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

Airworthiness Security Methods and Considerations

RTCA DO-356A
June 21, 2018

Prepared by: SC-216
© 2018 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 jointly by Special Committee 216 (SC-216) and EUROCAE Working Group 72 (WG-72). It was approved by the RTCA Program Management Committee (PMC) on June 21, 2018 and by the EUROCAE Council on June 19, 2018.

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 Telecommunication 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 and several advisory circulars.

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…… 1
1.3 How to use this document 2
1.4 Conventions of This Document 3
1.5 Relationship to Other Documents 4
1.6 Definition of Terms and Acronyms 4
1.6.1 Acronyms……. 16

2 REGULATORY CONSIDERATIONS 23

2.1 Intentional Unauthorized Electronic Interaction 23
2.1.1 Intentional Unauthorized Electronic Interaction - Definition and Meaning 23
2.1.2 Intentional Unauthorized Electronic Interaction – Some Principles 24
2.1.3 Intentional Unauthorized Electronic Interaction – Some Examples 24
2.2 Asset Protection Scope 25
2.2.1 Determination of Hazard Classification considering safety effect caused by intentional unauthorized electronic interaction 26
2.2.2 Analyzing Potential Impact on Surrounding Systems 27
2.2.3 Summary of Asset Protection 28
2.3 Type Design Changes and STC Considerations 28
2.4 Acceptable Compliance Demonstration Evidence Considerations 29
2.4.1 Certification…… 30
2.5 Considerations for Continued Airworthiness Security 31
2.5.1 Vulnerability and Threat Management 32
2.6 Trust Considerations in the Security Environment 33
2.7 Risk Acceptability 34
2.7.1 Introduction……. 34
2.7.2 Criteria for Communicating and Accepting Risk 34
2.7.3 Risk Acceptability Statement 35
2.7.4 Regulatory View of Continued Level of Threat Protection 36
2.8 Considerations in the use of Commercial Off The Shelf (COTS) and Previously Certified Products……. 36
2.8.1 Use of Previously Certified Systems 37
2.8.2 Use of Commercial Hardware Parts 37
2.8.3 Use of Parts without Security Data 38

3 RISK ASSESSMENT 41

3.1 Security Scope…. 41

3.1.1 Asset Identification 42
3.1.2 Security Perimeter.. 43
3.1.3 Security Environment and Trust 44
3.1.4 Changes in the Security Environment 46
3.1.5 Considerations on Decomposition of Assets, Security Perimeter and Environment 46
3.2 Risk Assessment Method Framework 47
3.2.1 Core Principles for Risk Assessment Methodology 47
3.3 Threat Condition Identification and Effect Evaluation 49
3.3.1 Characterization of Threat Conditions and Their Effects 49
3.3.2 Relationship of Threat Conditions to Failure Conditions 51
3.3.3 Threat Condition and Severity Effects Evaluation Method 52
3.4 Threat Scenario Identification 55
3.4.1 Threat Scenario Structure 55
3.4.2 Threat Scenario Consistency and Completeness 59
3.5 Security Measure Characterization 60
3.5.1 Security Measure Common Mode Analysis 63
3.6 Level of Threat Evaluation 64
3.6.1 Relation of Effectiveness and Likelihood 64
3.6.2 Evaluation Criteria Considerations 64
3.6.3 Combined Protection Assessment 67
3.6.4 Risk Evaluation…. 70
3.7 Risk consistency check 71
3.8 Risk Assessment for Change Management 72
3.8.1 New Vulnerability in Design 72
3.8.2 New Vulnerability in a Security Measure 73
3.8.3 Architecture / Implementation Change 73
3.8.4 Functional Change. 74
3.9 Considerations on Comparability of Risk Assessments 74

4 SECURITY ASSURANCE 77

4.1 Security Specific Assurance 78
4.1.1 Security Risk Assessment Objectives 78
4.1.2 Vulnerability Identification Objectives 79
4.1.3 Security Refutation Objectives 79
4.1.4 Security Deployment Objectives 80
4.1.5 Continued Security Effectiveness Objectives 80
4.2 Security Development Assurance 80
4.2.1 Requirements Objectives 81
4.2.2 Design Objectives.. 82
4.2.3 Implementation Objectives 82
4.2.4 Security Verification Objectives 82
4.2.5 Security Planning Objectives 83
4.2.6 Security Configuration Management Objectives 83

