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

Airworthiness Security Process Specification

RTCA DO-326A
August 06, 2014

Prepared by: SC-216

Copies of this document may be obtained from

RTCA, Inc.
1150 18th Street, N.W., Suite 910
Washington, DC 20036

Telephone: 202-833-9339
Facsimile: 202-833-9434
Internet: www.rtca.org

Please call RTCA for price and ordering information.

FOREWORD

This document was prepared by Special Committee 216 (SC-216) and was approved by the RTCA Program Management Committee (PMC) on August 06, 2014.

RTCA, Incorporated is a not-for-profit corporation formed to advance the art and science of aviation and aviation electronic systems for the benefit of the public. The organization functions as a Federal Advisory Committee and develops consensus-based recommendations on contemporary aviation issues. RTCA's objectives include but are not limited to:

- coalescing aviation system user and provider technical requirements in a manner that helps government and industry meet their mutual objectives and responsibilities;

- analyzing and recommending solutions to the system technical issues that aviation faces as it continues to pursue increased safety, system capacity and efficiency;

- developing consensus on the application of pertinent technology to fulfill user and provider requirements, including development of minimum operational performance standards for electronic systems and equipment that support aviation; and

- assisting in developing the appropriate technical material upon which positions for the International Civil Aviation Organization and the International Telecommunications Union and other appropriate international organizations can be based.

The organization's recommendations are often used as the basis for government and private sector decisions as well as the foundation for many Federal Aviation Administration Technical Standard Orders.

Since RTCA is not an official agency of the United States Government, its recommendations may not be regarded as statements of official government policy unless so enunciated by the U.S. government organization or agency having statutory jurisdiction over any matters to which the recommendations relate.

This Page Intentionally Left Blank

EXECUTIVE SUMMARY

The guidance of this document adds to current guidance for aircraft certification to handle the threat of intentional unauthorized electronic interaction to aircraft safety. It adds data requirements and compliance objectives, as organized by generic activities for aircraft development and certification, to handle the threat of unauthorized interaction to aircraft safety and is intended to be used in conjunction with other applicable guidance material, including SAE ARP 4754A/ED-79A, SAE ARP 4761/ED-135, DO-178C/ED-12C, and DO-254/ED-80 and with the advisory material associated with FAA AC 25.1309-1A and EASA AMC 25.1309, in the context of part 25 for Transport Category Aircraft which include an approved passenger seating configuration of more than 19 passenger seats. This guidance is not intended for CFR parts 23, 27, 29, 33.28, and 35.15, normal, utility, acrobatic, and commuter category airplanes, normal category rotorcraft, transport category rotorcraft, engines, and propellers.

This document does not address:

a. Physical security or physical attacks on the aircraft (or ground element),

b. Airport, Airline or Air Traffic Service Provider security (e.g., access to airplanes, ground control facilities, data centers),

c. Communication, navigation, and surveillance services managed by national agencies or their international equivalents (e.g., GPS, SBAS, GBAS, ATC communications, ADS-B).

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

RTCA/EUROCAE documents on Aeronautical Systems Security will address information security for the overall Aeronautical Information System Security (AISS) of airborne systems with related ground systems and environment. This guidance material is for equipment manufacturers, aircraft manufacturers, and anyone else who is applying for an initial Type Certificate (TC), and afterwards (e.g. for Design Approval Holders (DAH)), Supplemental Type Certificate (STC), Amended Type Certificate (ATC) or changes to Type Certification for installation and continued airworthiness for aircraft systems, and is derived from understood best practice.

The FAA publishes additional guidance that may be used in combination with this document. Since aircraft electronic security requirements and regulations change, it is highly recommended that applicants contact the applicable certification offices (FAA or International Civil Aviation Authorities) to obtain the most recent guidance on the use of this document for certification projects.

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

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

This Page Intentionally Left Blank

TABLE OF CONTENTS

TABLE OF FIGURES

TABLE OF TABLES

The Page Intentionally Left Blank

1 INTRODUCTION

This document is the joint product of two industry committees: the EUROCAE Working Group WG-72, titled “Aeronautical Systems Security” and the RTCA Special Committee SC216, also titled “Aeronautical Systems Security”. WG-72 was formed to address information security for the overall Aeronautical Information System Security (AISS) of airborne systems with related ground systems and environment, while SC216 was formed more specifically to address information security for certification of aircraft and its systems. Both committees agreed that the guidance provided by this document and its companion documents constitute an acceptable means to address the increasing potential for intentional unauthorized electronic interaction with aircraft information systems.

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

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

1.1 Purpose

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

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

The FAA publishes additional guidance that may be used in combination with this document. Since aircraft electronic security requirements and regulations change, it is highly recommended that applicants contact the applicable certification offices (FAA or International Civil Aviation Authorities) to obtain the most recent guidance on the use of this document for certification projects.

1.2 Scope

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

and with the advisory material associated with FAA AC 25.1309-1A and EASA AMC 25.1309, in the context of part 25 for Transport Category Aircraft which include an approved passenger seating configuration of more than 19 passenger seats. This guidance is not intended for CFR parts 23, 27, 29, 33.28, and 35.15, normal, utility, acrobatic, and commuter category airplanes, normal category rotorcraft, transport category rotorcraft, engines, and propellers.

This document does not address:

a. Physical security or physical attacks on the aircraft (or ground element),

b. Airport, Airline or Air Traffic Service Provider security (e.g., access to airplanes, ground control facilities, data centers),

c. Communication, navigation, and surveillance services managed by national agencies or their international equivalents (e.g., GPS, SBAS, GBAS, ATC communications, ADS-B).

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 aircraft 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 DO-355/ED-204 "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 an 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.
- Appendix E contains a Rationale for an Airworthiness Security Process.

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 ISO27005:2011.

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.

This Page Intentionally Left Blank

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.

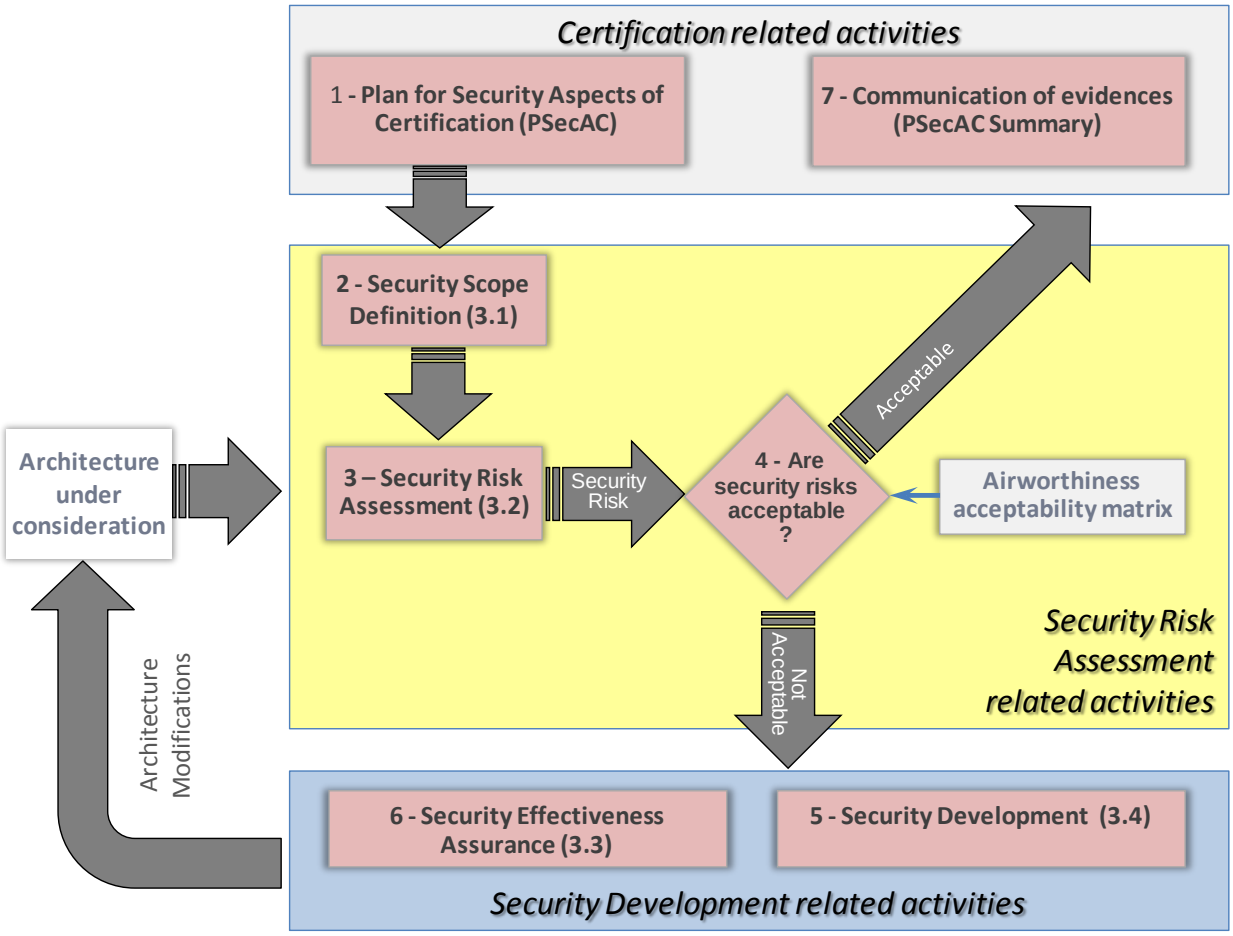

Figure 2-1 : Airworthiness Security Risk Management Framework

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 ISO27005 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 ISO27005 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 ISO27005 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 DO-355/ED-204)

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 ISO27005 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 DO-355/ED-204 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:

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

- At aircraft level: **Aircraft Security Operator Guidance (ASOG)**
- 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.

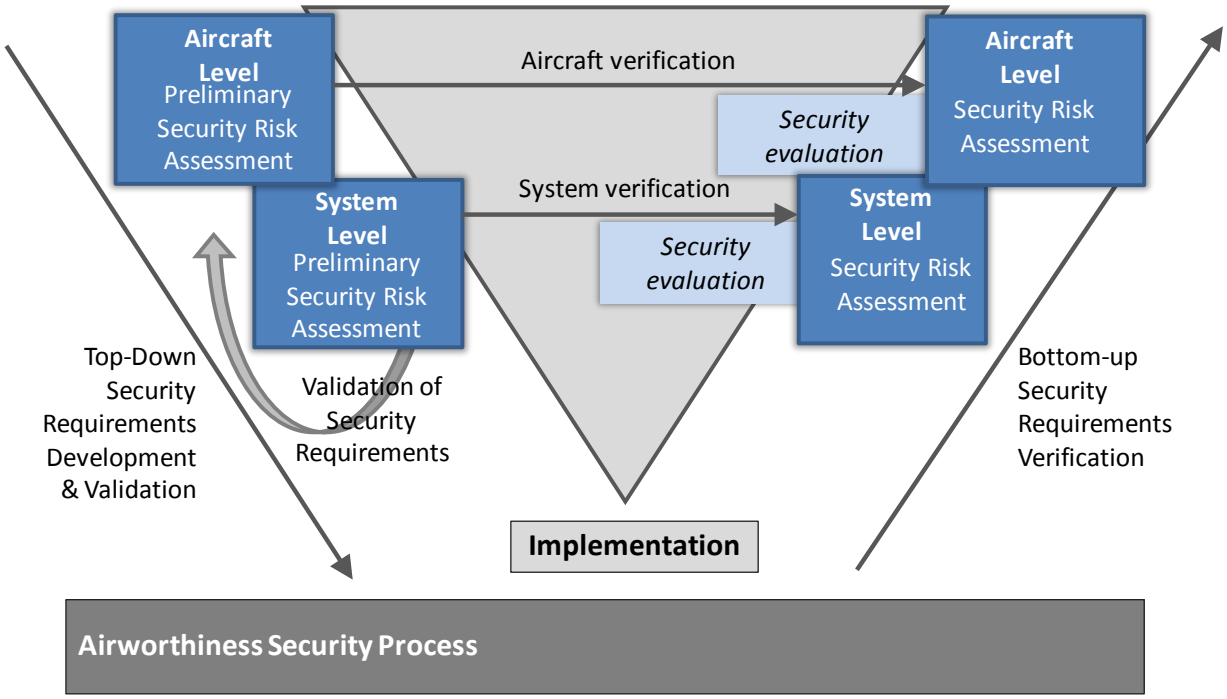

Figure 2-2 : Security Risk Assessment Related Activities in the development process V-model

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.

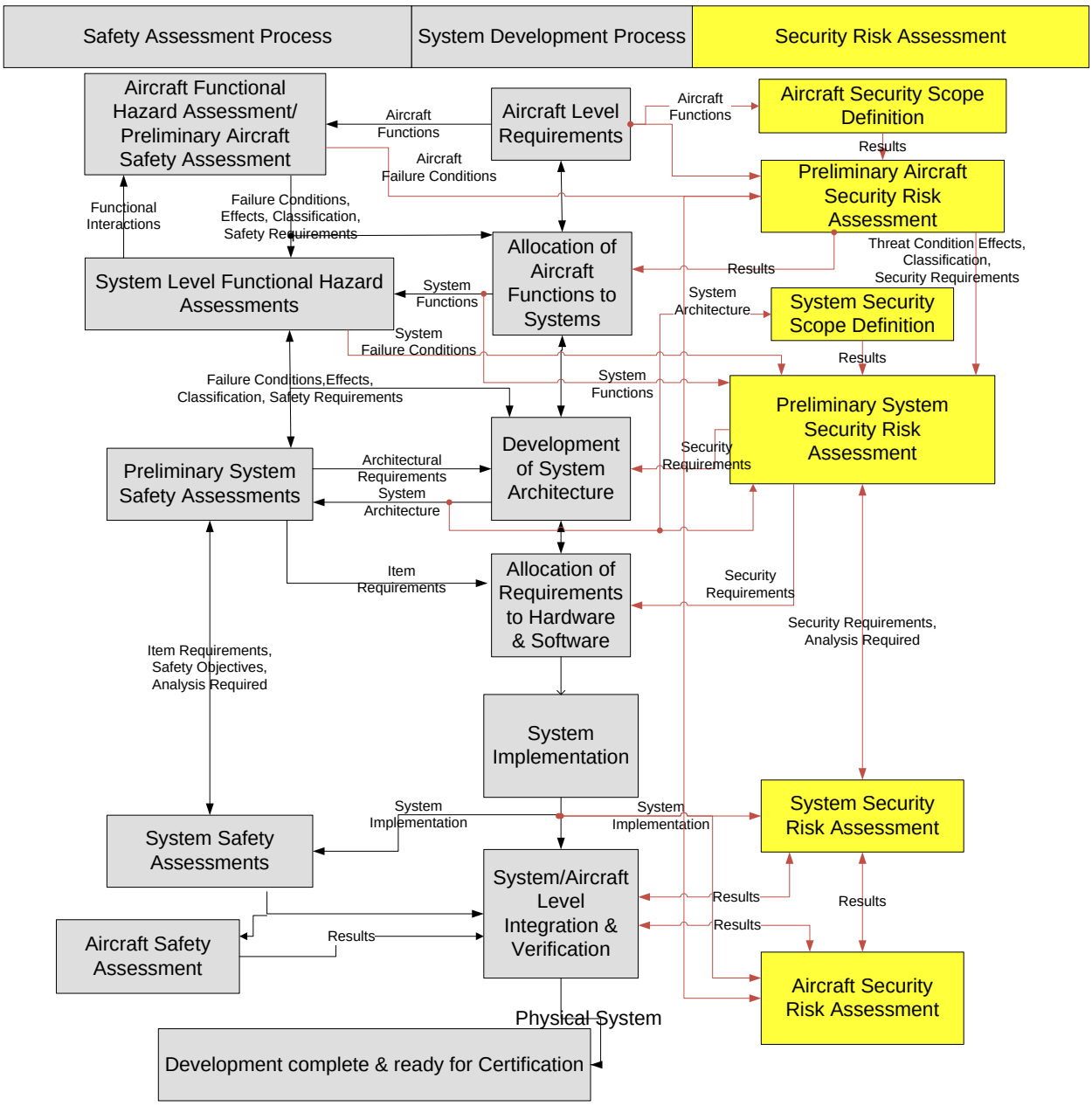

Figure 2-3 : AWSP as Part of Aircraft Certification Process

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.

