Designation: F3532 – 22

# Standard Practice for Protection of Aircraft Systems from Intentional Unauthorized Electronic Interactions[1]

This standard is issued under the fixed designation F3532; the number immediately following the designation indicates the year of original adoption or, in the case of revision, the year of last revision. A number in parentheses indicates the year of last reapproval. A superscript epsilon (ε) indicates an editorial change since the last revision or reapproval.

## 1. Scope

1.1 This practice covers methods for addressing Aircraft System Information Security Protection (ASISP) risks caused by Intentional Unauthorized Electronic Interactions (IUEIs). This practice was developed considering Level 1, Level 2, Level 3, and Level 4 normal category aeroplanes. The content may be more broadly applicable. It is the responsibility of the applicant to substantiate broader applicability as a specific means of compliance. The topics covered within this practice are threat identification, identifying security measures, conducting a security risk assessment, and security documentation.

1.2 An applicant intending to use this practice as means of compliance for a design approval must seek guidance from their respective oversight authority (for example, published guidance from applicable civil aviation authority (CAA)) concerning the acceptable use and application thereof. For information on which oversight authorities have accepted this practice (in whole or in part) as an acceptable Means of Compliance to their regulatory requirements (hereinafter "the Rules"), refer to the ASTM Committee F44 web page (www.astm.org/COMMITTEE/F44.htm).

1.3 *This standard does not purport to address all of the safety concerns, if any, associated with its use. It is the responsibility of the user of this standard to establish appropriate safety, health, and environmental practices and determine the applicability of regulatory limitations prior to use.*

1.4 *This international standard was developed in accordance with internationally recognized principles on standardization established in the Decision on Principles for the Development of International Standards, Guides and Recommendations issued by the World Trade Organization Technical Barriers to Trade (TBT) Committee.*

## 2. Referenced Documents

2.1 Following is a list of external standards referenced throughout this practice; the earliest revision acceptable for use is indicated. In all cases, later document revisions are acceptable if shown to be equivalent to the listed revision, or if otherwise formally accepted by the governing CAA; earlier revisions are not acceptable.

2.2 *ASTM Standards:*[2]

F3060 Terminology for Aircraft

F3061/F3061M Specification for Systems and Equipment in Small Aircraft

F3230 Practice for Safety Assessment of Systems and Equipment in Small Aircraft

2.3 *EASA Standard:*[3]

AMC 20-42 Airworthiness Information Security Risk Assessment

2.4 *EUROCAE Standards:*[4]

ED-202A Airworthiness Security Process Specification

ED-203A Airworthiness Security Methods and Considerations

ED-204A Information Security Guidance for Continuing Airworthiness

2.5 *FAA Advisory Circulars:*[5]

AC 20-115D Airborne Software Development Assurance Using EUROCAE ED-12( ) and RTCA DO-178( )

AC 20-153B Acceptance of Aeronautical Data Processes and Associated Databases

AC 119-1 Airworthiness and Operational Approval of Aircraft Network Security Program (ANSP)

2.6 *RTCA Standards:*[6]

RTCA DO-326A Airworthiness Security Process Specification

[1] This practice is under the jurisdiction of ASTM Committee F44 on General Aviation Aircraft and is the direct responsibility of Subcommittee F44.50 on Systems and Equipment.

Current edition approved Feb. 1, 2022. Published February 2022. DOI: 10.1520/F3532-22

[2] For referenced ASTM standards, visit the ASTM website, www.astm.org, or contact ASTM Customer Service at service@astm.org. For *Annual Book of ASTM Standards* volume information, refer to the standard's Document Summary page on the ASTM website.

[3] Available from European Union Aviation Safety Agency (EASA), Konrad-Adenauer-Ufer 3, D-50668 Cologne, Germany, https://www.easa.europa.eu.

[4] Available from European Organisation for Civil Aviation Equipment (EUROCAE), 9-23 rue Paul Lafargue, "Le Triangle" building, 93200 Saint-Denis, France, https://www.eurocae.net/.

[5] Available from Federal Aviation Administration (FAA), 800 Independence Ave., SW, Washington, DC 20591, http://www.faa.gov.

[6] Available from RTCA, Inc., 1150 18th NW, Suite 910, Washington, D.C. 20036, https://www.rtca.org.

RTCA DO-355A Information Security Guidance for Continuing Airworthiness
RTCA DO-356A Airworthiness Security Methods and Considerations

2.7 *Other Industry Guidance:*
ETSI EN 303 645 Cyber Security for Consumer Internet of Things: Baseline Requirements[7]
NIST SP 800-37 Risk Management Framework for Information Systems and Organizations[8]
NIST SP 800-57 Recommendation for Key Management[8]
NIST 800-131A Transitioning the Use of Cryptographic Algorithms and Key Lengths[8]

## 3. Terminology

3.1 *Definitions*—Terminology specific to this practice is provided in 3.2. For general terminology, refer to Terminology F3060.

3.2 *Definitions of Terms Specific to This Standard:*

3.2.1 *actor(s), n*—individuals, groups, or states with malicious intent.

3.2.2 *aircraft system information security protections (ASISP), n*—the process and design requirements implemented to reduce the impact of intentional unauthorized electronic interaction.

3.2.3 *assessment, n*—an evaluation based upon engineering judgment.

3.2.4 *assets, n*—resources of the aircraft and systems that are subject to attack or may be used as part of an attack, including functions, system, items, equipment, data, interfaces, and information.

