



AEROSPACE INFORMATION REPORT

AIR7368™

Issued

2023-09

Cybersecurity for Propulsion Systems

RATIONALE

As cybersecurity for propulsion systems emerges as a new and separate subject for regulatory agencies, guidance for the propulsion system manufacturer in addressing cybersecurity issues related to aircraft integration, field loading of data, continued airworthiness, and other areas is needed. This SAE Aerospace Information Report (AIR) will serve as a foundation for a common approach to cybersecurity airworthiness certification for propulsion system manufacturers.

FOREWORD

This SAE Aerospace Information Report (AIR) was developed as a joint effort by industry and regulatory members of the E-36 Cybersecurity subcommittee. It represents a starting point for guidance, and as such does not contain requirements for regulatory compliance. All of the guidance herein consists of examples and the use of recommendations ("should"). It is the responsibility of the applicant, working with airworthiness authorities, to determine the program-specific requirements for propulsion system certification.

TABLE OF CONTENTS

1.	SCOPE	4
1.1	Purpose	4
1.2	Use of Prescriptive Language	4
2.	REFERENCES	4
2.1	Applicable Documents	4
2.1.1	SAE Publications	4
2.1.2	Airlines for America (A4A) Publications	4
2.1.3	ARINC IA Publications	4
2.1.4	ASTM Publications	5
2.1.5	EASA Publications	5
2.1.6	EUROCAE Publications	6
2.1.7	EUROCAE/RTCA Publications	6
2.1.8	EUROCONTROL Publications	6
2.1.9	European Union Publications	6
2.1.10	FAA Publications	6
2.1.11	IEEE Publications	7
2.1.12	ISO/IEC Publications	7
2.1.13	NIST Publications	8
2.1.14	TIA Publications	8
2.1.15	Other Publications	8
2.2	Definitions	8
2.3	Acronyms and Symbols	9

SAE Executive Standards Committee Rules provide that: "This report is published by SAE to advance the state of technical and engineering sciences. The use of this report is entirely voluntary, and its applicability and suitability for any particular use, including any patent infringement arising therefrom, is the sole responsibility of the user."

SAE reviews each technical report at least every five years at which time it may be revised, reaffirmed, stabilized, or cancelled. SAE invites your written comments and suggestions.

Copyright © 2023 SAE International

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without the prior written permission of SAE.

TO PLACE A DOCUMENT ORDER: Tel: 877-606-7323 (inside USA and Canada)
Tel: +1 724-776-4970 (outside USA)
Fax: 724-776-0790
Email: CustomerService@sae.org
http://www.sae.org

SAE WEB ADDRESS:

Full document details: SAE AIR7368

For more information on this standard, visit
<https://www.sae.org/standards/content/AIR7368/>

Documents
Document Sharing Hub

3.	APPLICABILITY	13
4.	HISTORICAL BACKGROUND	15
5.	AIRWORTHINESS SECURITY PROCESS OVERVIEW	16
5.1	Aviation Security Environment	16
5.1.1	Aviation Information Domains	16
5.1.2	Electronic Connectivity Trends	18
5.1.3	Electronic Connectivity Risks	19
5.2	Airworthiness Security Process	20
5.2.1	Product Information Security Risk Assessment (PISRA)	22
5.2.2	Validation and Verification of the Security Protection	23
5.2.3	Instructions for Continued Product and Part Information Security Protection	24
5.2.4	Change Impact Analysis (CIA)	24
5.3	Cybersecurity Environment and Objectives for Propulsion Systems	24
5.3.1	Security Assurance Levels	26
5.3.2	Security Methods	27
5.3.3	Coordination of Design Approval Holders (DAHs)	27
5.4	Identification of Cybersecurity Assets in Propulsion Systems	28
5.5	Attack Paths for Propulsion Systems	30
5.6	Identification of Threats	30
5.7	Assessment of Safety Consequences of Threats (Impact)	31
5.8	Evaluate Likelihood of Safety-Related Cybersecurity Attacks	31
5.8.1	Aircraft Safety Measures and Operational Barriers	35
5.9	Assessment of Acceptability—Impact and Likelihood	35
5.10	Mitigation for Gaps	36
5.11	Evaluation of Mitigation Effectiveness	37
5.11.1	Verification	37
5.11.2	Penetration Testing	37
6.	MEANS TO MAINTAIN PROPULSION CYBERSECURITY	39
6.1	Instructions for Continued Airworthiness (ICA)	39
6.2	Security Incident Reporting and Management	39
6.3	Handling of Electronic Control Components	41
6.4	Control System Network Access Points	41
6.5	Ground Support Equipment	41
6.6	Information Security in Operations and Maintenance	42
6.6.1	DAH Support for Operator Aircraft Network Security Program	42
6.6.2	DAH Support for the Operator Organization Risk Assessment	42
6.6.3	DAH Input for Operator Personnel Training	43
6.6.4	Software Management During Maintenance Activities	43
7.	FIELD LOADING OF SOFTWARE AND FIRMWARE	43
7.1	Process Elements for Field Loading of Software	43
7.2	Data Integrity Verification	45
7.2.1	System Configurability	47
7.2.2	Wired or Wireless Communication Interfaces	47
7.2.3	Interfaces to Removable Media and Electronic Devices	48
7.3	Protections for Software Data Loading for Legacy Systems	48
7.4	Test Interfaces and Adjustment/Trim Capability	49
7.5	Ground Support Information Systems (GSIS)	49
7.6	Operational Considerations for Software	50
8.	SUMMARY	50
9.	NOTES	50
9.1	Revision Indicator	50

