

ED-204A

INFORMATION SECURITY GUIDANCE FOR CONTINUING AIRWORTHINESS

LEGAL NOTICE

This document is the exclusive intellectual and commercial property of EUROCAE. It is presently commercialised by EUROCAE. This electronic copy is delivered to your company/organisation for internal use exclusively. In no case it may be re-sold, hired, lent or exchanged outside your company. It may not be reproduced, in whole or in parts, without prior written permission by EUROCAE.

09/2020

SUPERSEDES ED-204

FOREWORD

1. This document was prepared jointly by EUROCAE Working Group 72 “Aeronautical System Security” and RTCA Special Committee 216 “Aeronautical System Security” and was approved by the Council of EUROCAE on 10 September 2020.
2. This document supersedes ED-204 Information Security Guidance for Continuing Airworthiness (June 2014).
As compared with the previous version, the main changes are listed in a revision history table in [APPENDIX F](#).
3. This document is technically identical to RTCA DO-355A Information Security Guidance for Continuing Airworthiness. Coordination has been achieved with RTCA SC-216 “Aeronautical System Security”.
4. EUROCAE, an international non-profit organisation, is the European leader in the development of worldwide recognised standards for aviation. This is achieved by utilising the expertise from our members and stakeholders across the global aviation community.
5. EUROCAE standards are developed following an open, transparent and consensus-based process, governed by process and quality management principles, which are clearly documented and is in line with the World Trade Organisation (WTO) Technical Barriers to Trade (TBT) Agreement, Annex 3 “Code of Good Practice for the Preparation, Adoption and Application of Standards”.
6. EUROCAE standards and other deliverables are recommendations and best industry practices. EUROCAE is not an official body of the European governments. EUROCAE standards are intended to complement and support the regulatory and certification framework.
7. Whilst efforts are made during the standards-development process to avoid the inclusion of proprietary information and material, some of the elements of this document may be the subject of patent, copyright or other proprietary rights. EUROCAE shall not be held responsible for identifying any such rights. Trade names and similar terms used within this document do not constitute an endorsement by EUROCAE thereof.
8. Copies of this document may be obtained from:

EUROCAE

9 – 23 rue Paul Lafargue
93200 Saint-Denis
France

Telephone: +33 1 49 46 19 65

Email: eurocae@eurocae.net

Website: www.eurocae.net

TABLE OF CONTENTS

CHAPTER 1	INTRODUCTION	1
1.1	PURPOSE	1
1.2	SCOPE	2
1.3	HOW TO USE THIS DOCUMENT	4
1.4	CONVENTIONS OF THIS DOCUMENT	4
1.5	RELATIONSHIP TO OTHER DOCUMENTS.....	5
1.6	GENERAL CONSIDERATIONS	5
1.6.1	DESIGN APPROVAL HOLDER (DAH).....	5
1.6.2	INSTRUCTIONS FOR CONTINUED AIRWORTHINESS (ICA)	5
1.6.3	CONTRACTED MAINTENANCE AND SERVICE PROVIDERS	6
CHAPTER 2	AIRBORNE SOFTWARE.....	7
2.1	GENERAL	7
2.2	OPERATIONAL SECURITY MEASURES.....	9
2.2.1	RECEPTION	9
2.2.2	CREATION/MODIFICATION	9
2.2.3	STORAGE	9
2.2.4	MEDIA.....	9
2.2.5	SOFTWARE TOOLS.....	10
2.2.6	SOFTWARE DISTRIBUTION	10
2.2.7	DATA LOADING	11
2.2.8	CONFIDENTIALITY	11
2.2.9	INCIDENT MANAGEMENT.....	11
2.3	DAH RESPONSIBILITIES	11
2.4	OPERATOR RESPONSIBILITIES	11
CHAPTER 3	AIRCRAFT COMPONENTS.....	12
3.1	GENERAL	12
3.2	OPERATIONAL SECURITY MEASURES.....	12
3.2.1	STORAGE	12
3.2.2	TRANSPORT	12
3.2.3	REPAIR	12
3.2.4	TOOLS	12
3.2.5	DECOMMISSIONING	12
3.2.6	INCIDENT MANAGEMENT.....	12
3.3	DAH RESPONSIBILITIES	13
3.4	OPERATOR RESPONSIBILITIES	13
CHAPTER 4	AIRCRAFT NETWORK ACCESS POINTS	14
4.1	GENERAL	14
4.2	OPERATIONAL SECURITY MEASURES.....	14
4.3	DAH RESPONSIBILITIES	14
4.4	OPERATOR RESPONSIBILITIES	15
CHAPTER 5	GROUND SUPPORT EQUIPMENT (GSE).....	16
5.1	GENERAL	16
5.2	OPERATIONAL SECURITY MEASURES.....	16
5.2.1	EQUIPMENT SECURITY AND OPERATIONS MANAGEMENT.....	16
5.2.2	ACCESS CONTROL	17
5.2.3	USAGE	17