3.2.5 *attack vector, n*—the path, interface, and actions by which an attacker executes an attack.

3.2.6 *availability, n*—item is in a functioning state at a given point in time.

3.2.7 *connectivity, n*—capacity for the interconnect of platforms, systems, and applications.

3.2.8 *corruption, n*—the act to change something from its original function or use to one that is failed or erroneous.

3.2.9 *data flow (logical), n*—identifies "what" information is conveyed between points in a system (that is, applications and protocols).

3.2.10 *data flow (physical), n*—identifies "how" information is conveyed between points in a system (that is, specific physical buses and interconnections).

3.2.11 *event, n*—an internal or external occurrence that has its origin distinct from the aeroplane. For purposes of this practice, the event is the IUEI.

3.2.12 *external (aeroplane), n*—reference point outside of the aeroplane systems, not part of the aeroplane type configuration; may include carried on devices.

3.2.13 *external (system), n*—reference point outside of the system under consideration. This includes other systems on the aeroplane or elements meeting the definition of "external (aeroplane)."

3.2.14 *failure, n*—an occurrence that affects the operation of a component, part, or element such that it can no longer function as intended (this includes both loss of a function and malfunction).

3.2.15 *failure condition, n*—condition on the aircraft/system that is contributed by one or more failures.

3.2.16 *field loadable software, n*—software that can be loaded without removing the system or equipment from its installation. The safety-related requirements associated with the software loading function are part of the system requirements.

3.2.17 *function, n*—intended behavior of a product based on a defined set of requirements regardless of implementation.

3.2.18 *hazard, n*—an unsafe condition resulting from failure, malfunctions, external events, error, or combination thereof.

3.2.19 *integrity, n*—attribute of a system or an item indicating that it can be relied upon to work correctly on demand.

3.2.20 *intentional unauthorized electronic interaction (IUEI), n*—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 or system interfaces, or both. This includes the consequences of malware and forged data and the effects of external systems on aircraft systems, but does not include physical attacks or electromagnetic disturbances.

3.2.21 *mitigation, n*—reduction of risk either through lessening of impact or lessening of occurrence.

3.2.22 *requirement, n*—an identifiable function specification (Technical) that can be validated and implementation can be verified.

3.2.23 *risk, n*—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 or, conversely, the effectiveness of protection.

3.2.24 *security environment, n*—the assumptions about the persons, organizations, and external systems outside of the security perimeter that interact with the asset (aeroplane, systems), so that the potential threat sources may be identified.

3.2.25 *security event, n*—an occurrence in a system that is relevant to the security of the system.

3.2.26 *security measure, n*—used to mitigate or control a threat condition. Security measures may be features, functions, or procedures. Security measures can be technical, operational, or management.

3.2.27 *security perimeter, n*—the security perimeter is the boundary between an asset's internal security context and its security environment.

3.2.28 *system boundary, n*—a logical element in a system that designates where a change in trust occurs in the system.

[7] Available from ETSI, 650, Route des Lucioles, 06560 Valbonne - Sophia Antipolis, France, https://www.etsi.org.
[8] Available from National Institute of Standards and Technology (NIST), 100 Bureau Dr., Stop 1070, Gaithersburg, MD 20899-1070, http://www.nist.gov.

3.2.29 *threat condition, n*—a condition having an effect on the aeroplane or its occupants, or both, either direct or consequential, which is caused or contributed to by one or more acts of intentional unauthorized electronic interaction (IUEI).

3.2.30 *threat scenario, n*—the specification of the IUEI, 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.

3.2.31 *threat source, n*—either *(1)* intent and method targeted at the intentional exploitation of a vulnerability, or *(2)* a situation and method that may mistakenly trigger a vulnerability. The threat source of a threat is intent and method: the attacker and the attack vector.

3.2.32 *validation, n*—the determination that the requirements for a product are correct and complete.

3.2.33 *verification, n*—the evaluation of an implementation to determine that applicable requirements are met.

3.2.34 *vulnerability, n*—a flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised and result in a security event.

3.3 *Abbreviations:*

3.3.1 *ADS-B, n*—automatic dependent surveillance – broadcast

3.3.2 *COTS, n*—commercial off-the-shelf

3.3.3 *CVE, n*—common vulnerabilities and exposures

3.3.4 *DAH, n*—design approval holder

3.3.5 *DHCP, n*—dynamic host configuration protocol

3.3.6 *EFB, n*—electronic flight bag

3.3.7 *FHA, n*—functional hazard assessment

3.3.8 *FPGA, n*—field programmable gate arrays

3.3.9 *GNSS, n*—global navigation satellite system

3.3.10 *ICA, n*—instructions for continued airworthiness

3.3.11 *IP, n*—intellectual property

3.3.12 *IUEI, n*—intentional unauthorized electronic interaction

3.3.13 *LAN, n*—local area network

3.3.14 *LRU, n*—line replaceable unit

3.3.15 *MFD, n*—multifunctional display

3.3.16 *PC, n*—personal computer

3.3.17 *PED, n*—portable electronic device

3.3.18 *PLD, n*—programmable logic device

3.3.19 *PSCP, n*—project specific certification plan

3.3.20 *PSecAC, n*—plan for security aspects of certification

3.3.21 *PSRA, n*—preliminary security risk assessment

3.3.22 *SD, adj*—secure digital

3.3.23 *SOC, n*—system on a chip

3.3.24 *SRA, n*—security risk assessment

3.3.25 *USB, n*—universal serial bus

3.3.26 *WAN, n*—wide area network

3.3.27 *WEP, n*—wired equivalent privacy

3.3.28 *WPA, n*—wireless protected access

## 4. Significance and Use

4.1 The purpose of this practice is to establish methods that can be used to satisfy the Function and Installation requirements, and the Safety Requirements, provided in 4.1 and 4.2, respectively, in Specification F3061/F3061M.

