AIA Civil Aviation Operational Technology Cybersecurity Recommendations Report

Civil Aviation Cybersecurity Subcommittee

Stefan Schwindt– WG Chair (GE Aviation)

AIA Report Contributors:

Kathleen Finke	Astronautics
Mario Lenitz	Austria, Civil Aviation Air Traffic Controls
Sofian Abbasi	Boeing Commercial Airplanes
Taylor Lamb	Boeing Commercial Airplanes
Tom McGoogan	Boeing Commercial Airplanes
Alimuddin Mohammad	Boeing Commercial Airplanes
Siobvan Nyikos	Boeing Commercial Airplanes
Patrick Morrissey	Collins Aerospace
Kanwal Reen	Collins Aerospace
David Harvie	Embry-Riddle Aeronautics University
Sean Crouse	Embry-Riddle Aeronautics University
Isidore Venetos	FAA
Michele Tumminelli	Gulfstream Aerospace
Gabe Elkin	MIT/Lincoln Laboratory
Jonathan Lee	MIT/Lincoln Laboratory
Lily Lee	MIT/Lincoln Laboratory
Wes Ryan	Northrop Grumman

Executive Summary

The Civil Aviation industry increasingly relies on software driven Operational Technology (OT) for the design, development, production, testing, operations, and maintenance of aircraft and ground systems. This growing dependence on digital OT, coupled with its increased connectivity and data sharing, has made these systems potentially more vulnerable to cyberattacks.

Within Civil Aviation, the Aerospace Industries Association (AIA) is seeing much increased use of OT in all facets of air and ground operations including air traffic management, and in the fabrication, production, maintenance, and testing of aviation products and services.

At the same time, OT systems are becoming more vulnerable to attacks due to increasing connectivity and exposure to internet facing networks, cloud-hosted environments, and data sharing with other IT/OT devices and communications systems. If not adequately protected, OT vulnerabilities can be exploited by threat actors and result in potentially critical impacts to, including to human safety, the environment, brand/reputation, quality, and the resilience of civil aviation air and ground operations.

In response to the growing importance of OT to Civil Aviation, the Aerospace Industries Association (AIA) Civil Aviation Cybersecurity Subcommittee has developed this report to provide strategic recommendations for enhancing the cybersecurity of OT systems within the civil aviation sector.

Key Findings

- OT Specific Vulnerabilities and Exposures: Many OT systems continue to operate with legacy operating systems and other known vulnerabilities, and may be at least periodically exposed to cyber threats due to increased connectivity with internet-facing networks, cloud-hosted environments, or connections with other potentially compromised IT/OT devices and software.
- OT Specific Threats: Recent and growing threats to OT systems come from various sources, including hostile governments, terrorist groups, disgruntled employees, malicious intruders, natural disasters, and human errors.
- Impact of OT Cyberattacks: Cyber incidents can lead to blocked or delayed information flows between OT systems and networks, unauthorized changes to system settings, inaccurate information to operators, and interference with air traffic control and other safety and quality systems and networks.

Strategic Recommendations

- Governance and Industry Standards: Advocate for more greater clarity and consistency in regulations and appropriately scalable industry standards specific to cybersecurity for Civil Aviation OT systems and networks (including aircraft production, energy & facility management, testing/labs, and air traffic and ground control systems).
- Community Engagement: Increase Civil Aviation sector engagement with NIST, DHS CISA, and other industry sectors and communities of interest related to OT Hardware and Software Security.
- OT Asset and Configuration Inventories: Develop and implement new methods to identify and maintain cybersecurity relevant OT asset and configuration inventories.
- Secure Development Practices: Develop new Civil Aviation OT secure coding standards and security testing methods reduce cyber-related risks to OT systems and networks.
- Risk Management and Resilience: Establish new Civil Aviation OT safety and security risk management frameworks to enhance OT system resilience to withstand and recover from cyberattacks, including best practices for architecture and partitioning of critical and non-critical functions.
- Workforce Development and Training: Develop roadmaps and industry resources to address lack of Operational Technology-specific cybersecurity skills and training.

Report Conclusions

The Civil Aviation industry, as a vital segment of the Transportation Sector, has arrived at a unique juncture to move to a more secure future in protecting and defending its most vital Operational Technology systems and networks.

- As required for all else in Aviation, Operational Technologies used in Civil Aviation must ensure aviation operations, products, and services remain **safe and secure** both for the flying public as well as for aviation industry partners and their employees that make use of these technologies every day.

- With the advent of ongoing massive gains in Artificial Intelligence and active use of smart devices and systems into all aspects of aviation, the Civil Aviation industry is now at a unique juncture to move to a more secure future in protecting and defending its most vital Operational Technology systems and networks.

