

RTCA, Inc.
1828 L Street, NW, Suite 805
Washington, DC 20036-5133 USA

Airworthiness Security Process Specification

RTCA/DO-326
December 8, 2010

Prepared by: SC-216
© 2010, 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 RTCA Special Committee 216 (SC-216) and EUROCAE Working Group 72 and approved by RTCA Program Management Committee (PMC) on December 8, 2010. It was approved by the Council of EUROCAE on December 2, 2010

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.

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 may be used in conjunction with other existing guidance, such as FAA AC25.1309, EASA AMC25.1309, ED-79/SAE ARP 4754, DO-178B/ED12B, and DO-254/ED-80 for the mitigation of security issues related to aircraft systems. This document adds data requirements and compliance objectives, as organized by generic activities for aircraft development and certification, to handle the information security threat to aircraft systems and is intended to be used in conjunction with other applicable guidance material. This guidance excludes:

- 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 (for example: GPS, SBAS, GBAS, ATC data communications, ADS-B).
- d. Aircraft other than large commercial transports. This guidance may be applicable in other contexts, if tailored in a manner appropriate to the operating environments of other types of aircraft. The intent of SC-216 is to provide guidance in future versions of this document that extend to other types of aircraft and are appropriate to their operating environment.

This is the first of a series of documents on Aeronautical Systems Security that together will address information security for the overall Aeronautical Information System Security (AISS) of airborne systems with related ground systems and environment. This document addresses only Aircraft Type Certification and is not yet widely implemented, but is derived from understood best practice. Because of the impending introduction of aircraft with significant security-related features, it has been released in advance of the other documents in this series to address immediate industry concerns and to establish feedback on its implementation challenges.

Special caution is recommended when applying this guidance to developments or operations already in place. This guidance is designed to be implemented across the full life cycle of an aircraft from design, through operations, to disposal. As such, it should first be applied to the design stage before its use in subsequent stages of the life cycle. If objectives are applied to aircraft which were not subject to these objectives during all stages, then it should be borne in mind that some aspects will not be applicable. These aspects should be described and dealt with separately.

Compliance with the guidance of this document is shown by demonstrating that the complying process will provide necessary certification data and that the complying process will satisfy the compliance objectives. The data requirements and compliance objectives are organized by generic activities for aircraft development and certification (see [Figure 1-3](#) or Chapter 3) which generate and manage the data and establish the compliance objectives. If the data produced and managed by a process and its activities are found to satisfy the compliance objectives, then that process has complied with the guidance of this document.

The compliance objectives specify the required characteristics of the data associated with each generic activity at the end of the program, and are not intended to represent completion criteria for each activity during the program. Nonetheless, they have been defined so that establishing tentative compliance during the preliminary phases based on the incomplete knowledge available will be timely, prudent and useful to the final success of the development process.

Compliance may be accomplished through a blended process that integrates safety with security, or through a segregated process that defines a differentiated but interacting security process from the safety process. However, both processes must be sufficiently integrated to maintain overall consistency and the outputs of the safety process must include all hazards identified as a result of the security analyses.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