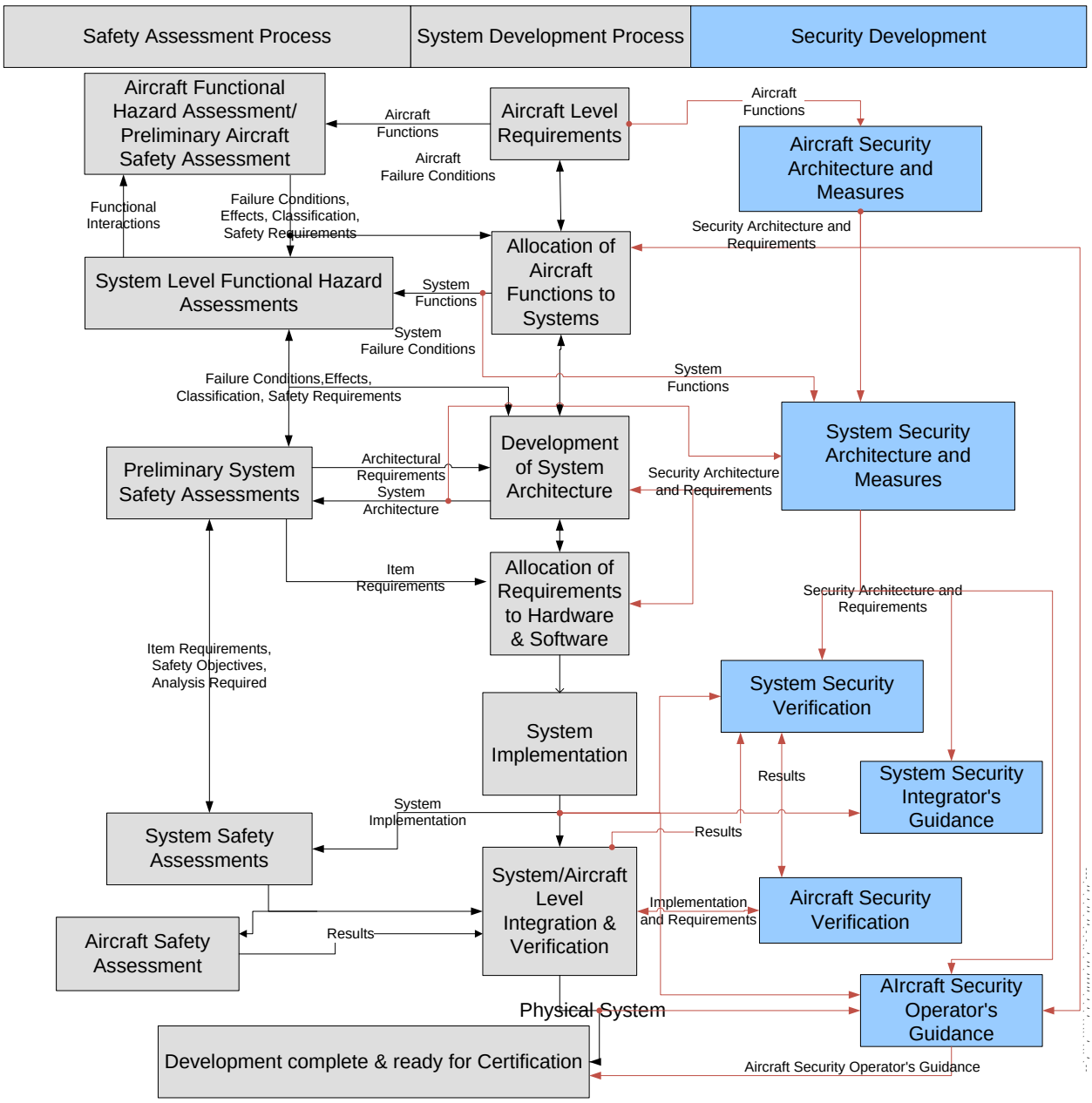

Figure 2-4 : Security Development as Part of Aircraft Certification Process

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.

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 DO-355/ED-204), 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.

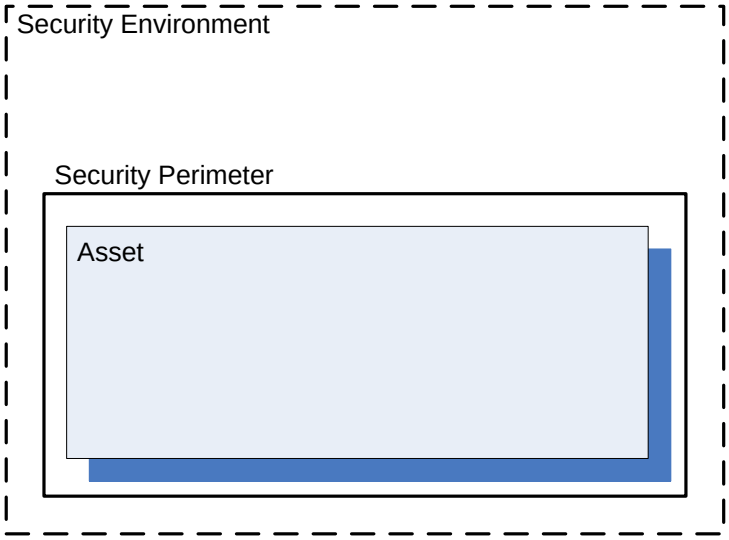

Figure 3-1 : Security Scope

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.
  - 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:
  - Roles and entities (e.g. their responsibilities and access to the aircraft/system),
  - External tools and systems (e.g. airport IT network), and
  - External security measures (e.g. operational controls, airport passenger screening, firewall within airline ground IT).
- External dependencies:
  - Regulations, and
  - National laws.
- External Agreements, including:
  - Contracts (e.g. between operator and MRO), and
  - 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.

The level of threat is a qualitative evaluation of the possibility that the threat condition might occur. To assess the security risk of a threat scenario, the applicant performs the following related activities:

- Threat Condition Identification and Evaluation (Section 3.2.1),
- Threat Scenario Identification (Section 3.2.2),
- Security Measures Characterization (Section 3.2.3), and
- Level of Threat Evaluation (Section 3.2.4).

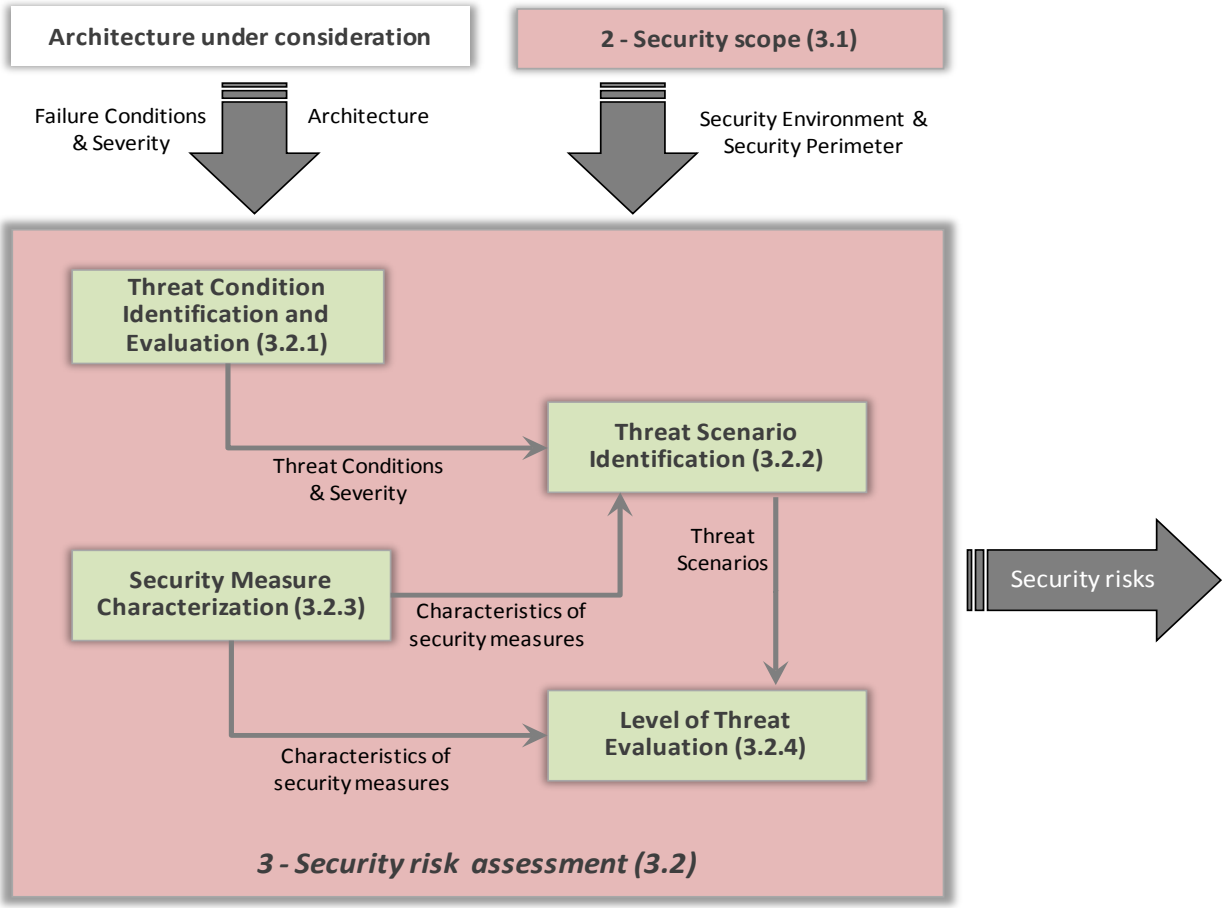

Figure 3-2 : Security Risk Assessment

3.2.1 Threat Condition Identification and Evaluation

Threat condition identification determines threat conditions, which arise through the existence of vulnerabilities. Each threat condition represents the condition of a system having a safety effect on the aircraft due to intentional unauthorized electronic interaction.

The threat condition identification should be carried out at aircraft and system levels. They should provide the following information:

- Identification of threat condition(s).
- Identification of the safety effects of the threat condition(s).
- Classification of the severity of each threat condition based on the identified severity of effects (i.e., Catastrophic, Hazardous/Severe-Major, Major, Minor, or No Safety Effect), as defined in e.g. AMC/AMJ 25.1309 and AC23.1309-1E extended to include the No Safety Effect classification.
- A statement outlining what was considered and what assumptions were made when evaluating each threat condition (e.g., adverse operational or environmental conditions and phase of flight).

The goal in conducting this step is to clearly identify the circumstances and severity of each threat condition along with the rationale for its classification.

Threat conditions are caused or contributed to by a loss of a security attribute of an asset, see Table 3-1.

Table 3-1: Asset Security Attributes and Threat Conditions

Asset Security Attribute	Threat Conditions of the System due to the loss of the Asset's Security Attribute (non-exhaustive)
Integrity	Conditions representing misuse or interference with the Function
Availability	Conditions representing denial of access to the Function, including intermittent failures in the continuity of data over a required service interval.
Confidentiality	Conditions resulting from exposure of data to an unauthorized entity.

In this evaluation, the classification of all failure conditions of a function/system, which may be an asset, is supplemented by the classification of all threat conditions.

Threat conditions allow for the introduction of:

- Either the consideration of conditions which have not been considered by the FHA (e.g. root cause is neither an error nor a failure); or
- The consideration of combinations of conditions, which will have a safety effect, but were originally considered being functionally independent by the FHA.

The severity of these conditions is evaluated in the same manner as by the FHA. The most severe threat condition effect may be higher than the most severe failure condition effect.

3.2.2 Threat Scenario Identification

A threat is a potential attack targeting an asset, and a threat can be conducted through

several scenarios, which are the threat scenarios.

The purpose of the activity is to build the list of threat scenarios leading to each threat condition, and associated severity.

A threat scenario is built, at least from:

- The threat source of the attack from the security environment (see Section 3.1.2),
- The identification of the attack vector through the security perimeter (see Section 3.1.1),
- The track of the attack path through the security architecture up to the asset (see Section 3.4.1),
- The characteristics of the security measures on the attack path that would mitigate the attack (see Section 3.4.2), and then
- The final threat conditions that were the effects of the successful attack (see Section 3.2.1).

The list of all relevant threat scenarios should be complete to obtain a correct risk overview. In consequence, the applicant should determine, with the agreement of the AA, a structured methodology to identify relevant threat scenarios with the appropriate validation actions to ensure completeness. Examples of methods will be proposed in a forthcoming companion document.

3.2.3 Security Measure Characterization

The purpose of the activity is to identify and characterize those security measures which protect the aircraft and occupants against unauthorized interaction.

Each security measure is characterized by (see Section 3.4.2):

- Its type of effect: preventive, deterrent, detective, corrective, or restorative,
- Its capabilities and limitations,
- Its security vulnerabilities (vulnerabilities of the design during preliminary assessment, vulnerabilities of the implementation after implementation).

Security Risk Assessment should use a structured methodology:

- to identify the security measures, and
- to characterize the security measures according to their type, effectiveness and vulnerabilities.
- to use the characteristics in Security Risk Assessment.

Methods to characterize security measures will be available in a forthcoming companion document.

3.2.4 Level of Threat Evaluation

The level of threat is a qualitative evaluation of the possibility that threat scenarios cause a threat condition. For each threat condition, the level of threat evaluation is based on the threat scenarios, security environment and security measure characteristics. Methods to assess the level of threat will be proposed in a forthcoming companion document.

Note: The security measure characteristics could change during the lifetime. To be able to manage the continuing airworthiness, the applicant should have a clear traceability, for each threat scenario, between the security measure characteristics and level of threat evaluation.

3.3 Security Effectiveness

3.3.1 Introduction

3.3.1.1 Concept of Security Effectiveness

Airworthiness security is the protection of the airworthiness of an aircraft from unauthorized interactions, and "security effectiveness" is the concept and term that describes how well the aircraft is protected against unauthorized interactions. Therefore security effectiveness is defined as the ability of a security measure to protect an asset against the threat scenarios identified during Security Risk Assessment.

3.3.1.2 Scope limitations

Effectiveness and Efficiency: The notion of effectiveness is used in this document to represent the relationship between obtained results and objectives, while the notion of efficiency, defined as the relationship between obtained results and resources engaged, is not considered in this standard.

Continued Security Effectiveness: The assertion for security effectiveness of a security measure/architecture is that it is sufficient or not sufficient to protect the asset. This statement remains valid as long as the security scope remains unchanged (i.e. similar to the one at the time of the evaluation).

During the Aircraft lifetime, the security scope can evolve. Continued operational safety processes that address safety risks for aircraft are found in guidance such as SAE ARP 5150 and ARP 5151, which rely on establishing the appropriate monitors for events of concern to safe operations. This guidance should be adapted and additional guidance produced in the future to more effectively address security concerns related to continued operational safety, where ever appropriate. In the absence of additional guidance aircraft manufacturers and operators should address continued operational safety through the approved processes.

3.3.1.3 Security Effectiveness in the Airworthiness Security Process

The security effectiveness is supported by a subset of activities inside each part of the Airworthiness Security Process as shown in Figure 3-3.

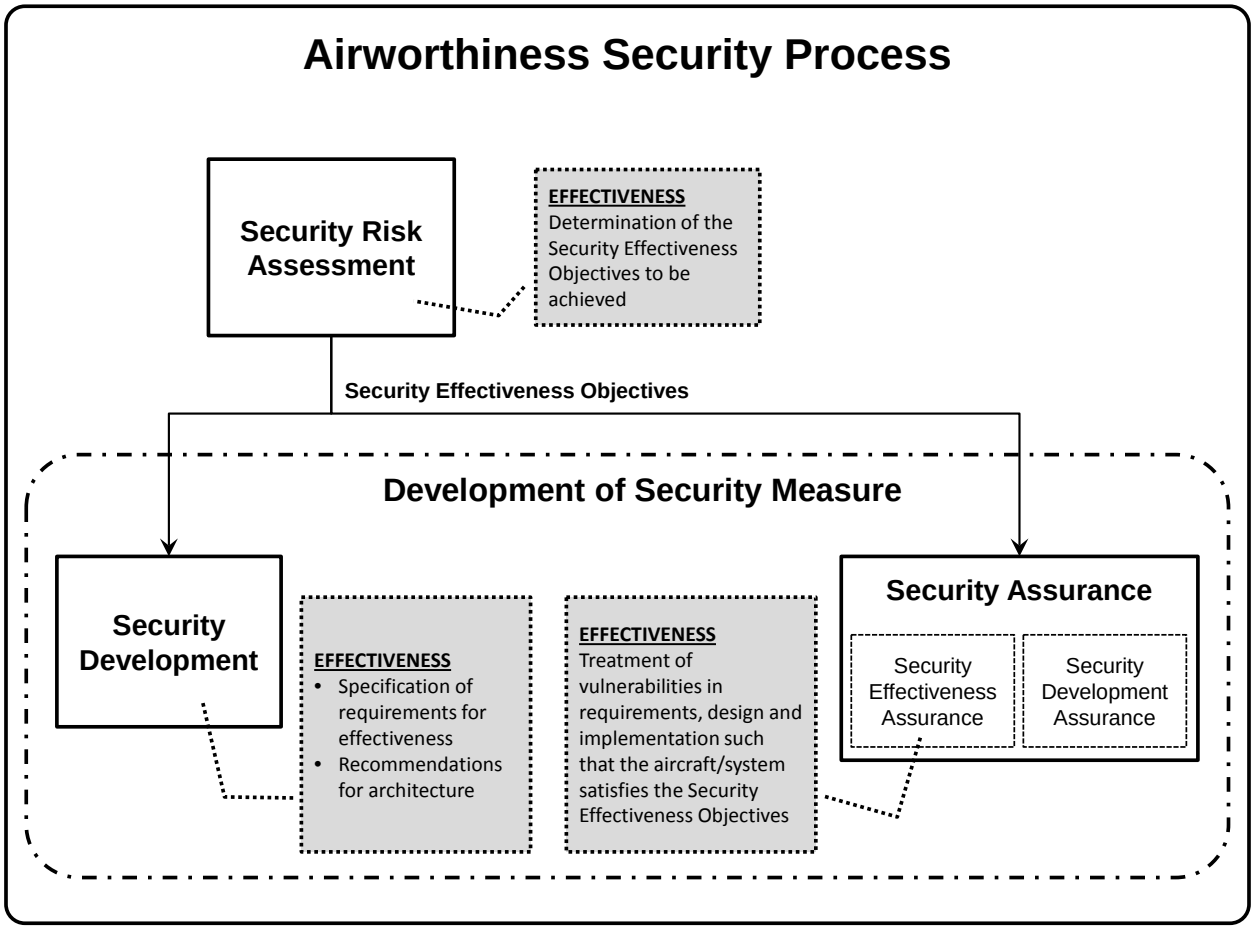

Figure 3-3 : Security Effectiveness for the AWSP

Following are the activities relating to security effectiveness for each part of the AWSP:

Security Effectiveness Objectives are determined by Security Risk Assessment (considering the security scope) (see Section 3.3.2.1)

Then security effectiveness objectives are used as inputs to:

Security Effectiveness Requirements are determined by Security Development within Security Architecture and Measures, consisting of recommendations and requirements about how to achieve the security effectiveness objectives (see Section 3.3.2.2)

Security Assurance (see Section 3.3.2.3), consisting of two classes of assurance actions:

- **Security Development Assurance Actions**: actions that are intended to address development errors having a potential security issue (but not related to security effectiveness),
- **Security Effectiveness Assurance Actions**: actions that are intended to address vulnerabilities. So security effectiveness assurance is about all of those planned and systematic actions used to substantiate, at an adequate level of confidence, that vulnerabilities in requirements, design and implementation have been identified and corrected such that the aircraft/system satisfies the security effectiveness objectives.

