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

Information Security Guidance for Continued Airworthiness

RTCA DO-355A
September 10, 2020

Prepared by: SC-216
© 2020 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) and EUROCAE Working Group 72 (WG-72). It was approved by the RTCA Program Management Committee (PMC) and by the EUROCAE Council on September 10, 2020.

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; and

- assisting in developing the appropriate technical material upon which positions for the International Civil Aviation Organization and the International Telecommunications Union and other appropriate international organizations can be based.

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

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

TABLE OF CONTENTS

1 INTRODUCTION 1

1.1 PURPOSE 1
1.2 SCOPE 2
1.3 HOW TO USE THIS DOCUMENT 3
1.4 CONVENTIONS OF THIS DOCUMENT 4
1.5 RELATIONSHIP TO OTHER DOCUMENTS 4
1.6 GENERAL CONSIDERATIONS 5
1.6.1 Design Approval Holder (DAH) 5
1.6.2 Instructions for Continued Airworthiness (ICA) 5
1.6.3 Contracted Maintenance and Service Providers 7

2 AIRBORNE SOFTWARE 9

2.1 GENERAL 9
2.2 OPERATIONAL SECURITY MEASURES 11
2.2.1 Reception 11
2.2.2 Creation/Modification 12
2.2.3 Storage 12
2.2.4 Media 12
2.2.5 Software Tools 13
2.2.6 Software Distribution 13
2.2.7 Data Loading 14
2.2.8 Confidentiality 14
2.2.9 Incident Management 14
2.3 DAH Responsibilities 14
2.4 OPERATOR RESPONSIBILITIES 14

3 AIRCRAFT COMPONENTS 17

3.1 GENERAL 17
3.2 OPERATIONAL SECURITY MEASURES 17
3.2.1 Storage 17
3.2.2 Transport 17
3.2.3 Repair 17
3.2.4 Tools 17
3.2.5 Decommissioning 17
3.2.6 Incident Management 18
3.3 DAH RESPONSIBILITIES 18
3.4 OPERATOR RESPONSIBILITIES 18

4 AIRCRAFT NETWORK ACCESS POINTS 19

4.1 GENERAL 19
4.2 OPERATIONAL SECURITY MEASURES 19
4.3 DAH RESPONSIBILITIES 19
4.4 OPERATOR RESPONSIBILITIES 20

5 GROUND SUPPORT EQUIPMENT (GSE) 21

5.1 GENERAL 21
5.2 OPERATIONAL SECURITY MEASURES 21
5.2.1 Equipment Security and Operations Management 21
5.2.2 Access Control 22
5.2.3 Usage 23
5.2.4 Storage 23
5.2.5 Incident Management 23
5.2.6 Lifecycle Management 23
5.2.7 Decommissioning 23
5.3 DAH RESPONSIBILITIES 23
5.4 OPERATOR RESPONSIBILITIES 24

6 GROUND SUPPORT INFORMATION SYSTEMS 25

6.1 GENERAL 25
6.2 OPERATIONAL SECURITY MEASURES 25
6.2.1 Connection 25
6.2.2 Access Control 25
6.2.3 Data Exchange 26
6.2.4 System Hardening Of Ground Support Information Systems 26
6.2.5 Repair 27
6.2.6 Decommissioning 27
6.2.7 Incident Management 27
6.2.8 Lifecycle Management 27
6.3 DAH RESPONSIBILITIES 27
6.4 OPERATOR RESPONSIBILITIES 28

7 DIGITAL CERTIFICATES 29

7.1 GENERAL 29
7.2 OPERATIONAL SECURITY MEASURES 30
7.3 DAH RESPONSIBILITIES 30
7.4 OPERATOR RESPONSIBILITIES 31

8 AIRCRAFT INFORMATION SECURITY INCIDENT MANAGEMENT 33

8.1 GENERAL 33
8.2 OPERATIONAL SECURITY MEASURES 33
8.3 DAH RESPONSIBILITIES 33
8.4 OPERATOR RESPONSIBILITIES 34

9 OPERATOR AIRCRAFT INFORMATION SECURITY PROGRAM 35

9.1 GENERAL 35
9.1.1 AISP Relation to ISMS 35
9.1.2 AISP RELATION TO SECURITY MANAGEMENT SYSTEM 36
9.2 OPERATIONAL SECURITY MEASURES 37
9.3 DAH RESPONSIBILITIES 37
9.4 OPERATOR RESPONSIBILITIES 37