1	INTRODUCTION	1
1.1	PURPOSE.....	1
1.2	SCOPE.....	1
1.3	COMPLIANCE AND USE OF THIS DOCUMENT	4
1.4	AIRWORTHINESS SAFETY PROCESS OVERVIEW.....	4
1.5	AIRWORTHINESS SECURITY PROCESS OVERVIEW	5
1.6	CONVENTIONS OF THIS DOCUMENT	5
2	AIRCRAFT AND SYSTEM SECURITY RISK MANAGEMENT.....	9
2.1	OVERVIEW	9
2.2	IDENTIFYING THE SECURITY PERIMETER.....	11
2.2.1	SECURITY PERIMETER WITH ASSETS, AND EXTERNAL DEPENDENCIES	11
2.2.2	SECURITY PERIMETER FOR AIRCRAFT	11
2.2.3	SECURITY PERIMETER FOR SYSTEMS AND ITEMS	12
2.3	IDENTIFYING THE THREATS	12
2.3.1	THREAT SOURCE PROFILES.....	12
2.3.2	THREAT CONDITIONS.....	12
2.3.3	INTERACTION WITH FUNCTIONAL HAZARD ASSESSMENT.....	13
2.3.4	THREAT IDENTIFICATION FOR SYSTEMS AND ITEMS	13
2.4	DEVELOPING THE SECURITY ARCHITECTURE.....	13
2.4.1	VULNERABILITIES	14
2.4.2	THREAT SCENARIOS.....	15
2.4.3	VALIDATION OF THE SOUNDNESS OF THE SECURITY ARCHITECTURE	16
2.4.4	SECURITY ARCHITECTURE FOR SYSTEMS AND ITEMS	17
2.5	ASSESSING THE PRELIMINARY SECURITY RISK	17
2.5.1	IMPACT.....	17
2.5.2	LIKELIHOOD.....	18
2.5.3	RISK LEVEL ACCEPTABILITY	19
2.5.4	PRELIMINARY SECURITY RISK ASSESSMENT FOR AIRCRAFT AND SYSTEMS	20
2.5.5	PRELIMINARY SECURITY ASSESSMENT FOR ITEMS	20
2.6	ADDRESSING THE SECURITY RISK	21
2.6.1	SECURITY COUNTERMEASURES.....	23
2.6.2	SECURITY EFFECTIVENESS	23
2.6.3	SECURITY LEVELS	23
2.6.4	CONSIDERATIONS IN DEFENSE-IN-DEPTH AND LAYERED ARCHITECTURE	24
2.6.5	SAFETY AND SECURITY REQUIREMENTS CONSISTENCY	25
2.7	ASSURING THE IMPLEMENTATION	25
2.7.1	SECURITY OBJECTIVES	26
2.7.2	SECURITY REQUIREMENTS FOR SECURITY LEVEL	26

2.7.2.1	Strength of Mechanism Requirements	27
2.7.2.2	Implementation Assurance Requirements	27
2.7.3	DEVELOPMENT AND PRODUCTION ENVIRONMENT SECURITY	27
2.7.4	SECURITY VERIFICATION AND TESTING	28
2.7.4.1	Security Verification	28
2.7.4.2	Security Testing— Intended Function, Robustness, and Vulnerability	28
2.7.4.3	Security Test Planning.....	29
2.7.4.4	Vulnerability Testing.....	30
2.8	ENSURING SECURITY OF THE FINAL PRODUCT	31
2.8.1	FINAL SECURITY RISK ASSESSMENT FOR AIRCRAFT AND SYSTEMS.....	32
2.8.2	FINAL SECURITY ASSESSMENT FOR ITEMS	32
2.8.3	USER GUIDANCE AND EXTERNAL AGREEMENTS FOR SYSTEMS AND ITEMS.....	32
2.8.4	CONTINUING AIRWORTHINESS FOR AIRCRAFT.....	32
2.8.4.1	Operator Guidance.....	33
2.8.4.2	External Agreements for Aircraft	33
3	SPECIFICATION FOR AIRWORTHINESS SECURITY PROCESS	35
3.1	CERTIFICATION CONSIDERATIONS	36
3.1.1	CHOOSING AIRWORTHINESS SECURITY CERTIFICATION DATA AND ACTIVITIES	36
3.1.2	APPLICATION TO DESIGN CHANGES	38
3.1.2.1	Design Change for Aircraft after Certification with Airworthiness Security	38
3.1.2.2	Design Change for Legacy Aircraft.....	38
3.1.3	USE OF PREVIOUSLY DEVELOPED SYSTEMS AND ITEMS	39
3.2	CERTIFICATION PLAN PROCESSES	39
3.2.1	CERTIFICATION PLANNING SECURITY DATA (CPSD)	39
3.3	PRELIMINARY AIRCRAFT PROCESSES	40
3.3.1	AIRCRAFT SECURITY PERIMETER (ASP)	40
3.3.2	AIRCRAFT THREAT IDENTIFICATION (ATI)	41
3.3.3	PRELIMINARY AIRCRAFT SECURITY RISK ASSESSMENT (PASRA).....	42
3.3.4	AIRCRAFT SECURITY ARCHITECTURE AND COUNTERMEASURES (ASAC)	43
3.4	PRELIMINARY SYSTEM PROCESSES	44
3.4.1	SYSTEM SECURITY PERIMETER (SSP)	44
3.4.2	SYSTEM THREAT IDENTIFICATION (STI)	45
3.4.3	PRELIMINARY SYSTEM SECURITY RISK ASSESSMENT (PSSRA).....	46
3.4.4	SYSTEM SECURITY ARCHITECTURE AND COUNTERMEASURES (SSAC)	47
3.5	ITEM PROCESSES	47
3.5.1	ITEM SECURITY PERIMETER (ISP)	47
3.5.2	ITEM THREAT IDENTIFICATION (ITI)	48
3.5.3	PRELIMINARY ITEM SECURITY ASSESSMENT (PISA)	49
3.5.4	ITEM SECURITY VERIFICATION (ISV).....	49
3.5.5	FINAL ITEM SECURITY ASSESSMENT (FISA).....	50
3.6	FINAL SYSTEM PROCESSES	51
3.6.1	SYSTEM SECURITY INTEGRATION AND IMPLEMENTATION (SSII).....	51