3.3.1.4 Security and Security Effectiveness in the Aircraft Development Process

Activities in the aircraft development process model are divided into two parts (see Figure 3-4):

- the aircraft/system development process that addresses the development of the function, architecture, design and implementation,
- the integral processes that support the development process, including the development assurance actions.

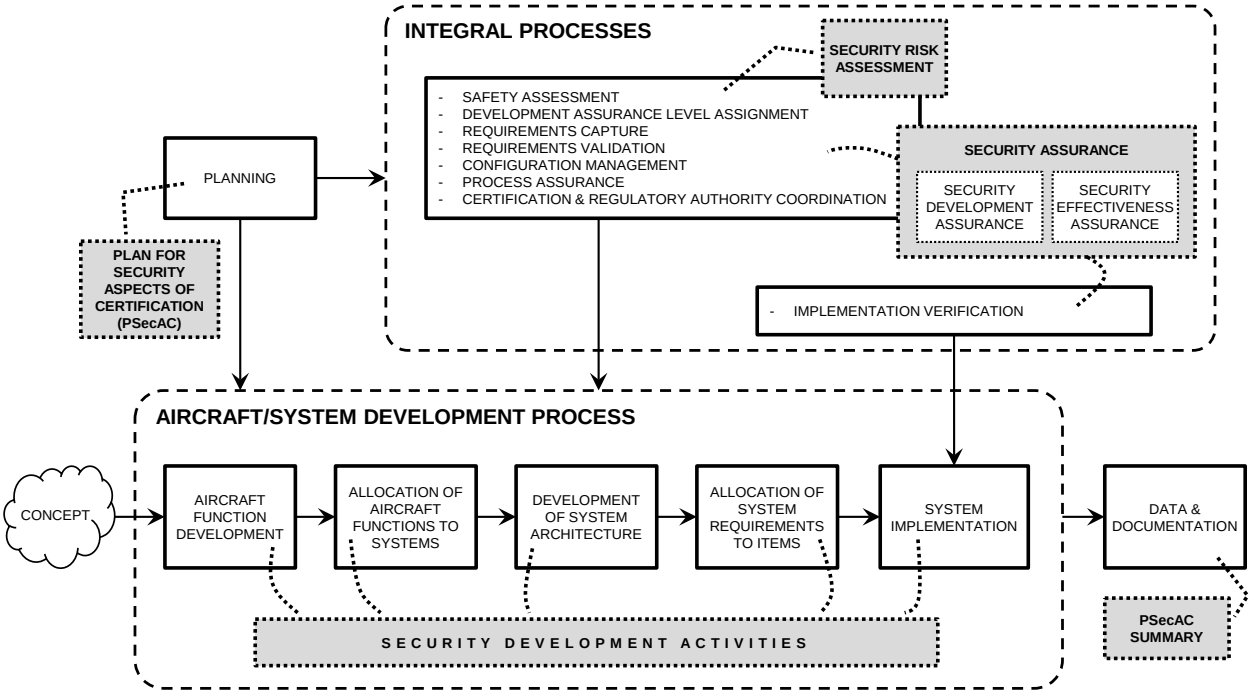

Figure 3-4 : Security Activities in ED-79A/ARP 4754A Aircraft Development Process Model

The Airworthiness Security Process is part of the aircraft development process model (refer to Fig 3-4 above): the “Security Development” is part of the aircraft/system development process, while the “Security Risk Assessment” and the “Security Assurance” belong to the integral processes as they participate in demonstrating that the aircraft/system performs as intended.

However, although the Airworthiness Security Process fits into the aircraft development process model and consequently all development assurance actions from integral processes are applicable to it, it also brings a new class of assurance actions through the concept of security effectiveness that is dedicated to the treatment of vulnerabilities (unlike development assurance that deals with errors. While development assurance actions are essential to show security compliance, they need to be supplemented by security effectiveness evidence that the aircraft is adequately protected).

3.3.2 Implementation of Security Effectiveness

3.3.2.1 Determination of Security Effectiveness

The required security effectiveness for a security measure/architecture is given by the security effectiveness objectives.

These security effectiveness objectives are derived from the airworthiness acceptability matrix, with respect to:

- The level of threat for each threat scenario, and
- The severity of threat condition effects for the considered threat scenario.

The security effectiveness objectives could take various forms as level, scale, or just qualitative requirements providing a measure of the ability of a security measure /architecture to reduce the risks to an acceptable level. The characterization of the security effectiveness objectives depends on the methods defined in a forthcoming companion document.

3.3.2.2 Requirements for Security Effectiveness

Security measures are identified during the development of the security architecture and requirements are generated to implement the security measure. Many of these requirements are typical aircraft and system requirements. However, some of the requirements are specifically derived from the security effectiveness objectives (performance) and need specific assurance actions (see section 3.3.2.3) to substantiate that the aircraft/system satisfies the security effectiveness objectives. These are termed **security effectiveness requirements**.

NOTE: It's an engineering task to specify adequate security effectiveness requirements to comply with the expected security effectiveness objectives.

3.3.2.3 Security Assurance

In the traditional development process as defined in ARP4754A (see Figure 3-4) the Integral Processes address development assurance actions. The Safety Assessments evaluate the severity of the failure condition effects on aircraft safety. The Assignment of Development Assurance Levels determines the development assurance actions for all functions, systems and items. Consequently, those also apply for the concerned security measures.

Security Assurance actions (see Figure 3-4) for the concerned security measures are defined according to the Security Risk Assessment, which evaluate the severity of the threat condition effects on aircraft safety and the level of threat of each threat scenario. Security Assurance consists of two types of actions:

- **Security Development Assurance** actions are necessary to assure the security measure performs as intended. Their scope, depth and rigor of development are determined by the methods described in a forthcoming companion document.

NOTE: These actions apply to all security requirements (typical aircraft and system requirements and security effectiveness requirements).

- **Security Effectiveness Assurance** actions are necessary to ensure that the security

measure and security architecture is free of known and unacceptable exploitable vulnerabilities and therefore as effective as required by the methods described in a forthcoming companion document.

NOTE: These actions apply ONLY to security effectiveness requirements.

In addition to all security assurance actions, the development assurance actions (assigned through the DAL and the safety assessment) apply to all security requirements. One should know these development assurance actions may overlap with security development assurance actions. As a result, the security development assurance actions may benefit from the DAL implementation, and one should avoid duplication of assurance actions if any.

An overview of the classes of security requirements and related assurance actions with some specific examples applicable to a security measure is given in Figure 3-5.

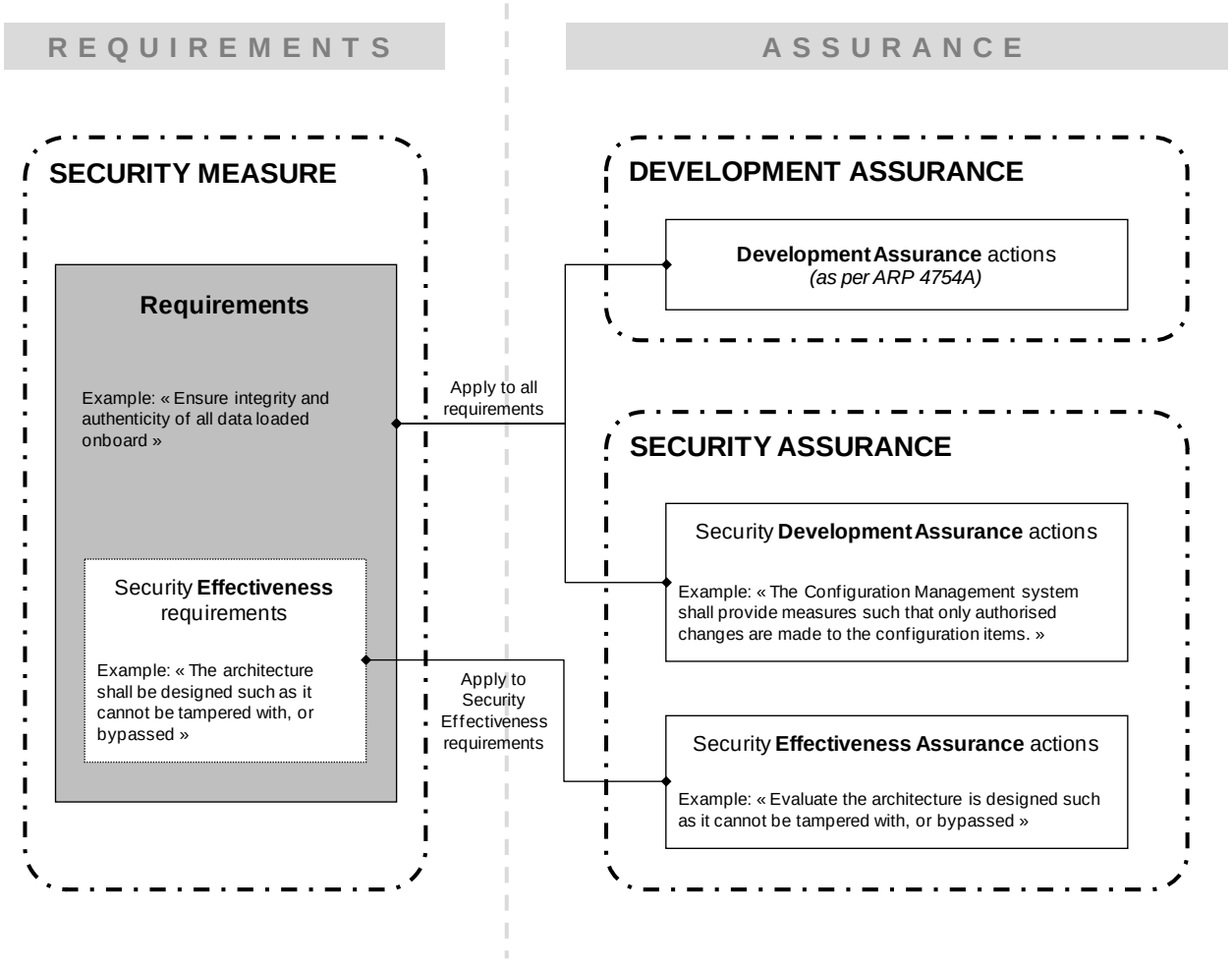

Figure 3-5 : Relationship between Effectiveness Requirements and Assurance Actions

3.4 Security Development Activities

As with all functional requirements, Security Development should be compliant with the

ED-79A/ARP 4754A or comparable process.

In addition to the safety process, the following topics should be highlighted to cover security requirements:

- Security Architecture (Section 3.4.1),
- Security Measures (Section 3.4.2),
- Security Guidance (Section 3.4.3), and
- Security Verification (Section 3.4.4).

Security measures can exist at any level of implementation (aircraft, system, and lower). Security requirements and architectures are functionally decomposed from the aircraft level down to the item level in a hierarchical structure.

3.4.1 Security Architecture

Aircraft Security Architecture and Measures organizes the systems and their security perimeters. Each system has

- A defined security environment (see Section 3.1.2 “Security Environment”) derived from the aircraft security environment, and
- Requirements based on the documented aircraft security architecture.

Similarly each subsystem receives a definition of its security environment and requirements from the system security environment and security architecture.

Once the aircraft security architecture is sufficiently mature, it is iteratively evaluated by Preliminary Aircraft Security Risk Assessment (see Section 3.2 “Security Risk Assessment”). Iterative evaluation has to be understood as repetition of the process activities in Appendix A.2 and A.3. Although an initial version of security risk assessment data may be created when the initial security architecture is available, it should not be expected to be complete in most cases. Whenever additional details or changes to the initial security architecture become known, the security architecture and security risk assessment data need to be updated iteratively. The resulting Aircraft Security Architecture and Measures:

- Decomposes the aircraft functions necessary to implement the aircraft security measures and to define the systems necessary to implement the system security measures (see Section 3.4.2),
- Documents the affected interfaces and dependencies between systems, and
- Provides a consistent overall level of protection by allocation of system security requirements according to each system’s needs and possibilities.

3.4.2 Security Measures

A security measure is a feature, function or procedure used to mitigate security risk, even if it was not implemented specifically for that purpose. In addition to aircraft systems, a security measure may also include operational requirements within the security environment (features, policies, or procedures documented in security guidance or external agreements).

Types of measures include, but are not limited to:

- Deterrent: The aim is to discourage a malicious user from causing an unauthorized event. One example is the policy or law frequently displayed when a user starts a session.
- Preventive: All measures intended to prevent an occurrence of unauthorized events.
- Detective: All measures intended to detect and report an unauthorized event. Examples include monitoring and auditing of security logs, and file integrity checkers.
- Corrective: All measures intended to react to an occurrence of unauthorized events or a security policy violation (other than restoring the original measures to normal function, see "restorative/recovery" below"). For example, after incident detection by a detective measure, a new rule on the firewall is setup in order to block the malicious access.
- Restorative/recovery: After the occurrence of a security event, all measures intended to put the System back into a normal state. For an example, if the Integrity of data is lost after an attack, the data could be restored from a trusted backup.

Figure 3-6 is an example showing how different types of security measures could be applied to aircraft architecture to reduce the risks of a specific assumed attack path.

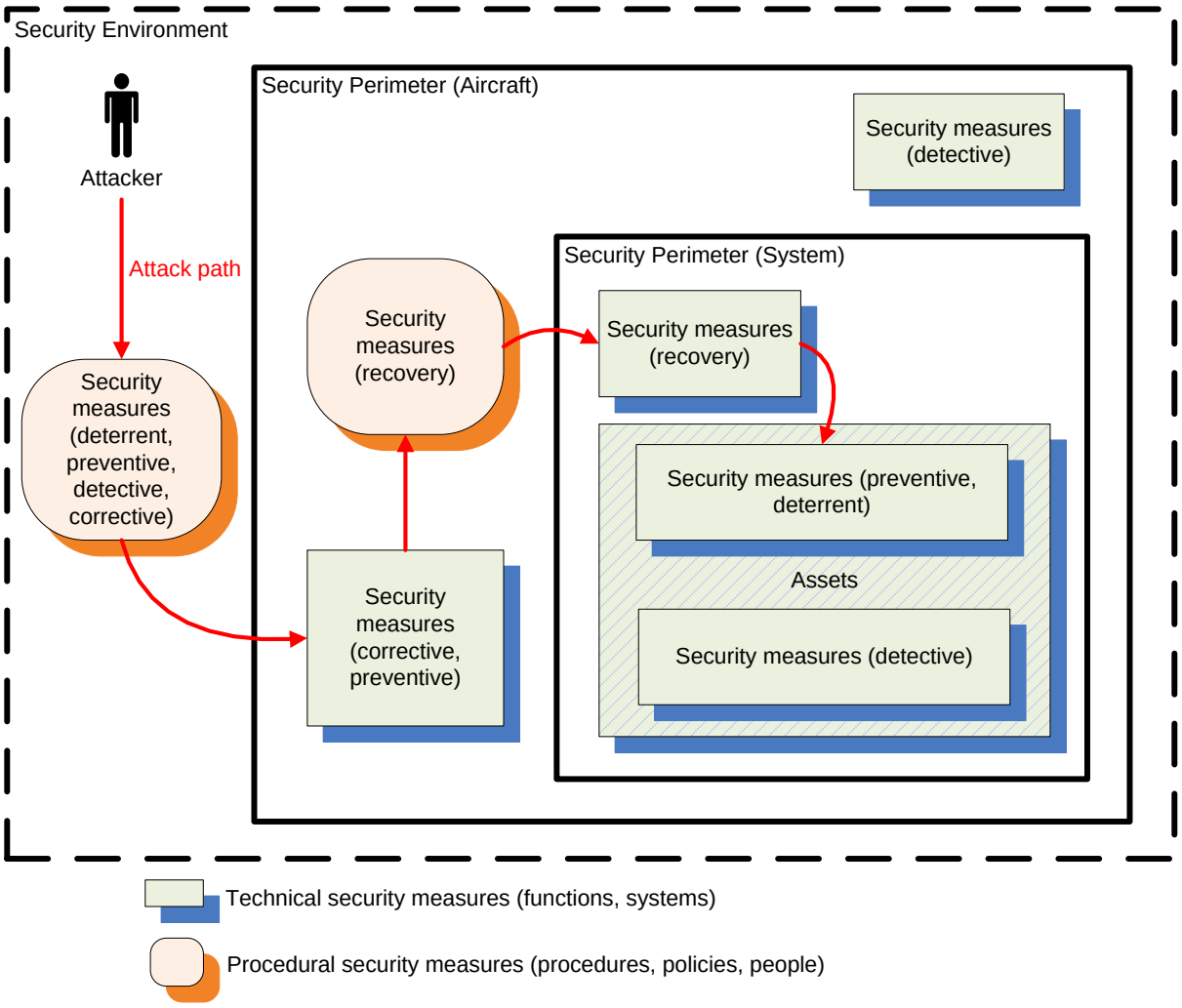

Figure 3-6 : Simplified Example of a Security Architecture with Different Types of Technical and Procedural Security Measures

3.4.3 Security Guidance

The security guidance defines requirements necessary for correct integration, and the secure operation and maintenance for each aircraft system. This includes the operational support needed to operate the Aircraft (e.g., database installers, operation centers, repairs). It may also include secure disposal of security measures. For example, if equipment with sensitive cryptographic material is disposed, deletion of the material may need to be ensured.