4.2 Threat conditions that can cause Hazardous or Catastrophic failure conditions, including those that can propagate through interconnected systems causing Hazardous or Catastrophic failure conditions, are required to be addressed using this practice.

## 5. Security Process Overview

5.1 Modern avionics systems often include connectivity between the avionics systems and external devices such as portable electronic devices or ground networks. These communication paths introduce the possibility of the external device adversely affecting the avionics system. Fig. 1 shows the process that is used to evaluate the possible impact of IUEI, determine necessary security measures, and show that the security architecture implemented mitigates risks to an acceptable level.

5.2 Fig. 1 shows the process to implement system security into an existing system development process. It is assumed that applicants have existing system design and system safety processes. These processes include the development of system architecture, functional hazard assessments, and system safety assessments.

5.3 The process in Fig. 1 addresses five key questions:

5.3.1 What are we building? See 6.1, Define Intended Function.

5.3.2 What can go wrong? See 6.2, Threat Identification.

5.3.3 What are we going to do to address the threats? See 6.3, Analyze Threats and Identify Security Measures.

5.3.4 Did we do an acceptable job addressing the threats? See 6.4, Conduct Security Assessment.

5.3.5 Did we adequately and accurately document the approach to security in support of the approval process? See 6.5, Security Documentation.

5.4 As an alternative to this practice, applicants can consider the Airworthiness Security Process Specification defined in the ED-202A/DO-326A, ED-203A/DO-356A, and ED-204A/DO-355A family of documents. An example of the application of these documents to the aircraft certification process is described in EASA AMC 20-42.