3.6.2	SYSTEM SECURITY VERIFICATION (SSV).....	51
3.6.3	FINAL SYSTEM SECURITY RISK ASSESSMENT (FSSRA)	52
3.7	FINAL AIRCRAFT PROCESSES.....	53
3.7.1	AIRCRAFT SECURITY INTEGRATION AND IMPLEMENTATION (ASII).....	53
3.7.2	AIRCRAFT SECURITY VERIFICATION (ASV).....	54
3.7.3	FINAL AIRCRAFT SECURITY RISK ASSESSMENT (FASRA)	55
3.8	CERTIFICATION COMPLIANCE DEMONSTRATION	55
3.8.1	COMPLIANCE DEMONSTRATION FOR AIRWORTHINESS SECURITY (CDAWS).....	55
3.8.2	INDEPENDENCE AND COMPLIANCE DEMONSTRATION	56
3.9	DEVELOPMENT LIFE CYCLE DATA	56
3.9.1	CONFIGURATION MANAGEMENT.....	57
3.9.2	AIRWORTHINESS SECURITY DEVELOPMENT LIFE CYCLE DATA.....	58
3.9.2.1	Additional Validation Study Requirements and Results, Aircraft/System/Item	58
3.9.2.2	Compliance Demonstration for Airworthiness Security, Aircraft.....	58
3.9.2.3	External Dependencies, Aircraft/System/Item	59
3.9.2.4	Final Security Assessment, Item	59
3.9.2.5	Final Security Risk Assessment, Aircraft/System	59
3.9.2.6	Implementation Assurance Requirements, Aircraft/System/Item	59
3.9.2.7	Negotiated Security Certification Data, Aircraft.....	59
3.9.2.8	Operator Guidance and Aircraft External Agreements	59
3.9.2.9	Preliminary Security Assessment, Item.....	60
3.9.2.10	Preliminary Security Risk Assessment, Aircraft/System	60
3.9.2.11	Security Architecture, Aircraft/System	60
3.9.2.12	Security Certification Planning Data, Aircraft/System/Item	60
3.9.2.13	Security Levels, Item.....	60
3.9.2.14	Security Level, System.....	60
3.9.2.15	Security Objectives, Aircraft/System/Item.....	60
3.9.2.16	Security Perimeter with Assets, Aircraft/System/Item.....	61
3.9.2.17	Security Requirements, Aircraft/System/Item.....	61
3.9.2.18	Security Verification and Test Results and Analysis, Aircraft/System/Item	61
3.9.2.19	Strength of Mechanism Requirements, Aircraft/System/Item.....	61
3.9.2.20	Threat Condition Identification and Classification, Aircraft/System	61
3.9.2.21	Threat Source Profiles, Aircraft/System/Item	61
3.9.2.22	User Guidance and External Agreements, System/Item	61
3.9.2.23	Vulnerability Dossier, Aircraft/System/Item.....	62
3.9.3	STANDARD AIRWORTHINESS LIFE CYCLE DATA.....	62
3.9.3.1	Aircraft Certification Data.....	62
3.9.3.2	Functional and Operational Description, Aircraft/System	62
3.9.3.3	Functional Hazard Assessment, Aircraft	62
3.9.3.4	Implementation, Aircraft/System/Item.....	62
3.9.3.5	Instructions for Continued Airworthiness	62
3.9.3.6	Maintenance Procedures.....	62

