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

Process Standard for Security Certification and Declaration of ATM ANS Ground Systems

RTCA DO-393
June 23, 2023

Prepared by: SC-216
© 2022 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 by Special Committee 216 (SC-216) Aeronautical Information Systems Security jointly with EUROCAE Working Group 72 (WG-72) and approved by the RTCA Program Management Committee (PMC) on June 23, 2022and the EUROCAE Council on July 13, 2022.

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 Standards Development Organization 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 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 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 Scope And Purpose Of This Document 1
1.2 Background 2
1.3 Users Of This Document 4
1.4 Guidance In Defining Relevant Systems Within Scope Of Information Security Certification 5
1.5 Assets And Resources That Are Outside The Scope Of Information Security Declaration 6
1.6 How To Use This Document 6
1.7 Structure Of This Document 7
1.8 Relationship To Other Documents 7
1.9 Overview and Summary of Evolving Aviation Information Security Regulations 8
1.10 Summary of Requirement Groups of Part-Is 8

2 ATM/ANS GROUND SYSTEMS INFORMATION SECURITY PROCESS 11

2.1 Process Overview 11
2.2 Plan Certification/Declaration 13
2.2.1 Define Planning Scope For Certification 14
2.2.2 Define Certification/Declaration Objectives 15
2.2.3 Create, Coordinate And Approve Project Plan 16
2.3 Organization Level Information Security Objectives 17
2.3.1 Organization Information Security Policies Objectives 18
2.3.2 Personnel and Resources 18
2.3.3 Record Keeping 18
2.3.4 Internal Reporting 18
2.3.5 Response to Findings 18
2.3.6 Changes to the Organization 18
2.3.7 Information Security Management Manual 19
2.3.8 Maturity and Continuous Improvement 19
2.3.9 Management of Contracted Services 19
2.4 Manage Risk 19
2.4.1 Gathering Risk Management Resources 21
2.4.2 Assessing Information Security Risk 22
2.4.3 Categorize Resources 30
2.4.4 Analyse Information Security Risk 31
2.4.5 Ground System Risk Acceptance 36
2.4.6 Risk Comparability 38
2.4.7 Evaluate Information Security Risk 38
2.4.8 Treat Information Security Risk 38
2.4.9 Implement Controls 42
2.4.10 Consult On Risk 42
2.5 Information Security Incident Monitoring And Reporting 43
2.6 Set Claims And Collect Evidence 43
2.6.1 Formulate claims 45
2.6.2 Extract Relevant Evidence 46
2.6.3 Apply Access Policies 47
2.7 Verify Compliance 47

2.7.1 Self Assessment Compliance 48
2.7.2 Format and Send Evidence 49
2.7.3 Compliance Assessment by the Authority 49

3 SUPPORTING CONSIDERATIONS 51

3.1 Information Security Solutions Design Activities 51
3.1.1 Information Security Modelling 51
3.1.2 Information Security Layer-1: Perimeter Defence Information Security Systems 52
3.1.3 Information Security Layer-2: Operating Systems (OS) and Application Servers Information Security Systems 52
3.1.4 Information Security Layer-3: Host Protection 52
3.1.5 Information Security Layer-4: Data/Information Protection 52
3.2 Relationship With the Information Security Product Development Lifecycle 53
3.2.1 Information Security Effectiveness 54
3.2.2 Continued Information Security Effectiveness 55
3.2.3 Overview of Established Assurance Methods 55
3.2.4 Information Security Requirements Traceability 56
3.2.5 Functional Versus Assurance Requirements 56
3.2.6 Information Security Requirements Validation 57
3.2.7 Information Security Solutions Verification 57
3.2.8 Commercial Off The Shelf (COTS) Information Security Assurance 58
3.2.9 Information Security Evidence 58
3.2.10 Information Security Assessments 59
3.2.11 Information Security Assurance For System Operators 59
3.2.12 Reuse Of Common Criteria 60
3.2.13 Reuse Of ISO/IEC 27001 Certifications 61
3.2.14 Reuse Of Other Standards 61
3.3 ATM Information Security And Safety Relationship 61
3.3.1 Introduction 61
3.3.2 Process Interactions 62
3.3.3 Recommendations 63

APPENDIX A COLLABORATION NEED BETWEEN SAFETY AND INFORMATION SECURITY A-1

A.1 Introduction A-1
A.2 Aviation Information Security Reference Documents A-2

APPENDIX B DEFINITIONS B-1

APPENDIX C ACRONYMS AND ABBREVIATIONS C-1

APPENDIX D REFERENCES D-1

APPENDIX E WG-72 AND SC-216 MEMBERSHIP E-5

TABLE OF FIGURES

Figure 2-1: Certification / Declaration Organization Process 12
Figure 2-2: Plan Certification / Declaration Overview 14
Figure 2-3: Risk Management Process Overview 21
Figure 2-4: Assssing Risk Process Overview 23
Figure 2-5: Defining Information Security Scope 25
Figure 2-6: ATM/ANS Ground System Information Security Scope 27
Figure 2-7: Generic Likelihood Formula 35
Figure 2-8: Risk Treatment Process Overview 40
Figure 2-9: Formulate Claims And Collect Evidence Overview 45
Figure 2-10: Verify Compliance Process Overview 48
Figure 3-1: Relationship With The Secure Product Development Lifecycle Diagram 54
Figure 3-2: Process Interactions 63