	5.2.4	STORAGE	17
	5.2.5	INCIDENT MANAGEMENT.....	18
	5.2.6	LIFECYCLE MANAGEMENT	18
	5.2.7	DECOMMISSIONING	18
	5.3	DAH RESPONSIBILITIES	18
	5.4	OPERATOR RESPONSIBILITIES	18
CHAPTER 6		GROUND SUPPORT INFORMATION SYSTEMS.....	19
	6.1	GENERAL	19
	6.2	OPERATIONAL SECURITY MEASURES.....	19
	6.2.1	CONNECTION.....	19
	6.2.2	ACCESS CONTROL	19
	6.2.3	DATA EXCHANGE	20
	6.2.4	SYSTEM HARDENING OF GROUND SUPPORT INFORMATION SYSTEMS	20
	6.2.5	REPAIR	20
	6.2.6	DECOMMISSIONING	20
	6.2.7	INCIDENT MANAGEMENT.....	21
	6.2.8	LIFECYCLE MANAGEMENT	21
	6.3	DAH RESPONSIBILITIES	21
	6.4	OPERATOR RESPONSIBILITIES	21
CHAPTER 7		DIGITAL CERTIFICATES.....	22
	7.1	GENERAL	22
	7.2	OPERATIONAL SECURITY MEASURES.....	22
	7.3	DAH RESPONSIBILITIES	23
	7.4	OPERATOR RESPONSIBILITIES	23
CHAPTER 8		AIRCRAFT INFORMATION SECURITY INCIDENT MANAGEMENT	24
	8.1	GENERAL	24
	8.2	OPERATIONAL SECURITY MEASURES.....	24
	8.3	DAH RESPONSIBILITIES	24
	8.4	OPERATOR RESPONSIBILITIES	24
CHAPTER 9		OPERATOR AIRCRAFT INFORMATION SECURITY PROGRAM	25
	9.1	GENERAL	25
	9.1.1	AISP RELATION TO ISMS	25
	9.1.2	AISP RELATION TO SECURITY MANAGEMENT SYSTEM	26
	9.2	OPERATIONAL SECURITY MEASURES.....	27
	9.3	DAH RESPONSIBILITIES	27
	9.4	OPERATOR RESPONSIBILITIES	27
CHAPTER 10		OPERATOR ORGANIZATION RISK ASSESSMENT	28
	10.1	GENERAL	28
	10.2	OPERATIONAL SECURITY MEASURES.....	28
	10.3	DAH RESPONSIBILITIES	28
	10.4	OPERATOR RESPONSIBILITIES	28
CHAPTER 11		OPERATOR PERSONNEL ROLES AND RESPONSIBILITIES	30
	11.1	GENERAL	30
	11.2	OPERATIONAL SECURITY MEASURES.....	30
	11.2.1	SKILLS REQUIRED FOR OPERATOR INFORMATION SECURITY MANAGEMENT	30
	11.2.2	AIRCRAFT INFORMATION SECURITY SPECIALIST	30
	11.2.3	SPECIFIC TASK SKILLS	31
	11.3	DAH RESPONSIBILITIES	31

11.4	OPERATOR RESPONSIBILITIES	31
11.4.1	GENERAL	31
11.4.2	AIRCRAFT INFORMATION SECURITY CENTER	32
CHAPTER 12	OPERATOR PERSONNEL TRAINING	33
12.1	GENERAL	33
12.2	OPERATIONAL SECURITY MEASURES.....	33
12.2.1	TRAINING, AWARENESS, AND COMPETENCE	33
12.2.2	EDUCATION AND CERTIFICATION.....	33
12.3	DAH RESPONSIBILITIES	33
12.4	OPERATOR RESPONSIBILITIES	33
12.4.1	TRAINING ORGANIZATION	33
12.4.2	SCOPE OF TRAINING (GENERAL AND SPECIFIC)	33
12.4.3	GENERAL TRAINING	34
12.4.4	SPECIFIC TRAINING.....	35
12.4.5	TRAINING RECORDS.....	37
12.4.6	REGULATORY REQUIREMENTS FOR OPERATOR TRAINING	37
12.4.7	RECURRENT TRAINING	37
12.4.8	ORGANIZATIONAL COMMUNICATION REGARDING AIRCRAFT INFORMATION SECURITY	37
APPENDIX A	WG-72 MEMBERSHIP	38
APPENDIX B	AIRPLANE INFORMATION SECURITY PLAN (AISP)	43
APPENDIX C	GLOSSARY OF TERMS	49
APPENDIX D	ACRONYMS	53
APPENDIX E	REFERENCES	55
APPENDIX F	REVISION HISTORY - ED-204A.....	57
	IMPROVEMENT SUGGESTION FORM.....	58

LIST OF FIGURES

FIGURE 1:	AIRCRAFT INFORMATION SECURITY GUIDANCE	3
FIGURE 2:	A COMMON SECURITY METHODOLOGY FOR ELECTRONIC SOFTWARE DISTRIBUTION	8

CHAPTER 1

INTRODUCTION

This document is a 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 and the overall Aeronautical Information System Security (AISS) of airborne systems in conjunction with related ground systems and environment, while SC-216 was formed more specifically to address information security for certification and operation of aircraft and its systems. The guidance provided by this document is intended to constitute an Acceptable Means of Compliance for approving information security aspects of Continuing Airworthiness activities performed by Design Approval Holders and Operators.

This document provides guidance for the operation and maintenance of aircraft and for organizations and personnel involved in these tasks. It is intended to support the responsibilities of the Design Approval Holder (DAH) to obtain a valid airworthiness certificate and aircraft operators to maintain their aircraft to demonstrate that the effects on the safety of the aircraft of information security threats are confined within acceptable levels. As all information security threats may have an intentional origin, this document also covers Intentional Unauthorized Electronic Interaction (IUEI).

