



The European Organisation for Civil Aviation Equipment
L'Organisation Européenne pour l'Équipement de l'Aviation Civile

AIRWORTHINESS SECURITY PROCESS SPECIFICATION

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, or hired, lent or exchanged outside your company.

ED-202A

June 2014

Supersedes ED-202

102 rue Etienne Dolet
92240 MALAKOFF, France
Web Site: www.eurocae.net

Tel: 33 1 46 55 62 65
Fax: 33 1 46 55 62 65
Email: eurocae@eurocae.net

Documents
Document Sharing Hub

AIRWORTHINESS SECURITY PROCESS SPECIFICATION

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, or hired, lent or exchanged outside your company.

ED-202A

June 2014

Supersedes ED-202

FOREWORD

1. This document was prepared jointly by EUROCAE Working Group 72 "Aeronautical Systems Security" and RTCA SC-216 "Aeronautical Systems Security", and was approved by the Council of EUROCAE on 16 June 2014.
2. EUROCAE is an international non-profit making organisation in Europe. Membership is open to manufacturers and users of equipment for aeronautics, trade associations, national civil aviation administrations, and, under certain conditions, non-European organisations. Its work programme is principally directed to the preparation of performance specifications and guidance documents for civil aviation equipment, for adoption and use at European and world-wide levels.
3. The findings of EUROCAE are resolved after discussion amongst Members of EUROCAE and in collaboration with RTCA Inc, Washington D.C., and/or the Society of Automotive Engineers (SAE), Warrendale PA, U.S.A., through their appropriate committees.
4. This document supersedes ED-202 "Airworthiness Security Process Specification" (December 2010).
For a discussion of the history of ED-202A / DO-326A and the differences from the original ED-202 / DO-326, please see Appendix E: "Background of the ED-202 / DO-326 Document".
5. This document is technically identical to RTCA DO-326A.
6. EUROCAE performance specifications and other documents are recommendations only. EUROCAE is not an official body of the European Governments. Its recommendations are valid as statements of official policy only when adopted by a particular government or conference of governments.
7. Copies of this document may be obtained from:

EUROCAE
102, rue Etienne Dolet
92240 MALAKOFF
France

Telephone: 33 1 40 92 79 30
Fax: 33 1 46 55 62 65
Email: eurocae@eurocae.net
Website: www.eurocae.net

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 ED-79A / SAE ARP4754A, ED-135 / SAE ARP4761, ED-12C / DO-178C, and ED-80 / DO-254 and with the advisory material associated with FAA AMJ25.1309 and EASA AMC25.1309, in the context of Part 25, CS-25, and JAA JAR-25. Tailoring of this guidance may allow it to be applicable in other contexts such as CS-23, CS-27, CS-29, CS-E, Part 23, Part 27, Part 29, and Part 33. For a discussion of the history of ED-202A / DO-326A and the differences from the original ED-202 / DO-326, please see Appendix E: Background of the ED-202 / 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.

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 previously subject to these objectives during all stages of its life cycle, then it should be borne in mind that some aspects of the objectives will not be applicable. These aspects should be described and dealt with separately. For existing aircraft or aircraft in development, alternate processes are acceptable which may utilize some or all of processes of this document.

Compliance may be accomplished through differentiated but interacting security process and 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.

TABLE OF CONTENTS

1	INTRODUCTION	1
1.1	Purpose	1
1.2	Scope	1
1.3	How to use this document	2
1.4	Conventions of this document	4
1.5	Relationship to other documents	4
2	AIRWORTHINESS SECURITY PROCESS	5
2.1	Process Overview	5
2.1.1	The Security Risk Assessment Related Activities	7
2.1.2	The Security Development Related Activities	8
2.1.3	Compliance	8
2.2	Security Risk Assessment Activities in the Development Process	9
2.2.1	Interactions with the Integral Processes of ED-79A/ARP 4754A	10
2.2.1.1	Relationship between Threat Condition Identification/Evaluation and FHA	12
2.2.1.2	Relationship between Preliminary Security Risk Assessment, PASA/PSSA and Aircraft/System Architecture	12
2.2.1.3	Relationship between Aircraft/System Security Risk Assessment and ASA/SSA	12
2.2.2	Integration of Security Development Activities in the Development Process	12
3	FUNDAMENTAL CONCEPTS	14
3.1	Establishing the Security Scope	14
3.1.1	Security Perimeter	15
3.1.2	Security Environment	15
3.2	Security Risk Assessment	16
3.2.1	Threat Condition Identification and Evaluation	17
3.2.2	Threat Scenario Identification	18
3.2.3	Security Measure Characterization	19
3.2.4	Level of Threat Evaluation	19
3.3	Security Effectiveness	19
3.3.1	Introduction	19
3.3.1.1	Concept of Security Effectiveness	19
3.3.1.2	Scope limitations	19
3.3.1.3	Security Effectiveness in the Airworthiness Security Process	20
3.3.1.4	Security and Security Effectiveness in the Aircraft Development Process ..	21
3.3.2	Implementation of Security Effectiveness	22
3.3.2.1	Determination of Security Effectiveness	22
3.3.2.2	Requirements for Security Effectiveness	22
3.3.2.3	Security Assurance	22
3.4	Security Development Activities	23
3.4.1	Security Architecture	24
3.4.2	Security Measures	24
3.4.3	Security Guidance	25
3.4.4	Security Verification	26

4	AIRCRAFT MODIFICATIONS.....	28
4.1	Aircraft Level versus System Level Security Risk Assessment Determination	28
4.1.1	Security Definitions and Risk Management	29
4.1.2	Aircraft Related Services.....	30
4.2	Modification Process Activities.....	31
4.2.1	Change Impact Analysis.....	32
4.2.2	Service History	32
4.2.3	Interconnectivities of New or Modified Aircraft Systems	32
4.2.4	Installing New Aircraft Systems and Networks.....	33
4.2.5	Replacing Aircraft Systems and Networks	33
4.2.6	Modifying Existing Aircraft Systems and Networks	33
4.2.7	CTSO / ETSO / TSO Installation Requirements	34
4.3	Airworthiness Security Process and Security Risk Assessment Criteria	34
4.3.1	Instructions for Continued Airworthiness.....	34
4.4	Data Submittals for Aircraft System Modifications	35
4.4.1	Plan For Security Aspects of Certification Summary (PSecAC Summary)..	35
APPENDIX A	DEFINITION OF THE AIRWORTHINESS SECURITY ACTIVITIES	36
A.1	Security Aspects of Certification.....	38
A.2	Security Risk Assessment Related Activities	40
A.3	Security Development Activities	46
APPENDIX B	GLOSSARY	52
APPENDIX C	ACRONYMS AND ABBREVIATIONS	57
APPENDIX D	REFERENCES	59
APPENDIX E	BACKGROUND OF THE DO-326/ ED-202 DOCUMENT	61
E.1	History of Document and Versions.....	61
E.2	Rationale for an Airworthiness Security Process	61
E.3	Information on the Changes Between ED-202 / DO-326 and ED-202A / DO-326A.....	62
APPENDIX F	COMMITTEE MEMBERSHIP.....	63
	IMPROVEMENT SUGGESTION FORM	68