TABLE OF TABLES

Table 1-1*:* EUROCAE and RTCA Relevant Documents 8
Table 1-2*:* Overview of Aviation Cyber Security Regulation Categories 9
Table 2-1*:* Define Scope For Plan 15
Table 2-2*:* Process to Establish Certification Objectives 15
Table 2-3: Process to Establish Project Plan 16
Table 2-4: Process for Coordination of Project Plan 17
Table 2-5: Process for Project Plan Approval 17
Table 2-6: Pre-Risk Assessment Materials Checklist Guidance 22
Table 2-7: Scope Risk Assessment 24
Table 2-8: Information Security Threat Safety Impact Criteria for Ground Systems 31
Table 2-9: Information Security Threat Impact Criteria for Organization Non-Safety Ground Systems or Safety Related Assessment Utilizing the Safety Support Assessment Under EU 2017/373 33
Table 2-10: Ground System Safety Criteria for Likelihood 36
Table 2-11: Likelihood Criteria for Ground Non-Safety Risk 36
Table 2-12: Risk Acceptance Matrix for Ground System Risk With a Safety Impact 37
Table 2-13: Risk Acceptance Matrix for Ground Systems and Safety Support Assessment 38
Table 2-14: Treat Information Security Risk Process Overview 39
Table 2-15: Risk Treatment Acceptance Process Overview 42
Table 2-16: Risk Treatment Implement Controls Process Overview 42
Table 2-17: Safety Risk Consultation And Coordination Process Overview 43
Table 2-18: Set Claims And Evidence Process Steps Overview 44
Table 2-19: Process Overview Formulate Claims 46
Table 2-20: Overview Of Process For Relevant Evidence 46
Table 2-21: Overview Of Apply Policies To Information Security Evidence 47
Table 2-22: Self Assessment Compliance Process Overview 48
Table 2-23: Process Overview for Evidence 49
Table 2-24: Process Overview for Authority Compliance Assessment 49

Table A-1: Aviation Information Security Documents……..A-2
Table B-1: List Of Definitions……B-1
Table C-1: List Of Acronyms…….C-1
Table D-1: List Of Standards……..D-1

1 INTRODUCTION

This process standard is the product of the EUROCAE WG-72 and RTCA SC-216, titled "Aeronautical Information Systems Information security". WG-72/RTCA SC-216 was formed to address information security for the overall Aeronautical Information System Security (AISS) of organizations that operate, manage or maintain Air Traffic Management (ATM) and Air Navigation Systems (ANS) ground systems and environments or systems that support ground-ground and ground-air communications and information exchange.

The European Aviation Regulation for the information security of ATM/ANS ground/ground-air systems, and the organizations that provide, product, manage, operate, subscribe or use ATM/ANS data are currently evolving to meet the current and future needs of aviation. Information security management is a must for organizations that are providers of ATM/ANS who need to address risks with a potential impact on aviation safety, operational delivery, economic concerns and others.

The information contained within this document (ED-205A/DO-393) will guide organizations and ensure the ATM/ANS ground and ground-air systems they will manage, operate, maintain, or provide are secure.

1.1 Scope And Purpose Of This Document

This document will guide an organization that manages and operates ATM/ANS ground-to-ground and ground-to-air systems and services in becoming approved for operations by a Civil Aviation Appropriate Authority (AA).

It's important to understand that the regulator and the new EASA information security rule known as Part IS (Opinion published 03/2021) focuses on providing requirements for an organization to implement. It's expected that organizations will further develop more internal policies and guidance for lower level systems on the appropriate internal methods each organization will implement to meet these new rules. This document is intended to be organization level guidance only on implementing these new rules.

ED-205A/DO-393 was developed to guide organizations in its implementation of a information security framework that is consistent with aviation regulations EU 2017/373 and will be subject to Part IS (Opinion published 03/2021) for information security that would allow the local Civil Aviation Appropriate Authority its ability and attest that organizations and the systems, services and other capabilities that have an impact on aviation safety are compliant with aviation regulations standards for information security. This document will provide answers to the following:

- What level of protection does an ATM/ANS ground system include to mitigate unauthorized interaction?
- Will the organisation's implemented information security framework applied to the ATM/ANS ground and ground-air systems not be compromised when the unauthorized interaction originates from the aircraft or other ground systems?
- What is the criteria and standard for risk acceptance unique to ground and ground-air ATM/ANS systems (safety and non-safety)?
- What is the acceptable level of information security assurance that is consistent with evolving aviation information security regulation?
- What are the methods for evaluation that can be utilized as part of the organization's declaration that provides a validation of the organization's implemented framework and maturity level?

 © 2022 RTCA, Inc.