APPENDIX A	AVIATION ECOSYSTEM CYBERSECURITY INCIDENTS	51
APPENDIX B	THREAT LIKELIHOOD ASSESSMENT	52
APPENDIX C	PROPULSION RELATED AIRCRAFT SAFETY EFFECTS	55
Figure 1	Aircraft connectivity example	14
Figure 2	Engine control and monitoring system	14
Figure 3	Simple security architecture example	28
Figure 4	Security architecture example with distributed control.....	29
Figure 5	Example of attack path map	32
Figure 6	Example of security architecture diagram with attack path indication	32
Figure 7	Example of attack tree	34
Table 1	Information security guidance matrix	21
Table 2	PISRA activity application for propulsion systems	23
Table 3	Security assurance levels	26
Table 4	Simple security architecture labeling	28
Table 5	Simple security architecture labeling	29
Table 6	Example of likelihood combination calculation	34
Table 7	Risk acceptability threshold	35

1. SCOPE

1.1 Purpose

The purpose of this SAE Aerospace Information Report (AIR) is to provide guidance for aircraft engine and propeller systems (hereafter referred to as propulsion systems) certification for cybersecurity. Compliance for cybersecurity requires that the engine control, propeller control, monitoring system, and all auxiliary equipment systems and networks associated with the propulsion system (such as nacelle systems, overspeed governors, and thrust reversers) be protected from intentional unauthorized electronic interactions (IUEI) that may result in an adverse effect on the safety of the propulsion system or the airplane. This involves identification of security risks, their mitigation, verification of protections, and their maintenance in service.

This document is intended to serve as suitable guidance for propulsion system manufacturers and applicants for propulsion system type certification. It is also intended to provide guidance for subsequent propulsion system integration into aircraft systems for aircraft certification and operational use.

1.2 Use of Prescriptive Language

This document is a technical report, and as such does not make use of the term “shall” to identify requirements (apart from the referencing of other SAE documents). The term “should” is used as an expectation of certain outcomes, which may then be given greater weight (selectively or as a whole) by agencies making use of this document as guidance.

2. REFERENCES

2.1 Applicable Documents

The following publications form a part of this document to extent specified herein. The latest issue of SAE publications shall apply. In the event of conflict between the text of this document and references cited herein, the text of this document takes precedence. Nothing in this document, however, supersedes applicable laws and regulations unless a specific exemption has been obtained.

2.1.1 SAE Publications

Available from SAE International, 400 Commonwealth Drive, Warrendale, PA 15096-0001, Tel: 877-606-7323 (inside USA and Canada) or +1 724-776-4970 (outside USA), www.sae.org.

ARP5150A Safety Assessment of Transport Airplanes in Commercial Service

2.1.2 Airlines for America (A4A) Publications

Available from Airlines for America (A4A), 1301 Pennsylvania Avenue, NW, Suite 1100, Washington, DC 20004, Tel: 202-626-4000, www.airlines.org.

ATA Spec 42 Aviation Industry Standards for Digital Information Security

2.1.3 ARINC IA Publications

Available from SAE ITC, ARINC Industry Activities, 16701 Melford Blvd, Suite 120, Bowie, MD 20715, Tel: +1 240-334-2578, <https://www.aviation-ia.com/>.

ARINC 429 Digital Information Transfer System (DITS)

ARINC 615 Airborne Computer High Speed Data Loader using ARINC 429 protocol

ARINC 615A Software Data Loader Using Ethernet Interfaces

ARINC 629 Multi-Transmitter Data Bus

ARINC 645-1 Common Terminology and Functions for Software Distribution and Loading



ARINC 664P5	Aircraft Data Network Part 5, NetworkDomain Characteristics and Interconnection
ARINC 665	Loadable Software Standards
ARINC 667-2	Guidance for the Management of Field Loadable Software.
ARINC 763	Network Server System
ARINC 811	Commercial Aircraft Information Security Concepts of Operation and Process Framework
ARINC 822A	On-Ground Aircraft Wireless Communication
ARINC 823P1	Datalink Security Part 1 - ACARS Message Security
ARINC 823P2	Datalink Security Part 2 - Key Management
ARINC 825	General Standardization of CAN (Controller Area Network) Bus Protocol for Airborne Use
ARINC 826	Software Data Loading Using CAN Interface
ARINC 827	Electronic Distribution of Software by Crate (EDS Crate)
ARINC 835	Guidance for Security of Field Loadable Software Parts Using Digital Signatures
ARINC 842	Guidance for Usage of Digital Certificates
ARINC 849	Data Loading Specifications for Aircraft Components
ARINC 852	Guidance For Security Event Logging in an IP Environment

2.1.4 ASTM Publications

Available from ASTM International, 100 Barr Harbor Drive, P.O. Box C700, West Conshohocken, PA 19428-2959, Tel: 610-832-9585, www.astm.org.