- At the same time, growing threats that are specifically targeting aviation OT systems and networks provides even greater urgency to develop more effective global OT cybersecurity regulations, industry standards, workforce skills, and technical security controls that are specific to Civil Aviation.

- As such this report provides a strategic context for improving OT protections in the Civil Aviation sector. AIA recommends its industry partners begin now to address critical OT cybersecurity shortfalls in technical capabilities and workforce skills across the entire Civil Aviation sector.

In implementing these recommendations, AIA believes these steps will enable the aviation industry to better safeguard its most critical OT systems and networks against evolving cyber threats, ensuring the safety and resilience of Civil Aviation aircraft and operations.

Contents

1 Setting the Context for Civil Aviation Operational Technology Cybersecurity

1.1 Overview

This AIA Civil Aviation Cybersecurity Subcommittee Recommendations Report emphasizes the growing reliance of the civil aviation industry on many types of Operational Technology (OT) that enable aircraft and ground system design, development, production, testing, operations, and maintenance used in civil aviation.

As noted by NIST in its NIST SP 800-82 Rev 3, "Guide to Operational Technology Security"; "Threats to OT systems can come from numerous sources, including hostile governments, terrorist groups, disgruntled employees, malicious intruders, complexities, natural disasters, malicious actions by insiders, and unintentional actions such human error or failure to follow established policies and procedures. OT security objectives typically prioritize integrity and availability, followed by confidentiality, but also must consider safety as an overarching priority."

Although some characteristics are similar, OT has characteristics that differ from traditional information technology systems and networks. Many of these differences stem from the fact that logic executing in OT has a direct effect on the physical world in terms of managing aviation operations and other technical processes. Additionally, while many of these OT systems and networks are normally segregated from direct internet access (e.g. Internet of Things), there are dependencies and network interfaces that must be activated at times for OT system updates and to connect to external data access and storage.

As such, AIA Civil Aviation Operational Technology Cybersecurity Recommendations Report seeks to identify these dependencies and recommend how civil aviation partners can work together to improve the cybersecurity postures of these critical OT systems and software used throughout the industry.

1.2 Threats to Civil Aviation in Operational Technology Systems

As Dragos noted in their recent OT Cyber Threat Intelligence Report Manufacturing Threat Perspective report; "The global manufacturing sector is at the center of the "Industry 4.0" revolution, a transformative concept for traditional industrial manufacturing environments. This trend is impacting all Civil Aviation organizations engaged in both operations and the manufacturing of airplanes and components.

As identified from this study, Dragos noted possible cybersecurity effects from incidents impacting an OT system could include:

- Blocked or delayed flow of information through OT networks, which could disrupt OT operation, including loss of view and loss of control.
- Unauthorized changes to instructions, commands, or alarm thresholds that could damage, disable, or shut down equipment, create environmental impacts, and/or endanger human life.
- Inaccurate information sent to system operators, either to disguise unauthorized changes or to cause operators to initiate inappropriate actions that could have various negative effects.
- Modified OT software or configuration settings or OT software infected with malware, which could have various negative effects.
- Interference with the operation of equipment protection systems, which could endanger costly and difficult-to-replace equipment.
- Interference with the operation of safety systems, which could endanger human life

Additionally, Dragos noted a 60 percent rise in ransomware groups affecting OT/ICS (operational technology/industrial control systems) in 2024. Notably, 69 percent of all ransomware attacks targeted 1,171 manufacturing entities across 26 distinct manufacturing subsectors, highlighting manufacturing as the primary target for ransomware, accounting for over 50 percent of attacks, totaling 1,171 incidents.

For the aviation sector specifically (per Sectrio report on OT/IT Cyberattacks in the Aviation Industry), Civil Aviation has become a rising target for cyberattacks due to its reliance on vastly interconnected digital infrastructures, global supply chains, and volume of the sensitive data it handles The report also cited former

Boeing Chief Security Officer Richard Puckett noting that "occurrences of ransomware inside the aviation supply chain" had shot up by 600% in 2022.

In 2023, the European Organization for the Safety of Air Navigation (EUROCONTOL) likewise reported that ransomware was the sector's leading attack trend in 2022, accounting for 22% of all malicious incidents.

