RTCA, Inc.
1150 18th Street, NW, Suite 910
Washington D.C. 20036

Airworthiness Security Methods and Considerations

RTCA DO-356
September 23, 2014

Prepared by: SC-216

Copies of this document may be obtained from

RTCA, Inc.
1150 18th Street, N.W., Suite 910
Washington, DC 20036

Telephone: 202-833-9339
Facsimile: 202-833-9434
Internet: www.rtca.org

Please call RTCA for price and ordering information.

FOREWORD

This document was prepared by Special Committee 216 (SC-216) and was approved by the RTCA Program Management Committee (PMC) on September 23, 2014.

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 functions as a Federal Advisory Committee and 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.

This Page Intentionally Left Blank

EXECUTIVE SUMMARY

This document is the product of the RTCA Special Committee SC216, titled “Aeronautical Systems Security” to provide additional guidance for applicants implementing an Airworthiness Security Process. It was developed in the context of DO-326A/ED-202A "Airworthiness Security Process Specification" which addresses type certification considerations during the first three life cycle stages of an aircraft type (Initiation, Development or Acquisition, and Implementation) and DO-355/ED-204, "Information Security Guidance for Continuing Airworthiness" which addresses airworthiness security for continued airworthiness.

The methods and considerations of this document address the assessment of the acceptability of the airworthiness security risk and the design and verification of the airworthiness security attributes as related to system safety and airworthiness. Other aspects of information security for aerospace systems that do not affect the airworthiness security of the type design are excluded. Recommendations for handling those aspects can be found in other guidance.

More specifically, this guidance addresses the following areas.

- It provides guidance for accomplishing the activities identified in DO-326A in the areas of Security Risk Assessment and Effectiveness Assurance.
- It provides specific methods for Security Risk Analysis and Network Security Domains.

It is intended to be used in conjunction with other applicable guidance material, including SAE ARP 4754A/ED-79A, SAE ARP 4761/ED-135, DO-178C/ED-12C, and DO-254/ED-80 and with the advisory material associated with FAA AC 25.1309-1A and EASA AMC 25.1309, in the context of part 25 for Transport Category Airplanes which include an approved passenger seating configuration of more than 19 passenger seats. This guidance is not intended for CFR parts 23, 27, 29, 33.28, and 35.15, normal, utility, acrobatic, and commuter category airplanes, normal category rotorcraft, transport category rotorcraft, engines, and propellers.

This document does not address:

a. Physical security or physical attacks on the aircraft (or ground element),

b. Airport, Airline or Air Traffic Service Provider security (e.g., access to airplanes, ground control facilities, data centers),

c. Communication, navigation, and surveillance services managed by national agencies or their international equivalents (e.g., GPS, SBAS, GBAS, ATC communications, ADS-B).

This document describes guidelines, methods and tools used in performing an airworthiness security process. The guidelines, methods and tools presented are not intended to be exhaustive and can be expected to be updated with additional methods and considerations. Applicants and authorities should consider alternative practices if and when they are proposed. Practices for airworthiness security are still undergoing evolution and refinement as new features are deployed and the security threat itself evolves.

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 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, and is derived from understood best practice.

The FAA publishes additional guidance that may be used in combination with this document. Since aircraft electronic security requirements and regulations change, it is highly recommended that applicants contact the applicable certification offices (FAA or International Civil Aviation Authorities) to obtain the most recent guidance on the use of this document for certification projects.

This Page Intentionally Left Blank

TABLE OF CONTENTS

1 **INTRODUCTION** **1**

1.1 Purpose 1
1.2 Scope 1
1.3 Document Overview 2
1.4 Conventions of This Document 2
1.5 Relationship to other documents 3