4.2.7 Security Certification Liaison Objectives 85
4.2.8 Tool Security Objectives 86
4.3 Configuration Management Control Categories 87
4.4 Security Assurance Levels 88
4.4.1 Security Assurance Level Assignment 89
4.4.2 Security Assurance Level Assignment for Products Already Certified without Security Requirements 91

5 DEVELOPMENT OF SECURITY ARCHITECTURE AND MEASURES 93

5.1 Purposes of Architecture 93
5.2 Concepts and Characteristics of Security Architectures 93
5.3 Decomposition of Assets in a Security Architecture 95
5.3.1 Considerations on Security Assurance Allocation Within the Aircraft 98
5.4 Security Architecture considerations 99
5.5 Threat Scenarios and Defense-in-Depth 100
5.6 Security Architecture Principles at Aircraft Level 100
5.6.1 Principle 1 – Defense-in-Depth 101
5.6.2 Principle 2 – Integrity of Connected Equipment 102
5.6.3 Principle 3 – Continued Airworthiness 102
5.6.4 Principle 4 – Prevent Bypass of Security Barriers 102
5.6.5 Principle 5 – Keep Security Architectures as Simple as Possible 103
5.6.6 Principle 6 - Detection and Restoration 103
5.7 Security Architecture Principles at (Multi-)System Level 103
5.7.1 Principle 7 – Attack Path Refinement at System Level 103
5.7.2 Principle 8 – Consider Security Process Specifics 104
5.7.3 Principle 9 – Minimize External Interfaces 104
5.7.4 Principle 10 – Disable All Unused Interfaces 104
5.7.5 Principle 11 – Independence and isolation 105
5.8 Security Architecture at Item Level 105
5.8.1 Principle 12 – Ensure Proper Error Handling 105
5.8.2 Principle 13 – Least Privilege 106
5.8.3 Principle 14 – Control Access to Connections 106
5.9 Security Considerations in Aircraft Development 106
5.9.1 Reaction Time…… 106
5.9.2 Security in Service. 107
5.9.3 Verification, Validation and Refutation of Security Requirements 107
5.9.4 Fail Secure Considerations 107

6 SECURITY EVENT LOGGING 109

6.1 Security Logging and Notifications 109
6.1.1 Security Notifications 109
6.1.2 Security Logging… 109
6.2 Concept of Operations for Logging and Audit 110

6.2.1 Goals and Objectives of Security Event Logging 110
6.2.2 Strategies, Tactics, Policies, and Constraints Affecting the Security Events Logging 111
6.2.3 Allocation of Responsibility Among Stakeholders 112
6.2.4 Operational Process 113

7 MEMBERSHIP……..115

APPENDIX A SECURITY ASSURANCE OBJECTIVES A-1

A.1 Security Assurance Objectives A-1
A.1.1 Security Specific Assurance A-2
A.1.2 Security Development Assurance A-4

APPENDIX B SECURITY ASSURANCE GUIDANCE B-1

B.1 Security Assurance Relation to Other Development Assurance Standards B-1
B.1.1 Security Specific Assurance B-1
B.1.2 Security Development Assurance B-3
B.2 Security Assurance Activities B-6
B.2.1 Security Risk Assessment Activities B-6
B.2.2 Vulnerability Identification introduction B-8
B.2.3 Vulnerability Identification Activities B-10
B.2.4 Security Refutation Introduction B-11
B.2.5 Security Refutation Activities B-13
B.2.6 Security Deployment Activities B-14
B.2.7 Continued Security Effectiveness Activities B-16
B.2.8 Requirements Activities B-16
B.2.9 Design Activities… B-17
B.2.10 Implementation Activities B-18
B.2.11 Security Verification Activities B-19
B.2.12 Security Planning Activities B-20
B.2.13 Security Configuration Management Activities B-21
B.2.14 Security Certification Liaison Activities B-22
B.2.15 Tool Security Activities B-23