The security guidance is generated at the aircraft (the Aircraft Security Operator Guidance), and at the system levels (the System Security Integrator Guidance for relevant systems and subsystems). It is used to ensure that the system is used in accordance with the operational requirements assumed in the type design.

Security guidance originates as needed with system developers to provide information for subsequent use in installation design (e.g., by the aircraft integrator or manufacturer) as well as information on system operation that ultimately will be conveyed to the operator. Security guidance for operators that is generated by system developers is collected by the aircraft manufacturer, combined with security guidance generated by the aircraft manufacturer, and transmitted to the operator in appropriate forms (see DO-355/ED-204). Security guidance should be adapted to any intended users, from large commercial operators to single individual owner-operators.

The scope of security guidance material is not limited to the aircraft itself, and captures requirements and assumptions involving elements outside the aircraft. The requirements, agreements, or assumptions about external organizations, systems, networks, and interfaces that are necessary in order to coordinate roles and responsibilities between dependent systems and external actors are initially captured in the security scope and are refined in the external agreements portion of the security guidance.

The Aircraft Security Operator Guidance is directed to the aircraft operator and contains the relevant operational security measures (aircraft and system level) and security assumptions as necessary. Please refer to ED-204 for more information.

3.4.4 Security Verification

Security verification has the following purposes:

- Verification that systems, hardware, and software meet security requirements (normal purpose in a standard development process such as ED-79A/ARP-4754A), and
- Contributes to evaluation of security effectiveness (specific to security),
- Identification of vulnerabilities for final Security Risk Assessment (specific to security).

Security verification should be commensurate with the development process. Security verification includes analysis and three kinds of testing. Other verification methods may be appropriate for security verification.

The first two, security requirements testing and security robustness testing, which are usual aircraft / system development activities, demonstrate that the implementation of the technical security requirements is correct even under abnormal inputs and conditions. The third, vulnerability testing, is a security specific activity that demonstrates that the implementation will function correctly within the security environment of the system. These are detailed below:

- Security Requirements Tests (standard testing): Intended function tests (i.e. expected behavior) are part of standard verification where the implementation is verified to meet its specified requirements. Security requirements tests are part of the intended function tests, and will include testing that the security measures perform correctly in response to unauthorized events.
- Security Robustness Tests (standard testing): Robustness testing is part of standard verification that establishes that intended functions behave correctly when submitted to abnormal inputs or conditions. Security robustness testing should include checks for insecure states.
- Vulnerability Tests: Vulnerability testing is a security specific testing activity that consists of vulnerability scanning methods as well as aggressive testing to attempt to break, bypass, or tamper with the security measures so as to demonstrate the ability to misuse the aircraft systems.

The security requirements, robustness, and vulnerability test plans should be assessed in relation to the set of threat scenarios and threat conditions to determine if there are any gaps in testing or analysis.

In addition to verification tests, security effectiveness evaluation requires vulnerability analysis. Because vulnerability testing is based on an up-to-date profile of information security attacks in the security environment and is independent of the requirements-based test cases, there might not be test cases to document correct behavior. Hence, an analysis of the vulnerability test results should be conducted to determine the severity of the effect of each significant result to determine the vulnerabilities. The analysis will be part of the vulnerability dossier.

The vulnerability dossier documents the vulnerabilities discovered during security verification and the resulting system's response. The vulnerability dossier is part of the supporting evidence for Aircraft or System Security Risk Assessment.

The following Figure 3-7 illustrates the security testing organization with their inputs and how they contribute to the required outputs.

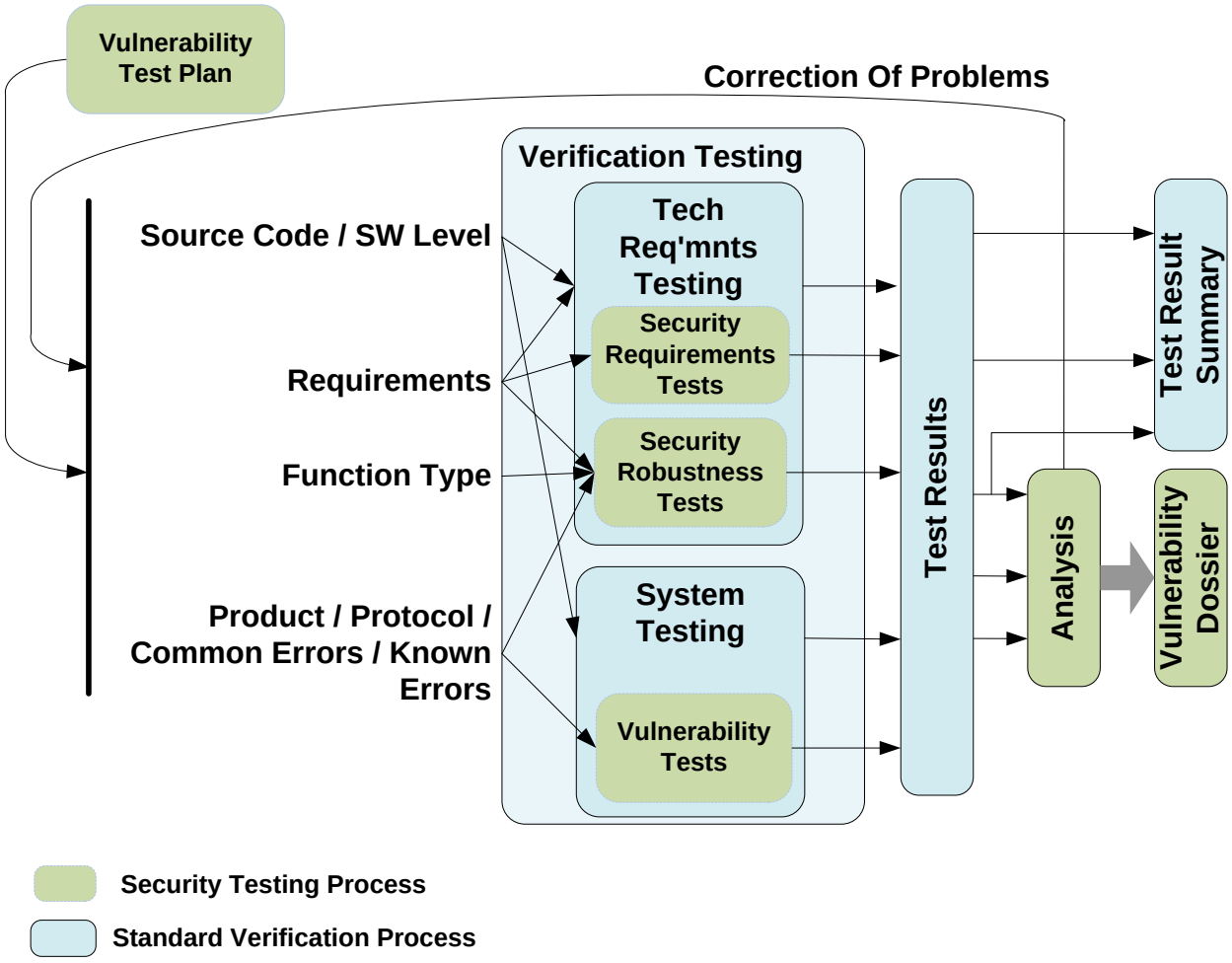

Figure 3-7 : Security Testing Activities

4 AIRCRAFT MODIFICATIONS

Chapter 4 introduces modifications to aircraft and systems and provides guidance to determine when aircraft level versus system level Security Risk Assessment is required.

Chapters 2 and 3 provide processes to conduct Aircraft Security Risk Assessment. When it is determined that System Security Risk Assessment is required and not aircraft level then some of the processes described in Chapters 2 and 3 are simplified. The Airworthiness Security Process described in chapter 2 (steps 1 through 8) are required to be completed and documented as part of System Security Risk Assessment. Chapter 3, fundamental concepts, establishing the security scope, security perimeter, security environment, threat condition identification and security risk evaluation process are also required to be completed and documented.

The main difference between the guidance of Chapter 4 and complying with Chapter 2 and 3 at the system level is that the level of effort is greatly reduced. Certain data submittals specified in Table 4-1(e.g., ASSD, PASRA, and ASRA) may also be eliminated.

Chapter 4 provides additional information for aircraft level security risk determination, but does not supersede any other security processes described in Chapter 2 and 3 of this document. When it is determined that Aircraft Security Risk Assessment is required, the processes described in Chapter 2 and 3 should be followed in all important aspects.

4.1 Aircraft Level versus System Level Security Risk Assessment Determination

For every aircraft modification, a Change Impact Analysis is required. The results of the Change Impact Analysis may be used to determine if aircraft level or system level Security Risk Assessment is required. Security Risk Assessment can be relatively simple or complex depending on the aircraft architecture and intended function of the information technology applications.

As an example, threat evaluation of portable electronic devices that are not connected or have read–only access to aircraft systems are less complicated than the devices that have read-write access. When they are receiving data, wireless or wired aircraft systems and networks should require a security threat evaluation from the threat of unauthorized interaction to ensure that the data is not intercepted or corrupted. The installation requirements for a security system should consider the aircraft avionics architecture, such as federated systems versus highly integrated modular avionics systems using bi-directional data busses to aid in determining if aircraft level or system level Security Risk Assessment is required.

In most cases, federated avionics systems with unidirectional data busses (e.g., ARINC-429) that connect to the threat of unauthorized interaction should have system level, not aircraft level, Security Risk Assessment. In determining the aircraft security scope with a unidirectional bus, only those systems receiving data from persons, organizations, or external systems would be considered part of the security perimeter. If the ARINC-429 has a reversible interface that could become a transmitter under software control additional controls will be needed. System Security Risk Assessment should show that threats are mitigated by the system(s) to which the threat of unauthorized interaction is connected. If it is not possible to determine if mitigations are adequate at the system level, then Aircraft Security Risk Assessment will be required. Also, if the unidirectional

nature of a bus cannot be guaranteed, then the mitigation measures should address all possible sources of data or interference on the bus.

When the threat of unauthorized interaction is connected to bi-directional data busses (e.g., AFDX) on highly integrated aircraft with integrated modular avionics systems, in most cases Aircraft Security Risk Assessment is required. The Supplemental Type Certificate (STC) applicant may obtain a data package or services from the Original Equipment Manufacturer (OEM) of the aircraft or system through a specific arrangement as required. Based on this data package, the STC applicant should provide evidence that the modification does not adversely impact safety based on the original Type Certificate (TC) approval. The applicant is responsible to obtain all necessary information and documentation in support of their proposed modification.

The necessary documentation is strongly affected by the proposed modification, such as whether it connects to a federated system or a highly interconnected aircraft network. Since the Design Approval Holder (DAH) holds all the system interface documentation, interconnected modifications may need data from the DAH. In cases where the applicant cannot obtain sufficient data from either the DAH or publicly available sources to show compliance, the proposed modification might not be possible. In cases where the applicant cannot obtain the necessary data, the applicant can propose an alternate method for compliance. A forthcoming companion document will discuss additional considerations.

This chapter describes how to apply this document when modifying aircraft systems including security aspects as part of the overall development process. Modifications to an aircraft system should be managed, validated, and verified, regardless of the reason for change. Modifications can be implemented to add new functionality, change existing functionality, address a security incident, or other rationale. Nevertheless modifications to aircraft systems should not compromise the existing level of security and safety of the aircraft.

This section describes operations to be performed:

- When modifying aircraft systems including the security aspects
- By equipment manufacturers, Aircraft manufacturers, and anyone else (e.g. for Design Approval Holders (DAH)) who is applying for, Supplemental Type Certificate (STC), Amended Type Certificate (ATC) or changes to Type Certification for installation and continued airworthiness of new or modified aircraft systems.

There are many different types of aircraft in world-wide operations. The rule basis, system architecture and security vulnerabilities are different across these aircraft types and affect the scope of the STC. For these reasons, the requirements for security may be different for Transport Category, Small Airplanes, and Rotorcraft.

The applicable aircraft certification basis is documented in TCDS (Type-Certificate Data Sheet). TCDS are publically available on Airworthiness Authority (AA) web sites. Every change to the Type Design (post-TC modification), should comply with the applicable certification basis described in the related TCDS. If security considerations are part of the certification basis (e.g., through an applicable CS-25/ 14 CFR Part 25/ AWM 525 or a dedicated Special Condition), then the STC applicant should produce evidence that the security features of the TC is not invalidated.

4.1.1 Security Definitions and Risk Management

The terms aircraft network security, systems security, information security, and security are not precisely defined and are often used interchangeably which can cause confusion as to their intended meaning. These terms includes the data link, internal aircraft data bus connections, switches and routers.

System Security Risk Assessment is required in combination with network security. This section assumes the terms ***Systems Security, Security Measure, and Security Risk*** include ***Network Security*** within the overall development process. When developing aircraft systems, Security Risk Assessment related activities should include Security Risk Assessment, and risk mitigation and evaluation. Information security is the term used to describe attacks on aircraft networks and systems from hackers. The term security includes network security, systems security, and information security.

4.1.2 Aircraft Related Services

The applicant should consider the integrity and robustness of configuration control measures on the device or service to which the proposed connection is made. Such consideration should additionally consider industry standards and specifications, such as Operational Approval or ARINC standards that address security measures. Such security measures can be described and verified/validated in order to demonstrate some level of threat mitigation outside of the airplane systems. Modifications that include connectivity with devices /services with no such security specifications or standards, such as the Internet, should be considered a larger threat of unauthorized interaction than devices/services that do have security standards/specifications.

Examples of external connections with security industry standards/specifications include but are not limited to:

- ARINC 822 Gatelink,
- Airline Networks with Operational Approval,
- Class 2 Electronic Flight Bag,
- Authorized Airport Infrastructure,
- Some satellite providers/technologies.

Examples of external connections without industry security/standards specifications include but are not limited to:

- Open wireless,
- Airline networks without operational approval (back-office networks),
- Passenger Owned Devices,
- Internet Service Provider Networks,
- Application Service Provider Networks,
- Some satellite providers/technologies.

The following are examples of the threat of Unauthorized Interaction that could be connected to Aircraft Systems and networks:

- Airline Networks including Airline Operations Center (AOC) communications,
- Airport Terminal Wireless Networks (e.g., Gatelink),
- Public Networks (e.g., the Internet),
- Portable Electronic Devices (PEDs) including laptops and tablet computers,
- Wireless Aircraft Sensors and Sensor Networks,
- Wireless Ground Support Equipment (GSE),
- Universal Serial Bus (USB) devices,
- Maintenance devices, including laptops.

Figure 4-1 provides an example of E-enabled architecture and infrastructure.

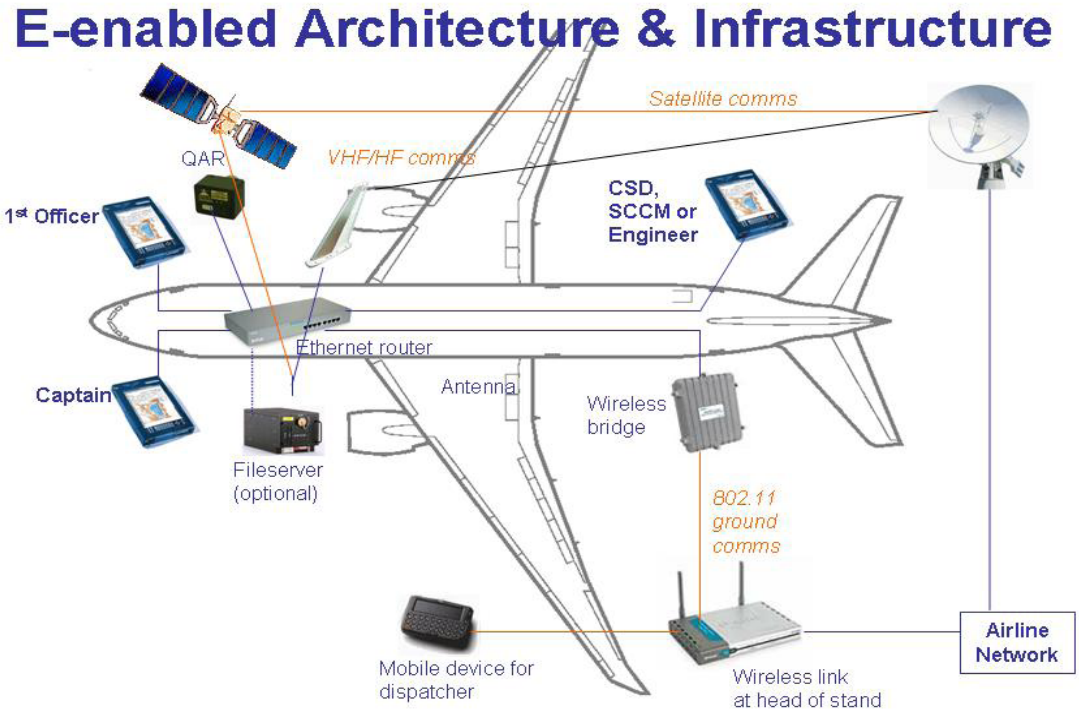

Figure 4-1 : Example of E-enabled Architecture and Infrastructure

4.2 Modification Process Activities

The modification management process for security aspects may be included in the system development processes. These processes provide a defined method for the stakeholders to coordinate activities. Stakeholders can include the applicant, system developers, customers, operators, etc. The results of the modification process are documented in the

certification plan. The PSecAC Summary for the safety and security aspects will be reviewed to determine the overall compliance to the certification plan. If aircraft interfaces are modified the security risk should be re-assessed or assessed if previous security risk assessment data does not exist. A Change Impact Analysis is thus required for modifications which permit access by unauthorized persons or equipment either during operations or maintenance.

