



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

AIRWORTHINESS SECURITY METHODS AND CONSIDERATIONS

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-203

September 2015

AIRWORTHINESS SECURITY METHODS AND CONSIDERATIONS

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-203

September 2015

FOREWORD

1. This document was prepared by EUROCAE Working Group 72 “Aeronautical System Security”, and was approved by the Council of EUROCAE on 2 September 2015.
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. 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.
5. 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

TABLE OF CONTENTS

FOREWORD	I
LIST OF FIGURES	III
LIST OF TABLES	IV
CHAPTER 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.....	2
1.5 RELATIONSHIP TO OTHER DOCUMENTS.....	3
CHAPTER 2 RISK MANAGEMENT	4
2.1 SECURITY SCOPE	4
2.1.1 ASSETS.....	4
2.1.2 SECURITY PERIMETER	6
2.1.3 SECURITY ENVIRONMENT	7
2.1.4 CHANGES IN THE SECURITY ENVIRONMENT	8
2.1.5 IDENTIFYING NESTED ASSETS	9
2.2 RISK ASSESSMENT METHOD FRAMEWORK	11
2.2.1 THREAT CONDITION IDENTIFICATION AND EVALUATION.....	12
2.2.2 THREAT SCENARIO IDENTIFICATION	14
2.2.3 SECURITY MEASURE CHARACTERIZATION	18
2.2.4 LEVEL OF THREAT EVALUATION	19
2.2.5 COMPARABILITY OF RISK ASSESSMENTS.....	25
2.3 RISK ACCEPTABILITY	26
2.3.1 INTRODUCTION	26
2.3.2 RELATION OF EFFECTIVENESS AND LEVEL OF THREAT	26
2.3.3 STATEMENT OF ADEQUATE LEVEL OF PROTECTION.....	27
2.3.4 PROCESS FOR CONTINUED EFFECTIVENESS OF PROTECTION	28
2.4 SECURITY ASSURANCE LEVELS.....	28
2.4.1 ASSURANCE LEVEL DEFINITION	28
2.4.2 PRINCIPLES OF SECURITY ASSURANCE ASSIGNMENT	29
CHAPTER 3 SECURITY ASSURANCE	31
3.1 SECURITY ASSESSMENT	32
3.1.1 SECURITY SCOPE OBJECTIVES.....	32
3.1.2 SECURITY ASSESSMENT OBJECTIVES	32
3.2 SECURITY DEVELOPMENT	33
3.2.1 PLANNING PROCESS OBJECTIVES.....	33
3.2.2 REQUIREMENTS PROCESS OBJECTIVES	33
3.2.3 DESIGN PROCESS OBJECTIVES	33
3.2.4 IMPLEMENTATION PROCESS OBJECTIVES	34
3.2.5 SECURITY VERIFICATION PROCESS OBJECTIVES	35
3.2.6 SECURITY REFUTATION OBJECTIVES	35
3.3 SECURITY CONFIGURATION MANAGEMENT	36
3.3.1 SECURITY CONFIGURATION MANAGEMENT OBJECTIVE	36
3.4 SECURITY CERTIFICATION LIAISON.....	36
3.4.1 SECURITY CERTIFICATION LIAISON OBJECTIVES	36
3.5 SECURITY DEPLOYMENT	37
3.5.1 SECURITY DEPLOYMENT OBJECTIVES.....	37

3.6	CONTINUED SECURITY EFFECTIVENESS	37
3.6.1	CONTINUED SECURITY EFFECTIVENESS OBJECTIVES.....	37
APPENDIX A	ACTIVITY INTERFACE SPECIFICATION	38
APPENDIX B	PROCESS LOOKUP TABLE.....	41
APPENDIX C	SECURITY ASSURANCE OBJECTIVES.....	43
APPENDIX D	EXAMPLE METHODS	45
D.1	RISK ASSESSMENT EXAMPLE METHOD	45
D.1.1	SECURITY RISK ASSESSMENT	45
D.1.2	IMPACT ANALYSIS	45
D.1.3	THREAT SCENARIO IDENTIFICATION	46
D.1.4	LEVEL OF THREAT EVALUATION	47
D.1.5	RISK CALCULATION	57
D.1.6	RISK CONSISTENCY CHECK.....	58
D.1.7	SECURITY ASSURANCE VS. EFFECTIVENESS	59
D.1.8	RISK ASSESSMENT FOR CHANGE MANAGEMENT	60
D.1.9	DIFFICULTY OF ATTACK EVALUATION EXAMPLE	62
D.2	THREAT CONDITION EVALUATION EXAMPLE TEMPLATE.....	63
D.3	EFFECTIVENESS LEVEL COMPUTATION EXAMPLE METHOD	64
APPENDIX E	EXAMPLES.....	65
E.1	SECURITY PERIMETER EXAMPLE.....	65
E.2	RISK MANAGEMENT EXAMPLE.....	67
E.2.1	EXAMPLE CONTEXTUALIZATION	67
E.2.2	SECURITY SCOPE (REFERENCE: SECTION 2.1).....	68
E.2.3	RISK ASSESSMENT METHOD FRAMEWORK (REFERENCE: SECTION 2.2)	76
APPENDIX F	ACRONYMS AND GLOSSARY OF TERMS	81
APPENDIX G	REFERENCES	84
APPENDIX H	WG-72 MEMBERSHIP	86
	IMPROVEMENT SUGGESTION FORM.....	89

LIST OF FIGURES

FIGURE 2-1: STEPS FOR DETERMINING SECURITY PERIMETER	7
FIGURE 2-2: NESTED ASSETS WITHIN AIRCRAFT.....	9
FIGURE 2-3: NESTED ASSETS WITHIN SYSTEM	9
FIGURE 2-4: NESTED SECURITY ENVIRONMENTS.....	10
FIGURE 2-5: INTERFACES BETWEEN NESTED SECURITY ENVIRONMENTS.....	11
FIGURE 2-6: THREAT SCENARIO EXAMPLE	14
FIGURE 2-7: THREAT SCENARIO COVERAGE	17
FIGURE 2-8: EVALUATION ORDER EXAMPLE 1	20
FIGURE 2-9: EVALUATION ORDER EXAMPLE 2	21
FIGURE 2-10: COMBINED EFFECTIVENESS ASSESSMENT	24
FIGURE 2-11: RELATION OF EFFECTIVENESS AND LEVEL OF THREAT.....	27
FIGURE 2-12: EXTENT OF DEVELOPMENT AND EFFECTIVENESS ASSURANCE	30
FIGURE D-1: THREAT SCENARIO COVERAGE.....	46
FIGURE D-2: SECURITY MEASURE BREAKDOWN.....	51
FIGURE D-3: SECURITY MEASURE COMPOSITION ASSESSMENT PROCESS.....	53
FIGURE D-4: DIFFICULTY OF ATTACK CONSISTENCY CHECK	59
FIGURE D-5: CONSISTENCY BETWEEN PARENT AND CHILDREN THREAT SCENARIOS	59
FIGURE E-1: IFE EXAMPLE - STEPS FOR DETERMINING SECURITY PERIMETER	65

FIGURE E-2: IFE EXAMPLE - SECURITY PERIMETER AT AIRCRAFT SYSTEM LEVEL.....	66
FIGURE E-3: IFE EXAMPLE - SECURITY PERIMETER AT LOWEST SYSTEM LEVEL	66
FIGURE E-4: EXAMPLE CONTEXT	67
FIGURE E-5: AIRCRAFT SECURITY SCOPE.....	68
FIGURE E-6: AMS SECURITY SCOPE.....	69
FIGURE E-7: AMS SECURITY PERIMETER	72
FIGURE E-8: AMS ASSETS HIERARCHY	73
FIGURE E-9: ONE STAGE ATTACK PATHS	78
FIGURE E-10: MULTI-STAGE ATTACK PATH	79