1.1

PURPOSE

This document is a resource for civil aviation authorities and the aviation industry when the operation and maintenance of aircraft and the effects of information security threats can affect aircraft safety. It deals with the activities that need to be performed in operation and maintenance of the aircraft related to information security threats.

This document gives also guidance that is related to operational and commercial effects (i.e. guidance that exceeds the safety-only effects).

ED-204A / DO-355A is a companion document to ED-202A / DO-326A "Airworthiness Security Process Specification" and ED-203A / DO-356A "Airworthiness Security Methods and Considerations" that support security in the development and modification part of the airworthiness process.

NOTE: *This document was developed in the European context of the European Aviation Safety Agency (EASA) Certification Specification CS-25 "Large Aeroplanes" and the United States context of Title 14 Code of Federal Regulations (14CFR) Part 25 "Transport Category Aircraft". Tailoring of this guidance may be used in other regulatory contexts including but not limited to CS-23, CS-27, CS-29, CS-E, CS-P, Part 23, Part 27, Part 29, Part 33, and Part 35.*

The most comprehensive possible area of the application of this guidance is deemed to be Large Transport Aircraft programs. However, this document does not make any assumptions about and is without prejudice to its applicability.

NOTE: *The measures proposed in this document may be subject to commercial terms between DAHs and operators. It is recommended that DAHs incorporate these elements into their commercial offers, especially for service and support related topics.*

1.2

SCOPE

ED-202A / DO-326A and ED-203A / DO-356A provide guidance in addressing airworthiness security during the aircraft product life cycle from project initiation until the aircraft Type Certificate (Amended Type Certificate, Supplemental Type Certificate and Amended Supplemental Type Certificate) is issued for the aircraft type design. In addition, it includes the handover of information about the Type Design that is necessary to ensure continuing airworthiness with respect to possible information security threats.

ED-204A / DO-355A (this document) provides guidance for the following stages of the product life cycle: operation, support, maintenance, administration, and decommissioning.

Where an organization subcontracts any activities in these stages, the organization retains the responsibility for aircraft information security (for contracted maintenance providers, refer to section 1.6.3).

A forthcoming document titled “Guidance on Information Security Event Management” (ISEM) will be jointly published by EUROCAE and RTCA. This document will provide guidance for managing security incidents and events that affect aircraft safety and it will support the existing safety event management guidance. It will provide guidance for processes, assessment and disposition, data exchanges, reporting, and other concerns that need to be performed in response to information security events.

Topics in the scope of Type Certification activities that are related to operation and maintenance of the aircraft such as Instructions for Continued Airworthiness (ICA) and security guidance documents are introduced in ED-202A / DO-326A and detailed in ED- 204A / DO-355A. In such cases ED-202A / DO-326A provides references to ED- 204A / DO-355A.

This document addresses information security risks only. The security measures to mitigate these risks are not limited to technical security measures; they may also be operational or management security measures.

Apart from the classical Instructions for Continued Airworthiness that are directly related to aircraft parts and systems, this document also provides guidance on Ground Support Equipment and Ground Support Information Systems that are related to the security of aircraft information systems and data networks as illustrated in [FIGURE 1](#). Only Airborne software that can have effect on aircraft safety are in the scope of this document