The system development artifacts should be maintained and updated as necessary, with the following additional considerations:

- Aircraft that are being modified might not have a baseline Security Risk Assessment. The means of compliance for the modification should be documented including the security aspects.
- Define the security boundary of the modification and state whether the function is intended for a security measure.
- Change Impact Analysis should consider the possible additional impact due to security vulnerabilities, security operational and maintenance procedures, and additional impact attributable to security measures, which add functionality to the aircraft.
- Security Risk Assessment may be required as a result of the Change Impact Analysis.
- Verification should define the testing performed on new and modified systems and items, including the security measures, vulnerability testing, and operational guidelines for security measures.
- Changes to the aircraft configuration data should be identified.
- Deviations from the expressed plan should be identified/discussed in the accomplishments summary.
- Guidelines should be defined for monitoring, auditing, and operation of security measures.

Aircraft network and systems security depends on the risk introduced by the new or modified system and on ensuring previous security measures are maintained. The level of security effectiveness required depends on the intended function, the integration level and the connectivity level of the system.

4.2.1 Change Impact Analysis

A Change Impact Analysis is required for modifications to aircraft interfaces which permit access by unauthorized persons or equipment either during operations or maintenance. Additional Aircraft interfaces could be physical, wireless, or logical. ED-79A/ARP 4754A describes the aircraft and systems modification process. Aircraft and systems may use their original system and safety development processes as the baseline.

In general, the Change Impact Analysis should verify that:

- The aircraft and its systems, networks, and other assets are protected from intentional unauthorized electronic interaction. If protection cannot be verified, then the risk should be assessed as acceptable or mitigated.
- Procedures exist to ensure the continuing airworthiness of the Aircraft.
- Malicious or inadvertent change to aircraft systems and networks required for safe

flight and operations are prevented.

- Previously approved security measures are maintained.

The Change Impact Analysis is an iterative document, which is updated as changes to the modification plans are made. The analysis should also be updated following validation and verification activities. The Change Impact Analysis accounts for the effects on the aircraft by the new or modified system, but also effects on the new or modified system by the connected systems. Unplanned modifications resulting from the modification process should be discussed and their impact also addressed. The effort required can vary greatly from a small task to a complete rework of the security risk assessment data, dependent on the extent of modification planned. Refer to Section 3.2 for additional detail on the security aspects of the modification process.

4.2.2 Service History

Applicants should coordinate their plan to apply for service history credit with the applicable Airworthiness Authority early in the program planning to ensure that their proposal is acceptable.

4.2.3 Interconnectivities of New or Modified Aircraft Systems

The applicant should address the integration issues between their proposed modification and the connectivity to existing aircraft networks and systems. Figure 4-2, “Interconnectivities of New or Modified Aircraft Systems” provides a high-level overview of the modification process. The applicant should consider the use of the guidance contained in this document during the modification process. The following text provides additional clarification for the bullets (e.g., letters and numbers) used in Figure 4-2.

A- Aircraft System baseline.

B- New or modified System(s): includes new, modified, or removed Networks and Systems.

C- Internal / External the threat of Unauthorized Interaction including onboard uncontrolled PED

1- Define data flow from the existing aircraft systems to the new or modified system(s)

2- Define data flow from the new or modified system(s) to existing aircraft systems

3- Define data flow from internal / external Service or Devices to the new or modified system(s)

4- Define data flow from the new or modified System(s) to Internal or External Services or Devices

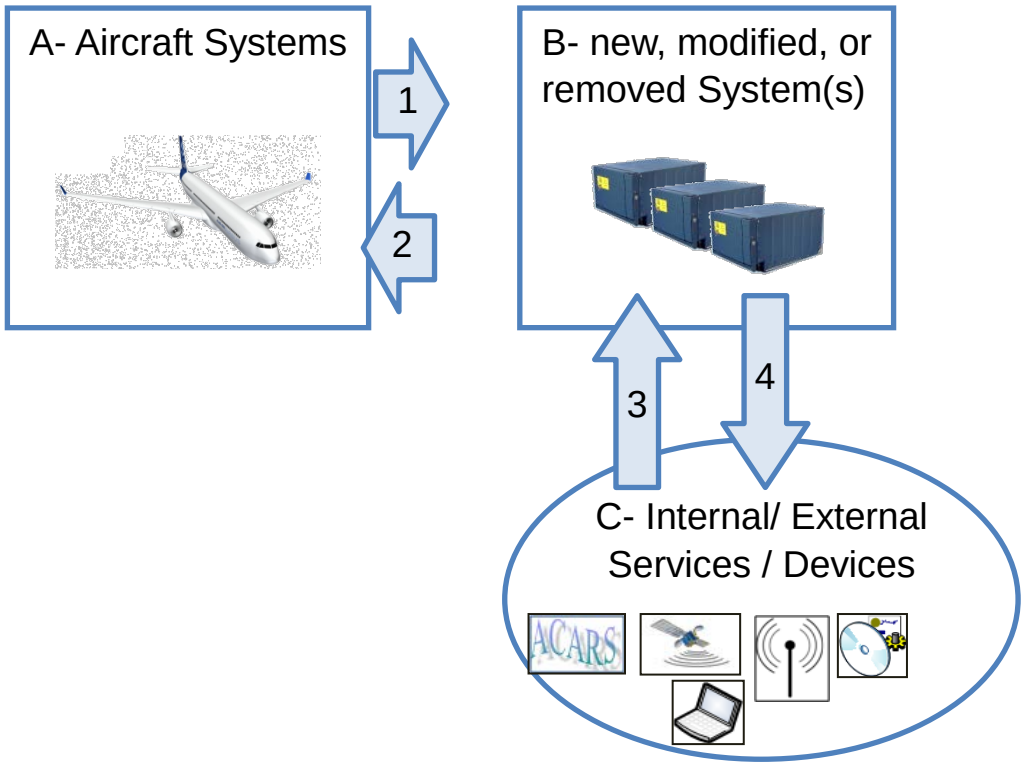

Figure 4-2 : Interconnectivities of New, Modified, or Removed Aircraft Systems

4.2.4 Installing New Aircraft Systems and Networks

Installing new aircraft systems and networks with connectivity to the threat of unauthorized interaction should include Security Risk Assessment. The interfaces with other networks and systems should be clearly defined during the Change Impact Analysis.

4.2.5 Replacing Aircraft Systems and Networks

Replacing aircraft systems and networks with connectivity to the threat of unauthorized interaction should include Security Risk Assessment. Examples of replacing systems and networks include parts obsolescence, supplier change, and replacing security measures with improved security measures. The interfaces with other networks and systems should be clearly defined during the Change Impact Analysis.

4.2.6 Modifying Existing Aircraft Systems and Networks

Modifying existing aircraft systems and networks with connectivity to the threat of unauthorized interaction should include Security Risk Assessment. The interfaces with other networks and systems should be clearly defined during the Change Impact Analysis.

4.2.7 CTSO / ETSO / TSO Installation Requirements

Installing, replacing or modifying Canadian Technical Standard Order (CTSO) / European Technical Standard Order (ETSO) / Technical Standard Order (TSO) functions with connectivity to the threat of unauthorized interaction may require Security Risk Assessment based on the change impact analysis. The interfaces with other networks and systems should be clearly defined during the Change Impact Analysis. Security measures that have been added to CTSO /ETSO / TSO as a non- CTSO / ETSO / TSO function will need to be evaluated during the aircraft installation approval process.

4.3 Airworthiness Security Process and Security Risk Assessment Criteria

Current industry standards for the safety of aircraft and occupants are focused on the failure of aircraft systems and not intentional unauthorized electronic interaction. As a result there are gaps when intentional acts are introduced to aircraft systems. This guidance was developed to address these gaps by coordinating the safety assessment process with appropriate security processes. The goal is to identify any unacceptable risks resulting from threat conditions following the process described in the chapter 3.2 of this document and to set the security requirements in order to implement security measures to mitigate the risks identified. Appendix E of this document “Rationale for an Airworthiness Security Process” provides additional information on this subject.

Meeting the objectives of this section is the most important part of the Aircraft System modification process. How the applicant meets the objectives of this section are dependent in part on the development assurance actions that are chosen as part of the modification process.

For this reason, applicants who proposed alternative methods to the Airworthiness Security Process described in Section 2, should obtain agreement with the applicable Airworthiness Authorities early in the program planning to ensure that their proposal is acceptable.

4.3.1 Instructions for Continued Airworthiness

The applicant should submit Instructions for Continued Airworthiness (ICA) and security guidance including but not limited to the following issues:

- The system (including any means used for its updating), should be secure from unauthorized intervention (e.g. malicious software),
- There are adequate security procedures in place to protect the system,
- There are adequate security measures in place to ensure that the system/function does not accept a data load that contains corrupted contents, and
- There are adequate measures in place for compilation of load/data and secure distribution of load/data to the aircraft.

DO-355/ED-204 “Information Security Guidance For Continuing Airworthiness” provides guidance for ICA. This document provides guidance for the Airworthiness Authorities and the aviation industry for the operation and maintenance of aircraft and the effects of unauthorized interaction which can affect aircraft safety. DO-355/ED-204 provides information on the activities that need to be performed during operation and

maintenance of the aircraft to address the threat of unauthorized interaction.

4.4 Data Submittals for Aircraft System Modifications

The Change Impact Analysis will determine if a Security Risk Assessment is necessary. If necessary, data submittals to the regulatory authorities should be documented in the Certification Plan. Packaging of the information is at the discretion of the applicant provided all of the required data is submitted. These activities may be packaged and addressed within the PSecAC or distributed into others system, hardware or software documents (e.g: HDD, HVP etc). The documentation effort can vary greatly from a small task to an extensive effort based on the complexity of the planned modification and the change impact. Simple modifications should require reduced documentation submittals.

See Table 4-1 for data submittals.

Table 4-1 Data Submittals for the Security Aspects of Aircraft System Modifications

AWSP Activity	Appendix	Severity of Aircraft Security Effect			
		Catastrophic / Hazardous	Major	Minor	No Effect
Plan for Security Aspects of Certification (PSecAC)	A.1.1	Yes	Yes	AsNeg	No
Aircraft Security Scope Definition (ASSD)	A.2.1	AsNeg	AsNeg	AsNeg	No
Preliminary Aircraft Security Risk Assessment (PASRA)	A.2.2	AsNeg	AsNeg	AsNeg	No
Aircraft Security Risk Assessment (ASRA)	A.2.3	AsNeg	AsNeg	AsNeg	No
System Security Scope Definition (SSSD)	A.2.4	Yes	Yes	AsNeg	No
Preliminary System Security Risk Assessment (PSSRA)	A.2.5	Yes(I)	Yes	AsNeg	No
System Security Risk Assessment (SSRA)	A.2.6	Yes(I)	Yes	AsNeg	No
PSecAC Summary	A.1.2	Yes	Yes	AsNeg	No

LEGEND:

Yes(I) *Recommended for certification with Process Independence*
Yes *Recommended for certification*
AsNeg *as Negotiated with certification authority*
No *Not recommended for certification*

NOTE: Process Independence is the requirement that a process objective must be demonstrated through means which are not constrained by the organizational objectives of the organization responsible for the activity. The purpose is to not compromise compliance for expediency when there is conflict with other organizational goals.

4.4.1 Plan for Security Aspects of Certification Summary (PSecAC Summary)

Produce certification evidence relative to security concerns as described in Table 4-1 and Appendix A.1.2 of this document. When security risk assessment data exists for the aircraft and the scope of the modifications proposed, the existing security risk assessment data may be supplemented with additional architectural, analytical, and testing results.

If it is determined by the applicant and the regulatory authority that the system security risk assessment data is adequate then the aircraft specific documents (e.g., A.2.1, A.2.2, A.2.3), referenced in Table 4-1 are not required.

5 MEMBERSHIP

Special Committee 216

Aeronautical Systems Security

Chairmen:		**Organization**
Chuck	Royalty	The Boeing Company
Daniel	Johnson	Honeywell International, Inc.
Jean-Paul	Moreaux	Airbus

Designated Federal Official:		**Organization**
Ray	Decerchio	Federal Aviation Administration

Secretary		**Organization**
Derek	Schatz	The Boeing Company

RTCA Program Director		**Organization**
Harold	Moses	RTCA, Inc.

Members		**Organization**
Susan	Adams	The Boeing Company
William	Adams	Federal Aviation Administration
Jayson	Agagnier	Bombardier Aerospace
Hal	Aldridge	Sypris Electronics
Sohail	Alvi	Bombardier Aerospace
Yohannes	Amare	The Boeing Company
John	Angermayer	The MITRE Corporation
Stephen	Arentz	United Airlines, Inc.
Serge	Barbagelata	Eurocopter
Gerald	Bauer	The Boeing Company
William	Beacham	Pratt & Whitney United Technologies
Craig	Belling	United Parcel Service
John	Benson	Federal Aviation Administration
Samuel	Biller	Raytheon Systems Company
William	Blanchette	Information Tool Designers Inc.

Kenny	Blankenship	American Airlines, Inc.
Paul	Bousquet	Volpe National Transportation Systems Center
Ben	Brandt	The MITRE Corporation
Jeff	Breunig	ICF International
Chelle	Brisco	Federal Aviation Administration
Arne	Bruflat	Consultants - Independent
John	Bruggemann	GE Aviation
Jason	Burdette	Cessna Aircraft Company
Eric	Butner	The MITRE Corporation
Steve	Carver	Aviation Management Associates, Inc.
Cláudio	Castro	EMBRAER
Sally	Chambless	Raytheon Systems Company
Jean-Daniel	Chauvet	Thales
Ricky	Chitwood	Federal Aviation Administration
Andrew	Chumney	The Boeing Company
Joe	Comeaux	Alion Science and Technology
Keith	Conzachi	Gulfstream Aerospace Corporation
Cedric	Cyprien	Airbus Americas, Inc.
John	Dalton	The Boeing Company
Michael	Davis	Federal Aviation Administration
Peter	Davis	UK Ministry of Defence (MOD)
Bruce	Dawson	Honeywell International, Inc.
Nadai	De	Airbus SAS
Guy	De Langis	Bombardier Aerospace
Jocelyn	Descaillot	SITA
Michael	Dierickx	Panasonic Avionics Corporation
Randy	Durand	Honeywell International, Inc.
Mike	Elliott	The Boeing Company
Laurent	Fabre	Critical Systems Labs, Inc.
Dennis	Faherty	Astronautics Corp of America
Edward	Falkov	State Research Institute of Aviation Systems (GosNIIAS)
Uma	Ferrell	Ferrell and Associates Consulting, Inc.
Tom	Fisher	Becker Avionics, Inc.
John	Flores	Federal Aviation Administration
Timothy	Force	The Boeing Company
Michael	Franceschini	Honeywell International, Inc.
Faye	Francy	The Boeing Company
Joacy	Freitas	ANAC-Brazil
Cindy	Freud	The MITRE Corporation
Edward	Gaitan	Delta Air Lines, Inc.
Alan	Gallagher	Volpe National Transportation Systems Center
Rodney	Gates	American Airlines

Chris	Geschke	Booz Allen Hamilton Inc.
Daryl	Gilbertson	SANS
Carol	Giles	FJ Leonelli Group
Gilles	Gobbo	Airbus Americas, Inc.
Eugene	Gonzales	U.S. Navy
Stuart	Gooding	CESG
Randy	Gouge	ARINC Incorporated
Elena	Gromova	State Research Institute of Aviation Systems (GosNIIAS)
Ross	Hannan	Sigma Associates (Aerospace) Limited
Larry	Hannert	LCH Engineering
Charles	Harkey	Delta Air Lines, Inc.
Kevin	Harnett	Volpe National Transportation Systems Center
Pat	Healy	CESG
Thomas	Hediger	Swiss International Air Lines Ltd.
Ann	Heinke	Overlook Consulting, Inc.
Ryan	Hennigar	Transport Canada
Thomas	Hetschold	Lufthansa German Airlines
Robert	Holcomb	American Airlines, Inc.
Julien	Holstein	Aerospace Vision
John	Hooder	Defense Information Systems Agency
Laura	House	The Boeing Company
Allan	Howell	Transport Canada
Darlene	Hughes	Universal Avionics Systems Corp.
David	Huhn	GE Aviation
Carla	Hunt	Defense Information Systems Agency
Jeannie	Hunt	A Cisco Company
Graham	Ison	Thales
Shreyas	Iyer	Honeywell International, Inc.
Andrew	Jackson	GCHQ
Bruce	Jackson	Air Informatics LLC
Paul	Jackson	Federal Aviation Administration
Owen	Jing	Amtek Engineering Ltd.
Lisa	Kaiser	U.S. Department of Homeland Security
Ron	Kallio	Bombardier Aerospace
Kathleen	Kearns	SITA
Mark	Kelley	Esterline AVISTA
Amber	Kemmerling	The Boeing Company
Steve	Kennedy	Honeywell International, Inc.
Peter	Kertzner	The MITRE Corporation
Varun	Khanna	Federal Aviation Administration
Charles	Kilgore	Federal Aviation Administration
Nathan	King	United Airlines, Inc.