ASTM F3532-22	Standard Practice for Protection of Aircraft Systems from Intentional Unauthorized Electronic Interactions
---------------	--

2.1.5 EASA Publications

Available from European Union Aviation Safety Agency, Konrad-Adenauer-Ufer 3, D-50668 Cologne, Germany, Tel: +49 221 8999 000, www.easa.europa.eu.

AMC 20-42	Airworthiness Information Security Risk Assessment
AMC 20-25A	Airworthiness Consideration for Electronic Flight Bags (EFBs)
CS-E	Engines
CS-P	Propellers
Decision 2020/006/R	Aircraft Cybersecurity
NPA 2019-01	Aircraft Cybersecurity
Opinion 03/2021	Management of Information Security Risks

2.1.6 EUROCAE Publications

Available from EUROCAE Secretariat, 9-23 Rue Paul Lafargue, 93200 Saint-Denis, France, Tel: +33 1 40 92 79 30, <https://www.eurocae.net/>.

ED-246 Process Specification for Wireless On-Board Avionics Networks

2.1.7 EUROCAE/RTCA Publications

Available from RTCA, Inc., 1150 18th Street, NW, Suite 910, Washington, DC 20036, Tel: 202-833-9339, www.rtca.org.

ED-12B/DO-178B Software Considerations in Airborne Systems and Equipment Certification

ED-12C/DO-178C Software Considerations in Airborne Systems and Equipment Certification

ED-202A/DO-326A Airworthiness Security Process Specifications

ED-203A/DO-356A Airworthiness Security Methods and Considerations

ED-204A/DO-355A Information Security Guidance for Continuing Airworthiness

ED-206/DO-392 Guidance on Information Security Event Management

ED-260/DO-378 Minimum Aviation System Performance Standard (MASPS) for Coexistence of Wireless Avionics Intra-Communication Systems within 4200-4400 MHz

2.1.8 EUROCONTROL Publications

Available from EUROCONTROL, <https://www.eurocontrol.int/>.

Think Paper #3 Cybersecurity in Aviation

2.1.9 European Union Publications

Available from the European Commission, https://ec.europa.eu/info/index_en.

EU 748/2012 Initial Airworthiness

EU 2023/203 Requirements for the management of information security risks with a potential impact on aviation safety for organisations and competent authorities

EU 2022/1645 Commission Delegated Regulation (EU) 2022/1645 of 14 July 2022 laying down rules for the application of Regulation (EU) 2018/1139 of the European Parliament and of the Council, as regards requirements for the management of information security risks with a potential impact on aviation safety for organisations covered by Commission Regulations (EU) No 748/2012 and (EU) No 139/2014 and amending Commission Regulations (EU) No 748/2012 and (EU) No 139/2014

2.1.10 FAA Publications

Available from Federal Aviation Administration, 800 Independence Avenue, SW, Washington, DC 20591, Tel: 866-835-5322, www.faa.gov.

14 CFR Part 21 Certification Procedures for Products and Articles

14 CFR Part 25 Airworthiness Standards: Transport Category Airplanes

14 CFR Part 33 Aircraft Engines

14 CFR Part 35 Airworthiness Standards: Propellers

14 CFR Part 43	Maintenance, Preventative Maintenance, Rebuilding, and Alteration
14 CFR Part 121	Operating Requirements: Domestic, Flag, and Supplemental Operations
14 CFR Part 125	Certification and Operations: Airplanes Having a Seating Capacity of 20 or More Passengers or a Maximum Payload Capacity of 6,000 Pounds or More; and Rules Governing Persons on Board Such Aircraft
14 CFR Part 135	Operating Requirements: Commuter and On Demand Operations and Rules Governing Persons on Board Such Aircraft
80 FR 5880	Federal Register Volume 80, Issue 22
AC 00-66	Research Report DOT/FAA/TC-14/49 - Selection of Cyclic Redundancy Code and Checksum Algorithms to ensure critical data integrity
AC 00-72	Best Practices for Airborne Electronic Hardware Design Assurance Using EUROCAE ED-80() and RTCA DO-254()
AC 20-115D	Airborne Software Development Assurance Using EUROCAE ED-12() and RTCA DO-178()
AC 20-152A	Development Assurance for Airborne Electronic Hardware
AC 20-156	Data Bus Assurance
AC 20-173A	Installation of Electronic Flight Bag Components
AC 43-216	Software Management During Aircraft Maintenance
AC 119-1	Software Operational Authorization of Aircraft Network Security Program (ANSP)
PS-AIR-21.16-02 Rev2	Establishment of Special Conditions for Aircraft Systems Information Security Protection

2.1.11 IEEE Publications

Available from IEEE Operations Center, 445 and 501 Hoes Lane, Piscataway, NJ 08854-4141, Tel: 732-981-0060, www.ieee.org.