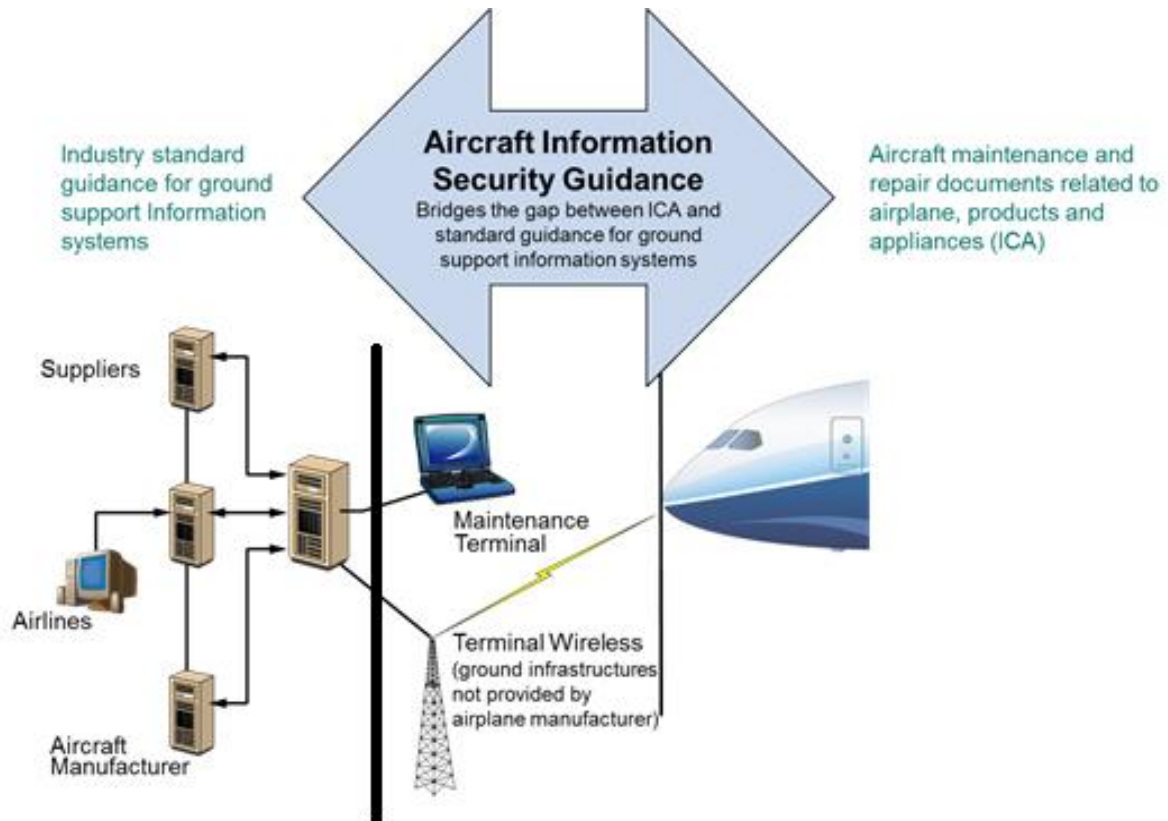


FIGURE 1: AIRCRAFT INFORMATION SECURITY GUIDANCE

NOTE: *The material in subsequent sections is only applicable if the aircraft and the operator use the features described.*

1.3 HOW TO USE THIS DOCUMENT

This document contains material intended to be used as Guidance Material and Acceptable Means of Compliance. The Guidance Material provides explanatory information and helps the applicant understand how to satisfy the objectives described in the Acceptable Means of Compliance in this document. Chapters X.1 and X.2 provide the Guidance Material whereas chapters X.3 and X.4 may be used as an Acceptable Means of Compliance.

This document is organized in 12 chapters plus informative appendices.

- Chapter 1 introduces the document.

The remainder of this document is organized into the following chapters and appendices. The substructure of these chapters is harmonized as follows:

- Chapter X.1 gives **General** information to introduce and define the topic
- Chapter X.2 gives an overview of what Operational Security Measures can be taken to manage the topic
- Chapter X.3 lists the Design Approval Holder (DAH) Responsibilities
- Chapter X.4 lists the Operator Responsibilities

The following topics are addressed:

- Chapter 2 Airborne Software
- Chapter 3 Aircraft Components
- Chapter 4 Aircraft Network Access Points
- Chapter 5 Ground Support Equipment
- Chapter 6 Ground Support Information Systems
- Chapter 7 Digital Certificates
- Chapter 8 Aircraft Information Security Incident Management
- Chapter 9 Operator Aircraft Information Security Program
- Chapter 10 Operator Organization Risk Assessment
- Chapter 11 Operator Personnel Roles and Responsibilities
- Chapter 12 Operator Personnel Training
- Appendix A lists all members of the working groups that have been involved during the creation of this document.
- Appendix B contains an example Airplane Information Security Plan
- Appendix C contains an informal Glossary of Terms.
- Appendix D contains a list of acronyms.
- Appendix E contains a list of cited and relevant documents. This list is neither exhaustive nor does it characterize any of the documents therein to be applicable. However, these documents constitute a solid starting point when addressing the subject matter.
- Appendix F contains a revision history table

1.4 CONVENTIONS OF THIS DOCUMENT

Within this document, “should” is used for recommendations, “may” and “need not” are used for permission, “can” and “might not” are used for possibility, “cannot” is used for impossibility and “will” is used for an expectation arising from activities satisfying objectives from a referenced standard or regulation. The use of “must” and “shall” is avoided. Other terms that are not defined in APPENDIX B are intended to have their common dictionary meaning. This document recognizes that the guidance herein is not mandated by law, but represents a consensus of the aviation community. It also recognizes that alternative methods to the ones described herein may be available to the applicant. For these reasons, the use of words such as “shall” and “must” is avoided.

1.5 RELATIONSHIP TO OTHER DOCUMENTS

Any mention of other documents is for information only. Thus, it is expected that the cited documents are often used in the development and airworthiness certification of aircraft. A list of cited documents can be found in APPENDIX E

REFERENCES.

1.6 GENERAL CONSIDERATIONS

1.6.1 Design Approval Holder (DAH)

A Design Approval Holder (DAH) is the holder of a type certificate, a Parts Manufacturer Approval (PMA) or a Technical Standard Order (TSO) authorization or the licensee of a Type Certificate (TC) or Supplemental Type Certificate (STC).

NOTE: *All design approval holders must (source FAA):*

- *Report failures, malfunctions, and defects*
- *Make Instruction for Continued Airworthiness (including changes) available to each aircraft, aircraft engine or propeller owner*
- *Satisfy Additional Obligations for: Parts Manufacturer Approval Holder, Technical Standard Order.*

1.6.2 Instructions for Continued Airworthiness (ICA)

Instructions for Continued Airworthiness are the instructions and information that are necessary for the continued airworthiness of the aircraft, engine, propeller, parts and appliances, which are required in accordance with the applicable Certification Basis or Standard to be developed and/or referenced by the Design Approval Holder.

ICAs are not limited to the maintenance of the aircraft; they can also be operational instructions.