As noted by NIST in its NIST SP 800-82r3, while not specific to aviation, some high-profile threat events that have impacted OT systems and networks included;

- Stuxnet (2010) - Stuxnet was a Microsoft Windows computer worm discovered in July 2010 that specifically targeted SCADA systems and devices that were configured to control and monitor specific industrial processes.
- Shamoon (2012) - Saudi Aramco experienced a malware attack that targeted their refineries and overwrote the attacked systems' master boot records (MBRs), partition tables, and other data files.
- BlackEnergy (2015) - Ukrainian power companies experienced a cyberattack that caused power outages and impacted over 225,000 customers in Ukraine. The actors also corrupted the firmware of serial-to-Ethernet devices at the substations.
- NotPetya (2017) - NotPetya malware encrypted computers globally with no method for decryption. Although the malware initially targeted Ukrainian companies, it spread throughout the world with significant impacts to Maersk, FedEx, Merck, and Saint-Gobain.
- Triton (2017) - A petrochemical facility in Saudi Arabia was attacked using malicious software that targeted the industrial safety management controls.
- Norsk Hydro (2019) - Norsk Hydro experienced a cyberattack that used LockerGoga ransomware to encrypt its computer files, forcing the company to transition to manual only operations.
- Colonial Pipeline (2021) - Colonial Pipeline was a victim of a ransomware cyber-attack that encrypted their IT systems by exploiting a legacy VPN profile. Colonial made the decision to shut down the physical operations on the pipeline to contain any potential damage.

Per NIST SP 800-82r3, "threats to OT can come from numerous sources that can be classified as adversarial, accidental, structural, or environmental."

The following table list types of known threats to OT as identified in NIST SP 800-82r3.

Types of OT Threats	Descriptions	Ranges of Effects
ADVERSARIAL - Bot network operators - Criminal groups - Hackers/hacktivists - Insiders - Nations - Terrorists	Individuals, groups, organizations, or nation-states that seek to exploit the organization's dependence on cyber resources (e.g., information in electronic form, information and communications technologies, and the communications and information-handling capabilities provided by those technologies)	Both immediate and longer-term effects depending on adversary access
ACCIDENTAL - User - Privileged User or Administrator	Erroneous actions taken by individuals in the course of executing their everyday responsibilities (e.g., operator accidentally typing 100 instead of 10 as a set point; engineers making a change in the operational technology environment while thinking that they are in the development environment)	Multiple effects, depending on systems impacted by accident
STRUCTURAL - Hardware failure - Software failure	Failures of equipment, environmental controls, or software due to aging, resource depletion, or other circumstances that exceed expected operating parameters, including failures of critical infrastructures within the control of the organization	Multiple structural, functional and business impacts
ENVIRONMENTAL - Natural or human-caused - Environmental controls - Communications	Natural disasters and failures of critical infrastructures on which the organization depends but that are outside of the control of the organization.	Multiple environmental impacts

As such, US Civil Aviation companies engaged in aviation operations and manufacturing must prepare for a wide range of physical and cybersecurity risks, in developing and applying both more effective risk reduction measures while also increasing the resilience Aviation OT systems and networks.

1.3 US and International Civil Aviation Regulatory Requirements for OT Systems

Within the Civil Aviation Sector, the need for securing information systems that enable airplane safety and ground support has long been recognized in regulatory requirements, however Operational Technology (OT) is only now receiving more focus in terms of regulatory requirements. For Civil Aviation "Design Approval Holders" and aviation system and component manufacturers this security focus extends to ensuring the safety and airworthiness of aircraft in operations as well as any aviation critical ground support functions.

The following provides a regulatory basis for meeting and maintaining both production and type certifications to validate the safety and airworthiness of aircraft in design and in operations (See Appendix A for complete list).

Regulatory Basis	**Relevant Civil Aviation Regulations and Orders**
Regulatory Requirements	14 CFR Part 25, Parts F & G – AIRWORTHINESS STANDARDS: TRANSPORT CATEGORY AIRPLANES 14 CFR Part 21.3 – FAA Design Holder Reporting Requirements, "Reporting of failures, malfunctions, and defects." 14 CFR Part 21.137 – FAA Design Holder Reporting Requirements, "Quality System" EASA Certification Specification CS-25, Subpart F – Equipment (CS 25.1319) EASA Part-IS – Information Security (Part-IS)
Orders and Guidance	FAA Order 8110.105A -Simple and Complex Electronic Hardware Approval Guidance FAA Order 8120.12A - Operational technology Approval Holder Use of Other Parties to Supplement Their Supplier Control Program FAA Order 8120.16Suspected Unapproved Parts Program FAA Order 8220.23A -Certificate Management of Operational technology Approval Holders EASA AMC 20-42 - General Acceptable Means of Compliance for Airworthiness of Products, Parts, and Appliances

While not specifically identifying OT, in addition to existing Federal Aviation Administration (FAA) and Transportation Safety Administration (TSA) regulations, many other international aviation industry regulatory authorities expect international operators to follow regulatory requirements and guidance related to data security, data rights, testing, and other verification of compliance that would also apply to operational technologies and networks used in civil aviation.