IEEE 802.3	Standard for Ethernet
IEEE 802.11	Wireless Local Area Networks
IEEE 1149.1	Standard for Test Access Port and Boundary-Scan Architecture

2.1.12 ISO/IEC Publications

Copies of these documents are available online at <https://webstore.ansi.org/>. Copies are also available from IEC Central Office, 3, rue de Varembe, P.O. Box 131, CH-1211 Geneva 20, Switzerland, Tel: +41 22 919 02 11, www.iec.ch.

ISO/IEC 27035-1:2016 Part 1: Principles of incident management

ISO/IEC 27035-2:2016 Part 2: Guidelines to plan and prepare for incident response

ISO/IEC 27037:2012 Guidelines for identification, collection, acquisition, and preservation of digital evidence

2.1.13 NIST Publications

Available from NIST, 100 Bureau Drive, Stop 1070, Gaithersburg, MD 20899-1070, Tel: 301-975-6478, www.nist.gov.

FIPS 140-3	Security Requirements for Cryptographic Modules
SP 800-61	Computer Security Incident Handling Guide
SP 800-86	Guide to Integrating Forensic Techniques into Incident Response
SP 800-131A	Transitioning the Use of Cryptographic Algorithms and Key Lengths

2.1.14 TIA Publications

Available from Telecommunications Industry Association, 1310 North Courthouse Road, Suite 890, Arlington, VA 22201, Tel: +1 703-907-7700, <https://tiaonline.org/>.

TIA/EIA-232-F	Interface Between Data Terminal Equipment and Data Circuit-Terminating Equipment Employing Serial Binary Data Interchange
TIA/EIA-422-B	Electrical Characteristics of Balanced Voltage Differential Interface Circuits

2.1.15 Other Publications

Wynsma, H. and Sullivan, S. (2021). *Civil aviation cybersecurity subcommittee cybersecurity testing recommendations*. Aerospace Industries Association. Available at <https://www.aia-aerospace.org/publications/aia-civil-aviation-cyber-security-subcommittee-testing-white-paper-2021/>.

ASISP. (2016). *Recommendations regarding ASISP rulemaking, policy, and guidance on best practices for airplanes and rotorcraft including both certification and continued airworthiness*. Aviation Rulemaking Advisory Committee (ARAC) Aircraft System Information Security/Protection (ASISP) Working Group to the Federal Aviation Administration. Available at https://www.faa.gov/regulations_policies/rulemaking/committees/documents/media/ARACasisp-T1-20150203R.pdf.

Killcrece, G., Kossakowski, K.-P., Ruefle, R., and Zajicek, M. (2003). *Organizational models for computer security incident response teams (CSIRTs)* (Report no. CMU/SEI-2003-HB-001). Pittsburgh, PA: Carnegie Mellon University, Software Engineering Institute. <https://doi.org/10.1184/R1/6575921.v1>.

MITRE. (2021). *CAPEC list version 3.9*. Available at <https://capec.mitre.org/data/>.

Verizon. (2009). 2009 data breach investigations report (DBIR). Verizon. Available at <https://www.fbiic.gov/public/2009/april/VBA60069WPDBIR8x1109pdfv1singleR.pdf>.

Verizon. (2019). 2019 data breach investigations report (DBIR). Verizon. Available at <https://www.verizon.com/business/resources/reports/2019-data-breach-investigations-report.pdf>.

2.2 Definitions

AIRCRAFT DATA LOADER (ADL): A device installed into an aircraft that is capable of connecting to aircraft line replaceable units (LRUs) and performing data transfers, such as downloading data recorded by the LRU during flight or uploading replacement field-loadable software.

CRATE: A set of field-loadable software that may be digitally signed or unsigned, and formatted into a standardized software package.

DESIGN APPROVAL HOLDER (DAH): The organization that applies for and receives a type certificate, such as an aircraft manufacturer or an engine manufacturer. For the purposes of this publication, the DAH will be the manufacturer of the propulsion system unless otherwise noted.

DIGITAL CERTIFICATE: A set of digital credentials that link the holder of the certificate to a specific public/private key pair, issued by a trusted third party known as a certificate authority (CA). Also known as a public key certificate, a digital certificate commonly includes additional metadata such as a validity date range, information about the issuing CA, and a serial number.

DIGITAL SIGNATURE: In its most basic form, a digital signature is a hash of digital file or set of files that has been encrypted by the private key of the signer. In public key infrastructure (PKI), this is usually accomplished with the use of a digital certificate and includes information tracing the private key back to its root key.

GLOBAL NAVIGATION SATELLITE SYSTEM (GNSS): A navigation system that uses satellites to provide autonomous geo-spatial positioning transmitted to relatively small receivers. One such specific system in the global positioning system (GPS).

INTENTIONAL UNAUTHORIZED ELECTRONIC INTERACTION (IUEI): This term is defined in ED-203A/DO-356A as “[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. This includes the consequences of malware and forged data and the effects of external systems but does not include physical attacks or electromagnetic disturbance.”

NEGATIVE REQUIREMENT: Generally accepted as a requirement that states what a system or product should not do (rather than what it should do). Cybersecurity requirements that require a system or product to be free of susceptibilities to certain attacks or free of malicious code are often considered negative requirements. Negative requirements can be difficult to test because of the amount of testing that may be necessary to prove the absence of something.