LIST OF FIGURES

Figure 2-1:	Airworthiness Security Risk Management Framework.....	6
Figure 2-2:	Security Risk Assessment Related Activities in the development process V-model.....	9
Figure 2-3:	AWSP as Part of Aircraft Certification Process	11
Figure 2-4:	Security Development as Part of Aircraft Certification Process	13
Figure 3-1:	Security Scope.....	14
Figure 3-2:	Security Risk Assessment	17
Figure 3-3:	Security Effectiveness for the AWSP.....	20
Figure 3-4:	Security Activities in ED-79A / ARP 4754A Aircraft Development Process Model	21
Figure 3-5:	Relationship between Effectiveness Requirements and Assurance Actions	23
Figure 3-6:	Simplified Example of a Security Architecture with Different Types of Technical and Procedural Security Measures.....	25
Figure 3-7:	Security Testing Activities.....	27
Figure 4-1:	Example of E-enabled Architecture and Infrastructure.....	31
Figure 4-2:	Interconnectivities of New, Modified, or Removed Aircraft Systems	33
Figure A-1:	Airworthiness Security Process Activities.....	37

LIST OF TABLES

Table 3-1:	Asset Security Attributes and Threat Conditions	18
Table 4-1:	Data Submittals for the Security Aspects of Aircraft System Modifications.....	35

CHAPTER 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 electronic sabotage (as used in AMJ 25.1309, AC 23.1309-1E, and AMC 25.1309).

For a discussion of the history of ED-202A / DO-326A and the differences from the original ED-202 / DO-326, please see Appendix E: Background of the ED-202 / DO-326 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 "What"). A forthcoming companion document will suggest methods and considerations (the "How"). The document ED-204/DO-355 "Information Security Guidance for Continuing Airworthiness" addresses airworthiness security for continued airworthiness.

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 ED-79A / SAE ARP4754A, ED-12C / DO-178C, and ED-80 / DO-254 and with the advisory material associated with FAA AMJ25.1309 and EASA AMC25.1309, in the context of Part 25, CS-25, and JAA JAR-25. Tailoring of this guidance may allow it to be applicable in other contexts such as CS-23, CS-27, CS-29, CS-E, Part 23, Part 27, Part 29, and Part 33. For a discussion of the history of ED-202A / DO-326A and the differences from the original ED-202 / DO-326, please see Appendix E: "Background of the DO-326/ ED-202 Document".

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.

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 previously subject to these objectives during all stages of its life cycle, then it should be borne in mind that some aspects of the objectives will not be applicable. These aspects should be described and dealt with separately. For existing or aircraft in development, alternate processes are acceptable which may utilize some or all of processes of this document. Intentional unauthorized electronic interaction (also known as "unauthorized interaction" within the scope of this document) is defined as human-initiated actions with the potential to affect the aircraft due to unauthorized access, use, disclosure, denial, disruption, modification, or destruction of electronic information or electronic aircraft system interfaces. This definition includes the effects of malware on infected devices and the logical effects of external systems on aircraft systems, but does not include physical attacks or electromagnetic jamming.

Certification Context: Airworthiness security is the protection of the airworthiness of an aircraft from unauthorized interaction.

While the airworthiness certification process addresses failures and errors, this guidance extends this to address intentional unauthorized electronic interaction with aircraft systems resulting in safety effect. Just as failures and errors are treated as manageable risks to aircraft safety by the airworthiness certification process, the threat of Unauthorized Interaction is treated equally through the airworthiness security activities. In this context airworthiness security activities do not directly address the interfaces, policies, and procedures of external systems. However, aircraft systems may depend upon external systems to perform their functions and so the dependencies of airworthiness security on external systems are included in the considerations. To address these considerations, the applicant documents the assumptions about external factors as part of the Airworthiness Security Process.

Product Lifecycle Context: This document provides guidance in addressing the Airworthiness Security during the Aircraft product life cycle from project initiation until the aircraft Type Certificate is issued for the aircraft type design, including afterwards the issuance of STCs and ATCs. In addition, it includes the handover of information about the type design that is necessary to ensure continuing airworthiness with respect to unauthorized interaction. For the other stages of the product life cycle (operation, support, maintenance, administration, and disposal) guidance may be found in a companion document ED-204 / DO-355 "Information Security Guidance for Continuing Airworthiness".

Those aspects of information security that have no safety effect are not in the scope of this document.

1.3 HOW TO USE THIS DOCUMENT

This document is organized into four chapters plus informative appendices. First time readers should read Chapter 3 before Chapter 2 to understand the concepts being used in the overview.

- Chapter 1 introduces the document.
- Chapter 2 provides an overview of the Airworthiness Security Process.
- Chapter 3 introduces fundamental concepts used by the Airworthiness Security Process activities, such as Security Scope Definition, Security Risk Assessment, considerations about the Security Development activities, and the assignment of security effectiveness requirements.
- Chapter 4 introduces modifications to aircraft and systems, including Supplemental Type Certification (STC) and Amendments to Type Certification.

- Appendix A introduces the details of the Airworthiness Security Process activities, their interfaces and artifacts, the dependencies between those activities and the dependencies with activities that are part of the safety assessment process or the system development process, as per ED-79A / ARP 4754A.
- Appendix B contains an informal Glossary. An extended version of the Glossary is published as a EUROCAE report, and serves as the centralized and normative Definition of Terms to be shared by all EUROCAE documents addressing Aeronautical Information Systems Security. The use of the definitions is encouraged beyond their use in EUROCAE documents.
- Appendix C contains a list of acronyms used in this document.
- Appendix D 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.
- Appendices E, F, and G contain other supplementary material, including a Rationale for an Airworthiness Security Process, Membership list of the standards committees at the time of publication, and an Improvement Suggestion Form.