3.9.3.7	Operating Procedures	62
3.9.3.8	Preliminary Safety Assessment, System	63
3.9.3.9	Safety Architecture, Aircraft/System	63
3.9.3.10	Safety Assessment, Aircraft/System.....	63
3.9.3.11	Verification and Test Plan, Aircraft/System/Item	63
APPENDIX A: REFERENCES		65
APPENDIX B: RATIONALE AND COMPLIANCE WITH OTHER STANDARDS.....		67
B.1 RATIONALE FOR AN AIRWORTHINESS SECURITY PROCESS		67
B.2 COMPLIANCE WITH ISO/IEC 27005.....		68
B.3 CONSISTENCY WITH SAE ARP 4754		71
APPENDIX C: ACRONYMS AND GLOSSARY		77
C.1 ACRONYMS AND ABBREVIATIONS		77
C.2 GLOSSARY		78
APPENDIX D: COMMITTEE MEMBERSHIP.....		85
APPENDIX E IMPROVEMENT SUGGESTION FORM		89

LIST OF FIGURES

<u>FIGURE 1-1</u> DOCUMENT SCOPE FOR AIRWORTHINESS SECURITY.....	3
<u>FIGURE 1-2</u> GENERIC ACTIVITIES FOR AIRWORTHINESS SAFETY PROCESS FOR AIRCRAFT DEVELOPMENT AND CERTIFICATION	6
<u>FIGURE 1-3</u> GENERIC AIRWORTHINESS SECURITY ACTIVITIES DURING AIRCRAFT DEVELOPMENT AND CERTIFICATION	7
<u>FIGURE 2-1</u> AIRWORTHINESS SECURITY RISK MANAGEMENT	10
<u>FIGURE 2-2</u> REPRESENTATION OF THREAT SCENARIO AS THREAT TREE	21
<u>FIGURE 2-3</u> SECURITY ASSESSMENT CONCEPTS	22
<u>FIGURE 2-4</u> ESTABLISHING SECURITY COUNTERMEASURES	23
<u>FIGURE 2-5</u> ESTABLISHING SECURITY OBJECTIVES FOR SYSTEMS.....	26
<u>FIGURE 2-6</u> SECURITY TESTING ACTIVITIES	29
<u>FIGURE 3-1</u> ISO 27005 ISRM FRAMEWORK DURING PRELIMINARY DESIGN	68
<u>FIGURE 3-2</u> ISO 27005 ISRM FRAMEWORK DURING FINAL INTEGRATION.....	69
<u>FIGURE 3-3</u> AIRCRAFT DEVELOPMENT PROCESSES	71
<u>FIGURE 3-4</u> AWS ACTIVITIES DURING PRELIMINARY DESIGN	72
<u>FIGURE 3-5</u> AWS ACTIVITIES DURING FINAL INTEGRATION.....	73