Rainer	Koelle	EUROCONTROL
Andrew	Kornecki	Embry-Riddle Aeronautical University
Fred	Kujawski	Gogo LLC
Marc	Labay	Federal Aviation Administration
Jose	Lautenschlager	ANAC-Brazil
Harmon	Law	Assured Networking
Xiaogong	Lee	Federal Aviation Administration
Michael	Lemay	Bombardier Aerospace
Laurent	Leonardon	Rockwell Collins, Inc.
Jerome	Lephay	Rockwell Collins, Inc.
Barbara	Lingberg	Federal Aviation Administration
Wendy	Ljungren	GE Aviation
Marc	Lord	Transport Canada
Matt	Luallen	Encari
Michael	Lukaschewitsch	Lufthansa German Airlines
Leslie	Lyne	Federal Aviation Administration
Bruce	Mahone,	SAE International
Brandon	Mangold	United Airlines, Inc.
Bob	Manners	Lumark Technologies, Inc.
Dave	Manser	TASC, Inc.
David	Manville	U.S. Army
James	Marks	Federal Aviation Administration
Philippe	Marquis	Dassault Aviation
Mike	Maschino	General Dynamics
Greg	Maund	Federal Aviation Administration
Nathan	Maurer	Atlas Air
James	McLeroy	United Parcel Service
Kevin	Meier	Cessna Aircraft Company
Michel	Messerschmidt	Airbus Industries
Stephane	Miglio	Airbus SAS
Cecile	Morlec	Airbus SAS
Harold	Moses	RTCA, Inc.
Hugh	Mote	Aerospace Consulting Toulouse
Gil	Mulin	Airbus SAS
Mark	Mutchler	Federal Aviation Administration
Cliff	Neudorf	Transport Canada
Lee	Nguyen	Federal Aviation Administration
Robby	O'Dell	Gulfstream Aerospace Corporation
Robert	Oates	Rolls-Royce PLC
Thomas	Obert	Airbus Americas, Inc.
Michael	Olive	Honeywell International, Inc.
Steve	Paasch	Federal Aviation Administration

Frederic	Painchaud	DRDC Valcartier
Thomas	Parmer	Federal Aviation Administration
Vidyut	Patel	Federal Aviation Administration
Ted	Patmore	Delta Air Lines, Inc.
Michael	Paulitsch	EADS - Military Air Systems
Daniel	Pereira	EMBRAER
John	Philbin	Northrop Grumman Corporation
David	Pierce	GE Aviation
Stephane	Plichon	Thales
Jason	Posniak	Pratt & Whitney United Technologies
Ken	Przeslica	US Airways
Christian	Pschierer	Jeppesen
Chris	Riley	Volpe National Transportation Systems Center
Steven	Rines	Miltope Corporation
Philippe	Robert	AEROCONSEIL
David	Robertson	Sourcefire
Lionel	Robin	Sagem Avionics, Inc.
David	Robinson	Federal Aviation Administration
George	Romanski	VEROCEL, Inc.
Marc	Ronell	Federal Aviation Administration
Cyrille	Rosay	European Aviation Safety Agency
Ron	Ross	National Institute of Standards & Technology
Jayson	Rowe	Civil Aviation Safety Authority (CASA) Australia
Wes	Ryan	Federal Aviation Administration
Shohreh	Safarian	Federal Aviation Administration
Romuald	Salgues	Airbus Americas, Inc.
Steve	Saltz	ENEA
Javier	Sanchez	Black Hammer LLC
Cleber	Santos	Bombardier Aerospace
Timothy	Schroeder	Honeywell International, Inc.
Remzi	Seker	Embry-Riddle Aeronautical University
Phil	Simpson	UK Dept for Transport
Peter	Skaves	Federal Aviation Administration
Wilfried	Steiner	TTTech AG
Stephen	Sterling	Department of National Defence - CANADA
Thomas	Stevens	Securaplane Technologies
Charles	Stewart	United Airlines, Inc.
Joe	Stewart	Securaplane Technologies
David	Stinson	U.S. Air Force
Paul	Storck	Rockwell Collins, Inc.
Ronald	Stroup	Federal Aviation Administration
Will	Struck	Federal Aviation Administration

Wendy	Sullivan	Gulfstream Aerospace Corporation
Craig	Sweigart	The MITRE Corporation
Timothy	Tinney	Saab Shared Services
Robert "Rip"	Torn	Air Line Pilots Association
Tim	Totten	United Parcel Service
Gifflene	Toussaint	C2 Technologies Inc.
Mitchell	Trope	Garmin Ltd.
Ed	Valovage	Saab Sensis Corporation
Gary	Vanyek	Thales Avionics
Brian	Verna	Federal Aviation Administration
Patricia	Vicente	US Airways
Tong	Vu	Federal Aviation Administration
Mohammed	Waheed	Rockwell Collins, Inc.
Chris	Wargo	Mosaic ATM, Inc.
John	Warther	Green Hills Software, Inc.
Bernie	Watson	Hawaiian Airlines, Inc.
Philip	Watson	Panasonic Avionics Corporation
Todd	White	L-3 Communications
Thomas	Williams	Honeywell International, Inc.
Marcie	Wise	Delta Air Lines, Inc.
J. Leonard	Wood	Condor Aviation Corporation

APPENDIX A : DEFINITION OF THE AIRWORTHINESS SECURITY ACTIVITIES

This Appendix defines the activities, output data requirements, and compliance objectives for an Airworthiness Security Process to establish the security requirements for the aircraft and systems. Chapter 2 shows the generic Airworthiness Security Process activities which are defined in this appendix. See Figure A-1 for an overview of the activities and their principal data dependencies. See Chapter 3 for the concepts and principles of those activities. See Chapter 4 for the applicability of the activities for different types of certification efforts. This process is designed to apply 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.

In an actual development program, many activities are iterative and there are numerous updates and interactions between Activities and data. Indeed, for some activities, their inputs will not all be available on the first iteration, e.g. PSecAC. All activities should be reviewed at the end of the process, to ensure that their outputs are complete and consistent. The required relationships between the data produced and managed by the activities are defined in the compliance objectives under each activity which specify the required relationships of **correctness**, **consistency**, and **completeness** between the data.

This Appendix does not specify a document structure for the output data, but allows the applicant to define a structure with the agreement of the AA that best suits the two parties and takes advantage of existing practices. The output data and the specific form of the data should be specified in the Plan for Security Aspects of Certification.

The compliance objectives do not represent completion criteria for each activity, but rather specify the required characteristics of the data at the end of the overall development program. Nonetheless, they have been defined so that establishing tentative compliance at the end of each activity and then updating the data as additional information becomes available will be a prudent and useful step to ensure final success.

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.

Appendix A is organized in three sub-sections:

A.1 Security aspects of Certification

A.2 Security risk assessment related activities

A.3 Security development activities

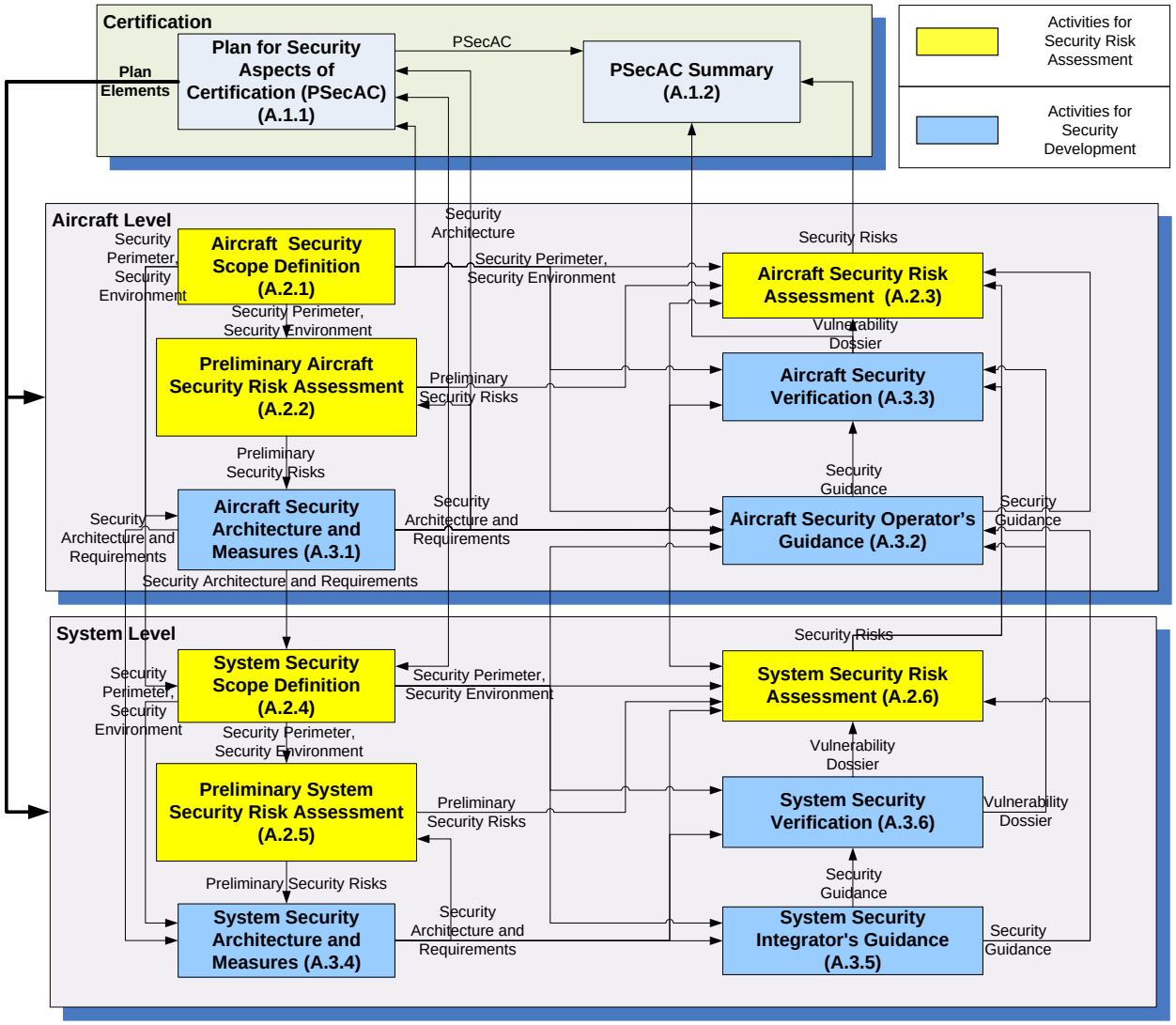

Figure A-1 : Airworthiness Security Process Activities

A.1 Security Aspects of Certification

A.1.1 Plan for Security Aspects of Certification (PSecAC)

Purpose

Identify means for demonstrating compliance with airworthiness regulations relative to security concerns.

Details

– Determine certification basis, including results of Change Impact Analysis, if any.
– Determine acceptable means of compliance.
– Determine certification data package.
– Identify definition and schedule of major milestones.
– Coordinate with other related certification materials.
– Resolve issues identified by the certification authority.
– Submit PSecAC and obtain approval.

Input

– (if any) regulatory requirements for Information Security
– Aircraft Certification Planning Data
– Aircraft Security Scope Definition (ASSD output)
– Aircraft security architecture(ASAM output)
– Aircraft threat conditions (PASRA output)

Output

– Plan for Security Aspects of Certification
– Provide links with aircraft certification planning data

Compliance Objectives

– Plan for Security Aspects of Certification is correct and complete, and includes:
  - o Addressing the regulatory requirements for security as necessary;
  - o Overview of aircraft-level architecture and system-level architecture of selected systems, with emphasis on elements pertinent to security threats and security measures;
  - o Identification of the elements of the aircraft certification basis that are applicable to security;
  - o Means and methods for showing compliance to the certification basis related to security;
  - o Overview of Preliminary Aircraft Security Risk Assessment;
  - o Definition of substantiating data to be produced, and responsibilities for delivery and approval;
  - o Relationship or dependencies to other certification plans;
  - o A schedule of interactions with certification authority.

A.1.2 Plan for Security Aspects of Certification Summary (PSecAC Summary)

Purpose

Produce certification evidence relative to security concerns.

Details	**Input**
– Provide evidence on activities which have been performed in compliance with their assigned objective. – Identify and justify deviations from PSecAC.	– Plan for Security Aspects of Certification (PSecAC output) – Aircraft Security Risk Assessment (ASRA output) – Aircraft vulnerability dossier (ASV output) – Aircraft security verification and test results and analysis (ASV output)
	Output – PSecAC Summary

Compliance Objectives

– PSecAC Summary is consistent and complete with respect to Plan for Security Aspects of Certification.
– PSecAC Summary is consistent to aircraft security verification and test results and analysis.
– Deviations are acceptable.

A.2 Security Risk Assessment Related Activities

A.2.1 Aircraft Security Scope Definition (ASSD)

Purpose

Determine aircraft operational environment for information security.

Details

- Determine the aircraft security perimeter and aircraft assets.
- Identify information interfaces.
- Identify existing security measures
- Define the roles and organizations that interact with the aircraft
- Determine the aircraft security environment.
- Identify trust relationships and security risk related to:
  - Roles and entities,
  - External tools and systems,
  - External security measures
  - Other external dependencies
- Identify assumptions about the operational and maintenance environments.
- Identify preliminary external agreements (e.g. operator requirements, maintenance requirements).
- Identify and classify the threat sources.

Input

- Functional and operational description of aircraft and systems

Output

- Aircraft Security Scope Definition (ASSD) (security perimeter, security environment)

Updates (if needed)

- Update to Plan for Security Aspects of Certification for the PSecAC Activity
- Update to aircraft functional requirements

Compliance Objectives

- Aircraft Security Scope Definition (security perimeter, security environment) is identified, correct and complete.

A.2.2 Preliminary Aircraft Security Risk Assessment (PASRA)

Purpose

Identify and assess all security risks at aircraft level.

Details

- Identify all threat conditions associated with the aircraft assets.
- Evaluate severity of effect of threat conditions and associated assets.
- Identify functional security dependencies between threat conditions and threat sources.
- Assess the aircraft security architecture and requirements.
- Identify existing security measures.
- Identify attack paths.
- Identify assets associated with threat conditions.
- Determine and classify threat scenarios for severity and level of threat.
- Evaluate security risk from intentional unauthorized electronic interaction.
- Determine need for risk mitigation, including possible gaps in security architecture and requirements.
- Residual risk identification.
- Security requirement identification
- Inform design groups of need for requirements for security measures or security guidance
- Inform design groups of need for security assurance actions
- Assess the risk.
- Residual risk assessment, including the decision action (choice between accept, mitigate, avoid, transfer risk).
-

Input

- Functional and operational description of aircraft and systems
- Aircraft Functional Hazard Assessment
- Aircraft Security Scope Definition (Security perimeter, security environment) (ASSD output)
- Aircraft security architecture and requirements (initial based on Aircraft Safety Architecture and subsequent from ASAM output)
- Preliminary Aircraft Safety Assessment

Output

- Preliminary Aircraft Security Risk Assessment (PASRA)

Updates (if needed)

- Update of new hazards or reclassified hazards (if needed) to AFHA based on threat condition assessment
- Update to Plan for Security Aspects of Certification for the PSecAC Activity
- Provide additional validation study requirements for the ASV Activity
- Update to aircraft requirements

Compliance Objectives

- PASRA is consistent with Aircraft Functional Hazard Assessment.
- PASRA is consistent and complete with respect to aircraft security scope, aircraft requirements, and aircraft security architecture.
- Preliminary aircraft security risks are acceptable.
- PASRA is consistent and complete with respect to PASA

.

A.2.3 Aircraft Security Risk Assessment (ASRA)

Purpose

Identify and assess the aircraft's security risks and vulnerabilities.

Details

- Finalize Aircraft Security Risk Assessment.
- Assess implementation of aircraft for security risks.
- Evaluate final security risk.
- Evaluate vulnerabilities and update vulnerability dossier.

Input

- Aircraft requirements and safety architecture
- Aircraft verification and test results and analysis
- Preliminary Aircraft Security Risk Assessment (PASRA output)
- System Security Risk Assessment (SSRA output)
- Aircraft Security Scope Definition (ASSD output)
- (if defined) Aircraft security architecture(ASAM output)
- Aircraft Security Operator Guidance (ASOG output)
- Aircraft vulnerability dossier (ASV output)

Output

- Aircraft Security Risk Assessment (ASRA)

Updates (if needed)

- Update to aircraft vulnerability dossier for the ASV Activity
- Update to Aircraft Security Operator Guidance for the ASOG Activity

Compliance Objectives

- Aircraft Security Risk Assessment is correct, complete, and consistent with aircraft requirements, and aircraft safety assessment.
- Aircraft Security Risk Assessment is consistent and complete with respect to aircraft & system security scope, security architecture, operator guidance, and vulnerability dossier.
- Aircraft Security Risk Assessment is consistent and complete with respect to System Security Risk Assessment.
- Aircraft security risks are acceptable.