LIST OF TABLES

TABLE 2-1: SECURITY MEASURE CHARACTERISTICS	19
TABLE 2-2: ACCEPTABLE RELATIONSHIP BETWEEN SEVERITY OF EFFECT AND EFFECTIVENESS	27
TABLE 2-3: DEFINITION OF EFFECTIVENESS OBJECTIVE CLASSIFICATION.....	28
TABLE A-1: SECURITY SCOPE	38
TABLE A-2: RISK ASSESSMENT METHOD FRAMEWORK	38
TABLE A-3: RISK ASSESSMENT – THREAT CONDITION IDENTIFICATION AND EVALUATION.....	39
TABLE A-4: RISK ASSESSMENT - THREAT SCENARIO IDENTIFICATION	39
TABLE A-5: RISK ASSESSMENT - SECURITY MEASURE CHARACTERIZATION	39
TABLE A-6: RISK ASSESSMENT - LEVEL OF THREAT EVALUATION	40
TABLE A-7: RISK ACCEPTABILITY.....	40
TABLE B-1: PROCESS ACTIVITY REFERENCES.....	41
TABLE C-1: SECURITY ASSURANCE OBJECTIVES.....	43
TABLE D-1: PREPARATION MEANS	48
TABLE D-2: WINDOWS OF OPPORTUNITY	49
TABLE D-3: EXECUTION MEANS	50
TABLE D-4: MAXIMUM EFFECTIVENESS PER SECURITY MEASURE TYPE.....	51
TABLE D-5: MAXIMUM COMBINED EFFECTIVENESS	55
TABLE D-6: DIFFICULTY OF ATTACK EVALUATION TABLE.....	55
TABLE D-7: RISK ACCEPTABILITY TABLE.....	57
TABLE D-8: RISK EVALUATION MATRIX.....	58
TABLE D-9: IDENTIFIED SECURITY MEASURES.....	62
TABLE D-10: COMBINED EFFECT ASSESSMENT	62
TABLE D-11: EXAMPLE THREAT SCENARIO 1	63
TABLE D-12: EXAMPLE THREAT SCENARIO 2	63
TABLE D-13: EXAMPLE THREAT CONDITION EVALUATION TEMPLATE.....	63
TABLE D-14: MEASURE EFFECTIVENESS SCORE VS EFFECTIVENESS OBJECTIVE.....	64
TABLE D-15: FINAL LEVEL OF THREAT	64
TABLE E-1: SECURITY SURVEY	71
TABLE E-2: IDENTIFIED INFORMATION ASSETS	72
TABLE E-3: APPLICABLE TYPE OF ATTACKS	75
TABLE E-4: THREAT CONDITION IDENTIFICATION AND EVALUATION	76
TABLE E-5: THREAT SCENARIO IDENTIFICATION	80

CHAPTER 1

INTRODUCTION

This document is the product of the EUROCAE Working Group WG-72, titled "Aeronautical Systems Security" to provide additional guidance for applicants implementing an Airworthiness Security Process as specified in ED-202A / DO-326A [14] to address information security for certification of aircraft and its systems.

1.1

PURPOSE

This document provides a set of methods and guidelines that may be used within the airworthiness security process defined in ED-202A / DO-326A. The current version of this document only provides the first set of guidance for methods; subsequent versions will provide further examples. Any of these sets of methods may be used to comply with the ED-202A / DO-326A process. The provision of only a single set of examples in this version is not intended to mean there is only one acceptable set of methods; there will be other equally valid methods described in subsequent versions. Applicants and authorities should consider these methods, and alternative practices if and when they are proposed.

This document presents a first stage on the way to provide methods and considerations for security aspects. Its publication aims at allowing the Industry to experiment these methods and to assess their applicability. The content of this document is not intended as a complete means of compliance for certification.

WG-72 considers this document as incomplete as it still exhibits open topics in need of further deliberations. In particular, section 2.2.1 (Threat Condition Identification and Evaluation), is to be detailed further. The approach described in sections

- 2.3.3 (Statement of adequate level of protection),
- 2.4.1 (Assurance level definition) and
- 2.4.2 (Principles of security assurance assignment)

for risk acceptability and security assurance in addition to some security verification process objectives (in particular the considerations about structural coverage in section 3.2.5.4, and the corresponding elements of the table C-1 in Appendix C) will be revised in the next version of this document.

This document will be updated following the feed-back received from the Industry.

1.2

SCOPE

Airworthiness security is the protection of the airworthiness of an aircraft from intentional unauthorized electronic interaction.

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.

This guidance provides methods and considerations for securing airworthiness during the aircraft life cycle. It was developed as a companion document to ED-202A / DO-326A "Airworthiness Security Process Specification" which addresses security aspects of aircraft certification and ED-204 / DO-355, "Information Security Guidance for Continuing Airworthiness" [15] which addresses airworthiness security for continued airworthiness.

This document assumes knowledge of other applicable guidance material, including e.g. ED-79A / ARP 4754A [11], ED-135 / ARP 4761 [13], ED-12C / DO-178C [10], and ED-80 / DO-254 [12] and with the advisory material associated with FAA AMJ25.1309 [1] and EASA AMC 25.1309 [9], 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, CS-P, Part 23, Part 27, Part 29, Part 33, and Part 35.

The methods and considerations of this document provide guidance for accomplishing the airworthiness security process activities identified in ED-202A / DO-326A.

More specifically, this version of the document addresses the activities in the areas of security risk management and security assurance.

A future version of this document is planned to address further activities in the areas of security development, aircraft modifications, continuing airworthiness and security aspects of certification.

Appendix B lists the ED-202A / DO-326A activities and references that are addressed in this version of the document.

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

Readers should be aware that this document provides additional guidance for the airworthiness security process specified in ED-202A / DO-326A.

This document is organized into three chapters plus appendices. The chapters can be used in concert with each other or stand alone.

- Chapter 1 introduces the document.
- Chapter 2 establishes methods for the risk management activities of the airworthiness security process.
- Chapter 3 provides security assurance considerations and methods.

The appendices contain summaries and additional informative material that may aid in the comprehension and usage of the document chapters.

- Appendix A summarizes the input and output data of risk management activities described in chapter 2.
- Appendix B links ED-202A / DO-326A process activities to the sections of this document.
- Appendix C summarizes the security assurance objectives from chapter 3.
- Appendix D contains example methods for the risk assessment framework in chapter 2.
- Appendix E contains examples for the methods in chapter 2 and appendix D.
- Appendix F contains the glossary of terms and acronyms. Readers are expected to be familiar with the definitions in the glossary in order to correctly interpret the body of this document.
- Appendix G contains the list of external references used in this document. On the first use of an external reference, a numbered link to the full reference in the appendix is added in the body of this document.

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 F and used.

- Terms intended to have a specific technical meaning are defined in the Glossary in Appendix F 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.

1.5

RELATIONSHIP TO OTHER DOCUMENTS

This document provides additional guidance for the airworthiness security process and is referenced by ED-202A / DO-326A.

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

CHAPTER 2

RISK MANAGEMENT

2.1 SECURITY SCOPE

This section discusses the definition of the security scope (assets, security perimeter and security environment) of an aircraft or system as referenced in section 3.1 of ED-202A / DO-326A.

For ED-202A / DO-326A and 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."

The security perimeter catalogues the elements of the aircraft or system that have an interface with external systems or persons. Of particular note are functional interfaces, software parts, configuration management, and data load processes, and any process which is used to operate or manage a system.

The security environment is defined to capture the assumptions about the persons, organizations, and external systems so that the potential threat sources may be identified, such as threats from airline business information systems.

The ED-202A / DO-326A Airworthiness Security Process Specification does not differentiate between process activities related to assets, security perimeter and security environment. To provide further guidance, more detail than in ED-202A / DO-326A is described in this document.

The first step to describe the security scope consists of the identification of assets and then the specification of their security perimeters. Both of these activities may be conducted without information on attackers or safety assessment. Needed inputs are the functional architecture and the aircraft/system interface specifications. No expert security knowledge is required to conduct this step.

The next step is the creation of the security environment description with all relevant assumptions.

The definition of the security scope should be performed on aircraft level.

When a security scope definition is performed on other levels of the aircraft development (system and subsystem) it only adds information that is not included in the aircraft security scope (for example assumptions about interactions between different systems within an aircraft). If a (sub)system security scope is defined, it should only contain information that does not conflict with the aircraft level security scope.

A (sub)system security scope should be defined when a (sub)system risk assessment relies on additional assumptions not included in the aircraft security scope.

A detailed example of how to define a security scope is found in Appendix E.

2.1.1 Assets

Assets are addressed in various different contexts throughout this document. While some sections apply to all assets in general, other considerations apply only to a specific kind of assets.

The asset identification should include a suitable level of detail to facilitate the risk assessment.

Considering a development process, which may be based on ED-79A / ARP 4754A in accordance with the applicable aircraft certification basis (see ED-202A / DO-326A, Figure 3-4: “Security Activities in ED-79A / ARP 4754A Aircraft Development Process Model”), the assets may be identified as outputs of development process activities. Typical activities are:

1. Identification of Aircraft-Level Functions, Function Requirements and Function Interfaces;
2. Allocation of Aircraft Functions to Systems;
3. Development of System Architecture;
4. Allocation of System Requirements to Items;
5. System Implementation;
6. Aircraft Function Development

These activities will mainly identify function, system and item assets. Item assets may range from a LRU to a binary stream loaded in a Programmable Logic Device.