## 6. Procedure

6.1 *Define Intended Function:*

6.1.1 The applicant shall document the intended function of the system.

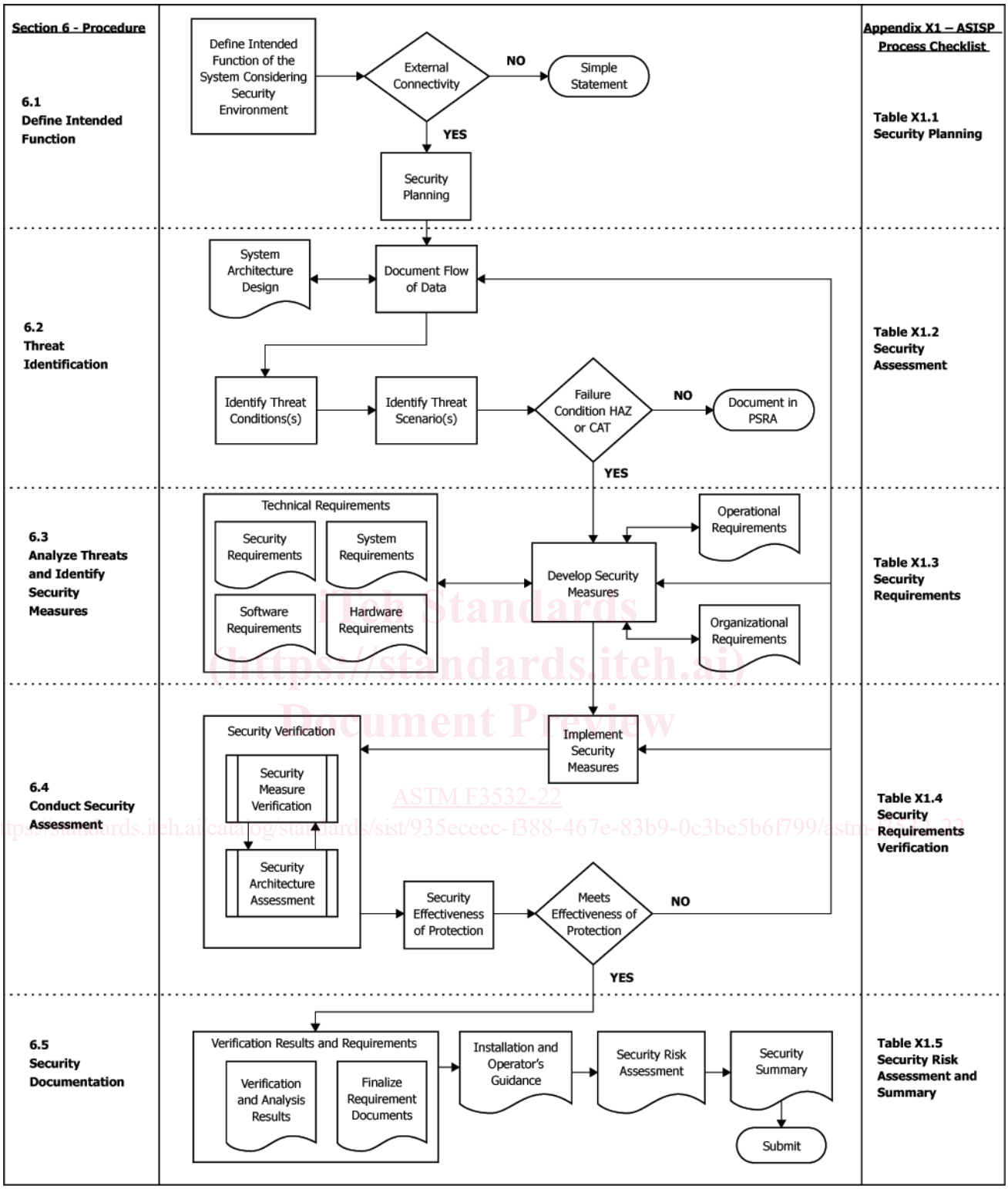


**FIG. 1 Security Process Flow Diagram**

6.1.2 In general, increased connectivity in aeroplane systems functionality can introduce new risks associated with IUEI that typically were not assessed during the traditional safety assessment process. A systematic examination of the aeroplane or system functionality shall be performed. The examination shall define the security environment when ASISP requirements apply. The examination should consider user interactions with aeroplane system functionality.

6.1.2.1 It is recommended that applicants contact their certification authority to understand the applicable regulatory security policies/requirements for their project.

6.1.3 The applicant shall determine if any elements of the system design includes connectivity to an external network or device on the aeroplane.

6.1.4 Identification of external connectivity to a network or device during operation or maintenance shall require identification of the information flow and the means of connectivity across the aeroplane security perimeter. Both physical (wired or wireless) and logical information flows shall be considered. Further, both new and changed information flow into the aeroplane system shall be considered. Changed data flows, whether physical or logical, may alter the existing security measures necessary to mitigate IUEI.

6.1.5 If the assessment shows no external connectivity, then a simple statement of non-applicability in a certification plan or change impact assessment is all that is required.

NOTE 1—A simple statement is one that provides all the information required to conclude that ASISP aspects do not apply. For example, "All information flow is outbound across the aeroplane security perimeter, no information is transmitted (TX) to the aeroplane systems. Therefore ASISP requirements do not apply."

6.1.5.1 System functions dealing with services provided by trusted service entities or air navigation service providers do not require aeroplane specific evaluation as a part of this process. Examples of excluded functions include: Global Navigation Satellite System (GNSS), ground-based navigation aids, Automatic Dependent Surveillance – Broadcast (ADS-B). These services have interoperability requirements defined in other regulations and guidance and are therefore outside the scope of this process.

6.1.6 The presence of information flow inbound across the aeroplane security perimeter shall require the applicant to address IUEI. As an aid to applicants, some examples of external connectivity requiring assessments are provided in 6.1.6.1 – 6.1.6.4. These examples are not exhaustive and are not intended to be used verbatim.

6.1.6.1 Does the system include one or more wireless connectivity methods intended for use by onboard Portable Electronic Devices (PEDs) or external devices? This may include Wi-Fi access points or clients, Bluetooth nodes, cellular nodes or devices with custom-designed radios and communications protocols.

6.1.6.2 Does the system include one or more wired connectivity methods accessible without special tools or access to the aeroplane harness? This may include an Ethernet or USB port for a PED such as a laptop, a USB port, or secure digital (SD) card slot for removable media or other accessible buses.

6.1.6.3 Does the system provide a new or updated means for field-loadable data such as aeronautical databases, software, or other information? These are considered a means of connectivity. For further understanding of the corruption protections to ensure integrity of field-loadable software and databases, refer to AC 20-115D and AC 20-153B.

6.1.6.4 Does the system include the use of any new or changed external services or functions over an existing physical link? This may include new applications or protocol modifications on an existing communications bus.

6.1.7 When it is determined that the project must address IUEI, then security activities and documentation shall be planned to support ASISP requirements.

6.1.8 The final scope of the security planning activities required for the project shall be determined after completing the process covered in 6.2 of this practice.

6.1.8.1 *Planning for Security Certification*—When examination of the system shows that ASISP aspects must be addressed, formally document ASISP aspects in a Project Specific Certification Plan (PSCP) or Plan for Security Aspects of Certification (PSecAC).

6.1.8.2 *Preliminary Security Risk Assessment (PSRA)*—A PSRA shall be completed to document the system information flow (Physical and Logical), and threat conditions related to these flows. If the assessment determines that the identified threat condition(s) result in hazards classified as Major or lower, the assessment may be documented without further activities. Assessments with threat condition(s) that result in hazards classified as Hazardous or Catastrophic shall complete the Security Risk Assessment activities of this practice.

6.1.8.3 *Security Verification*—Provide the planning needed to support the security verification process. Plans and reports that will be used to document the verification activities used to assess security measures shall be listed in the certification planning document, covered in 6.1.8.1 of this practice.

6.1.8.4 *Security Risk Assessment (SRA)*—Provide the planning needed to support the security risk assessment process. Planned SRA activities shall be listed in the certification planning document, covered in 6.1.8.1 of this practice.

6.1.8.5 *Security Continued Airworthiness*—Planning for installer, maintainer, and operator guidance expected to be required to ensure the integrity of the security architecture shall be listed in the certification planning document, covered in 6.1.8.1 of this practice.

6.2 *Threat Identification:*

6.2.1 Once the system architecture under evaluation is initially defined, the applicant shall document the flow of data across the security perimeter between components and systems. The documentation shall identify the physical and logical paths, data sources, and destinations. Existing security measures shall be identified and considered in this architecture evaluation.