PORTABLE DATA LOADER (PDL): A self-contained, portable device capable of connecting to an aircraft LRU and performing data transfers, such as downloading data recorded by the LRU during flight or uploading replacement field-loadable software.

PROPULSION CONTROL SYSTEM: The control system for an aircraft engine or propeller. May include health monitoring and other functions.

PROPULSION SYSTEM: An aircraft engine or propeller.

REFUTATION: The act of disproving an assumption or premise. Refutation testing is a broad category of verification activities that includes penetration testing and other activities designed to “break” or disprove the security of a system.

TYPE CERTIFICATE: A statement issued by an airworthiness authority indicating that a system is certified to operate in regulated air space.

2.3 Acronyms and Symbols

AC	Advisory Circular
ACARS	Aircraft Communications Addressing and Reporting System
ACD	Aircraft Control Domain
ADL	Aircraft Data Loader
ADS-B	Automatic Dependent Surveillance-Broadcast
AID	Avionics Interface Device
AIR	Aerospace Information Report
AISD	Airline Information Services Domain
AISP	Aircraft Information Security Program
AMC	Acceptable Means of Compliance

AMM	Aircraft Maintenance Manual
ANSP	Aircraft Network Security Program
APIS	Aircraft Positioning and Information System
ARAC	Aviation Rulemaking Advisory Committee
ARP	Aerospace Recommended Practice
ASISP	Aircraft Systems Information Security Protection
ASOG	Aircraft Security Operator Guidance
ASRA	Aircraft Security Risk Assessment
ASTM	American Society for Testing and Materials
ASSD	Aircraft Security Scope Definition Document
ATA	Air Transport Association
CA	Certificate Authority
CAN	Controller Area Network
CEOD	Continuous Engine Operating Data
CFR	Code of Federal Regulations
CMM	Component Maintenance Manual
CMU	Carnegie Mellon University
COTS	Commercial Off-The-Shelf
CRC	Cyclic Redundancy Code
CRP	Code Readout Protection
CS	Certification Specification
CVE	Common Vulnerabilities and Exposures
CVSS®	Common Vulnerability Scoring System®
DAH	Design Approval Holder
DAL	Design Assurance Level
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DTLS	Datagram Transport Layer Security
EASA	European Union Aviation Safety Agency
ECS	Engine Control System

ECTM	Engine Condition Trend Monitoring
EEC	Electronic Engine Control
EFB	Electronic Flight Bag
FAA	Federal Aviation Administration
FADEC	Full Authority Digital Engine Control
FLS	Field-Loadable Software
FMD	Failures, Malfunctions, and Defects
GNSS	Global Navigation Satellite System
GPS	Global Positioning System
GSE	Ground Support Equipment
GSIS	Ground Support Information Systems
HD	Hamming Distance
HUMS	Health and Usage Monitoring System
IAHM	Integrated Aircraft Health Management
ICA	Instructions for Continued Airworthiness
ICD	Interface Control Document
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IFE	In-Flight Entertainment
INS	Inertial Navigation System
ISO	International Organization for Standardization
IUEI	Intentional Unauthorized Electronic Interaction
JTAG	Joint Test Action Group
LOPC	Loss of Power Control
LOTC	Loss of Thrust Control
LRU	Line Replaceable Unit
LSAP	Loadable Software Airplane Part
MEL	Minimum Equipment List
MCU	Microcontroller Unit
NIST	National Institute of Standards and Technology

NPA	Notice of Proposed Amendment
OS	Operating System
PASRA	Preliminary Aircraft Security Risk Assessment
PDL	Portable Data Loader
PED	Portable Electronic Device
PIES	Passenger Information and Entertainment Services
PIESD	Passenger Information and Entertainment Services Domain
PISRA	Product Information Security Risk Assessment
PKI	Public Key Infrastructure
PMAT	Portable Maintenance Access Terminal
PMD	Portable Maintenance Device
POD	Passenger-Owned Device
PODD	Passenger-Owned Devices Domain
PSecAC	Plan for Security Aspects of Certification
PS	Policy Statement
PSK	Pre-Shared Key
PSSRA	Preliminary System Security Risk Assessment
Pud	Probability of undetected error
RA	Resolution Advisory
RTCA	Radio Technical Commission for Aeronautics
SAL	Security Assurance Level
SATCOM	Satellite Communications
SEI	Software Engineering Institute
SHA	Secure Hash Algorithm
SP	Special Publication
SPI	Serial Peripheral Interface
SSIG	System Security Integrator Guidance
SSRA	System Security Risk Assessment
SSSD	System Security Scope Definition Document
STAMP	Systems-Theoretic Accident Model and Processes

STPA	System-Theoretic Process Analysis
SWD	Serial Wire Debug
TCDS	Type Certificate Data Sheet
TIA	Telecommunications Industry Association
UART	Universal Asynchronous Receiver-Transmitter
UMD	Universal Maintenance Device
USB	Universal Serial Bus
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
WAIC	Wireless Avionics Intra-Communications Systems
WAN	Wide Area Network
WAP	Wireless Application Protocol
WDL	Wireless Datalink
WG	Working Group
WOBAN	Wireless On-Board Avionics Network
WPA	Wi-Fi Protected Access