APPENDIX C PROCESS LOOKUP TABLE C-1

APPENDIX D COMMON METHOD EXAMPLES D-1

D.1 Security Perimeter Example D-1
D.2 Risk Management Example D-3
D.2.1 Example Context… D-3
D.2.2 Security Scope…… D-3
D.2.3 Risk Assessment Method Framework D-13
D.3 Aircraft Airworthiness Security Process Example D-19

D.3.1 Scope……. D-19
D.3.2 Document Description D-19
D.3.3 Aircraft Development Process D-19
D.3.4 Aircraft Introduction D-20
D.3.5 Aircraft Concept…. D-20
D.3.6 Aircraft Planning…. D-22
D.3.7 Aircraft Functions.. D-22
D.3.8 Aircraft Level Safety Assessment Process. D-29
D.3.9 Aircraft Security Scope Definition Based on Functions D-35
D.4 Aircraft Architecture D-52
D.4.1 Avionic System Architecture D-53

APPENDIX E SECURITY EFFECTIVENESS METHOD AND EXAMPLES E-1

E.1 Effectiveness Risk Assessment Method E-1
E.1.1 Effectiveness of Protection Scale E-2
E.1.2 Effectiveness Evaluation Order E-3
E.1.3 Effectiveness Evaluation Criteria E-3
E.1.4 Combined Effectiveness Assessment E-9
E.1.5 Effectiveness Evaluation E-10
E.2 Risk Assessment Examples E-14
E.2.1 Effectiveness of Protection Evaluation Example 1 E-14
E.2.2 Effectiveness of Protection Evaluation Example 2 E-15
E.2.3 Effectiveness of Protection Evaluation Example 3 E-19
E.2.4 Effectiveness of Protection Example 4 E-26
E.3 Threat Condition Evaluation Example Template E-38
E.4 Order of Evaluation E-39

APPENDIX F LEVEL OF THREAT LIKELIHOOD METHOD AND EXAMPLES..... F-1

F.1 Risk Scoring…… F-1
F.1.1 Severity, Threat, and Protection Scoring F-1
F.1.2 Risk Scoring……. F-4
F.1.3 Scoring Guidance…. F-5
F.1.4 Scoring A Linear Threat Scenario F-8
F.1.5 Illustration of Risk Scoring a Threat Scenario F-8
F.2 Threat Trees for Risk Assessment F-11
F.2.1 Basic Threat Tree…. F-11
F.3 Example Security Risk Assessment F-14
F.3.1 Security Scope…… F-14
F.3.2 Modeling the Security Architecture F-18
F.3.3 Summary of Conclusion F-57

APPENDIX G ALTERNATE METHOD USING STPA-SEC G-1

G.1 Aircraft Airworthiness Security Process Example using STPA-Sec G-1
G.1.1 Scope……..... G-1
G.1.2 Document description G-1
G.2 Background…… G-1
G.3 Use Systems Engineering and Control Theory Foundations..... G-4
G.3.1 System Purpose and Goal G-4
G.3.2 STPA-Sec Losses and Accidents G-4
G.3.3 STPA-SEC Hazard G-4
G.3.4 Asset…… G-5
G.4 Aircraft Security Scope Definition..... G-5
G.4.1 Security Environment G-5
G.4.2 Security Perimeter.. ..... G-6
G.5 Aircraft Security Risk Assessment..... G-7
G.5.1 Threat Condition and Threat Scenario Identification..... G-7

APPENDIX H CYBERSECURITY RISK ASSESSMENT METHODOLOGY H-1

H.1 Process Overview..... H-1
H.2 Methodology in Detail H-2
H.2.1 Ease-of-Execution..... H-2
H.2.2 Threat Condition Assessment H-3
H.2.3 Required Security Assurance Level (SAL)..... H-4
H.2.4 Initial Risk Determination H-4
H.2.5 Operator Guidance..... H-4
H.2.6 Residual Risk Determination H-4
H.3 Example put through Methodology - GPWS H-5
H.3.1 Ease-of-Execution Example H-5
H.3.2 Threat Condition Assessment Example H-7
H.3.3 Required Security Assurance Level (SAL) Example..... H-7
H.3.4 Initial Risk Determination Example H-8

