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.