This document introduces the activities of the airworthiness certification process which address unauthorized interaction to aircraft systems. The body of the document describes how to achieve this objective at a relatively high level and appendices provide the information necessary to understand the details of the airworthiness security activities, their interfaces to activities of the airworthiness certification process, and the information or artifacts to be shared among them. These appendices also include definitions and links to relevant documents.

This document discusses both security specific activities and those "traditional" activities which are influenced by security considerations. This document only requires compliance with the security specific activities.

An overview of the Airworthiness Security Process is given in CHAPTER 2. FIGURE 2-1 presents the clustering of all specific Security Risk Assessment related activities, while the activities that concern the Security Development and security effectiveness assurance stay within the frame of the various stages of the system development process. This figure is also compliant with the Risk Management Process of ISO 27005:2011.

CHAPTER 3 introduces the concepts which are used throughout the Airworthiness Security Process. Their order has been selected in accordance with their use. One of the first activities is the Security Scope Definition. This activity will provide the scope of the problem: what's in and what's out, what are the interfaces and what are the possible interactions, authorized or not, between what is under the control of an applicant and what constitutes its respective environment. Analyses of severity of effects resulting from successful attacks are closely related to the analyses performed for failures and errors. They identify threat conditions on all aircraft functional and architecture levels. Security Risk Assessment links threat conditions with occurrences of successful attacks under consideration of their respective attack vectors and threat sources. Security measures will be evaluated according to their effectiveness to counter attacks and the assurance actions associated with it. These activities are all done in preparation for the development of security measures, which will determine their security requirements from the outputs of those prior process activities.

CHAPTER 4 addresses the situation when systems will be added to an existing aircraft architecture, when it has to be demonstrated to the Airworthiness Authorities (AA) that the interactions between the existing architecture and the new system, leading to the resulting architecture, will be secure.

1.4 CONVENTIONS OF THIS DOCUMENT

This document is addressed to audiences of two possible backgrounds, airworthiness certification and/or information security management. This results in difficulties in choosing terminology, as the two audiences share technical terms that have different meanings and usages for the different audiences. Since the primary impact of this document is within the area of airworthiness certification, the following practice has been followed:

- If a term with a suitable definition is available from the area of airworthiness certification, that term is used.
- If there is no suitable term in airworthiness certification, but there is a term with a suitable definition in information security management, and use of that term will not conflict with a similar-sounding term in airworthiness certification, that term is used.
- If there is no suitable term in either area, or if an available term has different meanings in the two areas, an alternate term which does not conflict is defined in the Glossary in Appendix B and used.
- Terms intended to have a specific technical meaning are defined in the Glossary in Appendix B regardless of the origin of the term. Terms that are not defined in the Glossary are intended to have their common dictionary meaning.

Within this document, "should" is used for recommendations, "may" and "need not" are used for permission, "can" and "might not" are used for possibility, and "cannot" is used for impossibility. The use of "must" and "shall" is avoided. Compliance with this document is shown through compliance with the compliance objectives listed in Appendix A.

1.5 RELATIONSHIP TO OTHER DOCUMENTS

A list of other documents that are cited for information only is found in Appendix D. The cited documents are commonly used in the development and airworthiness certification of Aircraft.

CHAPTER 2

AIRWORTHINESS SECURITY PROCESS

2.1 PROCESS OVERVIEW

The purpose of the Airworthiness Security Process (AWSP) is to establish that, when subjected to unauthorized interaction, the aircraft will remain in a condition for safe operation (using the regulatory airworthiness criteria). To accomplish this purpose, the Airworthiness Security Process:

- Establishes that the security risk to the aircraft and its systems are acceptable per the criteria established by the AWSP, and
- Establishes that the Airworthiness Security Risk Assessment is complete and correct.

This guidance also seeks to accomplish its goals efficiently. In most cases that results in the recommendation that the design, assessment, and development of security measures should be conducted both in close harmony and timing with the standard System design, assessment, and development processes. The process is designed to apply the same model as the safety process in that it allows for the adaptation of the effort needed to establish adequate security as a function of both severity of failure/threat condition effects and the level of threat of the threat scenarios to which the aircraft is exposed. Both factors are determined in the Security Risk Assessment (see [FIGURE 3-2](#)). The process applies to aircraft and systems that have security scope and is designed for its activities to be adapted in the same manner as ARP 4754A are adapted for the aircraft program. See [TABLE 4-1](#). The AWSP shown in [FIGURE 2-1](#) is composed of three major parts, first the dedicated **Certification Activities** (Steps 1 and 7) to manage the certification process itself, second the **Security Risk Assessment Related Activities** (Steps 2, 3 and Decision Gate 4) to evaluate risk based upon identified threat scenarios to determine acceptability and to assess the implemented security. Finally the acceptability of the risk (Decision Gate 4) will determine the role of third part, the **Security Development Related Activities** (Step 5 and 6) to implement the required security measures.

First time readers should read CHAPTER 3 at this point to understand the concepts being used in this overview.