Specifically for maintenance, the regulatory requirements for “Instructions for Continued Airworthiness Responsibilities, Requirements, and Contents” can be found in documents provided by civil aviation regulatory systems. For example:

- EASA
 - EU 748/2012 21.A.61
 - CS 25.1529 Instructions for Continued Airworthiness
 - CS 25, Book 1, Appendix H
- FAA
 - 14 CFR Part 21.50 – Instructions for continued airworthiness and manufacturer's maintenance manuals having airworthiness limitations sections.
 - 14 CFR Part 25.1529 – Instructions for Continued Airworthiness
 - 14 CFR Appendix H to Part 25 – Instructions for Continued Airworthiness (25.1529 directs the reader to Appendix H)
- TCCA
 - CAR 521.368 Instructions for Continuing Airworthiness
 - AWM Chapter 525.1529 Instructions for Continuing Airworthiness
 - AWM Chapter 525.1529 Appendix H

The term “Instructions for Continued Airworthiness” is defined and used in a very specific way within the applicable civil aviation regulatory systems. For the definition of the term ICA, refer to the glossary. Design Approval Holders negotiate the specific content of ICA packages with the regulatory authorities. For example within the FAA system, some ICA documents are approved by the Aircraft Certification Office, but all are submitted to the FAA Aircraft Evaluation Group for acceptance or approval prior to delivery of each aircraft to an operator.

The clear intent of ICA is to provide instructions for maintenance of the aircraft, to ensure that those instructions are available within the operator's system and to ensure that the instructions are used by technicians who maintain the operator's aircraft.

NOTE: *Whenever DAH applicants use commercial parts they can refer to the guidance in FAA AC 21-45 para.5.B Commercial Parts to satisfy the regulatory requirements of 14 CFR part 21 section 21.50c.*

1.6.2.1 ICA Related to Aircraft Information Security

ICA are written to allow maintenance technicians to perform their aircraft maintenance tasks and direct them to raise items of security concern to the appropriate area of the operator's organization. It is assumed that personnel implementing ICA are not information technology (IT) security specialists.

In addition to ICA, operators may also have extensive processes, tools, facilities and information technology systems that support aircraft maintenance. As shown in FIGURE 1, DAHs provide additional non-ICA guidance to support the security of Ground Support Equipment and Ground Support Information Systems whenever they contribute to information security of the aircraft.

1.6.2.2 Differences Between ICA and Non-ICA

To summarize the difference between ICA and non-ICA operational instructions/documentation:

- ICA
 - Any required maintenance activity affecting airworthiness and safety is to be covered by an ICA.
 - ICA provide documentation of methods, inspections, processes, and procedures.
 - ICA examples: Aircraft Maintenance Manual (AMM), Maintenance Review Board Report (MRBR), Fault Isolation Manual (FIM), Trouble Shooting Manual (TSM), Airworthiness Limitation Section (ALS).
 - ICA are required to maintain the continued airworthiness of the aircraft.
- Non-ICA
 - Aircraft or ground operations affecting operation (availability, commercial aspects).
 - Off-aircraft maintenance (e.g. Shop Maintenance) is not covered by ICA.
 - Non-ICA are recommended, but not required to maintain the continuous airworthiness of the aircraft.

1.6.3 **Contracted Maintenance and Service Providers**

Whenever there is an arrangement between an operator and a third party such as a Maintenance Repair and Overhaul organization (MRO) or an IT service provider, it is the responsibility of the operator to ensure that this third party complies with the operator's aircraft information security requirements.

CHAPTER 2

AIRBORNE SOFTWARE

2.1 GENERAL

The objective of this section is to give guidance to ensure the authenticity and integrity of airborne software is maintained during its reception, creation, modification, storage and distribution on the ground. As deemed necessary by the DAH, confidentiality throughout the supply chain may be used to avoid reverse engineering.

Developing a Supplier Controlled Software (SCS) is part of the type design and not part of continued airworthiness. However, lifecycle security considerations of airborne software are considered.

The term airborne software as used in this document refers to all software that is carried aboard an Aircraft certified system. This includes binary applications as well as databases, firmware (including configuration of FPGAs (Field Programmable Gate Arrays) and other complex electronic hardware), and configuration files. This document addresses only airborne software that can have effect on aircraft safety.

New generation aircraft come with a large number of airborne software parts with most of them delivered in an electronic form. Operators use software tools to verify the integrity and authenticity of airborne software. Operators can deliver the software to the aircraft through several connectivity means (e.g. wired, wireless, USB-key). Operators need to ensure that the airborne software delivered to the aircraft is authorized while maintaining its integrity and authenticity. Ensuring confidentiality of software during the entire software management process may help prevent unauthorized access and reverse engineering.

For legacy aircraft, the number of airborne software parts may be lower and the variety of connectivity means may be less. Nevertheless, integrity and authenticity need to be ensured for aircraft safety. Confidentiality aspects also need to be considered to avoid reverse engineering when relevant. If technical security measures are not possible, compensating operational and management security measures can be implemented.

Regardless of the aircraft type, operators are in transition from media-based airborne software distribution that depends on technical security measures to electronic airborne software distribution. The electronic distribution of software requires ground systems and processes that support information security.

Electronic airborne software distribution or Electronic Distribution of Software (EDS) is the process of moving software and data from one location to another location without the use of portable electronic media such as magnetic disks, optical disks, or flash drives. This classification of software distribution can make use of any data connectivity model such as wide area networks, local area networks, proprietary networks, and direct links. The connectivity method used within these models can be wired or wireless.

A common security methodology for electronic airborne software distribution is as follows.