APPENDIX I SECURITY ARCHITECTURE AND MEASURES..... I-1

I.1 Using Domains to Describe Security Architecture I-1
I.1.1 Domains under ARINC 811 and 664 Part 5 .....I-2
I.1.2 Network Security Domain Considerations I-3
I.1.3 Technical Basis for Network Security Domain Control I-5
I.2 Common Modes for Security Measures.....I-9
I.2.1 Example of an exhaustive table I-10

APPENDIX J REFERENCES J-1

APPENDIX K HISTORY OF THE ED-203A / DO-356A DOCUMENT K-1

IMPROVEMENT SUGGESTION FORM L-1

TABLE OF FIGURES

Figure 1-1: Scope of Airworthiness Security 2
Figure 2-1: Airworthiness Security Risk Management Framework 31
Figure 3-1: Security Scope Example 42
Figure 3-2: Security Risk Assessment 47
Figure 3-3: Example Threat Condition Identification and Evaluation Workflow 54
Figure 3-4: Threat Scenario Example 1 56
Figure 3-5: Threat Scenario Example 2 56
Figure 3-6: Threat Scenario Example 3 57
Figure 3-7: Threat Scenario Coverage 59
Figure 3-8: Combined Protection Evaluation Principles 69
Figure 3-9: Level of Threat Consistency Check 71
Figure 3-10: Example Consistency Check between Parent and Child Threat Scenarios 72
Figure 5-1: Nested Assets within Aircraft 95
Figure 5-2: Nested Assets within System 96
Figure 5-3: Nested Security Environments 97
Figure 5-4: Interfaces between Nested Security Environments 988
Figure 5-5: Composition vs Combination of Elements 988
Figure 6-1: Relation of Security Logging to Continuing Airworthiness 111
Figure D-1: IFE Example - Steps for determining Security Perimeter D-1
Figure D-2: IFE Example - Security Perimeter at Aircraft System Level D-2
Figure D-3: IFE Example - Security Perimeter at Lowest System Level D-2
Figure D-4: Example Context D-3
Figure D-5: Aircraft Security Scope D-4
Figure D-6: AMS Security Scope D-5
Figure D-7: AMS Security Perimeter D-9
Figure D-8: AMS Assets Hierarchy D-10
Figure D-9: One Stage Attack Paths D-16
Figure D-10: MultiStage Attack Paths D-17
Figure D-11: Aircraft and System Development Activities According to S-18 ..... D-19
Figure D-12: Aircraft User Interaction D-21
Figure D-13: Aircraft External Interfaces D-22
Figure D-14: Aircraft Functions Logical Interfaces D-25
Figure D-15: Aircraft Functions Logical Interfaces D-26
Figure D-16: Misuse Example D-41
Figure D-17: Aircraft Conceptual View D-52
Figure D-18: Aircraft Level Functions for Example Aircraft D-53
Figure D-19: Physical Aircraft Architecture Example D-54
Figure D-20: Logical Aircraft Architecture Example D-55