Within the European Union, the European Union Aviation Safety Agency (EASA) provides guidance and specifications as Instructions for Continuing Airworthiness, including;

- EASA AMC 20-42 - General Acceptable Means of Compliance for Airworthiness of Products, Parts, and Appliances provides European Union Aviation Safety Agency (EASA) Guidance for Airworthiness Information Security Risk Assessments
- EASA Certification Specification CS-25, Subpart F – Equipment (CS 25.1319) requires "aeroplane equipment, systems and networks be protected from intentional unauthorized electronic interactions (IUEA) that may result in adverse effects to the safety of the "aeroplane."
- EASA Part-IS [currently scheduled to go into effect in Oct 2025] - Introduces requirements for the identification and management of information security risks which could affect information and communication technology systems and data used for civil aviation purposes, including aviation OT systems that make use of these systems and networks.

2 Securing OT Within the Civil Aviation Ecosystem

As noted by DHS CISA and their international partners their recent "Secure by Demand: Priority Considerations for Operational Technology Owners and Operators when Selecting Digital Products"; "Many OT products are not designed and developed with Secure by Design principles." As such, CISA's

Secure by Design campaign is urging technology providers to take ownership of their customers' security outcomes by building cybersecurity into design and development."

Due to the difficulty Civil Aviation partners have in determining specific software/firmware details in aviation systems and components, Civil Aviation partners are looking to enhanced software security design principles to reduce risks across the aviation ecosystem; such as weak authentication & memory protections, known software vulnerabilities, limited logging, continued use of default settings and passwords, and insecure and no longer supported legacy operating systems and protocols.

See Aviation Industry Overview: https://sectrio.com/blog/complete-guide-to-ot-ics-security-in-aviation-industry/

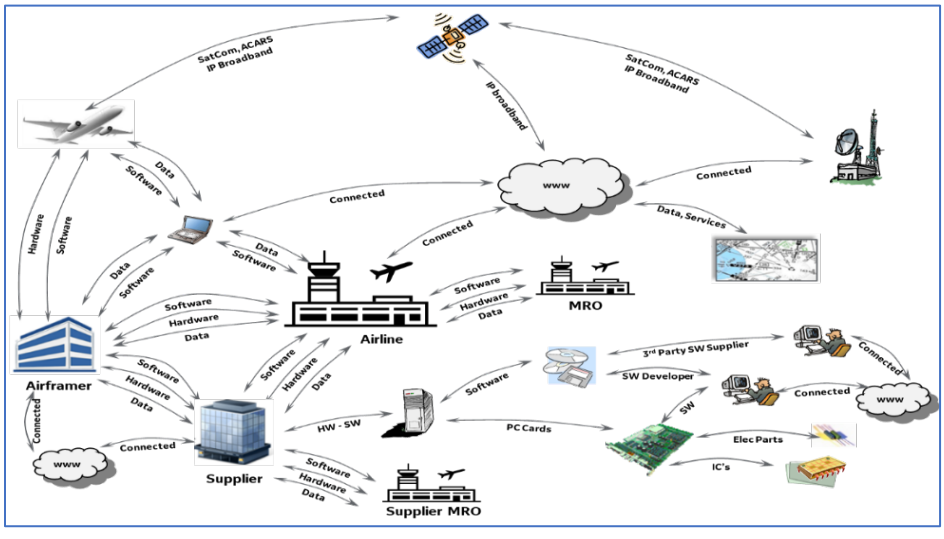

Figure 1: Securing Many Types of OT Used Across the Civil Aviation Ecosystem

ISO/IEC 62443 uses what is commonly referred to as the "Purdue Reference Model" (see figure below) to describe how data flows and is managed through industrial networks for computer-integrated manufacturing. It segments into distinct zones and conduits to indicate how Information Technology (IT) (Levels 4-5) systems and networks interact with Operational Technology (OT) (Levels 0-3) systems and devices.

The below "Purdue Model" provides additional detail on the relationship between IT enterprise level capabilities and the OT systems and assets while operating in different system layer zones. These zones may be primarily information technology or operational technology oriented as appropriate.

