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

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

LIST OF FIGURES

LIST OF TABLES

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