Figure D-21: Aircraft Architecture Example- Navigation Systems Ring Network Topology D-55
Figure D-22: Aircraft Architecture Example - Communication System Star network Topology D-56
Figure D-23: Aircraft Architecture Example - FMS/FMC D-57
Figure E-1: Security Measure Breakdown E-5
Figure E-2: Wireless System E-16
Figure E-3: Security Measures for Wireless System E-17
Figure E-4: Update of Security Measures for Wireless System E-18
Figure E-5: Threat Scenario TS1 ..... E-28
Figure E-6: Threat Scenario TS1-3 ..... E-29
Figure E-7: Threat Scenario TS1-4 ..... E-30
Figure E-8: Threat Scenario TS1-5a E-31
Figure E-9: Threat Scenario TS1-5b E-32
Figure E-10: Threat Scenario TS1-6 ..... E-34
Figure E-11: Threat Scenario TS1-7 ..... E-35
Figure E-12: Threat Scenario TS1-8 ..... E-36
Figure E-13: Evaluation Order Example 1 ..... E-39
Figure E-14: Evaluation Order Example 2 ..... E-39
Figure F-1: Diagram of Simple Network F-16
Figure F-2: Simple Network Security Architecture F-24
Figure F-3: Threat Tree (Page 1 of 15 figures) F-25
Figure F-4: Threat Tree (Page 2 of 15 figures) F-25
Figure F-5: Threat Tree (Page 3 of 15 figures) F-26
Figure F-6: Threat Tree (Page 4 of 15 figures) F-27
Figure F-7: Threat Tree (Page 5 of 15 figures) F-27
Figure F-8: Threat Tree (Page 6 of 15 figures) F-28
Figure F-9: Threat Tree (Page 7 of 15 figures) F-29
Figure F-10: Threat Tree (Page 8 of 15 figures) F-29
Figure F-11: Threat Tree (Page 9 of 15 figures) F-30
Figure F-12: Threat Tree (Page 10 of 15 figures) F-30
Figure F-13: Threat Tree (Page 11 of 15 figures) F-31
Figure F-14: Threat Tree (Page 12 of 15 figures) F-32
Figure F-15: Threat Tree (Page 13 of 15 figures) F-33
Figure F-16: Threat Tree (Page 14 of 15 figures) F-33
Figure F-17: Threat Tree (Page 15 of 15 figures) F-34
Figure G-1: Possible Causal Factors G-3
Figure G-2: Security Perimeter and Environment G-5
Figure G-3: Security Environment and Security Perimeter G-6
Figure G-4: Security Risk Assessment from DO-326A / ED-202A G-7
Figure H-1: Process Overview H-2
Figure H-2: GPWS Architecture H-5

Figure I-1: Domain Perimeter Devices....I-4
Figure I-2: Unsecured Security Domain....I-6
Figure I-3: Intrinsic Security Domain....I-7
Figure I-4: Enclaved Security Domain....I-8

TABLE OF TABLES

Table 1-1: Glossary 4
Table 1-2: Acronyms used in this Document 16
Table 2-1: Risk Management Stages and Criteria for Communicating Risk 35
Table 2-2: Airworthiness Risk Acceptability Matrix 36
Table 3-1: Threat Condition Flight Safety Effect Classification 50
Table 3-2: Security Measure Characteristics 61
Table 3-3: Level of Threat Scale 70
Table 4-1: Control Category Definition 87
Table 4-2: Control Category Assignment 88
Table 4-3: Security Assurance Level Definition 89
Table 4-4: Security Assurance Relation to Threat Condition Severity 90
Table A-1: Security Specific Assurance Objectives Allocation Table A-2
Table A-2: Security Development Assurance Objectives Allocation Table A-4
Table B-1: Traceability Security Specific Assurance Objectives B-1
Table B-2: Traceability Security Development Assurance Objectives B-3
Table B-3: Security Risk Assessment Activities B-6
Table B-4: Vulnerability Identification Activities B-10
Table B-5: Security Refutation Activities B-13
Table B-6: Security Deployment Activities B-14
Table B-7: Continued Security Effectiveness Activities B-16
Table B-8: Requirements Activities B-17
Table B-9: Design Activities B-18
Table B-10: Implementation Activities B-18
Table B-11: Security Verification Activities B-19
Table B-12: Security Planning Activities B-20
Table B-13: Security Configuration Management Activities B-21
Table B-14: Security Certification Liaison Activities B-22
Table B-15: Tool Security Activities B-23
Table C-1: Process Activity References C-1
Table C-2: List of DO-326A / ED-202A References C-2
Table D-1: Security Survey D-7
Table D-2: Identified Information Assets D-8
Table D-3: Applicable Types of Attacks D-12