- For electronic software distribution, integrity and authenticity are implemented by using a means of attaching one or more cryptographic signatures to the files that use a public/private key encryption method. If required, the entire software data payload may be encrypted using a public/private key method.
- Before sending a software package, a digital signature can be associated with this software package. This digital signature can only be created by the sender using its private key. The sender needs to share the associated public key. The signature is created using the contents of software, the sender's identification information, and other related information. The recipient has the public key required to verify that the software data came from the identified sender and that nothing in the data has been altered in any way.
- Additionally, if confidentiality needs to be maintained as directed by the DAH, the sender and receiver can select and implement appropriate methods so only the

recipient can use the software package or access data within it. Encrypting a payload is one common means of ensuring confidentiality.

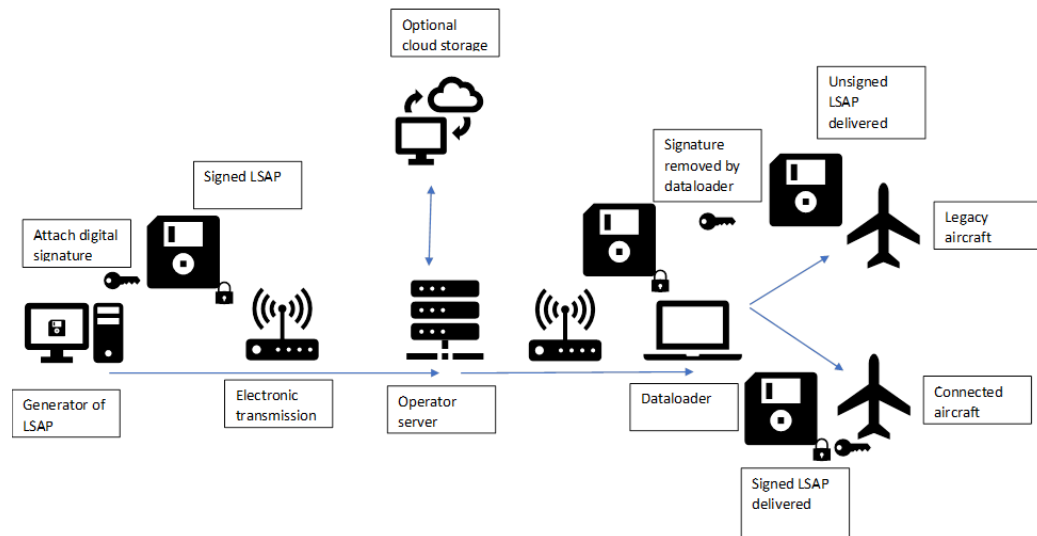


FIGURE 2: A COMMON SECURITY METHODOLOGY FOR ELECTRONIC SOFTWARE DISTRIBUTION

Refer to ARINC 667 and ARINC 827 for specific information regarding electronic distribution of airborne software.

Refer to CHAPTER 7 for specific information regarding public/private keys and the handling and management of digital certificates.

Media-based airborne software distribution uses portable electronic media. Media such as magnetic and optical disks as well as flash memory and similar media containing software and data can have a physical label attached that indicates the content information of the media.

A common security methodology for distribution of software stored on portable physical media is as follows.

- For media-based distribution, physical security is implemented by having trusted people in a physically secure environment with proper credentials prepare, label, package, and send physical media to the intended recipient.
- The media is received at the intended recipient location, checked, and processed by trusted people with proper credentials in a physically secure environment.

While this physical control process has been used extensively, it is now recommended that physical media containing airborne software also use cryptographic means as authentication and integrity mechanism.

Refer to ARINC 667 for specific information regarding physical distribution of airborne software.

NOTE: This section addresses on-aircraft loading as well as shop loading.

Related ARINC documents are:

- ARINC 645 Common Terminology and Functions for Software Distribution and Loading.
- ARINC 667 Guidance for the Management of Field Loadable Software can provide guidance for handling of field loadable software (terms used in this section comply with ARINC 667). However, it does not cover the security of field loadable software and data.

- *ARINC 827 Electronic Distribution of Software by Crate (EDS Crate) defines the industry standard method to be applied for electronic distribution of software.*
- *ARINC 835 Guidance for Security of Loadable Software Parts Using Digital Signatures.*

Airborne software distribution is a different process from data loading. Transferring airborne software from one location to another is software distribution. A location for distribution may include an onboard aircraft mass storage device (MSD) that is used to store software that may be loaded later. Moving airborne software into the actual onboard aircraft system components, other than a MSD, is data loading.

2.2 OPERATIONAL SECURITY MEASURES

The following subsections give an overview of what operational security measures can be taken for secure handling and managing of airborne software on the ground.

2.2.1 Reception

- Verify the authenticity and integrity of the software upon receiving. This can be done by verifying a digital signature or comparable methods, or by use of a combination of security measures to be agreed upon with the sender (aircraft manufacturer, supplier, etc.), using software tools that conform to the sender's specification.

NOTE: *A comparable method could be the usage of a sealed envelope in combination with physical media.*

- Define actions to take when software reception fails authentication or integrity checks. This would include notification to the software provider to resend the software or data. Also, include actions to take for inter-company distribution and reception authentication failures.

NOTE: *Resolve any issues with receipt of loadable software when it is received, not when it is needed.*

2.2.2 Creation/Modification

- Apply a secure process (personnel, tools) as defined in ED-202A / DO-326A and ED-203A / DO-356A and adapt the operator's environment in accordance with DAH recommendations provided in the ASOG for creating and modifying User Modifiable Software (UMS) and User Certifiable Software (UCS).