A.2.4 System Security Scope Definition (SSSD)

Purpose

Determine system operational environment for information security.

Details

- Determine the system security environment:
- Identify assumptions about the operational and maintenance environments.
- Identify trust relationships and security risk related to:
  - Roles and entities,
  - External tools and systems,
  - External security measures.
- Determine the system security perimeter. and system assets:
  - Identify hardware interfaces, including radio-frequency signals (e.g.,Wi-Fi, mobile cellular, GPS, VHF).
  - Identify software interfaces, including services and protocols running over the hardware interfaces.
  - Identify information exchanges, (e.g. file transfer, ACARS messages, software loads, database updates) (e.g. file exchanges going over a Virtual Private Network (VPN) session, protocols for exchanges), including all physical paths by which information from outside the perimeter could reach the inside.
- Update preliminary external agreements (e.g. operator requirements, maintenance requirements).
- Allocate threat source to systems.

Input

- Aircraft architecture
- System requirements
- Aircraft Security Scope Definition (ASSD output)
- (if defined) Aircraft Security Architecture and Measures (ASAM output)
- Preliminary Aircraft Security Risk Assessment (PASRA output)

Output

- System Security Scope Definition (SSSD) (security perimeter, security environment)

Updates (if needed)

- Update to Plan for Security Aspects of Certification: for the PSecAC Activity
- Update to system requirements
- Update to Aircraft Security Scope Definition: for the ASSD Activity

Compliance Objectives

- System requirements are identified, correct, and complete for security concerns.
- System security scope is identified, correct and complete.
- System security scope is consistent and complete with respect to aircraft security scope and adjacent system security environments.
- System security scope is consistent and complete with respect to aircraft security architecture and aircraft requirements for security concerns.

A.2.5 Preliminary System Security Risk Assessment (PSSRA)

Purpose

Identify and assess all security risks at system level.

Details

– Identify all threat conditions associated with the system assets.
– Evaluate severity of effect of each threat condition and associated assets.
– Identify functional security dependencies between threat conditions and threat sources.
– Identify assets associated with threat conditions.
– Assess the system security architecture and requirements.
– Identify existing security measures.
– Identify attack paths.
– Determine and classify threat scenarios for severity and level of threat.
– Evaluate risk from intentional unauthorized electronic interaction.
– Determine need for risk mitigation, including possible gaps in security architecture.
– Residual risk identification.
– Security requirement identification:
– Inform design groups of need for security measure requirements.
– Inform design groups of need for security assurance actions.
– Assess the risks.
– Residual risk assessment, including the decision action (choice between accept, mitigate, avoid, transfer risk).
– Validate assumptions about external agreements (e.g. operator requirements, maintenance requirements) when applicable to system.

Input

– System requirements and safety architecture
– Preliminary System Safety Assessment
– System Security Scope Definition (SSSD output)
– Preliminary Aircraft Security Risk Assessment (PASRA output)
– System security architecture and requirements (initial based on Aircraft Safety Architecture and subsequent from SSAM output)
– (if defined) Aircraft Security Architecture and Measures(ASAM output)

Output

– Preliminary System Security Risk Assessment (PSSRA)

Updates (if needed)

– Update to system requirements
– Provide additional validation study requirements for the SSV Activity

Compliance Objectives

– Preliminary System Security Assessment is correct and complete.
– Preliminary System Security Assessment is consistent and complete with respect to system security scope, system requirements, and system security architecture.
– Preliminary Aircraft Security Assessment is consistent and complete with respect to system security requirement and Preliminary System Safety Assessment.
– Preliminary system security risks are acceptable.

A.2.6 System Security Risk Assessment (SSRA)

Purpose

Identify and assess the system's security risks and vulnerabilities.

Details

– Finalize System Security Risk Assessment.
– Assess implementation of lower level systems or items for security risks.
– Evaluate final security risk.
– Evaluate vulnerabilities and update vulnerability dossier.

Input

– System requirements
– System Safety Assessment
– System verification and testing records
– Preliminary System Security Risk Assessment (PSSRA output)
– System Security Scope Definition (SSSD output)
– System Security Integrator Guidance (SSIG output)
– Aircraft Security Architecture (ASAM output)
– System vulnerability dossier (SSV output)

Output

– System Security Risk Assessment (SSRA)

Updates (if needed)

– Update to System Security Integrator Guidance for the SSIG Activity
– Update to vulnerability dossier for the SSV Activity
– Update to system requirements

Compliance Objectives

– System Security Assessment is correct, complete and consistent with system requirements and System Safety Assessment.
– System Security Assessment is consistent and complete with respect to system security scope, system security architecture, System Security Integrator Guidance, system requirements and system verification.
– System security risks are acceptable.

A.3 Security Development Activities

A.3.1 Aircraft Security Architecture and Measures (ASAM)

Purpose

Establish effective Aircraft Security Architecture and Measures.

Details

– Determine Aircraft Security Architecture and Measures.
– Determine security requirements for security measures.
– Determine and validate security effectiveness objectives and requirements.
– Allocate security measures to systems or operator guidance
– Determine security assurance actions.
– Provide means for periodically establishing airworthiness with respect to security issues.

Input

– Aircraft requirements and safety architecture
– Aircraft Security Scope Definition (ASSD output)
– Preliminary Aircraft Security Risk Assessment (PASRA output)

Output

– Aircraft security architecture and requirements
– Aircraft security effectiveness requirements

Updates (if needed)

– Update to Aircraft Security Scope Definition for the ASSD Activity
– Update to Preliminary Aircraft Security Risk Assessment for the PASRA Activity
– Update to Plan for Security Aspects of Certification for the PSecAC Activity (update of summary of Security Architecture)
– Update to aircraft requirements
– Update to system requirements

Compliance Objectives

– Aircraft security architecture and requirements are correct, complete and consistent with aircraft safety architecture.
– Aircraft security architecture and requirements are consistent with aircraft requirements.
– Aircraft security architecture is consistent and complete with respect to aircraft security scope.
– Aircraft security effectiveness requirements are correct, complete and consistent with Preliminary Aircraft Security Risk Assessment.
– Assurance actions are consistent with threat conditions for security measures.

.

A.3.2 Aircraft Security Operator Guidance (ASOG)

Purpose

Develop Aircraft Security Operator Guidance.

Details	**Input**
– Develop Aircraft Security Operator Guidance.	– Aircraft implementation – Aircraft Security Scope Definition (ASSD output) – System Security Scope Definition (SSSD output) – System Security Integrator Guidance (SSIG output) – Aircraft Security Architecture and Measures (ASAM output)
	Output – Aircraft Security Operator Guidance (ASOG)
	Updates (if needed) – Update to operating procedures – Update to maintenance procedures – Update to Instructions for Continued Airworthiness

Compliance Objectives

– Aircraft Security Operator Guidance is correct, complete and validated.
– Aircraft Security Operator Guidance is consistent and complete with respect to aircraft security scope.
– Aircraft Security Operator Guidance is consistent and complete with respect to aircraft requirements and implementation.
– Aircraft Security Operator Guidance is consistent and complete with respect to System Security Integrator Guidances.

A.3.3 Aircraft Security Verification (ASV)

Purpose

Show compliance with aircraft security requirements and evaluate the security effectiveness of the security measures of the aircraft for its intended environment.

Details

- Verify that aircraft security implementation is correct and that aircraft security requirements are met.
- Determine vulnerability dossier.
- Finalize security verification and test plan.
- Analyze problem reports for security verification and test results.
- Verify that aircraft security measures are effective against the aircraft threat scenarios.
- Finalize vulnerability test plan and evaluate how well it covers the security requirements in its context of the threat scenarios in the security risk assessment, including its security effectiveness.
- Assess Aircraft Security Operator Guidance.
- Conduct vulnerability assessment and testing and analyze results for security risk.

Input

- Aircraft implementation and requirements
- System vulnerability dossier(SSV output)
- Aircraft Security Operator Guidance (ASOG output)
- Aircraft Security Scope Definition (ASSD output)
- Aircraft security architecture (ASAM output)
- Aircraft security effectiveness requirements (ASAM output)
- Additional validation study requirements (PASRA output)

Output

- Aircraft vulnerability dossier
- Aircraft security verification and test results and analysis
- Additional validation study results

Updates (if needed)

- Update to Aircraft Security Operator Guidance for the ASOG Activity
- Update to aircraft implementation
- Update to operating procedures
- Update to maintenance procedures
- Update to Instructions for Continued Airworthiness

Compliance Objectives

- Security elements of aircraft verification and test plans are correct, complete, and approved.
- Aircraft verification is correct and complete for security concerns.
- Aircraft verification is consistent and complete with respect to aircraft requirements and aircraft security architecture.
- Aircraft vulnerability assessment and test results and analysis is consistent and complete with respect to aircraft security scope, aircraft requirements, Preliminary Aircraft Security Risk Assessment, and Aircraft Security Operator Guidance.
- Remaining vulnerabilities in aircraft vulnerability dossier are acceptable.
- Aircraft vulnerability dossier is correct and complete.

A.3.4 System Security Architecture and Measures (SSAM)

Purpose

Establish System Security Architecture and Measures.

Details

– Determine System Security Architecture and Measures.
– Determine security requirements for security measures.
– Determine and validate security effectiveness objectives and requirements.
– Allocate security measures to subsystems or items or security guidance
– Identify supporting lower level systems or item assets.
– Determine security assurance actions.

Input

– Systems requirements and safety architecture
– Aircraft security architecture (ASAM output)
– System Security Scope Definition (SSSD output)
– Preliminary System Security Risk Assessment (PSSRA output)

Output

– System security architecture and requirements
– System security effectiveness requirements

Updates (if needed)

– Update to system requirements

Compliance Objectives

– System security architecture and requirements are correct, complete and consistent with system safety architecture and Aircraft Security Architecture and Measures.
– System security architecture and requirements are consistent with system security scope.
– System security architecture and requirements are consistent with system requirements.
– System security effectiveness requirements are correct, complete and consistent with Preliminary System Security Risk Assessment.
– Assurance actions are consistent with threat conditions for security measures.

.

A.3.5 System Security Integrator Guidance (SSIG)

Purpose

Develop Security Integrator Guidance for operation and maintenance for the System.

Details

– Develop System Security Integrator Guidance.
– Finalize external agreements (e.g. operator requirements, maintenance requirements).

Input

– System implementation
– System Security Scope Definition (SSSD output)
– System Security Architecture and Measures (SSAM output)

Output

– System Security Integrator Guidance

Updates (if needed)

– (none)

Compliance Objectives

– System Security Integrator Guidance is correct and complete.
– System Security Integrator Guidance is consistent and complete with respect to system requirements, and system implementation.
– System Security Integrator Guidance is consistent and complete with respect to system security scope.

A.3.6 System Security Verification (SSV)

Purpose

Show compliance with system requirements and evaluate the security effectiveness of the security measures of the system for its intended environment.

Details

- Verify that system security implementation is correct and that system requirements are met.
- Determine vulnerability dossier.
- Finalize security verification and test plan and analyze coverage of threat scenarios.
- Analyze problem reports for security verification and test results.
- Verify that system security measures are effective for the security environment.
- Finalize vulnerability test plan and evaluate how well it covers the security requirements in its context of the threat scenarios in the security risk assessment, including its security effectiveness.
- Assess System Security Integrator Guidance.
- Conduct vulnerability assessment and testing, and analyze results.

Input

- System verification and testing records
- System implementation
- System security architecture (SSAM output)
- System Security Integrator Guidance (SSIG output)
- System Security Scope Definition (SSSD output)
- System security effectiveness requirements (SSAM output)
- Additional validation study requirements (PSSRA output)

Output

- System vulnerability dossier
- System security verification and test results and analysis
- Additional validation study results

Updates (if needed)

- (none)

Compliance Objectives

- Security elements of system verification and test plans are correct, complete, and approved.
- System verification is correct and complete for security concerns.
- System verification is consistent and complete with respect to aircraft security scope.
- System verification is consistent and complete with respect to system requirements and system security architecture.
- System vulnerability dossier is correct and complete.
- System vulnerability assessment and test results and analysis is consistent and complete with respect to system security scope, system requirements, and System Security Integrator Guidance.
- System vulnerability assessment and test results and analysis is consistent and complete with respect to Preliminary System Security Risk Assessment.

APPENDIX B : GLOSSARY

The following is informative. 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.

Term	Definition
Aeronautical Information System	The set of information resources organized expressly for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information involved in all aspects of aircraft operations. Note that this includes supplier's information systems supporting the development of onboard system software and data.
Aircraft Type Certification	The legal recognition that a product, service, organization or person complies with the applicable requirements. Such certification comprises the activity of technically checking the product, service, organization or person, and the formal recognition of compliance with the applicable requirements by issue of a certificate, license, approval or other document as required by national laws and procedures. In particular, certification of a product involves: a) The process of assessing the design of a product to ensure that it complies with a set of standards applicable to that type of product so as to demonstrate an acceptable level of safety. b) The process of assessing an individual product to ensure that it conforms to the certified type design. c) The issue of any certificate required by national laws to declare that compliance or conformity has been found with applicable standards in accordance with paragraph (a) or (b) above.
Airworthiness	The condition of an item (aircraft, aircraft system, or part) in which that item operates in a safe manner to accomplish its intended function.(ED-79A/ARP 4754A)
Airworthiness Security (AWS)	The protection of the airworthiness of an aircraft from intentional unauthenticated electronic interaction: harm due to human action (intentional or unintentional) using access, use, disclosure, disruption, modification, or destruction of data and/or data interfaces. This also includes the consequences of malware and forged data and of access of other systems to aircraft systems.
Assessment	An evaluation based upon engineering judgment. (ED-79A/ARP 4754A)
Asset	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
Assumptions	Statements, principles, and/or premises offered without proof. (ED-79A/ARP 4754A)
Assurance	The planned and systematic actions necessary to provide adequate confidence that a product or process satisfies given requirements. (ED-79A/ARP 4754A)
Attack	An assault on a system that derives from an act that is an attempt to violate the security policy of a system. This includes intentional and unintentional acts.
Attack Path	The path, interface, and actions by which an attacker executes an attack.
Attack Vector	The means of access which an attacker used to begin an attack.

Term	Definition
Attacker	The entity that initiates and directs an attack. This includes intelligent attackers as well the automatic actions of attack code such as a bot or worm and the authors of such code.
Availability (Security)	Ensuring authorized users have access to information and associated assets when required.
Completeness	Completeness of a requirement statement means that no attributes have been omitted and that those stated are essential. Completeness with respect to another requirement statement means completeness within the scope and attributes of the other statement.
Confidentiality	Ensuring that information is accessible only to those authorized to have access.
Consistent	Consistency between requirements statements means the attributes are in agreement within the scope of the intended purposes. A design specification is consistent with the requirements if neither contradicts the other. A power budget summary is consistent with a design specification if a quantity in the budget that refers to the design specification is equal to the quantity implied by the design specification.
Correctness	Correctness of a requirement statement means the absence of ambiguity or error in its attributes.
Data	Physical phenomena chosen by convention to represent certain aspects of our conceptual and real world.
Dependent System	An aircraft System that depends on an external system for correct function.
External (Aircraft)	A reference outside of aircraft systems. Note that this includes reference to systems on other aircraft and to systems that can be carried onboard but are not considered part of the aircraft type configuration. See System (Aircraft).
External Agreement	Assumptions and requirements for the purpose of coordinating roles and responsibilities between dependent systems and external actors.
External Population	Those persons, organizations, or external systems which can interact with the assessment asset under expected conditions of operation and/or failure.
Failure Condition	A condition having an effect on the airplane and/or its occupants, either direct or consequential, which is caused or contributed to by one or more failures or errors, considering flight phase and relevant adverse operational or environmental conditions, or external events.
Flight Safety Hazard	A potentially unsafe condition resulting from failures, malfunctions, external events, errors, or a combination thereof.
Function	Intended behavior of a product based on a defined set of requirements regardless of implementation. (ED-79A/ARP 4754A)
Information	Information is the (subjective) interpretation of data.
Information Security Threat	See "Intentional Unauthorized Electronic Interaction".
Information System	A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.
Integrity (Security)	Safeguarding the accuracy and completeness of information and processing methods.

Term	Definition
Intended Actions	Operational action or sequence of actions undertaken to interact with the assessment asset which the requirements intend to occur. Examples include access / manipulation / modification / deletion / creation / administration / maintenance / installation.
Intentional Unauthorized Electronic Interaction	A circumstance or event with the potential to affect the aircraft due to human action resulting from unauthorized access, use, disclosure, denial, disruption, modification, or destruction of information and/or aircraft system interfaces. Note that this includes malware and the effects of external systems on aircraft systems, but does not include physical attacks or electromagnetic jamming.
Item	A hardware or software element having bounded and well-defined interfaces (ED-79A/ARP 4754A)
Level of Threat	A qualitative evaluation of the possibility that a Threat Condition might occur.
Malware	Malicious software that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim's data, applications, or operating system or of otherwise annoying or disrupting the victim.
Misuse (Security)	Unintended (according to the design intent) actions undertaken by a person or system to interact with systems, interfaces, or data. See Use.
Mitigation	Reduction of risk either through lessening of severity or lessening of occurrence.
Objective (Process)	A statement of intent to ensure that identified properties will hold for the outputs of a process. The process objectives need not be goals of the process itself, but may be a consequence of the goals and activities of the process.
Operational Conditions	A condition of the aircraft which can result from operational events.
Operational Environment	The set of defined concepts of operations, regulations, plans, policies, and procedures of the external organizations and systems that interact with the dependant systems of the aircraft, together with any regulations and policies which apply internally to the aircraft systems themselves.
Operational Events	Events that are part of the intended function and operation of the aircraft.
Operational Span	The exposure of an aircraft type to the information security threat considered both over multiple aircraft and time.
Operations	In any architectural context, when two or more elements cooperate to achieve a stated objective, that objective is an operation.
Operator Guidance	Specifications and technical and organizational requirements for the secure operation and maintenance of an aircraft and aircraft systems by an operator. These are the restrictions or requirements on the policies and procedures needed to satisfy the security requirements and should include all relevant requirements involving use, administration, installation, maintenance, or disposal.
Requirement	An identifiable element of a function specification (technical) or a development assurance standard (assurance) that can be validated and against which an implementation can be verified.
Risk (Security)	Exposure to the possibility of harm. The risk of an event is a function of the severity of the adverse event and the level of threat of that event.
Risk Management	The continuous process of identifying, controlling, and mitigating problems according to their risk as identified through risk assessment.