10 OPERATOR ORGANIZATION RISK ASSESSMENT 39

10.1 GENERAL 39
10.2 OPERATIONAL SECURITY MEASURES 39
10.3 DAH RESPONSIBILITIES 39
10.4 OPERATOR RESPONSIBILITIES 39

11 OPERATOR PERSONNEL ROLES AND RESPONSIBILITIES 41

11.1 GENERAL 41
11.2 OPERATIONAL SECURITY MEASURES 41
11.2.1 Skills Required for Operator Information Security Management 41
11.2.2 Aircraft Information Security Specialist 41
11.2.3 Specific Task Skills 42
11.3 DAH RESPONSIBILITIES 43
11.4 OPERATOR RESPONSIBILITIES 43
11.4.1 General 43
11.4.2 Aircraft Information Security Center 43

12 OPERATOR PERSONNEL TRAINING 45

12.1 GENERAL 45
12.2 OPERATIONAL SECURITY MEASURES 45
12.2.1 Training, Awareness, and Competence 45
12.2.2 Education and Certification 45
12.3 DAH RESPONSIBILITIES 45
12.4 OPERATOR RESPONSIBILITIES 45
12.4.1 Training Organization 45
12.4.2 Scope of Training (General and Specific) 46
12.4.3 General Training 46
12.4.4 Specific Training 48
12.4.5 Training Records 50
12.4.6 Regulatory Requirements for Operator Training 50
12.4.7 Recurrent Training 50
12.4.8 Organizational Communication regarding Aircraft Information Security 50

APPENDIX A MEMBERSHIP A-1

APPENDIX B AIRPLANE INFORMATION SECURITY PLAN (AISP) B-1

APPENDIX C GLOSSARY OF TERMS C-1

APPENDIX D ACRONYMS D-1

APPENDIX E REFERENCES E-1

APPENDIX F REVISION HISTORY - ED-204A/DO-355A F-1

TABLE OF FIGURES

Figure 1-1: Aircraft Information Security Guidance 3
Figure 2-1: A Common Security Methodology for Electronic Software Distribution..... 10

1 INTRODUCTION

This document is a joint product of two industry committees: the EUROCAE Working Group WG-72, titled “Aeronautical Systems Security” and the RTCA Special Committee SC-216, also titled “Aeronautical Systems Security”. WG-72 was formed to address information security and the overall Aeronautical Information System Security (AISS) of airborne systems in conjunction with related ground systems and environment, while SC-216 was formed more specifically to address information security for certification and operation of aircraft and its systems. The guidance provided by this document is intended to constitute an Acceptable Means of Compliance for approving information security aspects of Continuing Airworthiness activities performed by Design Approval Holders and Operators.

This document provides guidance for the operation and maintenance of aircraft and for organizations and personnel involved in these tasks. It is 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. As all information security threats may have an intentional origin, this document also covers Intentional Unauthorized Electronic Interaction (IUEI).

1.1 Purpose

This document is a resource for civil aviation authorities and the aviation industry when the operation and maintenance of aircraft and the effects of information security threats can affect aircraft safety. It deals with the activities that need to be performed in operation and maintenance of the aircraft related to information security threats.

This document gives also guidance that is related to operational and commercial effects (i.e. guidance that exceeds the safety-only effects).

ED-204A / DO-355A is a companion document to ED-202A / DO-326A “Airworthiness Security Process Specification” and ED-203A / DO-356A "Airworthiness Security Methods and Considerations" that support security in the development and modification part of the airworthiness process.

Note 1: This document was developed in the European context of the European Aviation Safety Agency (EASA) Certification Specification CS-25 "Large Aeroplanes" and the United States context of Title 14 Code of Federal Regulations (14CFR) Part 25 "Transport Category Aircraft". Tailoring of this guidance may be used in other regulatory contexts including but not limited to CS-23, CS-27, CS-29, CS-E, CS-P, Part 23, Part 27, Part 29, Part 33, and Part 35.

The most comprehensive possible area of the application of this guidance is deemed to be Large Transport Aircraft programs. However, this document does not make any assumptions about and is without prejudice to its applicability.

Note 2: The measures proposed in this document may be subject to commercial terms between DAHs and operators. It is recommended that DAHs incorporate these elements into their commercial offers, especially for service and support related topics.

 © 2020 RTCA, Inc.

1.2 Scope

ED-202A / DO-326A and ED-203A / DO-356A provide guidance in addressing airworthiness security during the aircraft product life cycle from project initiation until the aircraft Type Certificate (Amended Type Certificate, Supplemental Type Certificate and Amended Supplemental Type Certificate) is issued for the aircraft type design. In addition, it includes the handover of information about the Type Design that is necessary to ensure continuing airworthiness with respect to possible information security threats.

ED-204A / DO-355A (this document) provides guidance for the following stages of the product life cycle: operation, support, maintenance, administration, and decommissioning.

Where an organization subcontracts any activities in these stages, the organization retains the responsibility for aircraft information security (for contracted maintenance providers, refer to section 1.6.3).