Significant information, data and process assets need to be identified as well, including:

- Data, characterized by external data connections from or to a system;
- Data, characterized by internal data connections through a system;
- Data kept by the system as part of its operation, including system logs and fault data; and
- Data used by the system to define its function and configuration, generally considered part of the system's installation and administration data, including:
 - Software parts,
 - Databases, such as navigation databases, and
 - Configuration information, such as subscriber information, firewall rules, security keys, digital certificates, personality modules.

2.1.1.1

Assets identification for a new development

Development activities, which may be produced by ED-79A / ARP 4754A, ED-12C / DO-178C, ED-80 / DO-254 in accordance with the applicable aircraft certification basis, generate a set of outputs that are registered by the system/software/AEH development process documents. The first activity registers the aircraft function, their requirements and interfaces among them and the security environment. The functions and the interfaces are the first group of assets (see e.g. ED-79A / ARP 4754A section 4.1.4).

The next activity should select the systems that support the aircraft functions and external interfaces. It also should identify the information flow between systems as well as human operators' interfaces considering operational and support aspects. The systems, system functions, interfaces, data consumed and provided are the next set of assets (see e.g. ED-79A / ARP 4754A section 4.1.5 and 4.3).

With the systems that constitute the aircraft and the information flow between them in hand, the next step is to develop the system architecture that enables the conceptual system to exist as a physical system. At this point, the item interfaces and associated technology to be used, data consumed and provided are the next set of assets (see e.g. ED-79A / ARP 4754A section 4.1.6 and 4.4).

The items are composed by software and hardware that have shared responsibility to provide the system functions. Its hardware-software interfaces as well as its protocols should be considered as part of the assets (see e.g. ED-79A / ARP 4754A section 4.6.1.2, 4.6.1.3 and 4.6.3). Software Design Process defined by ED-12C / DO-178C produces as a primary output the software architectures and low-level requirements where can be identified partitioning architecture and interfaces between software components (data flow and control flow).

For instance, the documents suggested by ED-12C / DO-178C (PSAC) and ED-80 / DO-254 (PHAC) when applicable can be used as sources to collect this information.

This is an iterative development process and the asset list may change with inclusion or removal of new items, e.g. as advised by ED-79A / ARP 4754A, due to architectural changes in the product and improvement of its maturity.

It is important to keep the traceability of the lower level assets and higher level to evaluate the impact of a piece of software to an aircraft function.

Another area of concern is the assets that are usually indirectly involved in aircraft operation or maintenance. ISO/IEC 27005:2011 Annex B provides some examples of assets that may be used in a threat scenario.

ED-204 / DO-355 provides guidance about the protection of supporting assets like transportable equipment (e.g. GSE), processing peripheral (e.g. removable disk drive), data medium (e.g. CD-ROM), electronic medium (e.g. memory, floppy disk) and others.

2.1.1.2 Identification for existing assets

If existing assets are modified or added to an aircraft (including re-use of system/item on a new aircraft), an update cycle has to be executed, in conjunction with a Change Impact Analysis (as described in ED-202A / DO-326A, chapter 4).

In this case the update cycle starts with a review and update of the list of assets and their security perimeters, if available from a previous assessment. If no list of assets is available, it should be created. It is recommended that an assessment of the impact of inclusion of a new or modification of a function at aircraft level (see ED-79A / ARP 4754A section 4.2) is performed.

2.1.1.3 Asset identification considerations

An applicant may use these considerations to identify potential assets. This survey may include the following questions for elements that have a safety effect:

1. Does the element under analysis use field-loadable software or reprogrammable hardware (FLS)?
2. Is the element under analysis configurable by the end user? A configurable system may use a configuration file.
3. Does the element under analysis use an aeronautical database?
4. Does the element under analysis use an operating system?
5. Does the element under analysis use network interfaces to shared media or resources? A networked connection and any resource used to communicate or store data should be considered.
6. Does the element under analysis use wired network interfaces to access ground resources?
7. Does the element under analysis use wireless network interfaces to access ground resources?
8. Does the element under analysis provide interfaces to removable media and electronic devices like Electronic Flight Bags, external hard disks, CD-ROMs or USB sticks?
9. Does the element under analysis provide interfaces to Ground Support Equipment?

NOTE: *These questions may help to identify assets and they may be verified via interviews with the system owner to assure the correct understanding of the question and answer contexts. The interviewer may exercise their elicitation skills to get the best understanding of the answers.*

2.1.2 **Security Perimeter**

The security perimeter catalogues the elements of the aircraft or system architecture that have an interface with external systems or persons. These are the elements by which an aircraft or system can be affected or interacted with. Of particular note are functional interfaces, software parts, configuration management, and data load processes, and any process which is used to operate or manage a system. External systems and persons are considered to be avenues for off-board threats, such as threats from airline business information systems.

The security perimeter description includes:

- Physical interfaces, i.e. interfaces that require a physical presence in or near the aircraft, for example Ethernet ports, wireless transceivers, USB plugs,
- Logical connections, i.e. interfaces that can be used remotely, often without any distance restriction, for example network connections, serial links, application interfaces. Useful details include:
 - Network protocols (e.g., IP, ICMP, ARINC664P7 [3], ARINC429 [2]),
 - Network services (e.g., DNS, webserver, monitoring/logging service, database server, IPSEC client), and
 - Information flows (e.g., unidirectional or bidirectional connection, data source/sink or forwarded data, connection endpoints).
- Intended accessibility:
 - Interfaces within the aircraft for use by passenger devices,
 - Interfaces within the aircraft for use by cabin and flight crew devices,
 - Interfaces within the aircraft for use by maintenance and product support devices.
 - Interfaces with ground systems,
 - Interfaces to other aircraft systems.

The amount of detail should be appropriate to the phase of the development. During preliminary design, the security perimeter needs not specify the particular protocol or technical design of the external interface as should be specified during final integration. It needs only to specify the general nature of the interface and the external persons that can contact that part through that interface.

Field-Loadable Software (FLS) and User Modifiable Software (UMS) are external data that are transmitted through the aircraft dataloading functions from the external interfaces that support maintenance. When there is an addition or modification of connectivity and interfaces that can add new opportunities for corruption and tampering through systems on the aircraft, then the interfaces for managing FLS and UMS should be included in the security perimeter and threat identification.

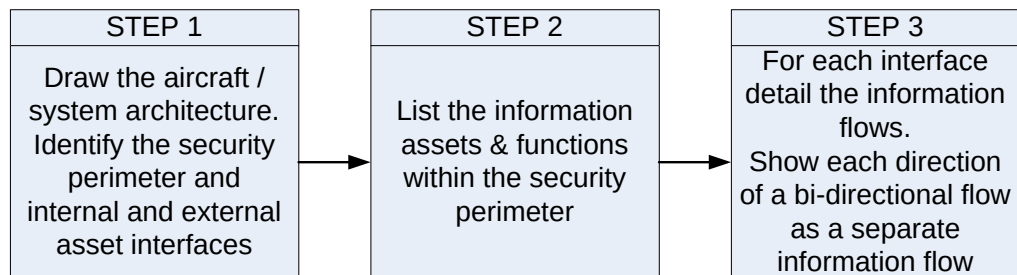


FIGURE 2-1: STEPS FOR DETERMINING SECURITY PERIMETER

2.1.3

Security Environment

The security environment describes the assumptions and requirements about the persons, organizations, and external systems outside the security perimeter that interact with the assets under consideration.

NOTE: *Assumptions are environmental conditions beyond the control of an operational authority and should be validated through a validation study within the Verification Activities. External requirements should be documented in the Security Guidance Documentation, see section 3.5.1.*

Considerations that may affect the risk assessment are relevant and should be expressed as assumptions in the security environment, including:

- Classify persons and organizations by their authorization and trust relationships, typically by defining roles.

Example: *If flight plans prepared by ground personnel are part of a security perimeter, then assumptions about the trustworthiness of the ground personnel role should be added to the security environment.*

- Classify the interfaces of the security perimeter by the roles and entities that have access to them.
- Describe the potential types of attack that are considered or not considered for an interface of the security perimeter.
- Threat source classification.

Example: *Classification according to ARINC 811 [4]*

- Any protection outside the aircraft / system under consideration that is taken as given in the risk assessment.

Examples: *Security measures within the ground IT networks, Airport physical security, access policies such as in air (e.g. avionics bay), on ground in airport environment or on ground in MRO operations*

- Relevant operational and maintenance policies

2.1.4

Changes in the Security Environment

The airworthiness security process reflects changes in security risks due to external evolution as part of the life-cycle security risk management.

The security environment is monitored and updated to capture the changing security environment of an aircraft/system. During development, it is updated as part of the development activities. During operation, it is updated as part of the continuing airworthiness activities.