Term	Definition
Safety Architecture	That aspect of the architecture which is concerned with the concepts and basic methods for satisfying the safety objectives and requirements. A safety architecture defines architectural elements, together with their roles, responsibilities and interrelationships, which will support the safety objectives. Elements may incorporate hardware, software, algorithms, procedures, and policies.
Security Architecture	That aspect of the architecture which is concerned with the concepts and basic methods for satisfying the security requirements. A Security architecture defines architectural elements, together with their roles, responsibilities and interrelationships, which will implement and support the security measures. Elements may incorporate hardware, software, algorithms, procedures, and policies.
Security Effectiveness	The ability of the security measure to mitigate misuse of the assets by the unauthorized elements of the external population, while permitting and preserving use of the assets by the authorized elements of the external population.
Security Effectiveness Objective	A statement of intent to achieve a level of security effectiveness against a specified security environment.
Security Environment	A security environment is the external security context in which an asset performs its function. For an aircraft, or system of an aircraft, the aircraft/system security environment is characterized by the set of security assumptions outside the control of the aircraft/system developer which are used in the safety assessment of the aircraft/system.
Security Measure	Used to mitigate or control a threat condition. Security measures may be features, functions, or procedures, both onboard or offboard. Security measures can be technical, operational, or management.
Security Perimeters	The security perimeter is the boundary between an asset's internal security context and its security environment.
Security Requirements	Requirements that are related to the implementation of a security measure.
Severity	Qualitative indication of the magnitude of the adverse effect of a Threat Condition.
System (Aircraft)	A combination of inter-related Items arranged to perform a specific function(s). (ED-79A/ARP 4754A)
System (Information)	A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. Note that information systems consist of people, processes, and technology.
System (Security)	An item or collection of items arranged to perform a specific function(s) which has a well-defined security environment.
Threat Condition	A condition having an effect on the airplane and/or its occupants, either direct or consequential, which is caused or contributed to by one or more acts of intentional unauthorized electronic interaction, involving cyber threats, considering flight phase and relevant adverse operational or environmental conditions. Also see failure condition.
Threat Scenario	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.

Term	Definition
Threat Source	Either (1) intent or method targeted at the intentional exploitation of vulnerability or (2) a situation and method that can mistakenly trigger vulnerability. The threat source of a threat is intent and method: the attacker and the attack vector.
Trust Relationship	The relationship whereby an external population can interact with the assessment asset. There is a trust relationship whenever an external population can use or misuse an asset.
Unauthorized Interaction	See "Intentional Unauthorized Electronic Interaction"
Use (Security)	Intended actions undertaken by the external population to interact with aircraft systems, interfaces, or data, in order to perform intended duties. See misuse.
Integrator Guidance	Specifications and technical and organizational requirements for the secure operation and maintenance of a system or item by an aircraft integrator or operator. These are the restrictions or requirements on the policies and procedures needed to satisfy the security requirements and should include all relevant requirements involving use, administration, installation, maintenance, or disposal.
Validation	The determination that the requirements for a product are correct and complete. (ED-79A/ARP 4754A)
Verification	The evaluation of an implementation of requirements to determine that they have been met.
Vulnerability	A flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised (unintentionally triggered or intentionally exploited) and result in a security breach or a violation of the system's security policy.
Vulnerability Assessment	Generic term encompassing the two existing methods, namely vulnerability analysis or vulnerability testing, used during the evaluation of the development and anticipated operation of the aircraft/ system/ item that could be exploited by a threat source.
Vulnerability Dossier	Listing, analysis, and classification of abnormalities and threats determined as vulnerabilities through analysis and vulnerability testing according to security risk assessment.
Vulnerability Testing	Methods for testing for unintended function and robustness, using exploratory testing methods to detect and probe vulnerabilities that can be present in an implementation and attempts to break or to circumvent the security measures.
Well-known Vulnerability	A vulnerability that has been documented during previous use of some portion of the system, and the documentation is known and available to the developer.

This Page Intentionally Left Blank

APPENDIX C : ACRONYMS AND ABBREVIATIONS

AA	Airworthiness Authorities
AC	Advisory Circular
AFHA	Aircraft Functional Hazard Assessment
AISS	Aeronautical Information System Security
AMC	Acceptable Means of Compliance
AMJ	Advisory Material Joint
AOC	Airline Operations Center
ARINC	ARINC, Inc
ARP	Aerospace Recommended Practice
ASRA	Aircraft Security Risk Assessment
ASAM	Aircraft Security Architecture and Measures
ASA/CCA	Aircraft Safety Assessment and Common Cause Analysis
ASSD	Aircraft Security Scope Definition
ASOG	Aircraft Security Operator Guidance
ASV	Aircraft Security Verification
ATC	Amended Type Certificate
ATS	Air Traffic Services
AWS	Airworthiness Security
AWSP	Airworthiness Security Process
CFR	Code of Federal Regulations
CISSP	Certified Information Systems Security Professional
DAH	Design Approval Holder
DAL	Development Assurance Level
EASA	European Aviation Safety Agency
EUROCAE	European Organization for Civil Aviation Equipment
FAA	Federal Aviation Administration
FHA	Functional Hazard Assessment
FISMA	Federal Information Security Management Act
GIAC	Global Information Assurance Certification
GSE	Ground Support Equipment
ICA	Instructions for Continued Airworthiness

ICAO	International Civil Aviation Organization
IDS	Intrusion Detection System
ISO	International Organization for Standardization
IT	Information Technology
LRU	Line Replaceable Unit
MRO	Maintenance Repair Organization
NIST	National Institute of Standards and Technology
OEM	Original Equipment Manufacturer
PASRA	Preliminary Aircraft Security Risk Assessment
PASA/PSSA	Preliminary Aircraft / System Safety Assessment
PED	Portable Electronic Device
PKI	Public Key Infrastructure
PRA	Particular Risk Analysis
PSecAC	Plan for Security Aspects of Certification
PSSRA	Preliminary System Security Risk Assessment
RTCA	RTCA, Inc
SAE	SAE, Inc
SC	Special Committee
SD	Security Development
SFHA	System Functional Hazard Assessment
SRA	Security Risk Assessment
SSA	System Safety Assessment
SSAM	System Security Architecture and Measures
SSSD	System Security Scope Definition
SSIG	System Security Integrator Guidance
SSRA	System Security Risk Assessment
SSV	System Security Verification
STC	Supplemental Type Certificate
TCDS	Type-Certificate Data Sheet
USB	Universal Serial Bus
VHF	Very High Frequency
VPN	Virtual Private Network

APPENDIX D : REFERENCES

The following standards are cited in this document.

1	ARINC 811	ARINC Technical Report 811, "Commercial Aircraft Information Security Concepts of Operation and Process Framework", July 2005
2	ABN-035A	ARINC Technical Application Bulletin ABN-035A, “Considerations for the Incorporation of Cyber Security in the Development of Industry Standards”.
3	AC 23.1309-1E	FAA AC 23.1309, Equipment, Systems and Installations in Part 23 Aircraft", Nov 2011
4	AMJ 25.1309	FAA/JAA AC/AMJ 25.1309, "System Design and Analysis (Draft)", June 2002
5	ARINC 667	ARINC 667, "Field Loadable Software", Nov 2010
6	ARINC 615A	ARINC 615A, "Software Data Loader Using Ethernet Interface", May 2002
7	ARINC 665	ARINC Report 665, "Electronic Distribution of Software", Aug 2002
8	CFR Title 14 25	Code of Federal Regulations Title 14, "Airworthiness Standards: Transport Category Airplanes"
9	EASA CS-25	EASA Certification Specification CS-25, "Large Aeroplanes", Oct 2003
10	EASA CS-25 AMC 25.1309	EASA AMC 25.1309,"Systems Design and Analysis", CS-25 Book 2 Subpart F, "Acceptable Means of Compliance", Oct 2003
11	ECR 2042/2003 Part M	European Commission Regulation EC 2042/2003: Annex I: Part M (Continuing Airworthiness), Nov 2003
12	ECR 1702/2003 Part 21	European Commission Regulation 1702/2003: Part 21 (Certification of aircraft and related products, parts and appliances, and of design and production organizations), Sep 2003
13	ED-12C/ DO-178C	EUROCAE ED-12C / RTCA DO-178C, "Software Considerations in Airborne Systems and Equipment Certification", Dec 2011
14	ED-79A/ ARP 4754A	EUROCAE ED-79A/SAE ARP 4754A, "Guidelines for Development of Civil Aircraft and Systems", Dec 2010
15	ED-80/DO-254	EUROCAE ED-80 / RTCA DO-254, "Design Assurance Guidance for Airborne Electronic Hardware", Apr 2000
16	ED-135/ ARP 4761	EUROCAE ED-135/SAE ARP 4761," Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment"
17	ISO 73:2009	ISO 73:2009, “Risk Management-Vocabulary”, Dec 2009
18	ISO/IEC 27001	ISO/IEC 27001, Information technology - Security techniques - ISMS requirements ", June 2005
19	ISO/IEC 27001 Annex A	ISO/IEC 27001 Annex A, "Controls/ ISO 27002, Code of Practice for Information security Management for additional information", June 2005
20	ISO/IEC 27002	ISO/IEC 27002, " Information technology - Security techniques - Code of practice for information security management ", June 2008

21	ISO/IEC 27005	ISO/IEC 27005, " Information technology - Security techniques - Information security risk management", June 2008
22	NIST SP 800-30	NIST SP 800-30 Rev. 1, "Guide for Conducting Risk Assessments", Sept 2012
23	NIST SP 800-37	NIST SP 800-37 Rev. 1, "Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach", Feb 2010"
24	NIST SP 800-53	NIST SP 800-53 Rev. 4, "Security and Privacy Controls for Federal Information Systems and Organizations", Apr 2013
25	NIST SP 800-53A	NIST SP 800-53A Rev. 1, "Guide for Assessing the Security Controls in Federal Information Systems and Organizations, Building Effective Security Assessment Plans", Jun 2010
26	NIST SP 800-57	NIST SP 800-57, " Recommendation for Key Management: Part 1: General (Revision 3)", Jul 2012
27	NIST SP 800-82	NIST SP 800-82, "Guide to Industrial Control Systems Security", Jun 2011
28	NIST SP 800-115	NIST SP 800-115, Technical Guide for Information Security Testing and Assessment", Sep 2008
29	NIST SP 800-131A	NIST SP 800-131A, "Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths", Jan 2011
30	SAE ARP 5150	SAE ARP 5150," Safety Assessment of Transport Airplanes in Commercial Service", Nov 2003

APPENDIX E: BACKGROUND OF THE DO-326/ ED-202 DOCUMENT

E.1 History of Document and Versions

This document is the joint product of two special industry committees: the EUROCAE Working Group WG-72, titled “Aeronautical Information System Security” and the RTCA Special Committee SC-216, also titled “Aeronautical Systems Security”. WG-72 was formed and began meeting in 2006 to address information security for the overall Aeronautical Information System Security (AISS) of airborne systems with related ground systems and environment. SC-216 was formed and began meeting in 2007 to specifically address information security for certification of aircraft and its systems. Both organizations agreed to develop joint documents through which the airworthiness of future aircraft will be enabled despite the potential for intentional or unintentional misuse of aircraft information systems.

DO-326/ED-202 "Airworthiness Process Specification" was published in 2010 to addresses Aircraft Type Certification (TC). Aeronautical Information Security was not yet widely implemented, so the guidance was derived from understood best practice. Because of the impending introduction of aircraft with significant security-related features, it was released to address immediate industry concerns and to establish feedback on its implementation challenges.

WG-72 and SC-216 continued to develop further guidance for methods and continuing airworthiness, to update and refine the guidance for the Airworthiness Security Process (AWSP), and to extend the guidance to include considerations for Amended Type Certification (ATC), Supplemental Type Certification (STC), and other changes to Type Certification. This was done by modifying DO-326/ED-202 to result in the publication of DO-326A/ED-202A and by developing and publishing two companion documents:

- ED-204/DO-355 " Information Security Guidance for Continuing Airworthiness ", and
- A forthcoming companion document on Methods and Consideration.

E.2 Rationale for an Airworthiness Security Process

Current industry standards for safety assessment processes (e.g. ED-79A/ARP 4754A process with methods from ED-135/ARP 4761) are focused on the failure of onboard Systems and not on malicious intent. As a result, there are gaps when malicious acts are considered. This guidance was developed to address these gaps by working along with the safety assessment process using relevant Security Risk Assessment elements from existing Security Risk Assessment standards. However, there remains enough coordination that any safety-oriented Security Risk Assessment activities should remain closely associated with the safety assessment activities. The gaps and overlaps identified by the editorial group are as follows.

CS-25 AMC 25.1309 excludes adverse events due to sabotage for assessing flight safety hazards. The standard practice uses a broad definition of "interference" that includes most but not all hazards that would occur due to deliberate electronic attack. The effect (on aircraft and crew) of a successfully executed attack is a condition which has an adverse effect on the aircraft or its occupants. Such a threat condition is much like a failure condition as defined in industry standards for safety assessment processes. The difference

is that a threat condition will occur through a willful (intentional or unintentional) action.

It is in the fundamental nature of airborne functions that proper operation and configuration are dependent on persons, organizations, and external systems. Standard practice in safety assessment already requires the consideration of hazards that arise from these external dependencies. However, the inclusion of the possibility of an electronic attack is new to the external agreements governing these external dependencies and should include Security Risk Assessment.

In general, aircraft safety and information security requirements may be approached in a similar way; however, designing for security is a specialty with its own expertise and practices and should be handled as such.

It is not unusual for requirements for security measures to be stated in terms of the absence of undesired attributes. Such requirements can present problems for verification and test and are the subject of specialized practices such as vulnerability analysis and test.

There is a large overlap between security and safety. This overlap represents an opportunity to avoid a large amount of duplicate analysis, but requires collaborative decisions on the resolution of disagreements or gaps. Therefore, a process which has not integrated system development and flight safety assessment with Security Risk Assessment should provide a means to ensure that the processes are consistent with each other and that together they are complete. Furthermore, there needs to be a means for classifying, discriminating, and managing classes of functions and controls which play roles in both flight safety and security to provide a means of maintaining consistency and completeness between safety and security activities.

E.3 Information on the Changes Between DO-326/ED-202 and DO-326A/ED-202A

From a global point of view, the document has been simplified in order to enhance its readability. It has been focused on the process aspects (the “WHAT”) while a forthcoming companion document will be focused on methods and considerations (the “HOW”). As a consequence, some considerations in the original document (including item level aspects) have been moved to that document.

The document body has been re-structured. Considering the new Table of Content, the main changes are detailed as follows:

- Section 2 is a new section whose objective is to provide an overview of the Airworthiness Security Process. This process is the set of activities to be performed to manage the security risks in the context of granting a TC (Type Certificate). It reuses former sections 1.4, 1.5, 2.1 and former Appendix B (except B1). Particular attention has been paid to segregate the Security Risk Assessment Process from the Safety Assessment Process and consider its interactions with ED-79A/ARP4754A like those of a Particular Risk Analysis.
- Section 4 is a complement to section 2 in a TC modification context, especially in the case of STC (Supplemental Type Certificate). This part is also more detailed than previous DO-326/ED-202 section 3.1.2
- Section 3 describes the concepts required to understand the activities to be performed. It is a re-organization and simplification of former section 2 according to the following

topics:

- Establishing the Security Scope (Perimeter + Environment) = Amended former section 2.2 + complement on Security Environment
- Security Risk Assessment = Merge of amended former sections 2.3, 2.5.1, 2.5.2, 2.5.3, 2.4.1 and 2.4.2
- Security Effectiveness = new sub-section reusing amended former sections 2.6.2, 2.7.1 and 2.7.2
- Security Development Activities
  - 3.4.1 Security Architecture = amended former section 2.6.4
  - 3.4.2 Security Measures = amended former section 2.6.1
  - 3.4.3 Security Guidance = amended former section 2.8.3
  - 3.4.4 Security Verification = amended former section 2.7.4

- Appendix A largely re-uses former Section 3 content, except introduction, sections 3.1 and 3.9 which have been deleted
- Other appendices are the same except former Appendix B reduced to Appendix B.1(= new Appendix E)
- Sections that have been moved to a forthcoming companion document are the following: 2.4.3, 2.4.4, 2.5.4, 2.6.3, 2.6.5, 2.8.1
- Deleted sections : 2.5.5, 2.8.2, 2.8.4

This Page Intentionally Left Blank