6.2.1.1 Data flow diagrams showing both physical and logical flows are a means to document the necessary information. The data flow diagrams can aid in understanding how systems are interconnected, and where data is ultimately consumed in the system. Reference Appendix X3 for information on how to create data flow diagrams.

6.2.2 Physical data paths shall include the type of interconnect (for example, Wi-Fi, Ethernet, RS-232) and the directionality.

6.2.3 Logical data paths shall include producing and consuming applications, and protocols used for the transfer of data. Multiple logical data flow representation may be necessary to describe information flow among different layers of a system.

6.2.4 Threat conditions shall be identified by considering the effect of the impacted functions on the aeroplane, system, and occupants in correlation to the safety failure condition's

severity identified in safety documentation (for example, Functional Hazard Assessment (FHA)). For further understanding of the development of threat conditions, refer to ED-203A/DO-356A, Section 3.3.3.

6.2.5 Following the development of all the threat conditions, at least one (1) threat scenario shall be identified for each threat condition. Threat scenarios include identification of the source of the threat, the attack vector (typically drawn from the physical or logical data flow), and where applicable the existing security measures implemented along the attack vector. The threat scenario also includes the impact of a successful attack; threat condition. For further understanding of the development of threat scenarios, refer to ED-203A/DO-356A, Section 3.4.1.

6.2.6 Using the threat condition severity, decide which elements of the security process are required; either 6.2.6.1 or 6.2.6.2.

6.2.6.1 If the related safety failure conditions for each threat condition has a severity of Major or lower, the outcome of the security assessment shall be documented in a PSRA. Provided that the assumptions in the PSRA are verified to remain applicable throughout the design process, the security activities that follow are not required to be accomplished.

6.2.6.2 If the related safety failure conditions for each threat condition have a severity of Hazardous or Catastrophic, then further security activities shall be conducted to show that the security risks are mitigated to an acceptable level. This is accomplished through completion of the security processes identified in 6.3 and 6.4. This will result in the complete set of security documentation described in 6.5, including the finalization of the SRA.

6.3 *Analyze Threats and Identify Security Measures:*

6.3.1 Using the threat conditions and threat scenarios developed in 6.2, identify security measures that reduce the risk from each threat to an acceptable level. A minimum of one (1) security measure for each threat scenario resulting in unacceptable risk shall be identified; more security measures where layered security architecture is required. Security measures may take the form of existing system functions, existing security measures, additional technical or procedural security measures, system architecture changes, or other modifications to design or operation. When identifying existing security measures or developing new security measures, the applicant shall consider the impact of the failure of the security measure(s) in conjunction with the functionality of the system.

6.3.2 Security measures for which credit will be sought to meet security requirements shall be clearly defined. The following information supports the documentation requirement for each security measure:

6.3.2.1 Each security measure shall be traceable to the aeroplane or system requirement(s) that define the security measure's functionality.

NOTE 2—It is recommended to utilize a unique Security Tag on any requirement with applicability to security measures to aid in tracing of security requirements.

6.3.2.2 Security measures shall have a description that includes its intended function and intended operating environment within the architecture. Such information as functional specifications, interfaces, where the security measure is implemented in the architecture, and where documented (Security, System, Software, Hardware, Organization, Operation) should be part of the security measure description when applicable.

6.3.2.3 When using Appendix X4, Security Risk Assessment Scoring, the type of security measure shall be defined: Technical (Cryptographic, Authentication, and Authorization) and Non-Technical (Operator, Operational, and Organizational). More than one type may be assigned. Reference Appendix X4 for descriptions covering security measure types.

6.3.2.4 The security measure's dependencies on other security measures, architecture features, and operational modes shall be documented.

6.3.2.5 If security measures are implemented in a context using software or hardware design assurance levels, those measures should be developed to an appropriate design assurance level in accordance with the applicable safety assessment. If used, the software or hardware design assurance level for a security measure should be documented.

6.3.3 Once the security measures have been identified, appropriate requirements shall be developed and identified as security requirements and fed into the technical requirements (System, Security, Software, and Hardware where applicable), operation requirements (if applicable), and organization requirements (if applicable). This results in the security measures requirements being subject to the same development requirements and assurance actions as other safety-related mitigation mechanisms.

6.3.4 Subsection 6.4 assesses whether or not each threat scenario has been mitigated to an acceptable level of risk following the implementation of the security measure(s). This is an iterative process, therefore it should be anticipated that further security measure development could be required.

6.4 *Conduct Security Assessment:*

6.4.1 The implementation of the security measures into the security architecture to address each threat scenario shall be accomplished. The intent of the implemented security measures is to protect assets from the identified threat scenarios. With an increase in severity of impact for a threat scenario, there is a need to increase the security effectiveness of protection. The activities in this section provide the requirements related to assess the effectiveness of protection:

6.4.1.1 *Moderate*—Adequate to protect against a Major Threat Condition.

6.4.1.2 *High*—Adequate to protect against a Hazardous Threat Condition.

6.4.1.3 *Very High*—Required to protect against a Catastrophic Threat Condition.

6.4.2 A layered security architecture shall be implemented where "Very High" effectiveness of protection is required. A layered architecture provides the added protection that multiple security measures are not defeated by a single attack, or attack technique. A layered protection architecture consists of multiple security measures that are independent, diverse, and isolated. The security measure attributes are assessed during the security common mode analysis.