Security environment updates could be triggered by new attack techniques, new technology introduced into the environment (e.g. wireless communication, IPv6, tablets), new services (e.g. cloud computing), capacity increase (e.g. 2G vs. 4G cellular protocols), etc.

Examples may include:

- A new wireless software loader might violate assumptions about physical access control for software loading.
- New attack techniques against 3G/UMTS encryption might violate assumptions about effectiveness for the encryption to protect the confidentiality of data used in aircraft to ground communication.

Updates to the security environment can affect threats and security risks for assets. A re-assessment of the threat identification, threat scenarios and security risks should be done if the updated security environment is not yet covered by the existing threats, threat scenarios and security risks. If modified security risks for assets are found to become unacceptable, risk reducing actions should be initiated. Another iteration of all relevant steps of the process has to be conducted until the updated security environment is completely addressed by the airworthiness security process.

As soon as the re-assessment on a process step results in no change, the remaining steps need not be executed again. Examples may include:

- A new attack technique against 802.11 wireless encryption is published. This invalidates an assumption in the security environment and triggers a re-assessment of security risks. The threat identification is updated with another threat scenario for an aircraft system. But since this (hypothetical) system design is always using an encrypted tunnel on top of all wireless connections, there is no change in severity and the security risk remains unchanged. Process steps regarding security measures and security requirements need not be conducted.

2.1.5

Identifying nested assets

Assets, security perimeters, and security environments are determined to the same detail as other related architectural features during development. That is, there are aircraft level assets, system level assets, subsystem level assets, item level assets, down to the lowest level.

At the aircraft level, the security perimeter and security environment primarily address off-board systems, persons and interactions, while at the lowest levels, the security perimeters and security environments primarily address the interactions between systems and localized effects on systems with interfaces at the aircraft perimeter.

NOTE: *In the following diagrams data and control flows are intentionally not represented to simplify the information presented. These diagrams do not represent a design or architecture but are only an abstract visualization of the concepts presented in this chapter.*

Assets can be comprised of or contain other assets (called “nested assets” hereafter). 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. See Figure 2.2.

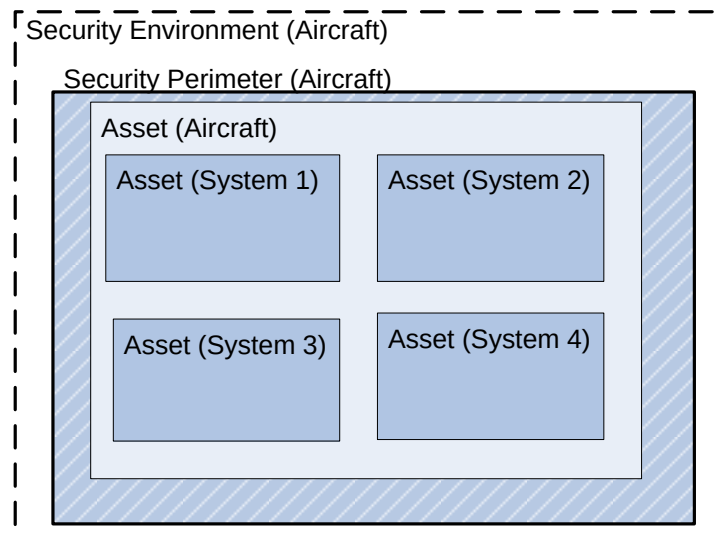


FIGURE 2-2: NESTED ASSETS WITHIN AIRCRAFT

Security perimeters can contain other security perimeters and/or assets. And multiple assets can share a single common security perimeter, as shown in Figure 2.3.

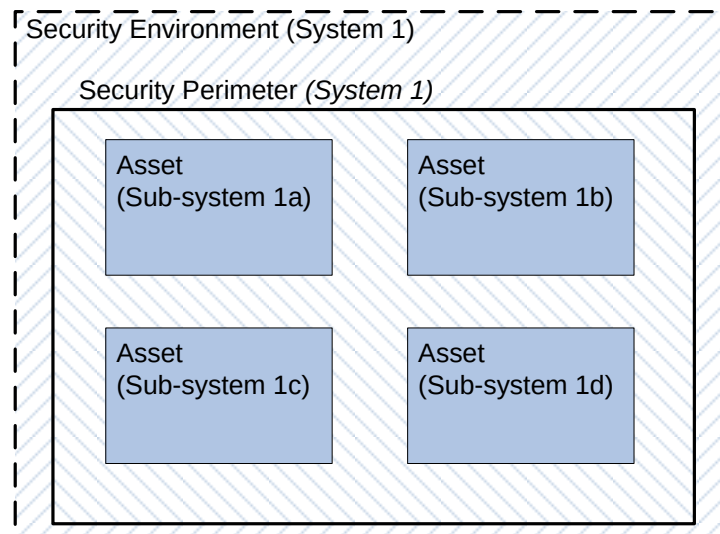


FIGURE 2-3: NESTED ASSETS WITHIN SYSTEM

A system can simultaneously share a perimeter with the aircraft external perimeter (e.g., a wireless system) and with internal perimeters.

The security environment of a nested asset is composed of the security environment of the parent security perimeter and the effects of any security measure within the parent security perimeter. In this definition, the “parent security perimeter” is the security perimeter of the next higher level in the design (i.e. the aircraft level for the system level). See Figure 2-4.

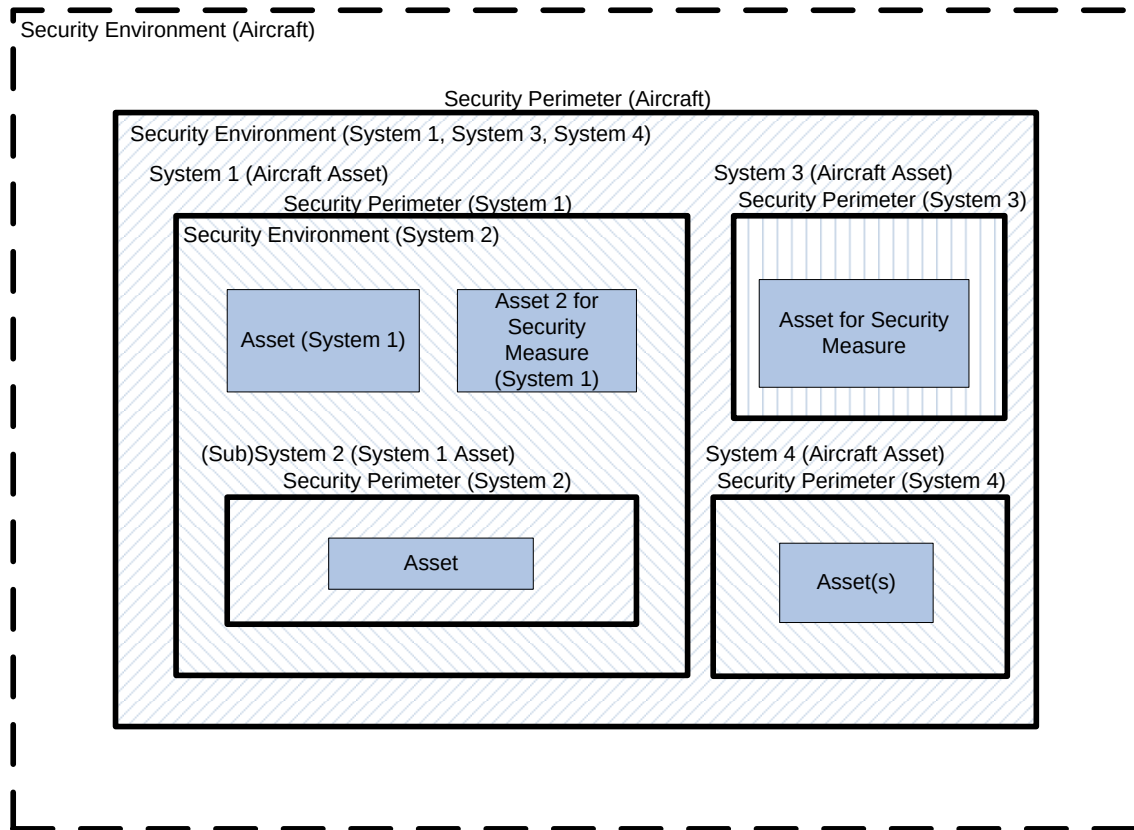


FIGURE 2-4: NESTED SECURITY ENVIRONMENTS

In the next illustration, Figure 2-5, asset F (e.g. a firewall) is a protection mechanism for the assets contained in security perimeters 2 and 3 (note the interfaces shown in this figure as dashed lines).

