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

Airworthiness Security Process Specification

RTCA DO-326A
August 06, 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 August 06, 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

The guidance of this document adds to current guidance for aircraft certification to handle the threat of intentional unauthorized electronic interaction to aircraft safety. It adds data requirements and compliance objectives, as organized by generic activities for aircraft development and certification, to handle the threat of unauthorized interaction to aircraft safety and 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 Aircraft 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, GBAS, GBAS, ATC communications, ADS-B).

For a discussion of the history of DO-326A and the differences from the original DO-326, please see Appendix E: Background of the DO-326 Document.

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.

A companion document will provide a set of methods and guidelines that may be used within the airworthiness security process defined in DO-326A. The provision of methods in that document is not intended to mean that will be the only acceptable set of methods; there will be other equally valid methods. Applicants and authorities should consider those methods, and alternative practices if and when they are proposed.

Compliance may be accomplished through a differentiated security process that interacts with the safety process. To sustain this principle, overall consistency between both processes should be maintained, by ensuring that the security process considers the outputs of the safety assessment process. As an alternative, when considered practicable, compliance may be accomplished through a blended process - documented by the applicant - that would integrate safety and security, including suitable evidences that security and safety requirements are met.

This Page Intentionally Left Blank

TABLE OF CONTENTS

TABLE OF FIGURES

TABLE OF TABLES

The Page Intentionally Left Blank

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 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 the guidance provided by this document and its companion documents constitute an acceptable means to address the increasing potential for intentional unauthorized electronic interaction with aircraft information systems.

This document provides guidance by defining activities for supplementing the aircraft development and certification process to demonstrate that the effects on the safety of the aircraft of such unlawful interferences are confined within acceptable levels. As intentional unauthorized electronic interaction includes intentional origin, this document covers some aspects of sabotage (in contrast to e.g., the exclusion of sabotage in AMJ 25.1309 5(j)).

For a discussion of the history of DO-326A/ED-202A and the differences from the original DO-326/ED-202, please see Appendix E: Background of the DO-326/ ED-202 Document.

1.1 Purpose

This document is a resource for Airworthiness Authorities (AA) and the aviation industry for certification when the development or modification of aircraft systems and the effects of intentional unauthorized electronic interaction can affect aircraft safety. It deals with the activities that need to be performed in support of the airworthiness process when it comes to the threat of intentional unauthorized electronic interaction. The companion document DO-355/ED-204 "Information Security Guidance for Continuing Airworthiness" addresses airworthiness security for continued airworthiness.

A companion document will provide a set of methods and guidelines that may be used within the airworthiness security process defined in DO-326A. The provision of methods in that document is not intended to mean that will be the only acceptable set of methods; there will be other equally valid methods. Applicants and authorities should consider those methods, and alternative practices if and when they are proposed.

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.

1.2 Scope

The guidance of this document adds to current guidance for aircraft certification to handle the threat of intentional unauthorized electronic interaction to aircraft safety. It adds data requirements and compliance objectives, as organized by generic activities for aircraft development and certification, to handle the threat of unauthorized interaction to aircraft safety and is intended to be used in conjunction with other applicable guidance material, including SAE ARP 4754A/ED-79A, DO-178C/ED-12C, and DO-254/ED-80