2 GENERAL METHODS AND CONSIDERATIONS **5**

2.1 Security Scope 5
2.1.1 Security Environment 6
2.1.2 Assets 7
2.1.2.1 Defining Nested Assets 7
2.1.3 Security Perimeter 10
2.1.3.1 In-Flight Entertainment (IFE) Example 10
2.1.4 Threat Identification 12
2.1.4.1 Threat Sources and Trustworthiness 12
2.1.4.2 Assuring Trustworthiness of External Populations 13
2.1.4.3 Organizational Trustworthiness Standards 14
2.2 Security Risk Assessment 14
2.2.1 Threat Conditions and Severity of Impact 15
2.2.2 Identifying Threat Scenarios 16
2.2.2.1 Chains of Protection 16
2.2.2.2 Threat Catalog 20
2.2.2.3 Assessing Threat Scenarios 20
2.2.2.4 Preliminary Identification of Access Paths 21
2.2.2.5 Correlation between Threat Conditions and Threat Scenarios 21
2.2.3 Level of Threat and Risk Assessment 24
2.2.3.1 Level of Threat and Likelihood 24
2.2.3.2 Threat Scenarios and Likelihood of Threat Condition 25
2.2.3.3 Risk Level Acceptability 26
2.3 Characterizing Security Measures 27

2.3.1 Characteristics of Security Architectures 27
2.3.2 Vulnerability Assessment and Classification 28
2.3.2.1 Assessment of System Design Vulnerabilities 28
2.3.2.2 Assessment of Test Results 28
2.3.2.3 Assessment of Well-Known Vulnerabilities 28
2.4 Security Logging and Alerts 29
2.5 Characterizing Security Effectiveness 30
2.5.1 Validation of Technical and Continuing Airworthiness Requirements for Effectiveness 31
2.5.2 Assurance Level for Effectiveness 31
2.5.3 Allocation of Assurance Levels for Layered Protection 32
2.6 Security Assurance 34
2.6.1.1 Qualification of Security Testing Tools 35
2.6.1.2 Anti-Malware Provisions 35
2.6.1.3 Functional Assurance 36
2.6.1.4 Secure Configuration Management, Integration, and Delivery 36
2.6.1.5 Linkage of Problem Reports to Vulnerability Assessment 36
2.6.1.6 Review of Derived Requirements 36
2.6.1.7 Source Code/Design Review 36
2.6.1.8 Independence in Reviews and Analyses 37
2.6.2 Use of Common Criteria to Evaluate Assurance Requirements 37
2.7 Recommended Resources 38
2.7.1 NIST SP 800-160 on Architecture Design 38
2.7.2 ITU-T X.1205/X.805 on Architecture Design and Network Security Domains 39

3 SPECIFIC METHODS 41

3.1 Threat Trees for Risk Assessment 41
3.1.1 Threat Tree Extract 44
3.2 Network-based Security Domains 49
3.2.1 Domains under ARINC 811 49
3.2.2 Security Domain Considerations 50
3.2.3 Technical Basis for Domain Control 52
3.2.4 Recommendations for Managing Residual Risks 56

4 MEMBERSHIP 57

APPENDIX A: REFERENCES **A-1**

APPENDIX B: ACRONYMS AND GLOSSARY **B-1**

B.1 Acronyms and Abbreviations B-1
B.2 Glossary B-2

TABLE OF FIGURES

Figure 2-1: Overview of AWSP Topics 5
Figure 2-2 : Nested Assets within Aircraft 8
Figure 2-3 : Nested Assets within System 8
Figure 2-4: Nested Security Environments 9
Figure 2-5: Dependencies between Nested Security Environments 9
Figure 2-6 Steps for Determining Security Perimeter 10
Figure 2-7: IFE Example- Steps for Determining Security Perimeter 11
Figure 2-8: IFE Example- Security Perimeter at Aircraft System Level 11
Figure 2-9: IFE Example- Security Perimeters at Lowest System Level 12
Figure 2-10 Single Stage Threat Scenario 17
Figure 2-11 Two Stage Threat Scenario 17
Figure 2-12 Simple Chain of Protection 18
Figure 2-13 Security Risk Assessment for Each Stage in Chain of Protection 18
Figure 2-14 Multi-stage attack on supporting assets 19
Figure 2-15 CoP with Tampering of Security Measure 20
Figure 3-1 Representation of Threat Scenario as Threat Tree 41
Figure 3-2 Extract of Threat Tree for Live Database Update 45
Figure 3-3 Extract of Threat Tree for Live Database Update (cont) 46
Figure 3-4 Domain Boundary Devices 51
Figure 3-5 Unsecured Security Domain 53
Figure 3-6 Intrinsic Security Domain 54
Figure 3-7 Enclaved Security Domain 55