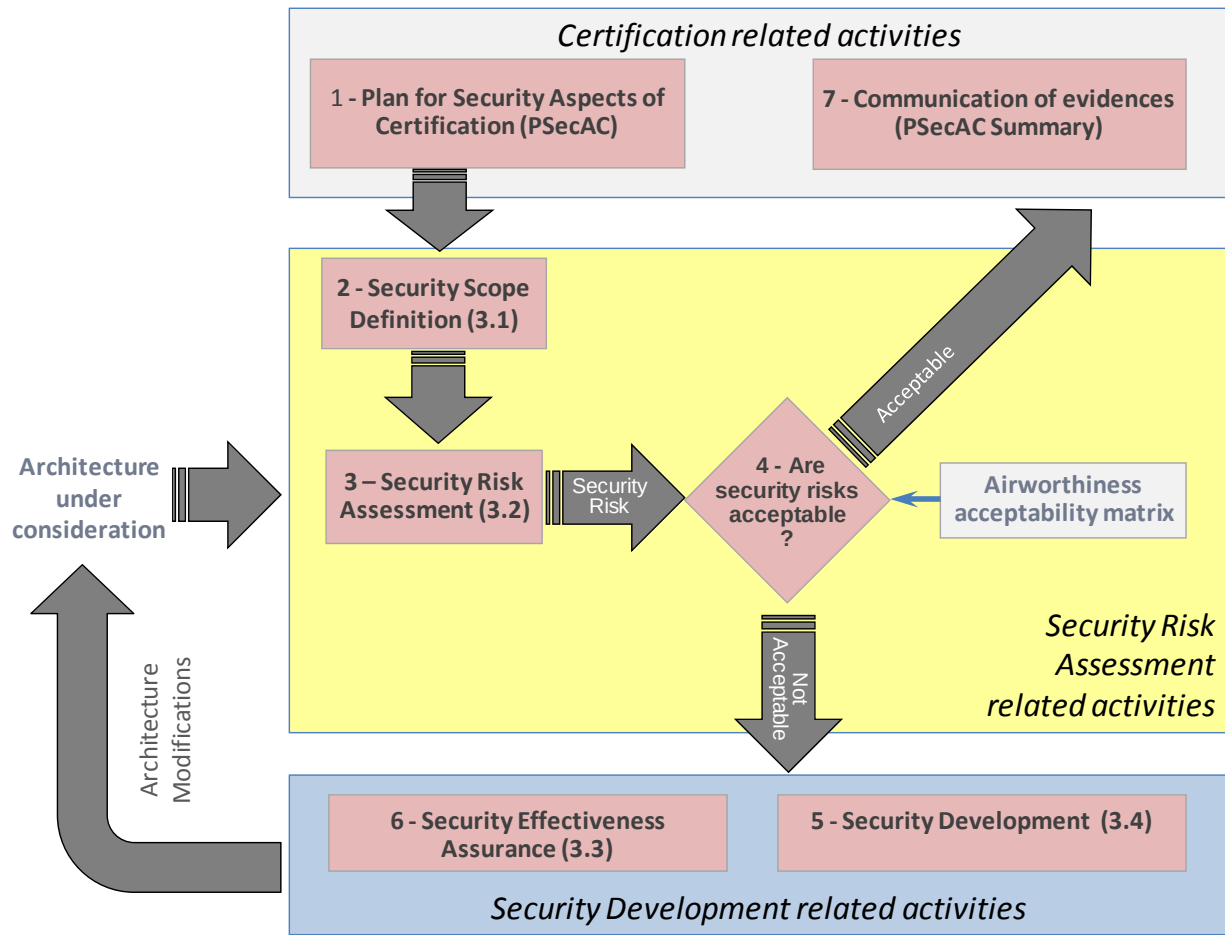


FIGURE 2-1: AIRWORTHINESS SECURITY RISK MANAGEMENT FRAMEWORK

The AWSP (see [FIGURE 2-1](#)) is composed of the following steps:

Step 1: Plan for Security Aspects of Certification: The plan is defined by the applicant and agreed to by the Airworthiness Authorities. It is an input for all further activities.

Step 2: Security Scope Definition: (equivalent to ISO 27005 Context Establishment) Establish the security scope as an input for Security Risk Assessment. For further information on Security Scope Definition, see Section 3.1.

Step 3: Security Risk Assessment: (equivalent to ISO 27005 Risk Assessment) Identify and evaluate security risks. For further information on Security Risk Assessment, see Section 3.2.

Decision Gate 4: “Are Security Risks acceptable?”: The security risk is acceptable or not according to an airworthiness acceptability matrix.

The airworthiness acceptability matrix, which defines the acceptable combination of level of threat and severity of threat condition effects, should be defined by the applicant with the agreement of the Airworthiness Authorities, unless provided by regulation.

- For all acceptable risks, there is no need to implement additional security measures. These risks may be retained in which case the associated evidence of assessment should be produced (See Step 7).
- All unacceptable risks should be mitigated to become acceptable (See steps 5 and 6) (equivalent to ISO 27005 Risk Treatment). These decisions usually lead to a modification of the architecture for which security effectiveness requirements and assurance activities are defined (see Section 3.3).

Step 5: Security Development: Risk mitigation results in the design of a security architecture that addresses the set of threat scenarios involved in the risks to be mitigated.

The concept of security architecture and the associated security specifics (i.e. security measures, security guidance and security verification) are presented in Section 3.3. New or modified security architectures (including operational requirements) should be taken into account as input of security risk re-assessment (Step 3).

Step 6: Security effectiveness assurance: This step represents the activities to be performed in order to give the appropriate confidence that the security risks are acceptable. The concept of security effectiveness is described in Section 3.3.

Step 7: Communication of evidences: When all risks are acceptable, the results of airworthiness security activities should be captured in the PSecAC Summary.

NOTE: *The process described above remains applicable during the whole aircraft lifetime including modifications to the type design, new threat scenarios, new vulnerabilities and modifications to the security environment (that may also trigger updates in the security guidance and Instructions for Continued Airworthiness, see Section 3.4.3 and ED-204 / DO-355).*

Access to information generated in the security process should have a set of rules or a process that limits access or places restrictions on certain types of information. An external agreement about how to protect security risk assessment data (e.g., architecture, security measures, vulnerabilities, residual risks) should be defined between stakeholders and applied during the life cycle of the aircraft.

2.1.1

The Security Risk Assessment Related Activities

Security Risk Assessment may be performed at two **levels** of development: aircraft and system. At each level, it has the responsibility to identify any unacceptable risks resulting from threat scenarios.

Security Risk Assessment should be performed at two **stages** of development:

- Preliminary Security Risk Assessment should be performed during the design phase to evaluate the design.
- Security Risk Assessment should be finalized during the integration phase to evaluate the implementation.

NOTE: *The Security Risk Assessment related activities are based on the ISO 27005 Information Security Risk Management process.*

NOTE: *Suggested methods to determine the airworthiness acceptability matrix and level of threat scale will be defined in a forthcoming companion document.*

The activities to be performed are organized according to the following breakdown, detailed in Appendix A:

Aircraft Security Scope Definition (ASSD) (step 2): Determine aircraft operational environment for information security.

Preliminary Aircraft Security Risk Assessment (PASRA) (step 3/4): Identify threat conditions and threat scenarios and assess all security risks at aircraft level.

System Security Scope Definition (SSSD) (step 2): Determine system operational environment for information security.

Preliminary System Security Risk Assessment (PSSRA) (step 3/4): Identify threat conditions and threat scenarios and assess all security risks at system level.

System Security Risk Assessment (SSRA) (step 3/4): Identify threat conditions and threat scenarios and assess the system's security risks and vulnerabilities.

Aircraft Security Risk Assessment (ASRA) (step 3/4): Identify threat conditions and threat scenarios and assess the aircraft security risks and vulnerabilities.

2.1.2 The Security Development Related Activities

The Security Development related activities support the implementation of security measures to mitigate the risks identified by Security Risk Assessment. When security measures are needed, security requirements should be generated as part of the system requirements (see ED-79A / ARP 4754A). This results in the security requirements being subject to the same development requirements and assurance actions as other safety-related mitigation mechanisms. However, as with any other specialized technical area (e.g., flight control), there are some particular development requirements and assurance actions. The Airworthiness Security Process defines additional assurance actions specifically for systems which have requirements relevant to the security measures through the Security Development related activities (see Sections 3.3 and 3.4).