2.2.3 Storage

- During storage of airborne software on the ground, implement the security measures sufficient to prevent and detect unauthorized access in order to protect the integrity and confidentiality of the software (e.g. usage of digital signatures, encryption, locked rooms, passwords, defined roles and responsibilities, and badges).
- Ensure procedures address the full life cycle of the physical storage device (e.g. aircraft server, maintenance laptop, data loader, development computer) and the airborne software stored on it.
- Address digital certificate expiration issues that might occur during storage.
- Use encryption in addition to access controls if deemed necessary by the DAH as another layer of defense against unauthorized software access.

2.2.4 Media

- If airborne software is stored on media:
 - Ensure that the media is free of malicious code before airborne software is stored on it and have the means to verify.
 - Ensure that the media is protected from malicious code during its lifecycle and be able to verify.

- Ensure that the airborne software maintains its integrity and be able to verify.
- Consider various types of media available and the possible use restrictions and life cycle associated with each type and the possibilities of commercially installed software products (e.g. read-only media or removable media like USB mass storage devices with preinstalled applications, Secure Digital (SD) cards, compact flash cards, etc.).
- Ensure that the media is appropriately labeled (e.g. part number, version, date).
- Ensure that removable media is physically controlled.
- Treat removable media as you would portable/mobile maintenance devices.
- Whenever necessary, ensure that media content is protected against disclosure during its lifecycle, including decommissioning.

NOTE: *Depending on the selected media type, be aware that each media type bears different risks and vulnerabilities to be considered (e.g. USB mass storage device compared to read-only CD-ROM).*

2.2.5

Software Tools

- Keep equipment used for running software tools secure and free of unauthorized code, and control the configuration of this equipment. Therefore, verify the integrity and authenticity of software tools when installed in this equipment.
- These software tools include applications that run on equipment related to airborne software distribution and storage such as Portable Data Loaders (PDL's), office desktops, servers, and maintenance laptops.
- Keep equipment used for running software tools secure and free of unauthorized code, and control the configuration of this equipment.
- Ensure software tools are not used for any other purpose or in any other way than that specified by the DAH or the software supplier.
- Consider the need for management of vulnerabilities in software tools. If vulnerabilities are identified in a tool or its operating platform, determine appropriate mitigations in coordination with the tool provider. These mitigations may be technical or procedural.

NOTE: *A software supplier or DAH may specify particular security measures to be used to protect software tools. A software supplier or DAH may also specify particular security measures to be used during operation of the software tool.*

NOTE: *For additional guidance, refer to CHAPTER 5 and CHAPTER 6.*

2.2.6

Software Distribution

- Only perform transfer of airborne software by personnel who are authorized by the operator to access, manage, and store software.
Examples of transfer within organizations:
 - Software Vault to Data Loader, Data Loader to Aircraft, and Vault to Aircraft Mass Storage.
 Examples of transfer between organizations:
 - DAH to operator, suppliers/vendors to operator or operator to MRO.
- Ensure the integrity, authenticity, and confidentiality of airborne software during transfer (physical and logical) between entities (e.g. flight ops, engineering, aircraft, airport, shop).
- Implement a chain of custody consistent with associated information security risk for transporting airborne software (record keeping) to detect information security events.

NOTE: *Airborne Software can be distributed on portable physical media or by electronic distribution. For additional guidance, refer to CHAPTER 6*

2.2.7 Data Loading

- Validate authenticity and integrity of airborne software before software loading to aircraft LRUs. This includes onboard and off aircraft software loading.
 - Ensure that airborne software is loaded as per ICA or other applicable documentation such as Component Maintenance Manual (CMM) or Service Bulletin

2.2.8 Confidentiality

- Where required, ensure that confidentiality which aims to ensure that information is not made available nor disclosed to unauthorized entities is maintained during the whole lifecycle of the airborne software (including decommissioning).
- Unauthorized disclosure of airborne software could facilitate reverse engineering. So if airborne software is distributed over open networks like the internet, use encryption techniques such as https.

2.2.9 Incident Management

- Report and investigate information security events so safety impacts can be properly understood and security can be improved in the future. Refer to CHAPTER 8.

2.3 DAH Responsibilities

The DAH will provide the security ICA and other guidance related to software distribution and data loading to the operators

NOTE: *The guidance will be based on:*

- *The information security requirements that have been identified by the DAH through a process as specified in ED-202A / DO-326A using ED-203A / DO-356A guidance.*
- *Applicable civil aviation regulations.*

The ICA will be kept current according to 14 CFR 21.50 and EASA Reg 21.A.61.

The DAH will provide information necessary to operate the system safely and securely. This may include information on log files, where necessary.

NOTE: *Operators are required to report incidents, including security incidents. The DAH needs to provide the operators with appropriate capabilities to monitor the aircraft for incidents to support mandatory and voluntary reporting.*

2.4 OPERATOR RESPONSIBILITIES

The operator should document and implement security policies and procedures for handling and managing of airborne software distribution and data loading.

NOTE: *The operators need to demonstrate that for every aircraft in their fleet, they are able to manage the security aspects relating to safety.*

The operators should document and implement policies and procedures dependent on the risk assessment, as referenced in Chapter 10.

The operator should collect, record, and process all available logs relating to airborne software security.