Table D-4: Threat Condition Identification and Evaluation D-14
Table D-5: Threat Scenario Identification D-17
Table D-6: Aircraft Function D-23
Table D-7: Aircraft Functions Interfaces D-26
Table D-8: Data Flows D-28
Table D-9: Phase of Flight D-30
Table D-10: Failure Condition Hazard Class Definition D-30
Table D-11: Partial AFHA D-31
Table D-12: Sequence of Security Scope Activities D-36
Table D-13: Aircraft Supporting Assets D-37
Table D-14: Aircraft Security Measures D-38
Table D-15: Security Perimeter Procedure D-38
Table D-16: Interfaces Summary D-38
Table D-17: Example of Threats D-40
Table D-18: Threats by Asset Types D-42
Table D-19: Generic Vulnerabilities and Enabled Threats D-43
Table D-20: Threat Classification D-45
Table D-21: Trustworthiness Assumptions D-49
Table E-1: Effectiveness Level Definition E-1
Table E-2: Relation of Effectiveness and Level of Threat Scales E-2
Table E-3: Effectiveness Calculation Scale E-2
Table E-4: Preparation Means E-5
Table E-5: Windows of Opportunity E-6
Table E-6: Execution Means E-7
Table E-7: Maximum Effectiveness per Security Measure Type E-8
Table E-8: Maximum Combined Effectiveness E-10
Table E-9: Effectiveness of Protection Evaluation Table E-11
Table E-10: Identified Security Measures E-14
Table E-11: Combined Effect Assessment E-14
Table E-12: Example Threat Scenario 1 ..... E-15
Table E-13: Example Threat Scenario 2 ..... E-15
Table E-14: Security measures Assessment E-17
Table E-15: Effectiveness of Protection Level E-18
Table E-16: Update of Security Measure Assessment E-19
Table E-17: Update of Effectiveness of Protection Level E-19
Table E-18: Identified Security Measures E-20
Table E-19: Combined Effectiveness Assessment E-20
Table E-20: Evaluation of TS.1 and TS.2 ..... E-21
Table E-21: Updated List of Security Measures E-22
Table E-22: Updated Combined Effect Assessment E-23

Table E-23: Updated Evaluation of TS.1 ..... E-24
Table E-24: Updated Evaluation of TS.2 ..... E-24
Table E-25: Updated Evaluation of TS.3 ..... E-25
Table E-26: Updated Evaluation of TS.4 ..... E-25
Table E-27: Identified Security Measures E-30
Table E-28: Level of Threat Security Measures E-31
Table E-29: Identified Security Measures E-32
Table E-30: Identified Security Measures E-33
Table E-31: Combined Effectiveness Assessment E-33
Table E-32: Identified Security Measures E-34
Table E-33: Additional Combined Effectiveness Assessment E-35
Table E-34: Level of Threat Evaluation E-36
Table E-35: Acceptability of Risk Treatment Options E-37
Table E-36: Example Threat Condition Evaluation Template E-38
Table F-1: Severity Score Calibration F-1
Table F-2: Likelihood Score Calibration F-2
Table F-3: Level of Protection Calibration F-4
Table F-4: Risk Scores F-5
Table F-5: A Few Examples of Level of Threat Assignment F-6
Table F-6: Example of Capping Level of Protection Based on Vulnerability Rating F-7
Table F-7: Example of Capping Level of Protection Based on Assurance F-7
Table F-8: Threat Tree Events F-13
Table F-9: Measure of Threat F-14
Table F-10: Measure of Failure of Protection F-14
Table F-11: Simple Network Attacker Populations F-19
Table F-12: Simple Network Information Assets F-19
Table F-13: Simple Network Access Conditions F-19
Table F-14: Simple Network Threat Conditions F-21
Table F-15: Simple Network Security Measures F-22
Table F-16: Simple Network Vulnerability Classes F-23
Table F-17: Simple Network Threat Scenarios F-36
Table F-18: Simple Network Vulnerability Classes, Original LOP F-56
Table F-19: Simple Network Security Measures LOP F-57
Table F-20: Threat Scenarios with Highest Risk Scores F-58
Table G-1: Relation Between DO-326A / ED-202A Activities and STPA-Sec Steps G-2
Table G-2: Losses and Accidents Considered During Analysis G-4
Table G-3: Hazards G-4
Table G-4: Assumptions G-5
Table G-5: Control Actions and Feedbacks G-6
Table G-6: Identify Types of Unsecure Control (STPA-Sec Activity 2) G-8