The Security Development related activities starts at the aircraft level, and proceeds iteratively to system level and may proceed lower as desired. The development of the security measures occurs as follows:

As part of “**Security Development**” (step 5):

- Choose effective security measures to mitigate security risks and organize them into the security architecture. Develop security requirements and assurance actions for the systems and items implementing the security measures.
- Develop guidance for the secure operation and maintenance of security measures by identifying the integration, operation, and maintenance requirements for the security measures and documenting them as System Security Integrator Guidance, and eventually as Aircraft Security Operator Guidance and external agreements or as Instructions for Continued Airworthiness. See Section 3.4.3 and companion document ED-204 / DO-355 for further details.
- Verify security requirements and evaluate the security effectiveness of the security measures of the aircraft/system for its intended environment.

Security requirements should also be validated, but as there are no particular security validation activities required, no additional information is provided here.

The associated activities mentioned in Appendix A are the following:

- o At aircraft level: Aircraft Security Architecture and Measures (ASAM)
- o At system level: System Security Architecture and Measures (SSAM)
- o At system level: System Security Integrator Guidance (SSIG)
- o At system level: System Security Verification (SSV)
- o At aircraft level: Aircraft Security Operator Guidance (ASOG)
- o At aircraft level: Aircraft Security Verification (ASV)

2.1.3 Compliance

Compliance with the guidance of this document will demonstrate that:

- the applicant has provided necessary certification data; and
- the applicant has satisfied the compliance objectives;

Appendix A organizes the AWSP into generic activities for aircraft development and certification 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 as presented in the tables in Appendix A, 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 knowledge available will be timely, prudent and useful to the final success of the development process.

Compliance may be accomplished through differentiated but interacting security process and 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.

2.2

SECURITY RISK ASSESSMENT ACTIVITIES IN THE DEVELOPMENT PROCESS

Airworthiness Security Process activities are related to the overall safety assessment and system development processes as shown in [FIGURE 2-2](#) and [FIGURE 2-3](#).

As shown in [FIGURE 2-2](#) below, these processes are instantiated at aircraft and system levels. The activities are described, including the specification of their objectives in Appendix A.

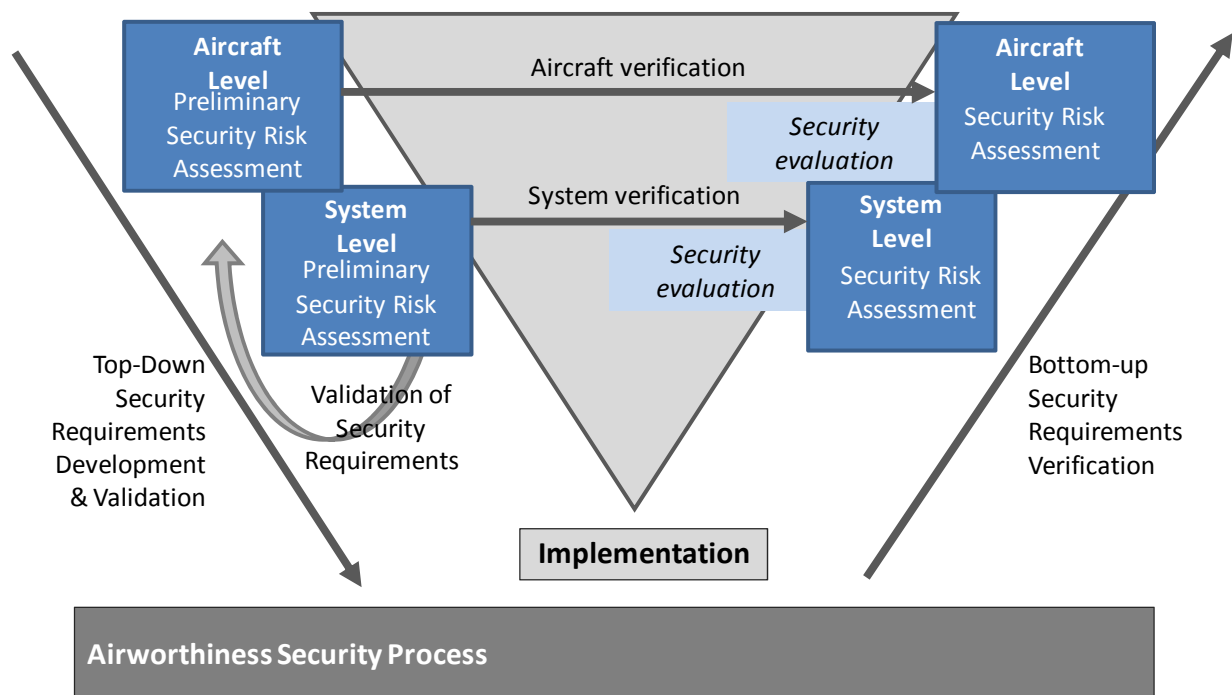


FIGURE 2-2: SECURITY RISK ASSESSMENT RELATED ACTIVITIES IN THE DEVELOPMENT PROCESS V-MODEL

The following Security Risk Assessment activities are performed:

- **Preliminary Security Risk Assessment:** Security Risk Assessment is started when the architecture/system is started, during the requirement identification phase (top-down development cycle). The purpose of Security Risk Assessment is to determine which part of the architecture /system is at an acceptable theoretical security risk level, and to communicate the need for new security requirements when the security risk is not acceptable.

In the early phase of the requirement identification, a detailed architecture/system might not be available. In this case, the applicant should perform a simplified Security Risk Assessment.

Preliminary Security Risk Assessment is part of the validation that the security requirements are complete and correct in terms of security effectiveness (see Section 3.3) before launching implementation of the product. Security Risk Assessment processes should maintain traceability from the aircraft requirements, through Security Risk Assessment to the derived system level and item level security requirements.

- **Security Risk Assessment:** When the implementation is available, during the verification phase (bottom-up development cycle), the applicant should launch Security Risk Assessment iterations. In this phase, Security Risk Assessment takes into account the vulnerabilities identified during Security Verification.

At the end of Security Risk Assessment, all evidences are available to show that security requirements have been satisfied.

2.2.1

Interactions with the Integral Processes of ED-79A / ARP 4754A.

This section is mainly useful to applicants following a ED-79A / ARP 4754A process with ED-135 / ARP 4761.