3. APPLICABILITY

A typical modern aircraft has multiple systems interconnected by data communication networks as shown in [Figure 1](#). The figure is a high-level depiction of data communications in an aircraft, not an exhaustive or universal configuration description. The propulsion control systems are typically connected directly or indirectly to some of the aircraft systems and operator interfaces. In some systems, the propulsion control can communicate externally using wireless datalinks. This document applies to security protection of propulsion control systems that may be susceptible to IUEI when connected to any of the following:

- Aircraft systems (e.g., air data computers, flight and thrust management computers, engine interface units).
- Equipment for field and factory loading of production software.
- Equipment for making adjustments to adjustable parameters in the embedded software.
- Equipment to download from or upload data to the propulsion control system using wired or wireless communication protocols.
- Any other systems with digital or network connectivity capability.

If the airplane includes secure networks with propulsion system participation, the requirements for secure participation in the aircraft network are documented (e.g., inter-operability specification or ICD). If an engine is certified prior to identification of an aircraft application, the engine manufacturer can identify the assumed aircraft interfaces in the installation manual. The linkages of a typical propulsion control and monitoring system to the aircraft and the airline systems are shown conceptually in [Figure 2](#).

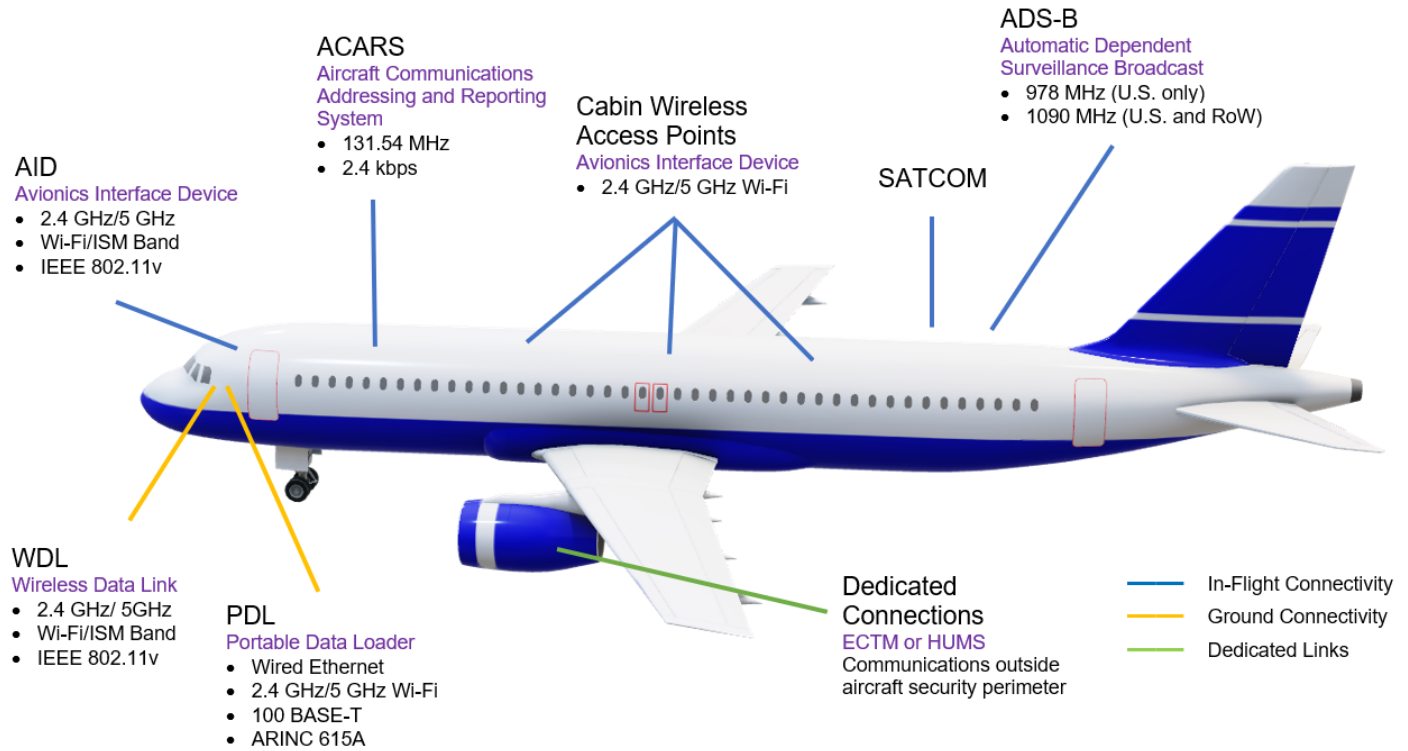


Figure 1 - Aircraft connectivity example

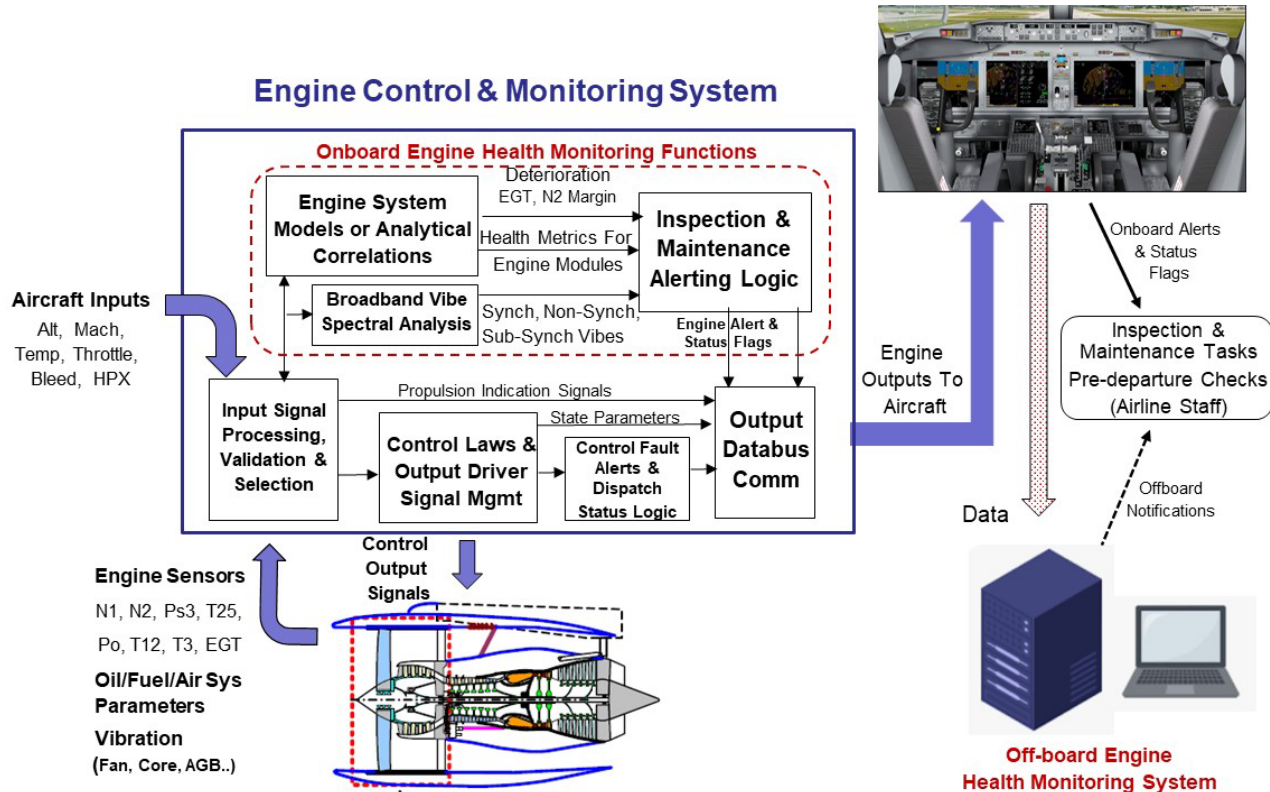


Figure 2 - Engine control and monitoring system

4. HISTORICAL BACKGROUND

The FAA has addressed electronic cybersecurity threats to aircraft systems and networks since 2005. This has been accomplished with special conditions and companion issue papers for specific aircraft models to require aircraft electronic systems security protection from:

- Public networks: Internet connections to aircraft systems are examples of potential vulnerability of intentional unauthorized external interaction from public networks which include:
 - Airline networks (airline operations centers)
 - Airport networks (e.g., GATELINK)
- Data loaders (e.g., field-loadable software (FLS) and databases)
- Wireless aircraft sensors and networks
- Ground support equipment
- Universal serial bus (USB) devices
- Electronic flight bags (EFBs)
- Cellular networks
- Electronic commercial off-the-shelf (COTS) parts (integrated circuits, data networks, data busses, and operating systems (OSs))
- Aircraft system domains (as described in ARINC 667 and ARINC 811)

FAA cybersecurity special conditions were issued for the Boeing 787-8 in 2007, Boeing 777 and Airbus A350-900 in 2013, and the Boeing 737 Max in 2014. As of mid-2021, the FAA has issued 52 electronic system security special conditions affecting 28 different aircraft type certifications.

There have been multiple cybersecurity incidents in the aviation ecosystem, impacting various aspects of aviation such as aircraft navigation and communication, airport management, ticketing and reservations, and other commercial IT systems. Some of these incidents were investigated and determined to be unfounded claims, but even these have served to raise awareness and highlight the need for a consistent approach to cybersecurity.

A non-exhaustive list of such events is included in [Appendix A](#). This list underscores the importance of cybersecurity protection in aircraft including propulsion systems, and their associated information systems for operations, maintenance, and IT infrastructure.

In August 2016, an Aviation Rulemaking Advisory Committee (ARAC) Working Group (WG), tasked under 80 FR 5880, made a number of recommendations concerning aircraft systems information security protection (refer to ASISP, 2016), including:

- Update 14 CFR 33.28 to establish information security protection for engines and 14 CFR 35.23 for propellers.
- Field-loadable software for propulsion control systems that is directly loadable using ground support equipment should contain authentication mechanisms for off-aircraft handling.