Table G-7: Identify Causes of Unsecure Control and Eliminate or Control Them (STPA-Sec Activity 3) G-8
Table G-8: Threat Condition and Threat Scenario Identification..... G-10
Table H-1: Ease-of-Execution Definition H-2
Table H-2: Attacks Step Evaluation……. H-7
Table H-3: Ease-of-Executive Evaluation…….H-7
Table H-4: Security Assurance Level Assignment……H-8
Table H-5: Risk Determination……..H-8
Table H-6: Risk Acceptance Determination……..H-8
Table I-1: Example of a General Common Mode Types, Sources and Failures/Errors List.....…I-10

1 INTRODUCTION

This document is the 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 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.

1.1 Purpose

This document provides a set of methods and guidelines that may be used within the airworthiness security process defined in RTCA DO-326A / EUROCAE ED-202A, *Airworthiness Security Process Specification*. It is recognized that alternative methods to the processes described or referenced in this document may be available to an organization desiring to obtain certification.

This document does not provide guidelines concerning the structure of an individual organization or how the responsibilities for certification activities are divided. No such guidance should be inferred from the descriptions provided.

1.2 Scope

Airworthiness security is the protection of the airworthiness of an aircraft from intentional unauthorized electronic interaction. Existing safety processes have not had to consider intentional disruption.

Intentional unauthorized electronic interaction (also known as "unauthorized interaction" within the scope of this document) is defined as a circumstance or event with the potential to affect the aircraft due to human action resulting from unauthorized access, use, disclosure, denial, disruption, modification, or destruction of information and/or aircraft system interfaces. This includes the consequences of malware and forged data and the effects of external systems on aircraft systems but does not include physical attacks or electromagnetic disturbance.

This document provides methods and considerations for showing compliance for airworthiness security during the aircraft design and development life cycle. It was developed as a companion document to DO-326A / ED-202A which addresses security process aspects of aircraft certification. Guidance for airworthiness security during the complete aircraft life cycle is provided through the additional companion document RTCA DO-355 / EUROCAE ED-204, *Information Security Guidance for Continuing Airworthiness*, which addresses the airworthiness security for the continued airworthiness outside of design and development.

This document assumes that its readers are knowledgeable of applicable guidance material. The guidelines in this document were developed in the context of 14 CFR Part 25 and EASA CS-25. It may be applicable to other regulations, such as Parts 23, 27, 29, 33, and 35 (CS-23, CS-27, CS-29, CS-E, CS-P). It does not assume that applicants are in compliance with the guidance materials referenced in this document but does assume that the applicant has in place a comprehensive flight safety program as part of development and continued airworthiness which is compliant with regulation, and an applicant may tailor this guidance appropriately in negotiation with regulatory authorities.

The methods and considerations of this document provide guidance for accomplishing the airworthiness security process activities identified in DO-326A / ED-202A. See section 1.3

 © 2018 RTCA, Inc.

for a discussion of the guidance provided. Appendix C lists the DO-326A / ED-202A activities and references that are addressed in this version of the document.

The scope of this document is limited to protection of airworthiness security - the aspects of information security which could compromise the safety of the aircraft. The safety aspects of physical attacks - known as Aviation Security - are out of scope of the document and can be found in documents such as ICAO Convention Annex 17. Any use of this document for aspects of information security outside of airworthiness security - e.g. security of business interests - is considered out of scope of this document. Figure 1-1 illustrates these uses of security.