LIST OF TABLES

TABLE 2-1 DEVELOPMENT LEVELS	10
TABLE 2-2 CLASSES OF VULNERABILITIES	15
TABLE 2-3 ELEMENTS OF A THREAT SCENARIO	15
TABLE 2-4 SOUNDNESS PROPERTIES OF ARCHITECTURE	16
TABLE 2-5 THREAT CONDITION SAFETY IMPACT CLASSIFICATION	17
TABLE 2-6 THREAT SCENARIO LIKELIHOOD CLASSIFICATION.....	18
TABLE 2-7 RISK MATRIX	20
TABLE 2-8 SECURITY LEVEL CLASSIFICATIONS	24
TABLE 2-9 MINIMUM SECURITY LEVEL FOR LAYERED DEFENSE-IN-DEPTH ARCHITECTURES	25
TABLE 2-10 STANDARD DEVELOPMENT VERIFICATION PLAN TESTING ELEMENTS	29
TABLE 2-11 ADDITIONAL VERIFICATION PLAN SECURITY TESTING ELEMENTS.....	30
TABLE 3-1 EXAMPLES OF ACTIVITY ASSOCIATIONS FOR AIRCRAFT DEVELOPMENT	35
TABLE 3-2 DETERMINING AIRWORTHINESS SECURITY CERTIFICATION ACTIVITIES	36
TABLE 3-3 EXAMPLE DATA ASSOCIATIONS FOR CONFIGURATION MANAGEMENT	57
TABLE 3-4 INFORMATION SECURITY RISK MANAGEMENT FRAMEWORK OUTPUTS	69
TABLE 3-5 INTERACTING WITH THE SAFETY PROCESS OF SAE ARP 4754	74

THIS PAGE INTENTIONALLY LEFT BLANK

1 INTRODUCTION

This document is the joint product of two special industry committees: the EUROCAE Working Group WG-72, titled “Aeronautical Systems Security” and the RTCA Special Committee SC216, 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 SC216 was formed more specifically to address information security for certification of aircraft and its systems. Both committees agreed that with the guidance provided by this document and its fellows, the airworthiness of future aircraft will be enabled despite the potential for intentional or unintentional misuse of aircraft information systems.

Credible examples of potential misuse include:

- The potential for malware to infect an aircraft system.
- The potential for an attacker to use onboard wireless to access aircraft system interfaces.
- The potential for denial of service of wireless interfaces.
- The potential for denial of service of safety critical systems.
- The potential for misuse of personal devices that access aircraft systems.
- The potential for misuse of off-board network connections to access aircraft system interfaces.

The potential for misuse increases with the additional interconnectivity of current and future aircraft information systems. This document provides information security guidance within the aircraft development and certification process to ensure that the effects of such misuses are limited to acceptable behaviors with no detrimental impact on the safety of the aircraft. The necessary additional guidance is presented in this document as the Airworthiness Security Process Specification.

1.1 Purpose

This document is a resource for certification authorities and the aviation industry for developing or modifying aircraft systems and equipment when there is the possibility of adversely affecting the safety of flight from human action involving information or information system interfaces. It specifies data requirements and compliance objectives of an airworthiness security process, presented using a set of representative generic activities for managing data and objectives.

An industry standard for methods and instructions for data, activities and compliance objectives defined in this document can be found in ED-203/DO-YYY "Airworthiness Security Methodology and Instructions" (in preparation).

1.2 Scope

Airworthiness security is the protection of the airworthiness of an aircraft from the information security threat: an adverse effect on safety due to human action (intentional or unintentional) using access, use, disclosure, denial, disruption, modification, or destruction of data and/or data interfaces. This includes the consequences of malware and forged data and access by other systems to aircraft systems.

Aircraft certification is the process whereby an applicant requests approval from a regulatory authority (referred to hereafter as the certification authority) for aircraft manufacturing, either as supplements or as amendments to aircraft. Aircraft certification processes use recommended standards, guidance, tests, methods, and procedures to establish certification approval. Additional