TABLE OF TABLES

Table 1 Trustworthiness Levels 13
Table 2 Examples of Trustworthiness Standards 14
Table 3 Threat Condition Flight Safety Impact Classification 15
Table 4 Assets and Failure Condition Classes 22
Table 5 Assets and Threat Condition Classes 22
Table 6 Likelihood Definitions 25
Table 7 Threat Condition Components 26
Table 8 Risk Matrix 27
Table 9 Effectiveness Classifications of Assurance Level 32
Table 10 Minimum Assurance Levels for Layered Defense-in-Depth Architectures 33
Table 11 Allocating Assurance Levels to Development or Organizational Trustworthiness 33
Table 12 Layering Onboard and Organizational Assurances 34
Table 13 Alternate Common Criteria EAL Levels for System Level Assurance 38
Table 14 ITU-T X.1205 Cybersecurity technologies 40
Table 15 Threat Tree Events 42
Table 16 Event Values for Likelihood of Attack 43
Table 17 Event Values for Likelihood of Exposure 43
Table 18 Event Values for Failure in Effectiveness 43
Table 19 Event Values for Loss of Safety Margin 44
Table 20 Cutsets for Threat Tree Extract 47
Table 21 Cutsets for Threat Tree Extract 48

1 INTRODUCTION

This document is the product of the RTCA Special Committee SC216, titled “Aeronautical Systems Security” to provide additional guidance for applicants implementing an Airworthiness Security Process as specified in DO-326A/ED-202A to address information security for certification of aircraft and their systems.

1.1 Purpose

This document describes guidelines, methods and tools used in performing an airworthiness security process. The guidelines, methods and tools presented are not intended to be exhaustive and can be expected to be updated with additional methods and considerations, including those needed to meet evolving regulatory assumptions. Applicants can propose alternative practices for consideration by the authorities. Practices for airworthiness security are still undergoing evolution and refinement as new features are deployed and the security threat itself evolves.

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 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, and is derived from understood best practice.

1.2 Scope

Airworthiness security is the protection of the airworthiness of an aircraft from intentional unauthorized electronic interference. This includes the consequences of malware and forged data and of access of other systems to aircraft systems.

This guidance provides methods and considerations for securing airworthiness during the aircraft development life cycle from project initiation until the Aircraft Type Certificate is issued for the aircraft type design. It was developed in the context of DO-326A/ED-202A "Airworthiness Security Process Specification" which addresses type certification considerations during the first three life cycle stages of an aircraft type (Initiation, Development or Acquisition, and Implementation) and DO-355/ED-204, "Information Security Guidance for Continuing Airworthiness" which addresses airworthiness security for continued airworthiness.

It is intended to be used in conjunction with other applicable guidance material, including SAE ARP 4754A/ED-79A, SAE ARP 4761/ED-135, DO-178C/ED-12C, and DO-254/ED-80 and with the advisory material associated with FAA AC 25.1309-1A and EASA AMC 25.1309, in the context of part 25 for Transport Category Airplanes which include an approved passenger seating configuration of more than 19 passenger seats. This guidance is not intended for CFR parts 23, 27, 29, 33.28, and 35.15, normal, utility, acrobatic, and commuter category airplanes, normal category rotorcraft, transport category rotorcraft, engines, and propellers.

This document does not address:

a. Physical security or physical attacks on the aircraft (or ground element),

b. Airport, Airline or Air Traffic Service Provider security (e.g., access to airplanes, ground control facilities, data centers),

c. Communication, navigation, and surveillance services managed by national agencies or their international equivalents (e.g., GPS, SBAS, GBAS, ATC communications, ADS-B).