6.4.3 Security Measure Common Mode Analysis shall be performed where layered security architecture is required. For

high and moderate protections that have multiple security measures in the security architecture, it is recommended to perform a common mode analysis. This analysis evaluates the following common mode attributes between the security measures mitigating a threat scenario. For further understanding of Security Measure Common Mode Analysis, refer to ED-203A/DO-356A, Section 3.5.1.

6.4.3.1 *Independence* between security measures means that each security measure can function without other security measure inputs or shared assets.

6.4.3.2 *Diversity* between security measures evaluates the commonality of design and implementation; common functionality, technology, and vulnerability to the same attack.

6.4.3.3 *Isolation* between security measures means that compromised or failed security measures do not propagate attacks across shared resources to other security measures.

6.4.4 A verification plan shall be developed that defines how each security measure will be shown to perform its intended function, either by test or by analysis test. Verification tests for security measures shall show functionality under normal range and robustness test conditions.

NOTE 3—Non-security requirements based testing, such as Vulnerability or Penetration "Pen" testing, may also be valuable to identify weaknesses in the security architecture. Details about this type of testing can be found in ED-203A/DO-356A, Section 4.1.3.

6.4.4.1 Intended "normal range" function test cases: normal system inputs and operating environment.

6.4.4.2 Robustness test cases: invalid and out of range test inputs and system failures that might invalidate mitigation assumptions.

6.4.5 Security measures may be verified at the system or aeroplane level, or both, using engineering judgment.

6.4.6 Upon the conclusion of the security architecture verification activity, a final risk assessment shall be performed. This risk assessment demonstrates that the implemented security architecture mitigates risks from attack to an acceptable level. This assessment shall show that the security effectiveness of protection is adequate for each threat scenario and its threat condition(s). There are numerous assessment processes provided in industry guidance/methods listed in Section 2 of this practice. An accepted Part 23 aeroplane method when using this practice is provided in Appendix X4, Security Risk Assessment Scoring. Early agreement on the security risk assessment process with the applicable CAA is encouraged.

6.4.6.1 The selected security risk assessment process shall provide an effectiveness of protection result that can be used to show the protections meet the security requirements provided in Table 1 or Table 2.

**TABLE 1 Required Minimum Effectiveness Levels**

| Threat Condition Severity | Effectiveness of Protection[A] |
|---|---|
| Catastrophic | Very High |
| Hazardous | High |

[A] Effectiveness Levels may be tailored to a reduced protection level. (Reference 6.4.7 and Table 2.)

**TABLE 2 Minimum Effectiveness Level with Tailoring**

| Assessment Level (F3230, Table 3) | Effectiveness of Protection | | |
|---|---|---|---|
| | Major[A] | Hazardous | Catastrophic |
| Level I | Moderate | Moderate | Moderate |
| Level II | Moderate | Moderate | Moderate |
| Level III | Moderate | Moderate | High |
| Level IV | Moderate | High | Very High |

[A] In accordance with Table 1, addressing Major Threat Conditions is not required. Applicants choosing to address such threat conditions in their design should use a measure with a minimum effectiveness of Moderate.

6.4.7 *Tailoring of Security Effectiveness by Aeroplane Level:*

6.4.7.1 Tailoring of security effectiveness may be incorporated with a reduced effectiveness protection level. This reduction by aeroplane assessment level may be allowed by the certification authorities and should be coordinated in advance of security verification activities.

6.4.8 The processes outlined in 6.2, 6.3, and this section are typically an iterative process requiring numerous cycles through the development of the data flows, and the development and implementation of security measures to address each threat scenario. When the risk assessment for each identified threat scenario shows that the effectiveness of protection meets Table 1 or, when applicable Table 2, then final security assessment documentation activities are the next step. When the assessment shows that the security architecture does not meet the effectiveness of protection requirements for the following reasons, return to the appropriate section of this practice to further develop the security architecture:

6.4.8.1 When the security architecture was inadequate to address the threat scenario due to missing system architecture and data flow assessment, return to 6.2 to evaluate the process steps.

6.4.8.2 When the security measures are shown to be inadequate for the effectiveness of protection level required, return to 6.3 for further development of existing or additional security measures.

6.4.8.3 When unable to meet the common mode analysis requirement or effectiveness of protection, return to 6.3 and 6.4 to re-evaluate the security architecture.

6.5 *Security Documentation:*

6.5.1 Evidence shall be provided by the applicant showing that all required activities, based on the project scope identified in the security planning document, have been completed.

6.5.1.1 Actual documentation structure for each of the requirements is not prescriptive for the need of a standalone document. Table 3 provides a list of possible security documentation as well as how security topics might be addressed within already required certification data. The listed data is intended to show how the activities and tasks discussed in this practice may be documented, but the exact packaging of the data is an applicant choice to propose as part of the planning effort.

6.5.2 Final coverage of the security measure verification test results and analysis shall be documented. Document that each security measure implemented in the security architecture functions as intended.