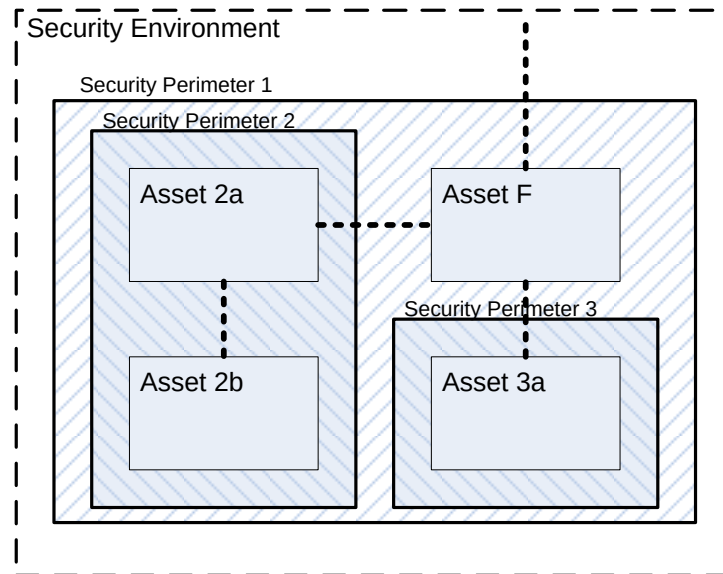


FIGURE 2-5: INTERFACES BETWEEN NESTED SECURITY ENVIRONMENTS

During the definition of a security perimeter or security environment, it may occur that the definition of a parent security perimeter or parent security environment is found to be incomplete or lacks detail. In such a case the parent security scope should be updated to ensure consistency of security scopes in the security architecture.

2.2

RISK ASSESSMENT METHOD FRAMEWORK

First of all, as a reminder, preliminary risk assessments are performed during the design phase while final security risk assessments are performed after implementation during the integration phase. Therefore, differences between preliminary and final assessments appear at objective level and in terms of data to be used by some activities as mentioned hereafter.

Preliminary security risk assessments objectives are two-fold: identify Security objectives and assess that the design is at an acceptable theoretical security risk level.

Final security risk assessment objectives are to demonstrate that residual risks are acceptable.

In terms of data to be used, the former use design data while the latter use actual data, mainly coming from robustness and penetration test results. This major difference impacts data used to perform "Security Measure Characterization" and "Threat Scenario Identification". Because the "Level of Threat Evaluation" takes their outputs in input, the level of threat is impacted as well.

For the purpose of airworthiness security, risk levels do not need to be defined explicitly, but can be expressed as statements about risk acceptability with the criteria given in section 2.3.

Results of a risk assessment need to be reproducible. Therefore the results of a risk assessment (i.e. the risk of the threat scenarios) should be traceable from inputs to outputs. If a risk assessment does not follow the method chosen by the applicant, all deviations with the regard to the method need to be justified.

Appendix D contains example methods that implement parts of the method framework defined here.

2.2.1

Threat Condition Identification and Evaluation

The purpose of this activity is to generate a list of threat conditions and associate them with a severity of the resulting failure for each security attribute (typically Confidentiality, Integrity and Availability).

This activity is intended to be initially conducted on a high level early in the development process.

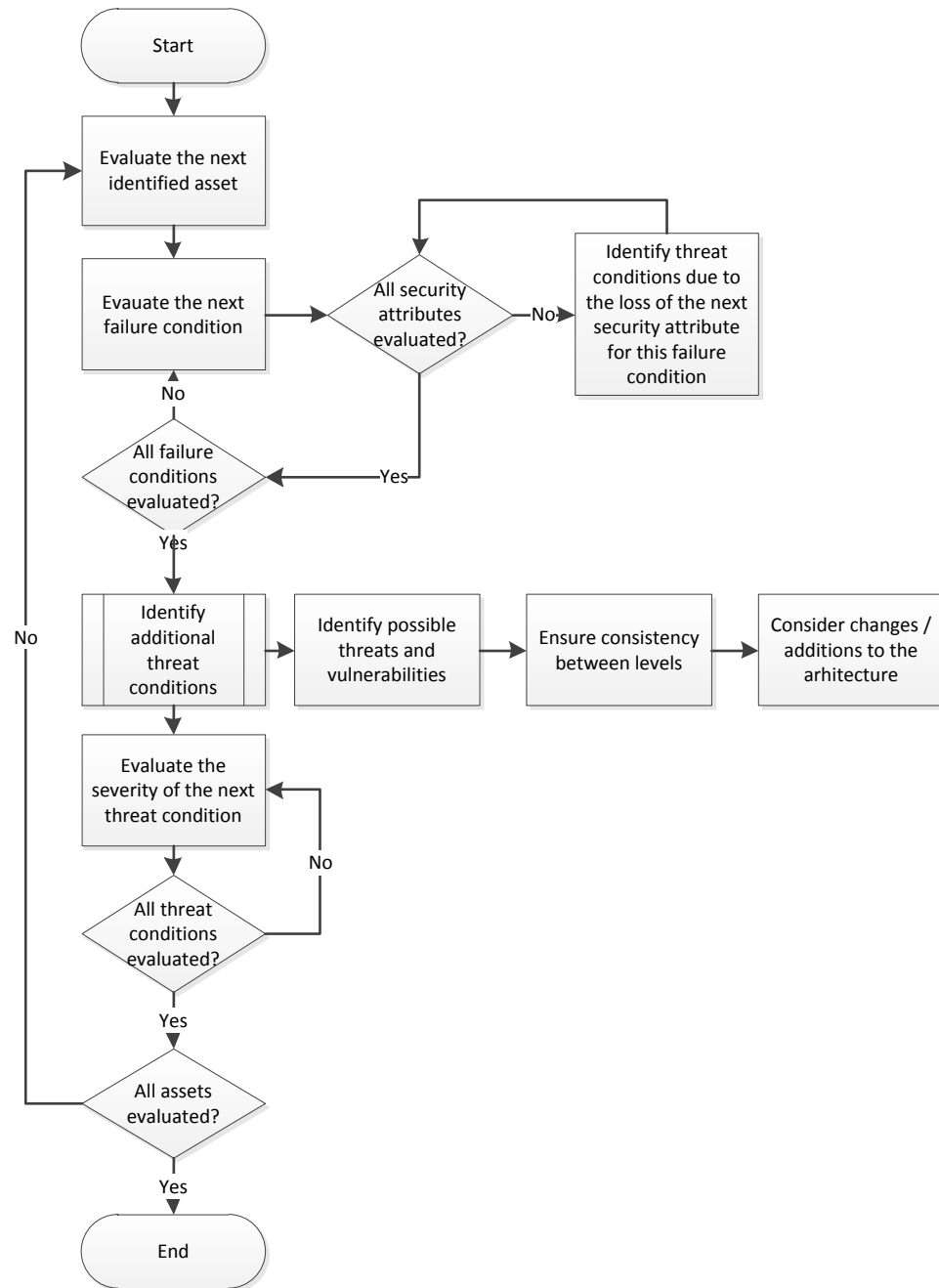
The inputs to this activity are the outputs of the design phase of the development process. It is important that all relevant threats are included. Pre-existing threat catalogues can be used but they are not a substitute for expert consideration of the threats at the time of the assessment.

Inputs for this activity generally include:

- Outputs of the aircraft/system design phase :
 - Aircraft/System Architecture;
- Functional Hazard Assessment (including failure conditions and their severity); Inputs from the initial stage of the security design process are also required:
 - Security environment;
 - Security perimeter including the asset inventory;
 - List of security attributes (typically Confidentiality, Integrity and Availability).
 - Other documents (when available) may also be useful, e.g. Common Cause Analysis, FMEA, depending on the maturity of the aircraft/system implementation.

The evaluation method is performed according to the following steps:

- Identify the initial threat conditions.
 - Identify those failure conditions on the assets that can be caused by a loss of security attributes. This can be performed by using a catalogue of threats for the specific environment. These threats are analysed to determine the potential for a threat to result in a failure condition.
- Identify additional threat conditions.
 - Additional threat conditions are identified through the completion of the analysis of possible threats and vulnerabilities. Threat and vulnerability catalogues and expert analysis reduce potential for missed threat conditions.
 - Ensure that there is consistency between the upper (aircraft) level and lower (system/subsystem) levels of the assessment (refer to section 2.2.2.2).
- Evaluate the effect of the threat condition on the asset as defined by the loss of the security attributes (loss of Availability, Integrity, Confidentiality). These attributes are addressed independently and a failure condition may result in multiple losses with differing effects and impacts. For example, the impact due to loss of Availability may be different than loss of Confidentiality.
- Associate the severity of the threat conditions against the effect on aircraft, flight crew and occupants and against the severity classification, as defined in e.g. AMC/AMJ 25.1309, AC23.1309-1E - extended to include the No Safety Effect classification -, AMC E210 and AMC E510. At this point there is no evidence that the classifications of severity of threat conditions can deviate from those for failure conditions.