The Security Risk Assessment related activities are a set of activities which interact with the safety assessment process to manage the added environment risk to aircraft when it is exposed to the threat of unauthorized interaction. It is analogous to a Particular Risk Analysis (PRA) in its interactions with ED-79A / ARP 4754A and ED-135 / ARP 4761.

The Security Scope definition is a set of activities to establish the intended operational environment relative to information security. (See detail in Section 3.1)

Security Risk Assessment is a set of Activities of the same nature as safety assessment activities. So according to the considered level, the Security Risk Assessment activities (see [FIGURE 2-2](#)) are related as follows:

- Preliminary Aircraft Security Risk Assessment is related to Aircraft Functional Hazard Assessment (AFHA) and Preliminary Aircraft Safety Assessment (PASA).
- Preliminary System Security Risk Assessment is related to System Functional Hazard Assessments (SFHAs) and Preliminary System Safety Assessments (PSSAs).
- System Security Risk Assessment is related to System Safety Assessments (SSA).
- Aircraft Security Risk Assessment is related to Aircraft Safety Assessment (ASA).

[FIGURE 2-3](#) shows the Security Risk Assessment related activities of [FIGURE 2-1](#) on different iterations and on different levels of the development (aircraft/system). The details are provided in the input and outputs of the activities defined in Appendix A.

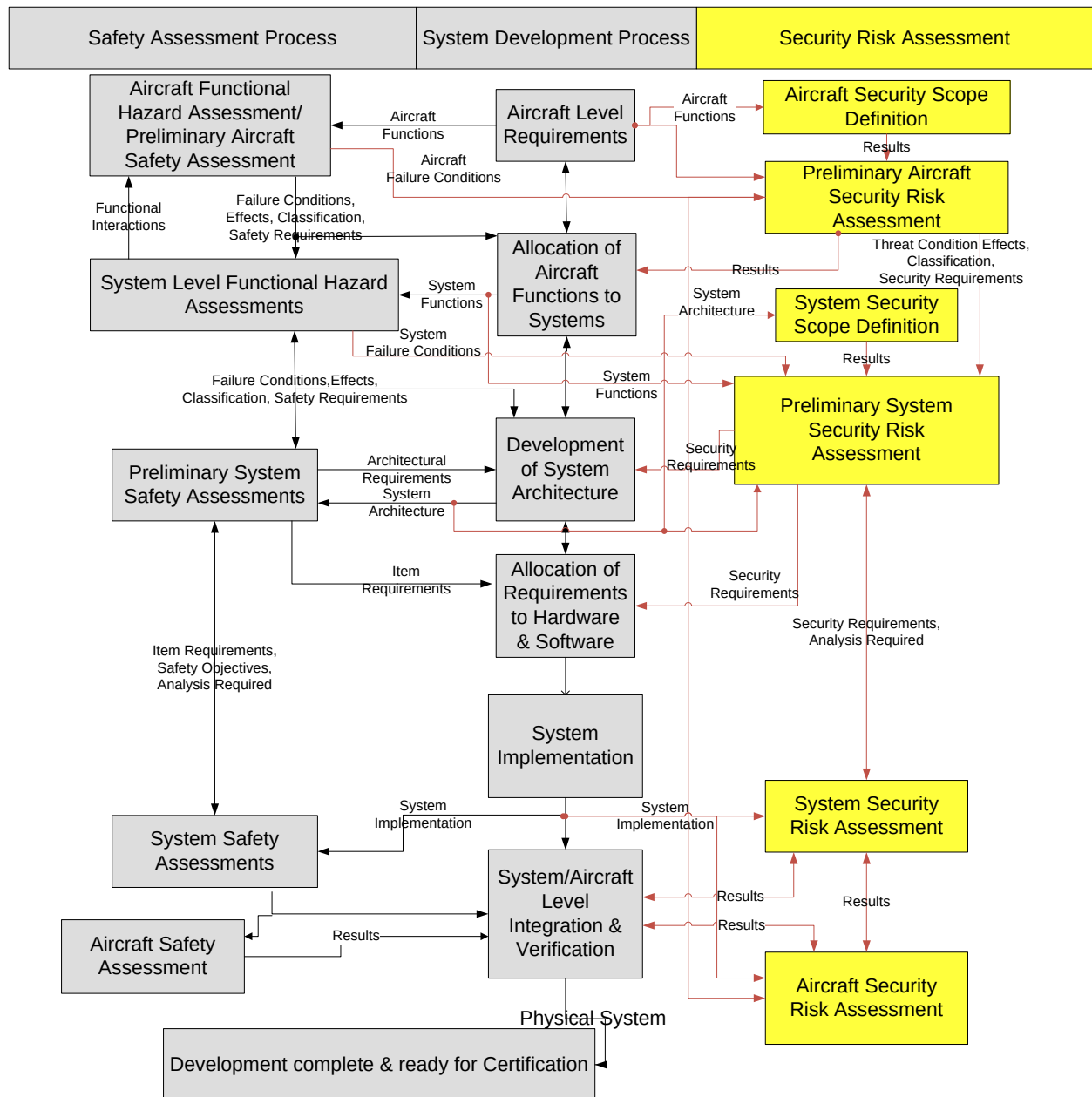


FIGURE 2-3: AWSP AS PART OF AIRCRAFT CERTIFICATION PROCESS

NOTE: For the sake of clarity, FIGURE 2-3 shows the most dominant of the many data exchanges that occur between activities. To determine the actual data exchanges, see the input/output entries in the activity tables in Appendix A.

NOTE: FIGURE 2-3 only shows the interactions involving Security Risk Assessment, Safety Assessment, and System Development. To see the interactions involving Security Development, see FIGURE 2-4. To see the interactions between Security Risk Assessment and Security Development, see FIGURE A-1.

2.2.1.1 Relationship between Threat Condition Identification/Evaluation and FHA

Threat condition identification is the initial set of actions of Security Risk Assessment to determine the threat conditions. It is followed by actions to determine the threat scenarios and security risk.

Aircraft threat condition identification is linked to AFHA, while the system threat condition identification is linked to the associated SFHA.

Failure conditions are initial inputs for any threat condition identification and are provided by aircraft and system level FHAs respectively. Those failure conditions are used for the identification of threat scenarios and associated threats causing them. In the second phase threats identified in the first phase are used to identify potential additional threat scenarios resulting in supplemental threat conditions causing safety effects. The severity of threat conditions is evaluated in the same manner as by FHAs. As such, any threat condition having an identical safety effect as a previously identified failure condition shares its severity.