A forthcoming document titled “Guidance on Information Security Event Management” (ISEM) will be jointly published by EUROCAE and RTCA. This document will provide guidance for managing security incidents and events that affect aircraft safety and it will support the existing safety event management guidance. It will provide guidance for processes, assessment and disposition, data exchanges, reporting, and other concerns that need to be performed in response to information security events.

Topics in the scope of Type Certification activities that are related to operation and maintenance of the aircraft such as Instructions for Continued Airworthiness (ICA) and security guidance documents are introduced in ED-202A / DO-326A and detailed in ED-204A / DO-355A. In such cases ED-202A / DO-326A provides references to ED-204A / DO-355A.

This document addresses information security risks only. The security measures to mitigate these risks are not limited to technical security measures; they may also be operational or management security measures.

Apart from the classical Instructions for Continued Airworthiness that are directly related to aircraft parts and systems, this document also provides guidance on Ground Support Equipment and Ground Support Information Systems that are related to the security of aircraft information systems and data networks as illustrated in Figure 1-1. Only Airborne software that can have effect on aircraft safety are in the scope of this document

© 2020 RTCA, Inc.

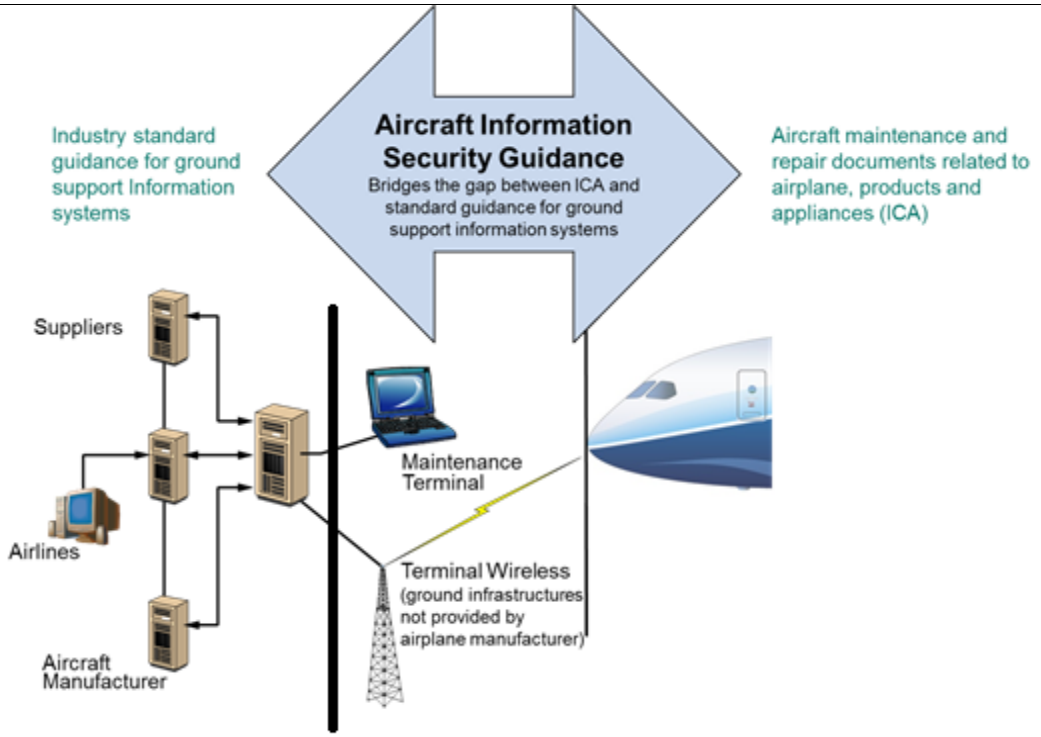


Figure 1-1: Aircraft Information Security Guidance

Note: The material in subsequent sections is only applicable if the aircraft and the operator use the features described.

1.3 How to Use This Document

This document contains material intended to be used as Guidance Material and Acceptable Means of Compliance. The Guidance Material provides explanatory information and helps the applicant understand how to satisfy the objectives described in the Acceptable Means of Compliance in this document. Chapters X.1 and X.2 provide the Guidance Material whereas chapters X.3 and X.4 may be used as an Acceptable Means of Compliance.

This document is organized in 12 chapters plus informative appendices.

- Chapter 1 introduces the document.

The remainder of this document is organized into the following chapters and appendices. The substructure of these chapters is harmonized as follows:

- Chapter X.1 gives General information to introduce and define the topic
- Chapter X.2 gives an overview of what Operational Security Measures can be taken to manage the topic
- Chapter X.3 lists the Design Approval Holder (DAH) Responsibilities
- Chapter X.4 lists the Operator Responsibilities

© 2020 RTCA, Inc.