It is recommended to use the same terms and expressions for threat conditions than used for failure conditions in order to ease keeping consistency between security and safety data.

Appendix D.2 provides an informative illustration of a template for capturing the required information.

2.2.1.1

Threat conditions not directly related to failure conditions

As discussed in ED-202A / DO-326A, threat conditions are conditions resulting from exploitation of vulnerabilities, which have a safety effect on the aircraft or the system.

In addition, in the iterative process of security risk assessment and security architecture development, unacceptable security risks are addressed by the definition of security measures, as described in section 2.2.3.

Security measures can themselves contain vulnerabilities that may lead to additional threat conditions.

In this case, the link between the threat conditions and the failure conditions is indirect through the security measure that mitigates some unacceptable security risk.

Therefore, any time a function/system/item, specifically (but not exclusively) a security measure is added or modified the threat condition identification and evaluation activity should be re-entered in order to assess the newly introduced element as an asset.

Example: A security measure prevents access to another function, but is itself subject to “Denial of Service” attacks, thus introducing an additional “loss of availability” threat condition.

2.2.2

Threat Scenario Identification

2.2.2.1

Identifying Threat Scenarios

Structure of a threat scenario:

- Threat sources: a list of threat sources (selected from the security environment) that may perform such a threat scenario
- Attack vector (Interface used to get into the security perimeter, type of attack)
- Track of the attack path: a list of assets used to reach the target, including the target itself, and including the assets of the preventive/deterrent security measures that have been by-passed or tampered to get through the attack path. On this path there may be the following elements:
 - Victims, that are systems/items which happen to be on the path but which do not provide protection that an applicant chooses to characterize (despite the possibility that they expose certain security properties, they will be ignored in the risk assessments). A victim is not a target of this attack;
 - The target of attack and its associated asset (the latter two may or may not be implemented in the same system/item);
- Security measures: a list of the preventive/mitigation security measures that could mitigate or prevent the attack at each stage of the attack path
- Threat conditions: a list of threat conditions triggered by the threat scenario

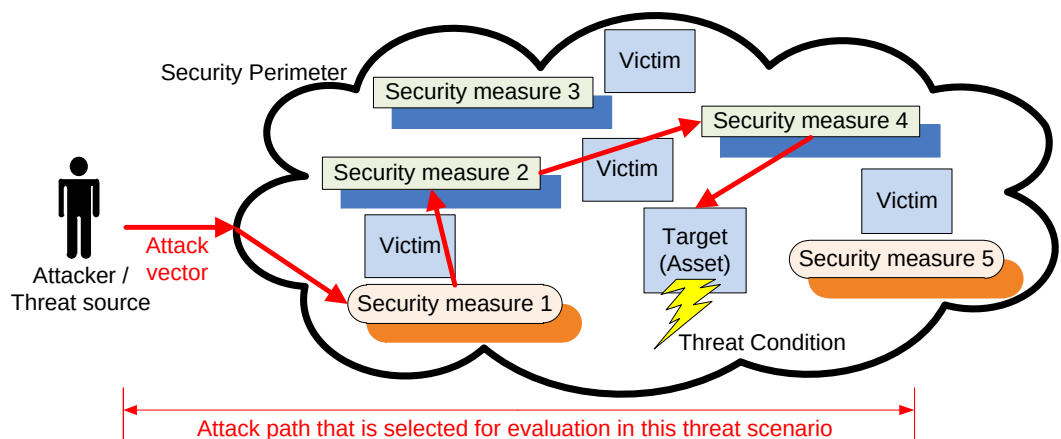


FIGURE 2-6: THREAT SCENARIO EXAMPLE

The term “Threat Scenario” is formally defined in ED-202A / DO-326A as “The specification of intentional unauthorized electronic interaction, consisting of the contributing threat source (attacker and attack vector), vulnerabilities, operational conditions, and resulting threat conditions, and events by which the target was attacked”, but seems to generate differing notions. This may be the result of the terminology also used in ED-202A / DO-326A, section 3.2.1, in which it is stated that “Threat conditions are caused or contributed to by a loss of a security attribute of an asset, see TABLE 3-1”.

To clarify the difference between the terms "Target" and "Asset" (as used in ED-202A / DO-326A), the usage in this document is as follows:

- **Target:** The destination of the attack associated with a specific threat scenario.
- **Asset:** The element which exposes a threat condition, having an effect on the aircraft.

NOTE: *An asset that has a safety effect on the aircraft (the subject of ED-202A / DO-326A and ED-203) could also be regarded as a "safety asset" if the scope of a threat scenario is extended beyond airworthiness security. This also means that generally this could be extended to other aspects as well, i.e. "operations asset", "business asset", "branding asset", etc.*

Conclusion: A target and an asset of a threat scenario may be the same element in the architecture.

Example: *A threat scenario identifies the coherent compromise of multiple pieces of independent information provided by multiple separate items/systems. These pieces of information are consumed by another ("third") item/system, which exposes a threat condition having a safety effect on the aircraft. Thus, the targets of the attack are those systems/items, which separately supply the independent pieces of information, while the asset is the system/item, which consumes them all and consequently exposes the safety related threat condition.*

Checklist for the completeness of the threat scenarios:

- Have all actors identified during the security environment identification been considered? If a new actor (person or system) appears, it should be included in the external actor list.
 - Unauthorized access by organization actor (e.g. pilot, crew member, mechanic);
 - Unauthorized access by third party actor (e.g. airport, cleaning, security staffs);
 - Unauthorized access by outside actor (e.g. passenger, criminal);
- Have all interfaces and connections identified in the security perimeter been considered?
 - Consider scenarios with GSE/EFB/PED as the first stage of the attack.
- Have all attack paths to assets within the security scope been considered?
 - Consider a multi-stage scenario (e.g. (1) a media is changed by tampered one in stock. (2) a mechanic installs the tampered file in the aircraft which leads to the threat condition);
 - Consider a parent asset and all nested assets contained in it (e.g. a LRU stores a set of FLS before they are installed in the target LRUs; once it is compromised all FLS may be compromised too leading to multiple threat conditions);
- The misuse case can help to develop the threat scenarios.

No order is imposed for the definition of a threat scenario. The identification of threat scenarios may start with the threat conditions or the threat sources or any other element of the threat scenario.

Attack paths are used to describe the possible ways that an attacker might attempt to attack a target. An attack path includes the relevant elements inside the security perimeter that an attacker will face while conducting the attack. The attack path description is not limited to security measures, victims and targets, but these have to be included because they will influence the level of threat. Multiple attack paths may be combined in a single threat scenario if the attack vectors and targets are similar or identical.

There will be many ways that an attacker may conduct an attack on a specific target. And there may be multiple attack vectors for the same target and multiple targets reachable from the same attack vector. Threat scenarios should be defined in such a way that different kind of attacks are assessed in separate threat scenarios while similar attacks can be combined in one threat scenario.

Example: *If an additional attack path is identified in Figure 2-6, that only attacks security measure 3 instead of security measure 4 before reaching the target, and if the effect of security measures 3 and 4 is comparable, then both attack paths should be assessed as part of the same threat scenario. If on the other hand an additional attack vector is identified that allows for attacks on security measure 5 and subsequent attacks on the same target, and security measure has a different effect than security measures 3 and 4, that attack path should be assessed in a separate threat scenario. For the completeness of a risk assessment not only the identification of all interfaces, connections, attack methods and threat conditions needs to be taken into account but also all relevant attack paths that an attacker may choose to explore.*

It is important to note that a threat scenario is used to assess the risk only within the security perimeter of the target. That means that a threat scenario (for example in a system security risk assessment) may be just one part of another attack path within a wider security scope (for example the aircraft security risk assessment).

The comparability and reproducibility of threat scenario analysis results may be achieved if the assessor:

- Uses the same decomposition of architecture in all risk assessments. For example if the network is partitioned into security domains, different descriptions of the architecture should use the same partitioning.
- Uses a consistent model to describe the architecture (for example UK IS1 [17] method describes such modelling).
- Uses a consistent model to describe the security scope.

The threat scenario will be used in subsequent steps of assessment in order to characterize the risks.

2.2.2.2

Threat scenario consistency

In order to ensure that all risks identified at aircraft level are covered, it has to be ensured that threat scenarios from one development level are linked to threat scenarios from the level above. Example: All threat scenarios in a system level risk assessment should be linked to threat scenarios in the aircraft level risk assessment.