**TABLE 3 Example Security Documentation**

| Security Activity | Example Documentation Package Content | Ref. |
|---|---|---|
| Planning | PSecAC or by means of a dedicated security section within the Project-Specific Certification Plan (PSCP) | 6.1<br>Table X1.1 |
| Statement when Airworthiness Security Aspects are not applicable; No connectivity | PSCP statement | 6.1<br>Table X1.1 |
| Assessment showing Major or lower Hazard classification; No further security activities required | Preliminary Security Risk Assessment (PSRA). PSRA may be included as a section in the PSCP. | 6.2<br>Table X1.2 |
| Assessment showing security activities are required; Hazardous or Catastrophic Threat Conditions | PSRA or draft SRA; inclusion of the assessment results including ties to FHA as needed | 6.2<br>6.3<br>6.5<br>Table X1.2 |
| Documentation of Security Requirements | System Requirements Document (SysRD)<br>Software Requirements Document (SRD)<br>Hardware Requirements Document (HRD) | 6.3<br>6.5<br>Table X1.3 |
| Verification | Test Plan and Procedures<br>Test and Analysis Reports | 6.4<br>6.5<br>Table X1.4 |
| Installer and Operator Guidance | Instructions for Continued Airworthiness (ICA)<br>Maintenance Manuals (MM)<br>Installation Manuals (IM) | 6.5<br>Table X1.5 |
| Security risk assessment | Security Risk Assessment (SRA) | 6.5<br>Table X1.5 |
| Security Summary | Security Summary included in SRA | 6.5<br>Table X1.5 |



6.5.3 Requirement documentation shall be finalized with any changes to the security-related requirements.

6.5.3.1 A list of known vulnerabilities for each security measure should be maintained to help evaluate the effectiveness of security measures.

6.5.3.2 Security measures implemented with commercial off-the-shelf (COTS) software or hardware should consider the event where one or more vulnerabilities are identified publicly, and the subsequent impact of this disclosure on their continued effectiveness.

NOTE 4—Due to the potential for changes outside the control of the system manufacturer or applicant, additional mitigations may be needed for security measures that rely on features within COTS software or hardware.

6.5.4 If the security risk assessment contains operational measures or other actions that are the responsibility of the installer or maintainer, the applicant shall provide appropriate instructions in the installation manual, operators manual, or other documents to ensure correct implementation of these measures.

6.5.4.1 A process shall be provided to secure delivery of field-loadable data from the design approval holder to the operator. The need for the operator to validate the authenticity and integrity of field-loadable data is covered in instructions for maintaining the security posture of the aeroplane.

6.5.5 If the security risk assessment contains operational measures or other actions that are the responsibility of the aeroplane operator, the applicant shall provide operator guidance. The guidance shall address the aspects related to ASISP to ensure system integrity and security for the lifespan of the aeroplane.

6.5.6 The SRA shall be documented to show security architecture effectiveness. The SRA covers the activities performed showing the data flow, threat condition and threat scenario development. An assessment shall be provided in the SRA that the security architecture shows no unacceptable risk in accordance with this practice.

NOTE 5—The operator guidance may be used by the operators for their use in getting approval for network security by their certification authority. (Reference AC 119-1.)

6.5.7 A security summary statement shall be provided, which includes a statement that all requirements within this practice have been met. The summary shall address any deviations from the security planning.

6.5.7.1 The tables in Appendix X1 are a means, but not the only means, to show that all necessary elements of this practice have been met.

6.5.7.2 If the applicant uses the material in Appendix X1, it is recommended to include a reference with each necessary row showing where in the applicant's documentation the supporting data is located. This aids both the applicant and certification authority in ensuring the documentation is complete.

## 7. Post Certification

7.1 System modifications shall be assessed for any changes that could impact the security assessment. The assessment of the proposed modifications shall be based on analysis and follow existing system security change impact analysis guidance. Reference Appendix X2 for one example of a security change impact analysis (CIA). If the CIA shows the proposed

alteration could impact the security risk analysis, the applicant shall assess the updated system design and its impact on the aeroplane using the process described in Section 6.

7.2 The applicant shall develop and provide operators with any instructions necessary to maintain the aeroplanes security architecture over its lifetime. Such information should include support for continued airworthiness of the aeroplane's system security measures. Information can include information security conditions for support for subsequent changes to the aeroplane type design performed by organizations other than the original applicant. Such information could also include directions on retrieval of security logs if deemed necessary by the applicant.

NOTE 6—If the information security conditions identified by an applicant cannot be met by a subsequent applicant, the subsequent applicant may need to contact the original applicant and obtain additional data.

7.3 A process for managing vulnerabilities over the entire course of a system's service life should be developed, including the following elements:

NOTE 7—Applicants can coordinate vulnerability management, with equipment suppliers, to ensure each component of the system has vulnerability feedback mechanisms enabled and vulnerability management processes applied at the appropriate point(s) in the supply chain.

7.3.1 A vulnerability disclosure policy that includes public dissemination of contact information for reporting of issues by third parties.

NOTE 8—The intent of the public aspect of the vulnerability disclosure policy is to help manage expectations with third parties that report potential security issues.

7.3.2 A policy on the reception of security issue reports, such as Common Vulnerabilities and Exposures (CVE) reports, as well as the monitoring for, identification of, and treatment of security vulnerabilities or changes to the security environment impacting the system.

7.3.3 A policy on responding to security incidents, including gathering appropriate data from impacted systems.

NOTE 9—Additional information on vulnerability management, monitoring for security risk, and incident response is available in ETSI EN 303 645, NIST SP 800-37, or other security guidance.

## APPENDIXES

**(Nonmandatory Information)**

### X1. ASISP PROCESS CHECKLIST

X1.1 References in Tables X1.1-X1.5 point to sections in this practice that provide additional guidance and background. Tables include:

X1.1.1 Description and references to the location(s) in this practice that provide(s) guidance to address each checklist item.