2.2.1.2 Relationship between Preliminary Security Risk Assessment, PASA/PSSA and Aircraft/System Architecture

Preliminary Security Risk Assessment may produce requirements for security measures which are provided to the process for Security Development.

Architecture modifications (for example, adding of security measures) are to be analyzed by both Safety Assessment and Security Risk Assessment.

2.2.1.3 Relationship between Aircraft/System Security Risk Assessment and ASA/SSA

Aircraft/System Security Risk Assessment and ASA/SSAs are performed on the same implemented architecture. The results of Security Risk Assessment are included in the Plan for Security Aspects of Certification Summary (PSecAC Summary).

2.2.2 Integration of Security Development Activities in the Development Process

As far as Security Development activities are concerned, the concerned activities are integrated into the development process as follows (see [FIGURE 2-4](#)).

Aircraft Security Architecture and Measures activity is integrated into the Allocation of Aircraft Functions to Systems activity.

The Aircraft Security Operator Guidance activity and Aircraft Security Verification activity are integrated into the Aircraft Level Integration & Verification activity.

The System Security Architecture and Measures activities are integrated into the Development of System Architecture.

The implementation of system security measures is integrated into the System Implementation like any other function implementation. Therefore, this activity being not specific, is not further detailed in Appendix A.

The System Security Integrator Guidance activity and System Security Verification activity are integrated into the System Level Integration & Verification activity.

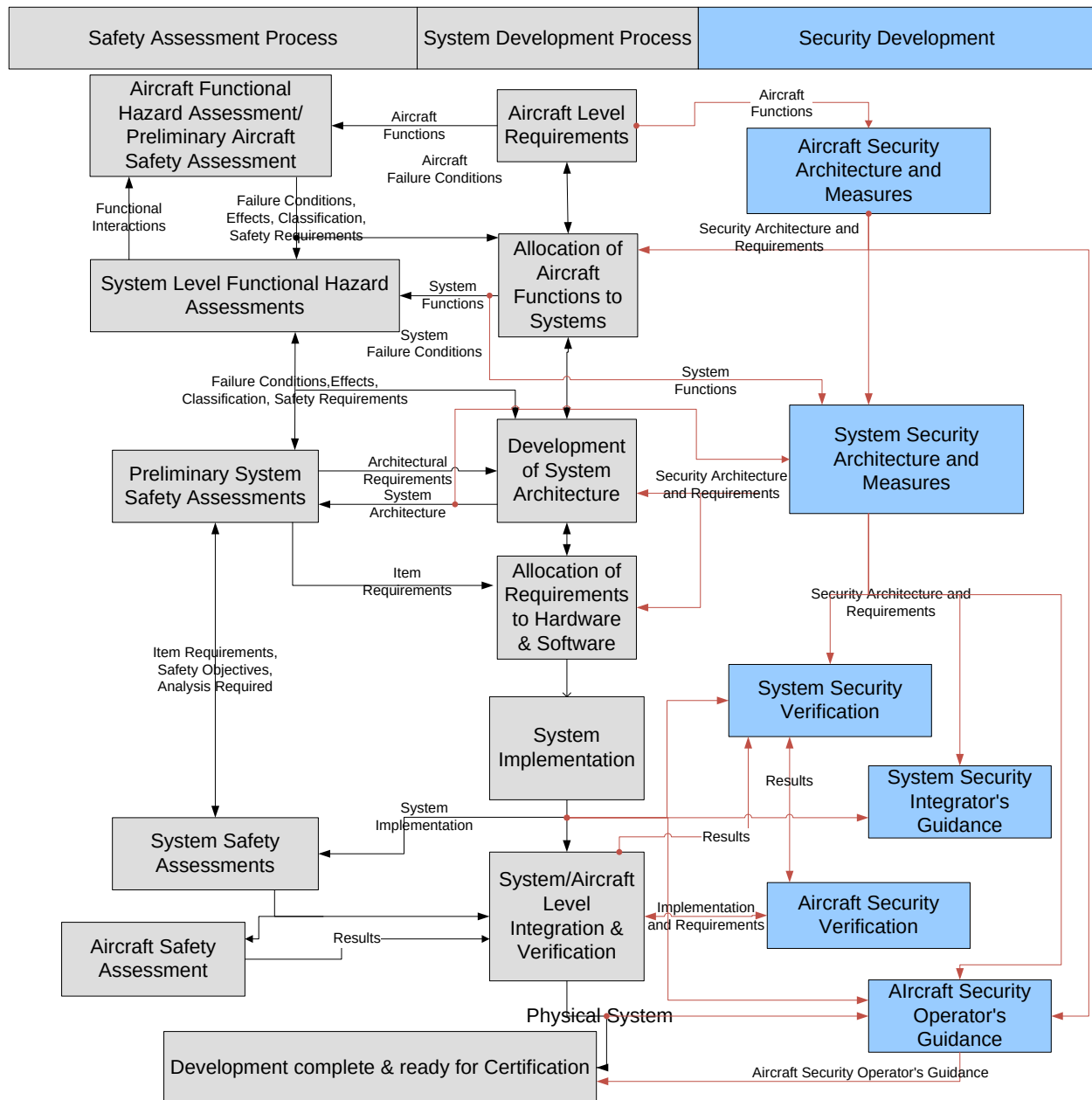


FIGURE 2-4: SECURITY DEVELOPMENT AS PART OF AIRCRAFT CERTIFICATION PROCESS

NOTE: For the sake of clarity, FIGURE 2-4 shows the most dominant of the many data exchanges that occur between activities. To determine the actual data exchanges, see the input/output entries in the activity tables in Appendix A.

NOTE: FIGURE 2-4 only shows the interactions involving Security Development, Safety Assessment, and System Development. To see the interactions involving Security Risk Assessment, see FIGURE 2-3. To see the interactions between Security Risk Assessment and Security Development, see FIGURE A-1.

CHAPTER 3

FUNDAMENTAL CONCEPTS

3.1 ESTABLISHING THE SECURITY SCOPE

Assets are the logical and physical resources of the aircraft which contribute to the airworthiness of the aircraft. The purpose of the Security Scope Definition is to identify the assets, document the points of entry to the assets, and determine their environment.

The Security Scope Definition outputs are used in two ways, as part of the:

- Airworthiness Security Process to derive architectural and design constraints and requirements; and
- Continuing Airworthiness Process (documented in ED-204 / DO-355), to derive Operator Guidance for the safe operation and maintenance of the aircraft.