NOTE: *Threat scenarios on different levels are not expected to be equivalent. Typically there will be a one-to-many relationship, because a parent level threat scenario will cover the same threats as several lower level threat scenarios.*

If a threat scenario is newly introduced at a specific development level and cannot be linked to a parent threat scenario, a new threat scenario is created in the parent levels so the risk at aircraft level is clearly identified.

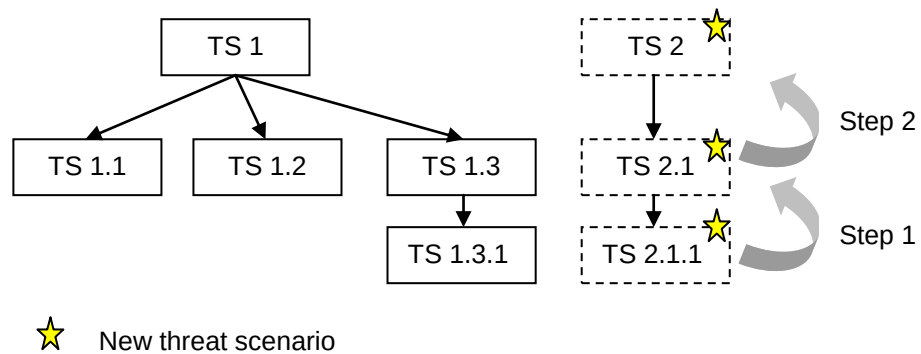


FIGURE 2-7: THREAT SCENARIO COVERAGE

New threat scenarios might appear at a specific development level (e.g. TS 2.1.1 in the case of Figure 2-7 above) due to the following reasons:

- Allocation of functions to platforms (shared resources) might uncover new ways of attacking them.

Example: Function A has a wireless interface. Functionally speaking, threats are identified from this wireless interfaces against function A. At a different development level, decision is made to allocate function B to the platform where function A is hosted. Because of this decision, function B is also potentially reachable via wireless (although not functionally specified). A new threat scenario is then created from wireless interface against function B (through a compromised function A).

- Implementation decisions: The way of implementing the functions might also uncover new ways of attacking them.

Example: Function A is supposed to forward passenger private information to a crew device. Implementation decision is made to store the information in a temporary file to be able to retransmit the information if a communication error occurs. Because of this decision, the storage device hosting the file becomes a new target and therefore new threat scenarios might need to be created.

In addition it has to be ensured that all applicable threat scenarios from a parent level risk assessment have been considered in the lower level risk assessments. Threat scenarios from the parent level are applicable if they affect the assets in scope of the lower level risk assessment.

Example: Three threat scenarios TS1, TS2 and TS3 have been identified for function A in the aircraft risk assessment. The risk assessment for the system that will implement function A needs to include threat scenarios that cover at least the same threats than TS1, TS2 and TS3.

An attack path for a specific target can cross multiple systems and/or devices. Risk assessments on a specific level (e.g. system) may identify threat scenarios that cover only parts of the complete attack path. In such cases a threat scenario for the complete attack path should be identified in a parent level risk assessment. Together with the above rules this ensures that the risk is properly considered in all affected systems.

2.2.3 Security Measure Characterization

Security measures are typically identified and specified during the design process for an efficient design process. Security measures may be identified and specified at other stages - this will form part of the continuing airworthiness activities. This section describes how security measures are characterized during the security development activities (see ED-202A / DO-326A figure 2-1). Security measures are not limited to designated security functions. Anything, including regular functions and procedures, can be taken into account if its effectiveness in a specific threat scenario can be justified. In general, anything that is able to reduce the level of threat should be regarded as a security measure.

All identified security measures need to be characterized to be applicable in a threat scenario. This activity needs to identify the security measure characteristics needed for the risk assessment: type, effectiveness and vulnerabilities.

Other security measure characteristics may be needed for other process activities but do not need to be identified within the risk assessment.

NOTE: *Security measures may include organisational requirements or operational instructions to crew (documented in FCOM, CCOM or Maintenance Manuals) that help prevent attacks. The methods for assessing the effectiveness of non-technical security measures taking into account human factors will be discussed in a future version of this document.*

The following information is required in order to be able to perform security risk assessment and elaboration of security requirements:

1. Known vulnerabilities in the system/subsystem/items of the security measures and victims, depending on current level of development.
2. Required effectiveness of the security measures in order to demonstrate acceptable security risk of the threat scenarios.
3. Sufficient interface and functional requirements (or reference/summaries to design data) about the security measures and the victims to build the attack paths and threat scenarios, and to allocate design requirements to systems/subsystem/items to conform with the threat scenarios and not introduce new unacceptable threat scenarios. Again, the level of detail (system/subsystem/item) will depend on the current level of development. More specifically:
 - a. When is the security measure applicable? E.g. what victims does it protect? E.g. what threat scenarios does it mitigate? When does it need to be effective? How is it bypassed?
 - b. When is the security measure exposed? E.g. what threat scenarios involve its assets? What are its interfaces and modes? How is it administered / maintained?

Assumption: The security architecture is an input for the security measure characterization activity.

NOTE: *The design of security measures and the security architecture is not addressed here, but will be provided in a future version of this document.*

TABLE 2-1: SECURITY MEASURE CHARACTERISTICS

Characteristic	Description
Description	Details that help to better understand and evaluate the security measure, including interfaces, functional specification, requirements, architectural and implementation details and references to external descriptions (e.g. security control from NIST SP800-53 [21] or SFC from Common Criteria [6])
Protected assets	List of elements that are protected by the security measure, including - Assets - Security attributes (Confidentiality and/or Integrity and/or Availability)
Type of effect	Preventive, Deterrent, Detective, Corrective or other types
Capability	Ability to protect in general (not specific to a threat scenario), e.g. ease of use, strength of mechanism, impact reduction
Dependencies	List of elements that support the security measure, including: - Assets and their known and inherent vulnerabilities
Implementation status	To track whether a security measure is planned, specified, implemented, verified,

The “Security Measure Characterization” activity provides different information to the “Threat Scenario Identification” and the “Level of Threat Evaluation” activities.

Outputs for the “Threat Scenario Identification” are used to determine whether a security measure exists on an attack path or may apply to a threat scenario. The relevant security measure characteristics are the type and its place in the architecture. Additional useful information includes protection capabilities, attack type coverage and dependencies (these characteristics will later be needed for the Level of Threat Evaluation).

Outputs for the “Level of Threat Evaluation” are used to evaluate the dependencies between security measures, their specific and combined effectiveness and their robustness against attacks on the security measures. In addition to the “Threat Scenario Identification” information, security measure characteristics should include the generic effectiveness, vulnerabilities and a detailed description (including available architectural, functional and technical details). Security effectiveness assurance will help to characterize the effectiveness and vulnerabilities more precisely.

2.2.4

Level of Threat Evaluation

The level of threat of one threat scenario needs to be evaluated on a scale of 5 levels to enable comparability of risk assessments with the risk acceptability criteria in section 2.3. Another reason is to ensure consistency with existing airworthiness regulations and standards.

The evaluation starts with the level of threat associated with the attack vector. Security measures applied to the threat scenario will reduce the level of threat. As a consequence, the level of threat at the attack vector will be the largest level of threat within the threat scenario. In this regard, anything that is able to reduce the level of threat should be regarded as a security measure.

The amount of reduction is determined by the effectiveness of the security measures. A numerical value may be assigned to the effectiveness of each security measure to allow calculation of the overall effectiveness of all security measures applied to one threat scenario. The relation of effectiveness and level of threat of a threat scenario is detailed in section 2.3.2.

The effectiveness assigned to a security measure is specific to the evaluated threat scenario and its combination of multiple security measures. A security measure may already have a capability identified in the security measure characterization activity. The effectiveness with regard to the specific circumstances of the threat scenario needs to be determined based on the capability of the security measure.

Example: a security measure may be designed to prevent against attacks on the confidentiality of a target. Such a security measure may have a high capability of protection against eavesdropping attacks but may be easily by-passed in the threat scenario and therefore would be evaluated with no effectiveness for attacks on the integrity of the target.

The order of the security measure effectiveness evaluation will not affect the overall result. But it is often desirable to identify intermediate results in the assessment. The number and order of evaluation steps should be defined and documented according to the intermediate results deemed useful.

One common order is the determination of an initial level of threat and a final level of threat to highlight the effect of added or modified security measures.

Another useful order is the determination of an intermediate level of threat taking into account only some types of security measures, for example only technical or operational or management security measures.

