATION PROCESS 13
FIGURE 3-1: SECURITY SCOPE 17
FIGURE 3-2: SECURITY RISK ASSESSMENT 20
FIGURE 3-3: SECURITY ACTIVITIES IN ED-79/ARP 4754 AIRCRAFT DEVELOPMENT PROCESS MODEL 24
FIGURE 3-4: RELATIONSHIP BETWEEN EFFECTIVENESS REQUIREMENTS AND ASSURANCE ACTIONS 26
FIGURE 3-5: SIMPLIFIED EXAMPLE OF A SECURITY ARCHITECTURE WITH DIFFERENT TYPES OF TECHNICAL AND PROCEDURAL SECURITY MEASURES 28
FIGURE 3-6: SECURITY TESTING ACTIVITIES 30
FIGURE 4-1: EXAMPLE OF E-ENABLED ARCHITECTURE AND INFRASTRUCTURE 34
FIGURE 4-2: INTERCONNECTIVITIES OF NEW, MODIFIED, OR REMOVED AIRCRAFT SYSTEMS 37
FIGURE A-1: AIRWORTHINESS SECURITY PROCESS ACTIVITIES A-2
FIGURE B- 1: DATAFLOW DIAGRAM ELEMENTS B-6
FIGURE B-2: ARCHITECTURE BLOCK DIAGRAM EXAMPLE B-7
FIGURE B-3: DATAFLOW DIAGRAM EXAMPLE B-8
FIGURE B-4: EXAMPLE ONE DATAFLOW DIAGRAM B-9
FIGURE B-5: ADDING WIRELESS INTERFACE TO A SINGLE AIRCRAFT SYSTEM B-14
FIGURE B-6: DFD FOR ADDING DO-297 IMA SYSTEM B-19
FIGURE B-7: ADDING SAS TO AIRCRAFT B-24
FIGURE B-8: ADDING CONNECTIVITY BETWEEN DIFFERENT LEVELS OF TRUST B-30
FIGURE B-9: ADDING CENTRALIZED DATA LOADING B-34
FIGURE B-10: NEW DATALOAD CONNECTIVITY B-39

LIST OF TABLES

TABLE 3-1: ASSET SECURITY ATTRIBUTES AND THREAT CONDITIONS 21
TABLE 4-1: DATA SUBMITTALS FOR THE SECURITY ASPECTS OF AIRCRAFT SYSTEM MODIFICATIONS 39
TABLE B-1: CHANGE IMPACT QUESTIONNAIRE B-2
TABLE B-2: EXAMPLE ONE CHANGE IMPACT QUESTIONNAIRE B-9
TABLE B-3: EXAMPLE TWO CHANGE IMPACT QUESTIONNAIRE B-14
TABLE B-4: EXAMPLE THREE CHANGE IMPACT QUESTIONNAIRE B-20
TABLE B-5: EXAMPLE FOUR CHANGE IMPACT QUESTIONNAIRE B-25
TABLE B-6: EXAMPLE FIVE CHANGE IMPACT QUESTIONNAIRE B-30
TABLE B-7: EXAMPLE SIX CHANGE IMPACT QUESTIONNAIRE B-35
TABLE B-8: EXAMPLE SEVEN CHANGE IMPACT QUESTIONNAIRE B-39

This Page Intentionally Left Blank

1 INTRODUCTION

This document is the joint product of two industry committees; the EUROCAE Working Group WG-72, titled “Aeronautical Information Systems Security” and the RTCA Special Committee SC-216, also titled “Aeronautical Information Systems Security.” WG-72 was formed to address information security for the overall Aeronautical Information System Security (AISS) of airborne systems with related ground systems and environment, while SC-216 was formed more specifically to address information security for certification of aircraft and its systems, the committee now works jointly with WG-72 to address airborne systems with related ground systems and environments. Both committees agreed that the guidance provided by this document and its companion documents constitute an acceptable means to address the increasing potential for Intentional Unauthorized Electronic Interaction (IUEI) with aircraft information systems.

This document provides guidance by defining activities for supplementing the aircraft development and certification process to demonstrate that the effects on the safety of the aircraft of such unlawful interferences are confined within acceptable levels. As IUEI includes intentional origin, this document covers some aspects of electronic sabotage (as used in AC 25.1309-1A and AMC 25.1309).

For a discussion of the history of ED-202B/DO-326B and the differences from the previous versions, please see Appendix F: Background of the ED-202/ DO-326 Document.