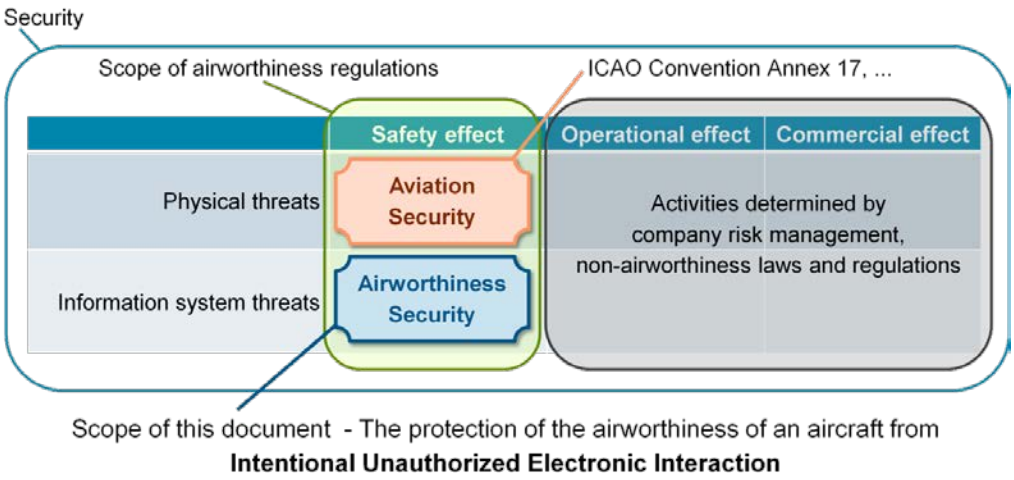


Figure 1-1: Scope of Airworthiness Security

1.3 How to use this document

Readers should be aware that this document provides additional guidance for the airworthiness security process specified in DO-326A / ED-202A.

This document contains material intended to be used as Guidance Material, Acceptable Means of Compliance and considerations for industry use. The Guidance Material provides explanatory information on the rule and helps applicant understand the background of the Acceptable Means of Compliance in this document as well as support for any Alternate Means of Compliance an applicant may choose. This document also contains considerations for industry that are not to be interpreted as regulatory material.

This document is organized into six chapters plus appendices. The chapters can be used in concert with each other or stand alone.

- Chapter 1 introduces the document and defines the terms and acronyms. Readers are expected to be familiar with the definitions in the glossary in order to correctly interpret the body of this document.
- Chapter 2 discusses specific regulatory considerations and provides the Guidance Material. The Acceptable Means of Compliance provides one – but not the only – means of complying with the regulations.
- Chapter 3 discusses Security Risk Assessments and provides the Acceptable Means of Compliance.

- Chapter 4 discusses Security Assurance and provides the Acceptable Means of Compliance.
- Chapter 5 discusses the Development of Security Architectures and Measures and provides considerations for industry use.
- Chapter 6, section 6.1 discusses Security Event Logging and provides the Acceptable Means of Compliance.
- Chapter 6, section 6.2 discusses Security Event Logging and provides considerations for industry use.
- Chapter 7, contains the list of WG-72 / SC-216 members.

Appendix A is a normative part of this document because it complements the security assurance level definition in chapter 4. Appendices B through L contain informative material that may aid in the comprehension and usage of this document.

- Appendix A lists security assurance objectives and their applicability to security assurance levels and provides the Acceptable Means of Compliance.
- Appendix B provides traceability of security assurance objectives to other standards. Appendix B also details security assurance activities for all security assurance objectives.
- Appendix C links DO-326A / ED-202A process activities to the sections of this document.
- Appendix D contains examples of common activities in the full airworthiness security process.
- Appendix E contains risk assessment methods and examples using the effectiveness approach for section 3.6 as well as security architecture examples.
- Appendix F contains risk assessment methods and examples using the likelihood approach for section 3.6.
- Appendix G contains an alternative method for risk assessments based on STPA-Sec.
- Appendix H contains risk assessment methods and examples using another cybersecurity risk assessment approach for section 3.6.
- Appendix I contains additional information concerning security architecture and measures.
- Appendix J contains the external references used in this document.
- Appendix K contains a history of this document.

1.4 Conventions of This Document

This document addresses audiences of two possible backgrounds, airworthiness certification and information security management. This results in difficulties in terminology, as the two audiences share technical terms that have different meanings and usages. Since the primary impact of this document is within the area of airworthiness certification, the following practice has been followed:

- If a term with a suitable definition is available from the area of airworthiness certification, that term is used.
- If there is no suitable term in airworthiness certification, but there is a term with a suitable definition in information security management and use of that term will not conflict with a similar-sounding term in airworthiness certification, that term is used.

 © 2018 RTCA, Inc.