The Security Scope Definition phase is comprised of two parts (as shown in FIGURE 3-1):

- Security Perimeter - the notional boundary between an internal security context and the external security environment of the aircraft or system under consideration. It marks the change of security control. The internal security context is comprised of the assets contained in the security perimeter and the relevant security measures.
- Security Environment – the description of everything outside the security perimeter that is relevant to the security of the aircraft or system under consideration. The definition of security environments is equivalent to the “external context” as used in ISO 27005:2011.

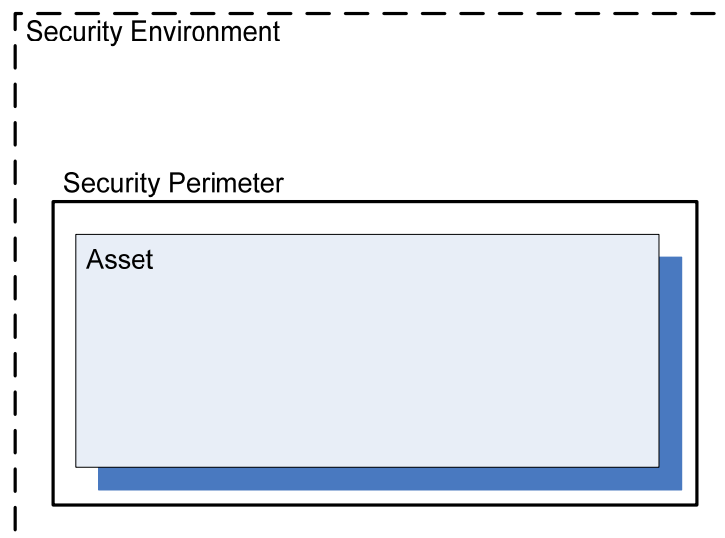


FIGURE 3-1: SECURITY SCOPE

At the aircraft level, the security perimeter and security environment primarily address off-board persons, external systems and interactions. At the lower hierarchy levels, the security perimeters and security environments primarily address the interactions between systems on these levels.

The purpose of identifying the assets is to define the logical and physical resources of the system under consideration, so that the threats against them can be identified and mitigated. For this document, assets are the logical and physical resources of the aircraft which contribute to the airworthiness of the aircraft, including functions, systems, items, data, interfaces, processes and information. Assets may be of physical (e.g. a LRU) or purely logical nature (e.g. software, data). For logical assets the dependencies on the implementing physical assets should be considered.

Assets may contain, or may be contained in, other assets. A higher level asset will typically be logically or physically broken down to a number of lower level assets, each with their own or shared lower level security perimeters.

Methods and examples how to compose, break down, and update security environments, security perimeters and their assets will be found in a forthcoming companion document.

3.1.1 Security Perimeter

The purpose of the security perimeter is to identify and trace points of entry to the assets in later process steps.

The security perimeter itself includes no functionality, and is not an asset. It separates the contained assets from the world outside and is crossed by logical and physical interfaces, possible interactions, and information exchanges with the outside world.

An aircraft or system is exposed to attack from systems or persons outside its security perimeter. Any interaction or information exchange that crosses the security perimeter should be documented and its potential for attacks should be considered later in the process.

Everything within the security perimeter may be controlled by the design of the contained assets. Everything outside the security perimeter is under external control and is not part of the design of the contained assets. Everything outside the security perimeter that can interact with the contained assets should be considered for inclusion in the security environment (see next section).

For the security perimeter, the following should be documented:

- All hardware interfaces, including radio-frequency signals (e.g., Wi-Fi, mobile cellular, GPS, VHF).
- All software interfaces, including services and protocols running over the hardware interfaces, and
- Information exchanges (e.g. file transfer, ACARS messages, software loads, database updates), including all physical paths by which information from outside the perimeter could reach the inside.

All associated interfaces used for operations and maintenance of the system, whether their use is routine or only under special circumstances, should be considered as part of the security perimeter of the aircraft.

3.1.2 Security Environment

The purpose of defining the security environment is to capture the assumptions about the persons, organizations, and external systems outside the security perimeter that interact with the asset under consideration, so that the potential threat sources may be identified.

A security environment should consider, but not be limited to:

- Roles and entities - define the roles and organizations that interact with the assets of the aircraft/system.
 - o This includes persons and organizations with the ability to access assets through the security perimeter. These may be either authorized or unauthorized and make up the potential threat sources.

- Responsibilities and risk related to:
 - o Roles and entities (e.g. their responsibilities and access to the aircraft/system),
 - o External tools and systems (e.g. airport IT network), and
 - o External security measures (e.g. operational controls, airport passenger screening, firewall within airline ground IT).
- External dependencies:
 - o Regulations, and
 - o National laws.
- External Agreements, including:
 - o Contracts (e.g. between operator and MRO), and
 - o Accredited connection, or other minimum standards and processes that an aircraft system should comply with in order to connect with an external system.
- Classification of threat sources and vulnerabilities, to structure the inputs for Security Risk Assessment. (An example classification is found in ARINC 811, Attachment 3, 3-4.2.1.).

While all of the above need to be considered, only assumptions relevant for or required by a specific design need to be included. Some assumptions may be provided by the Airworthiness Authorities.

Relevant properties of entities outside the aircraft security perimeter are documented in the aircraft security environment. On a system level, the system security environment of a system asset should consider everything outside the system security perimeter. This can include aircraft internal interfaces with other systems. But the security environment of a system within the aircraft will always be a refinement of the aircraft security environment. Therefore the security environment on a system level is always composed of two sets of assumptions:

- Portions of the aircraft security environment relevant to the system under consideration, and
- Additional assumptions about the security environment external to the system but within the aircraft security perimeter (e.g. interactions between this system and other aircraft systems, which may provide security measures).

A partial list of security environment assumptions is found in Appendix D of ARINC Technical Application Bulletin ABN-035A "Considerations for the Incorporation of Cyber Security in the Development of Industry Standards", and ISO Guide 73:2009 for other potential considerations for the environment.

3.2

SECURITY RISK ASSESSMENT

The purpose of Security Risk Assessment related activities described in Section 2.1.1 is to evaluate the security risk of a system/aircraft facing unauthorized interaction. This section describes the data necessary to define the threat scenarios, characterize the security measures, and evaluate the security risk associated with each threat scenario.

Security Risk Assessment may be conducted at either aircraft or system level of implementation. The applicant evaluates the security risk of each threat scenario having a safety effect on the system/aircraft assets.

The security risk of a threat scenario is defined by:

- Level of threat of this threat scenario, and
- Severity of the effect of the threat condition caused or contributed by this threat scenario.