X1.1.2 Failure Condition Severity, with applicability of each requirement shown by RQD, OPT, NR, and N/A; defined in the legend.

LEGEND:

| | |
|---|---|
| RQD | Required |
| OPT | Optional |
| NR | Not Required |
| N/A | Not Applicable |
| CAT | Catastrophic – Severity of the Treat Condition/Failure Condition |
| HAZ | Hazardous – Severity of the Treat Condition/Failure Condition |
| MAJ | Major and lower – Severity of the Treat Condition/Failure Condition |

X1.1.3 Table Item Numbers provided.

**TABLE X1.1 Security Planning**

| Checklist Item | | Ref. | Severity | | | Comments |
|---|---|---|---|---|---|---|
| No. | Description | | CAT | HAZ | MAJ | |
| 1 | Security certification planning is defined | 6.1.3<br>6.1.5<br>6.1.6<br>6.1.7 | RQD | | | Plans contain an overview of aeroplane or system-level architecture, or both, to be assessed for security, and the means of compliance to security requirements where connectivity has been identified.<br><br>Planning identifies the means of compliance to security requirements where connectivity has been identified.<br><br>Planning for security aspects may be included in a PSCP or PSecAC. |
| | | 6.1.3<br>6.1.4<br>6.1.5 | N/A | | | Security certification may consist of a simple statement providing evidence that ASISP aspects of certification do not apply.<br><br>This may be included in a PSCP or other certification documentation provided that:<br>• No connectivity is added to the aeroplane or systems<br>• Information flow is only outbound across the aeroplane security perimeter<br>• All information flow inbound across the aeroplane security perimeter is provided by trusted services governed by aviation interoperability standards |
| 2 | Security Environment is defined | 6.1.1<br>6.1.2 | RQD | | | Examine aeroplane and system functionality to define the security environment. |
| 3 | Certification considerations are defined | 6.1.2<br>6.1.4<br>6.1.6 | RQD | RQD | OPT | Identify the applicable regulatory security requirements based on aeroplane level. |
| 4 | Overview of aeroplane and systems where ASISP is required | 6.1.2<br>6.1.3<br>6.1.4<br>6.1.5 | RQD | RQD | OPT | Provide a description of the aeroplane and system(s) where connectivity requires ASISP to be addressed. |
| 5 | Planning for PSRA activity is provided | 6.1.8 | RQD | | | Identify the activities to determine and assess the severity of the threat conditions related to security vulnerabilities. |
| 6 | Planning for security verification activity is provided | 6.1.8 | RQD | RQD | OPT | Identify the planned verification activities, including test and analysis, and the means to document them. |
| 7 | Planning for SRA is provided | 6.1.8 | RQD | RQD | OPT | Identify the planned Security Risk Assessment activities, and the means to document them. |
| 8 | Planning for security-related continued airworthiness is provided | 6.1.8 | RQD | RQD | OPT | Identify the planned method for developing Instructions for Continued airworthiness and the means to document them. |

**TABLE X1.2 Security Assessment**

| Checklist Item | | Ref. | Severity | | | Comments |
|---|---|---|---|---|---|---|
| No. | Description | | CAT | HAZ | MAJ | |
| 1 | Flow of data identified | 6.2.1<br>6.2.2<br>6.2.3 | RQD | | | Ensure the flow of data is correct with respect to the aeroplane, systems, and security architecture. Existing security measures in the architecture are identified.<br><br>Documentation identifies the physical and logical paths, data sources, and destinations. Ensures flow of data developed during the preliminary risk assessment is complete and correct with respect to system architecture. |
| 2 | Threat Condition(s) developed | 6.2.4 | RQD | | | Ensure the threat conditions are developed from the safety FHA. |
| 3 | Threat Scenario(s) developed for each threat condition | 6.2.5 | RQD | RQD | OPT | Ensure that each threat condition has at least one (1) threat scenario. |
| 4 | Preliminary security risk assessment complete | 6.2.6 | OPT | OPT | RQD | If the worst-case threat condition is Major or lower, then ASISP requirements are complete with the PSRA.<br>or<br>If the threat conditions are Hazardous or Catastrophic, then further security activities are required. |

**TABLE X1.3 Security Requirements**

| Checklist Item | | Ref. | Severity | | | Comments |
|---|---|---|---|---|---|---|
| No. | Description | | CAT | HAZ | MAJ | |
| 1 | Security measures are identified | 6.3.1 | RQD | RQD | OPT | A minimum of one (1) Security Measure for each Threat Scenario.<br><br>Note: Threat Condition, Effectiveness of Protection, Defense in Depth (layered protection), and Common Mode Analysis during verification activities may show that the minimum is not acceptable to meet security requirements (6.4). |
| 2 | Security measures are defined | 6.3.2 | RQD | RQD | OPT | Each Security Measure documented with the following information:<br>• Security Measure Name or Number<br>• Security Measure Description<br>• Security Measure Type, *If using Appendix X4<br>• Security Measure Capabilities/Effect<br>• Security Measure Dependencies<br>• Traceability to requirements |
| 3 | Security requirements are defined | 6.3.3 | RQD | RQD | OPT | Security Measures documented in the applicable requirements documentation. Such as:<br>• Security Requirements<br>• System Requirements<br>• Software Requirements<br>• Hardware Requirements<br>• Operational Requirements<br>• Organizational Requirements |