In 2019, EASA proposed a new rule regarding cybersecurity (NPA 2019-01), including certification specification CS-25 for transport category airplanes, and certification specifications CS-E (engines) and CS-P (propellers). The EASA rule is based on widely accepted industry practice to address aircraft systems information security and protections for transport category airplanes.

In 2020, EASA published Decision 2020/006/R, which amended the aforementioned specifications. FAA is pursuing similar rulemaking, with expected completion in 2023 and corresponding special conditions being levied in the interim. The certification authorities have delivered a number of issue papers to propulsion system manufacturers, highlighting the need for specific regulatory guidance for propulsion control systems. A number of special conditions have also been issued to airframers for cybersecurity based on the PS-AIR-21.16-02 policy.

In 2019, EASA also proposed the “horizontal rule” in AMC 20-42, and subsequently issued Opinion 03/2021. This led to the issuance of two regulations, Implementing Regulation (EU) 2023/203 and Delegated Regulation (EU) 2022/1645. This is referred to as Part IS, which would affect the aviation ecosystem (including propulsion system manufacturers) by establishing requirements for support operations. While there is no parallel action for this at the FAA and it does not have a direct impact on initial certification, it is nonetheless an important regulatory development with respect to cybersecurity.

5. AIRWORTHINESS SECURITY PROCESS OVERVIEW

5.1 Aviation Security Environment

This section describes the key aspects of the aviation ecosystem to provide context for the application of airworthiness security process to propulsion systems.

5.1.1 Aviation Information Domains

The aircraft industry has the following notional domains in the context of information security, which are defined in documents such as ARINC 811 and ARINC 664 Part 5. The interaction between a propulsion control system and the other systems will vary with the architecture of the airplane. While the domains listed herein are not exclusive or all-encompassing, they represent a widespread concept that can provide guidance for a system architecture.

a. Aircraft Control Domain (ACD)

The ACD consists of airborne systems and networks, the primary functions of which are to support safe operation of the airplane, network routing, connectivity, and a safety perimeter between the ACD and other domains and networks. Examples of systems in the ACD include:

- Cockpit displays.
- Flight controls.
- Environmental controls.
- Electrical system.
- Propulsion systems.
- Cabin management services.
- Flight recorder system.

The ACD can be divided into two sub-domains. These include the flight and embedded control system sub-domain and the cabin core sub-domain. The flight and embedded control system sub-domain is where the aircraft is controlled from the flight-deck. The propulsion system’s safety-critical functions should also exist in this sub-domain. The cabin core sub-domain provides environmental functions dedicated to cabin operations, such as environmental control, passenger address, smoke detection, etc.

b. Airline Information Services Domain (AISD)

This domain enables operation of the airline. Examples of airline information services include the following:

- Flight operations. Includes weather, electronic manuals, charts, cabin surveillance, and surface moving maps.
- Airborne data loader.
- Maintenance access. Maintenance functions include flight data downloads, electronic logbook, maintenance data collection, and electronic minimum equipment list (MEL).
- Cabin crew information access.
- Network management facility.
- Network operation services. Includes domain name system (DNS), dynamic host configuration protocol (DHCP), virtual private network (VPN), etc.
- Network file/print services.

Electronic flight bags (EFBs) are typically considered part of the AISD. Depending on the functions performed by an EFB in a given application, special conditions or issue papers may be involved.

The propulsion system may be connected to the AISD as well. This is typically for the storage of continuous engine operating data (CEOD) or other non-safety critical information, as defined in the aircraft ICD. Adverse safety effects resulting from real-time compromise of CEOD or other propulsion data on this network, whether immediate or longer-term, should be considered.

The AISD can be subdivided into two sub-domains: the administrative sub-domain and the passenger support sub-domain. The administrative sub-domain provides operational and airline administrative information to both the flight deck and cabin. The passenger support sub-domain provides information to support the passengers.

c. Passenger Information and Entertainment Services Domain (PIESD)

This is a private, untrusted domain that informs and entertains the passengers. The PIESD is defined to include more than traditional in-flight entertainment (IFE) systems; that is, any device or function of a device that provides services to passengers.

Onboard and passenger related functions include live audio/video, email/wireless application protocol (WAP), buy on board, rebooking, etc.

A security risk assessment is required at the aircraft level to ensure that any potential intrusion into the passenger entertainment system will be isolated and not allowed to cross over to the other notional domains.

The propulsion system is typically not connected to the PIESD; however, it is mentioned here for completeness and should be evaluated for applicability on a case by case basis.

d. Passenger-Owned Devices Domain (PODD)

This is a public domain that is external to the aircraft domains and informs and entertains the passengers. The PODD is defined to include only those devices that passengers may bring on board. They may connect to the airplane network or to one another. Their connectivity to the airplane network is defined to be provided by the PIESD. Until they connect via the PIESD, the passenger-owned devices (PODs) should be considered external to the airplane network. They may connect to one another or directly off-aircraft to ground systems without involving the airplane network.

The propulsion system is typically not connected to the PODD; however, it is mentioned here for completeness and should be evaluated for applicability on a case by case basis.