1.1 PURPOSE

This document is a resource for Airworthiness Authorities (AA) and the aviation industry for certification when the development or modification of aircraft systems and the effects of IUEI can affect aircraft safety. It deals with the activities that need to be performed in support of the airworthiness process when it comes to the threat of IUEI (the “What”). ED-203/DO-356 provides methods and considerations (the “How”). The document ED-204/DO-355 "Information Security Guidance for Continuing Airworthiness" addresses airworthiness security for continued airworthiness. ED-206/DO-392 addresses guidance for managing security events.

1.2 SCOPE

The guidance of this document adds to current guidance for aircraft certification to handle the threat of IUEI to aircraft safety. It adds data requirements and compliance objectives, as organized by generic activities for aircraft development and certification, to handle the threat of IUEI to aircraft safety. This document is intended to be used in conjunction with related guidance material, including ED-203, ED-204, and ED-206. It is also intended to be used with other applicable guidance material, including ED-79/SAE ARP4754, ED-12/DO-178, and ED-80/DO-254, in the context of Part 25, CS-25, and JAA JAR-25. Tailoring of this guidance may allow it to be applicable in other contexts such as CS-23, CS-27, CS-29, CS-E, Part 23, Part 27, Part 29, and Part 33.

This process specification addresses electronic attacks (digital, not physical or electrical) and assumes trust may be placed in one or more of the following services, as negotiated with regulator:

- Airport, Airline or Air Traffic Service Provider security (e.g., access to airplanes, ground control facilities, data centers),
- Communication and surveillance services managed by national agencies or their international equivalents (e.g., ATC communications, ADS-B), and
- Navigation services managed by national agencies or their international equivalents (e.g., GPS, SBAS, GBAS).

 © 2024 RTCA, Inc.

This guidance material is 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.

This guidance is designed to be implemented across the full life cycle of an aircraft from design, through in-service, to disposal. As such, it is recommended to apply this guidance to the design stage before its use in subsequent stages of the life cycle. In cases where changes are made to an aircraft and all the previous security artifacts are not available (for example, the aircraft was not certified with security special conditions or security rules), this document provides guidance for the applicant to identify objectives applicable to the change (see 4).

IUEI is defined as human-initiated actions with the potential to affect the aircraft due to unauthorized access, use, disclosure, denial, disruption, modification, or destruction of electronic information or electronic aircraft system interfaces. This definition includes the effects of malware on infected devices and the logical effects of external systems on aircraft systems but does not include physical attacks or electromagnetic jamming.

Certification Context: Airworthiness security is the protection of the airworthiness of an aircraft from IUEI.

While the airworthiness certification process addresses failures and errors, this guidance extends this to address IUEI with aircraft systems resulting in a safety effect. Just as failures and errors are treated as manageable risks to aircraft safety by the airworthiness certification process, the threat of IUEI is treated equally through the airworthiness security activities. In this context airworthiness security activities do not directly address the interfaces, policies, and procedures of external systems. However, aircraft systems may depend upon external systems to perform their functions and so the dependencies of airworthiness security on external systems are included in the considerations. To address these considerations, the applicant documents the assumptions about external factors as part of the airworthiness security process.

Product Life Cycle Context: This document provides guidance in addressing airworthiness security during the aircraft product life cycle from project initiation until the aircraft Type Certificate is issued for the aircraft type design, including afterwards the issuance of STCs and ATCs. In addition, it includes the handover of information about the type design that is necessary to ensure continuing airworthiness with respect to IUEI. For the other stages of the product life cycle (operation, support, maintenance, administration, and disposal), guidance may be found in a companion document ED-204/DO-355 "Information Security Guidance for Continuing Airworthiness."

Those aspects of information security that have no safety effect are not in the scope of this document.

1.3 HOW TO USE THIS DOCUMENT

This document is organized into four chapters plus appendices. First time readers should read 3 before 2 to understand the concepts being used in the overview.

- Chapter 1 introduces the document.
- Chapter 2 provides an overview of the Airworthiness Security Process.
- Chapter 3 introduces fundamental concepts used by the Airworthiness Security Process activities, such as Security Scope Definition, Security Risk Assessment, considerations about the Security Development activities, and the assignment of security effectiveness requirements.
- Chapter 4 introduces modifications to aircraft and systems, including Supplemental Type Certification (STC) and Amendments to Type Certification.

© 2024 RTCA, Inc.