NOTE: *Where logs are available for aircraft components, operators should demonstrate that they obtain the logs, record them for supporting potential incidents, and process the logs to identify events and incidents.*

CHAPTER 3

AIRCRAFT COMPONENTS

3.1 GENERAL

Regulatory requirements exist to protect aircraft components during repair and maintenance. However, aircraft information security concerns may not have been fully addressed for electronic parts.

New generation aircraft are equipped with electronic components that may require specific handling during transport, storage, repair and decommissioning, as these components can contain sensitive or confidential information such as private keys and personal data. Legacy aircraft may be retrofitted with connected onboard data loaders. Components loaded via these mechanisms need to be secured using similar means to that of new generation aircraft. Where an onboard data loader does not exist, the expectations on securing the storage, transport, repair, tools, and decommissioning need to be protected throughout the distribution wherever technically possible.

This section provides operational security measures to protect these components off-aircraft from unauthorized access.

3.2 OPERATIONAL SECURITY MEASURES

The following subsections provide an overview of what operational security measures can be taken for secure handling and managing of aircraft components.

3.2.1 Storage

- Secure storage of aircraft components to prevent unauthorized access.

3.2.2 Transport

- Protect aircraft components and component interfaces against physical tampering.
- Verify protection means when the aircraft component enters trusted facilities.
- Use a chain of custody for transporting aircraft components (record keeping).

3.2.3 Repair

- Secure environment (personnel, tools, and infrastructure) for repair of components.
- Ensure isolation from potentially malicious systems and storage media.

3.2.4 Tools

- Use only tools approved/recommended by the DAH or equivalent tools.
- Restrict usage of these tools to the intended purpose only.
- Keep tools in good working condition.

3.2.5 Decommissioning

- Prevent confidential data such as access key codes and passwords from recovery from aircraft components by unauthorized personnel.
- Prevent confidential data such as access key codes and passwords from transfer in case of operator change.
- Comply with procedures for disposing of aircraft parts by following the Component Maintenance Manual (CMM) or applicable civil aviation regulations.

3.2.6 Incident Management

- Report and investigate information security events so safety impacts can be properly understood and security can be improved in the future. Refer to CHAPTER 8.

3.3 DAH RESPONSIBILITIES

The DAH will provide the security ICA and other guidance related to aircraft components to the operators.

NOTE: *The guidance will be based on:*

- The information security requirements that have been identified by the DAH through a process as specified in ED-202A / DO-326A using ED-203A / DO-356A guidance.
- Applicable civil aviation regulations.

The ICA will be kept current according to 14 CFR 21.50 and EASA Reg 21.A.61.

The DAH will provide information necessary to operate the system safely and securely. This may include information on log files, where necessary.

NOTE: *Operators are required to report incidents, including security incidents. The DAH needs to provide the operators with appropriate capabilities to monitor the aircraft for incidents to support mandatory and voluntary reporting.*

3.4 OPERATOR RESPONSIBILITIES

The operator should document and implement policies and procedures for the handling and managing of aircraft components regarding security.

NOTE: *The operators need to demonstrate that for every aircraft type in their fleet, they are able to manage the security aspects relating to safety.*

The operators should document and implement policies and procedures dependent on the risk assessment, as referenced in Chapter 10.

The operator should collect, record, and process all available logs relating to aircraft components security.

NOTE: *Where logs are available for aircraft components, operators should demonstrate that they obtain the logs, record them for supporting potential incidents, and process the logs to identify events and incidents.*

CHAPTER 4

AIRCRAFT NETWORK ACCESS POINTS

4.1 GENERAL

Aircraft may allow connectivity to external computer systems and networks and to passenger electronic devices. This may result in the exploitation of security vulnerabilities in aircraft systems.

Examples of areas with network access points include but are not limited to:

- Flight Deck
- Electrical/Electronics/Equipment bays
- In-Flight Entertainment and Cabin Services stations or panels
- Areas in the cabin with system interfaces
- Maintenance ports with system interfaces (inside and outside the aircraft)
- Wireless access points.

Network access points located in physically non-restricted areas need more electronic access control measures because they are difficult to physically secure against unauthorized access.

Access to restricted areas may also be controlled by various identity and access management methods or tools to further support physical security.

NOTE: *On General Aviation aircraft there might not be restricted areas due to their size and operational concept.*

4.2 OPERATIONAL SECURITY MEASURES

The following list gives an overview of what operational security measures can be taken for secure managing of aircraft access points.

- Identification and indication of network access points and restricted areas in the aircraft documentation
- Monitoring, protecting and securing of network access points and restricted areas
- Reporting and investigating information security events so safety impacts can be properly understood and security can be improved in the future. Refer to CHAPTER 8.

4.3 DAH RESPONSIBILITIES

The DAH will provide the security ICA and other guidance related to onboard network access points to the operators.

NOTE: *The guidance will be based on:*

- *The information security requirements that have been identified by the DAH through a process as specified in ED-202A / DO-326A using ED-203A / DO-356A guidance.*
- *Applicable civil aviation regulations.*

The ICA will be kept current according to 14 CFR 21.50 and EASA Reg 21.A.61.

The DAH will provide information necessary to operate the system safely and securely. This may include information on log files, where necessary.

NOTE: *Operators are required to report incidents, including security incidents. The DAH needs to provide the operators with appropriate capabilities to monitor the aircraft for incidents to support mandatory and voluntary reporting.*