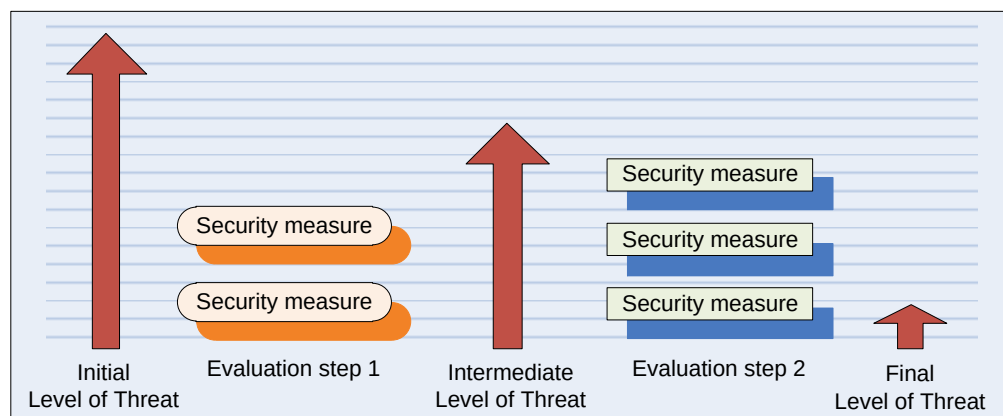


FIGURE 2-8: EVALUATION ORDER EXAMPLE 1

Example: The final level of threat is the same in Figure 2-8 and Figure 2-9. That means that there is no difference for the risk acceptance. But the different intermediate levels of threat may provide important considerations for the risk treatment strategy. The different representations of security measures in the figures are just a way to distinguish between measures security assessed in the first step from security measures assessed in the second step.

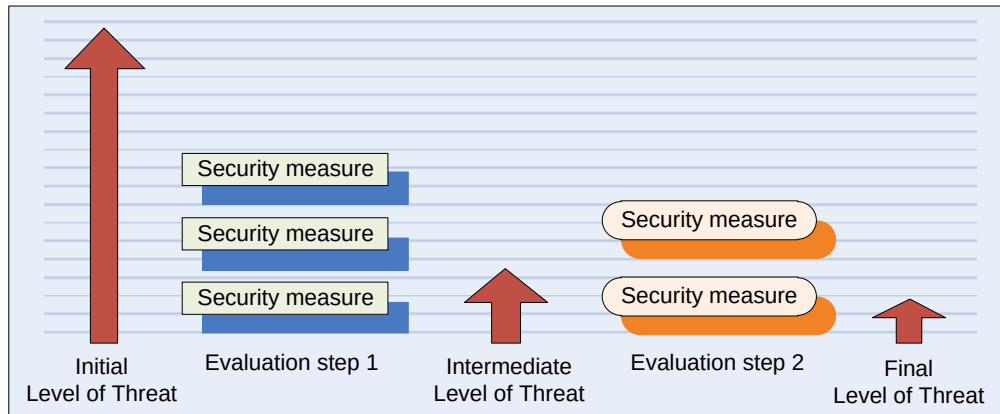


FIGURE 2-9: EVALUATION ORDER EXAMPLE 2

The level of threat will be evaluated using multiple criteria. The evaluation that is applied to determine the level of threat based on its criteria should be specified in the method. The method needs to express without ambiguity when and where human expert knowledge / engineering judgment is applied (and when and where it should not be applied).

The level of threat can be expressed by the effectiveness of security measures against an attack or by the exposure¹ of the target to an attack due to its vulnerabilities (summation of effectiveness or reduction of exposure).

Methods should at least evaluate the following criteria or be able to translate its criteria to these criteria in order to be comparable with the framework within this document. The mandatory criteria are defined as follows:

- **Elapsed time to prepare the attack** is the minimum amount of time taken by an attacker to identify the potential vulnerabilities that may exist in the target and the security measures, to identify potential attack vectors and attack paths, to acquire and/or build equipment and to develop and test potential attacks.
- **Elapsed time to perform the attack** is the minimum amount of time taken by an attacker to conduct an attack against the target.
- **Expertise required to prepare the attack** is the level of knowledge of a general topic needed for attack preparation. Examples include a specific technology, product, procedure or vulnerability identification method.
- **Expertise required to perform the attack** is the level of knowledge of a general topic needed to conduct the attack. Examples include a specific technology, product, procedure or attack method.
- **Knowledge of the target** is the specific level of knowledge or information about the target and attack path that is required to prepare and conduct the attack.
- **Window of opportunity** is the consideration that an attack is only possible at certain times (for example only during maintenance of the target) or under certain circumstances (for example an attack is only possible during other failure or attack events or an attack attempt that has to be sustained for an extended amount of time or repeated multiple times).

¹ Some methods may express exposure as a likelihood

- **Equipment required to prepare the attack** is the kind and amount of equipment, tools and resources needed to prepare and test the attack. Examples include samples of the target, software analysis tools, software and hardware attack tools, computing power (e.g. a server cluster to compute specific rainbow tables).
- **Equipment required to perform the attack** is the kind and amount of equipment, tools and resources needed to conduct the attack. Examples include use of specific technologies or products, software and hardware attack tools, botnets.

These criteria are not independent, but some of them may be substituted for each other in varying degrees. A method should include these criteria in such a way as to compensate for any dependence between criteria.

A method should define useful combinations of the mandatory criteria and possibly additional optional criteria for the Level of Threat Evaluation. It is not recommended that a method directly factors in all mandatory criteria in its evaluation (for the reasons given above). But a method should allow the reader to reconstruct how the mandatory criteria have been taken into account in a threat scenario evaluation.

NOTE: *These criteria are based on the factors given in CEM [7] section B.4.2.2 to support comparability with Common Criteria Methodology where needed. In contrast to the 5 factors used in CEM this document separates criteria for the attack preparation and attack execution so that the same underlying considerations result in 8 criteria. This allows for a more accurate evaluation of threat scenarios in which attack preparation and attack execution are separated by a significant amount of time or distinct roles and persons.*

Example: *An attacker with a high expertise will need much less elapsed time to perform an attack than an attacker with no expertise. If a method would consider the simple addition of “Elapsed time to perform the attack” and “Expertise required to perform the attack” criteria in the level of threat evaluation, it would account twice for what is actually the same consideration.*

The level of threat evaluation results in a statement about the effectiveness of protection in a specific threat scenario. Combined with the severity of effect as determined by the threat condition evaluation, it allows for a statement about the risk for a specific threat scenario as defined in ED-202A / DO-326A section 3.2. The risk is evaluated by the factors “severity” and “level of threat” and subject to the acceptance criteria detailed in section 2.3 of this document.

2.2.4.1 Combined Effectiveness Assessment

For an overall assessment of the combined effect of two or more security measures, special care needs to be taken so that in the specific case analysed, effects are not inflated. Such a mis-assessment would result in an underestimation of risks.

Care should be taken to analyse the relation between security measures involved in a threat scenario. Relations of different kinds should be analysed:

- **Independence**
A security measure that is independent from other security measures presents an additional barrier to the attacker in the specific threat scenario. A security measure that depends completely on another security measure will not increase the effectiveness for the specific threat scenario.
- **Diversity**
A security measure that is vulnerable to the same attacks than other security measures has a low diversity. Security measures are more diverse if they have less functionality, technology and code in common.
- **Isolation**
Are there physical or logical boundaries between security measures that prevent that compromise or failure of one security measure (or of a shared resource) also affects another security measure.

Examples for independent security measures:

- A firewall and an authentication service (for example password-based login)

Examples for dependent security measures:

- Security measure A (an Intrusion Detection System) that triggers security measure B (a secure mode, for example deactivation of network interfaces) if an attack is detected. If A fails to detect an attack, B will fail as well.

Examples for non-diverse security measures:

- Two firewalls that have the same implementation
- Two firewalls with different implementation but the same set of filter rules
- An authentication service and an input filter both implemented in Java (two different functions using the same technology and exposed to the same vulnerabilities in their implementation)

Examples for diverse security measures:

- Two firewalls that apply different filter rules and have different implementations using different sets of libraries on different operating systems

Examples for non-isolated security measures:

- Two security measures hosted on the same physical device using the same libraries, the same kernel or the same operating system resources (e.g. random number generator).

Examples for isolated security measures:

- Two security measures hosted on different physical devices
- Two security measures hosted on the same physical device but with strong logical segregation (e.g. hardware-assisted full virtualization of kernel, userspace and resources).

The following Figure 2-10 shows the principle to evaluate independence, diversity and isolation of security measures. The rules to apply to determine the combined effectiveness are given by the specific risk assessment method.