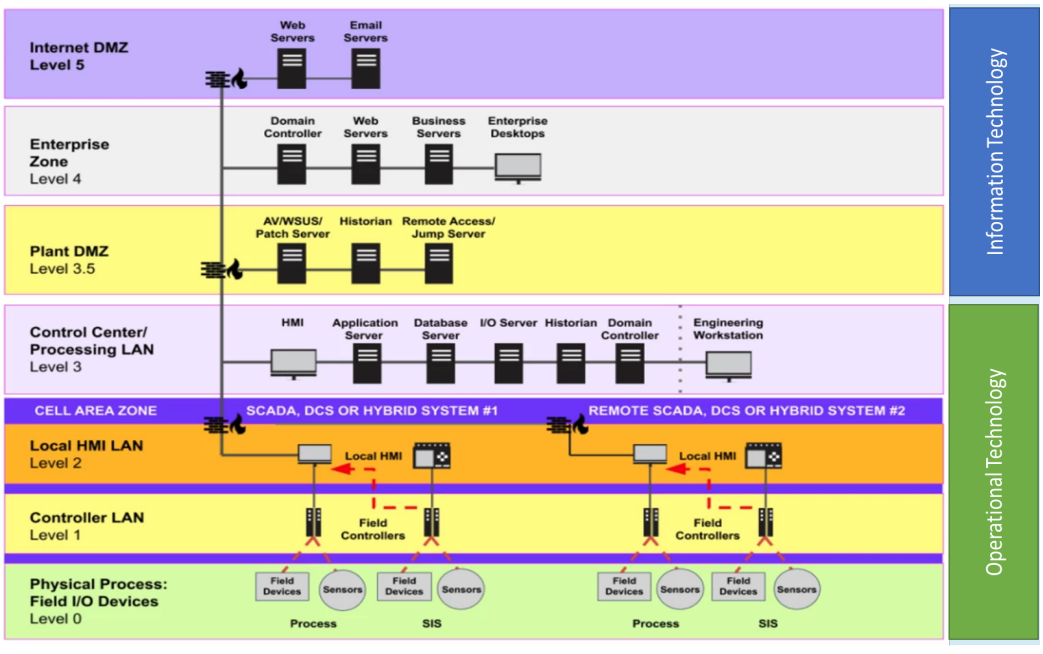

Figure 2: Purdue Model Showing Typical IT and OT System Level Zones (Source: Claroty © 2023)

The Purdue Model was developed to model data flows in computer-integrated manufacturing. It segments IT (Levels 4-5) from OT (Levels 0-3).

The Purdue Reference Model (See table of Purdue Reference Model level descriptions below; Source - SANS Institute ©), provides a model for enterprise control, which end users, integrators and vendors can share in integrating applications at key layers in the enterprise:

PURDUE REFERENCE MODEL LEVELS	DESCRIPTION	EXAMPLES
Level 5: Enterprise Networks	Corporate-level services supporting individual business units and users. These systems are usually located in corporate data centers.	• Enterprise Active Directory (AD) • Internal email • Customer Relationship Management (CRM) systems • Human Resources (HR) systems • Document Management systems • Backup solutions • Enterprise Security Operations Centre (SOC) • Cloud-hosted data & storage
Level 4: Business Networks	IT networks for business users at local sites. Connectivity to Enterprise wide area network (WAN) and possibly local Internet access. Direct Internet access should not extend below this level.	• Business workstations • Local file and print servers • Local phone systems • Enterprise AD replicas
IT/OT GENERAL BOUNDARY (DMZ)		
Level 3: Site-Wide Supervisory	Monitoring, supervisory, and operational support for a site or region.	• Management servers • Human-machine interfaces (HMIs) • Alarm servers • Analytic systems • Historians (if scoped for an entire site or region)

Level 2: Local Supervisory	Monitoring and supervisory control for a single process, cell, line, or distributed control system (DCS) solution. Isolate processes from one another, grouping by function, type, or risk.	• HMIs • Alarm servers • Process analytic systems • Historians • Control room (if scoped for a single process and not the site/region)
Level 1: Local Controllers	Devices and systems to provide automated control of a process, cell, line, or DCS solution. Modern ICS solutions often combine Levels 1 and 0.	• Programmable Logic Controllers (PLCs) • Control processors • Programmable relays • Remote terminal units (RTUs) • Process-specific microcontrollers
Level 0: Field Devices	Sensors and actuators for the cell, line, process, or DCS solution. Often combined with Level 1.	• Basic sensors and actuators • Smart sensors/actuators speaking fieldbus protocols • Intelligent Electronic Devices (IEDs) • Industrial Internet-of-Things (IIoT) devices • Communications gateways • Field instrumentation

2.1 Functional Security Objectives for OT Systems

The development of NIST IR 8183r1, "Cybersecurity Manufacturing Profile" included the identification of common business/mission objectives to the manufacturing sector. These business/mission objectives provide the necessary context for identifying and managing applicable cybersecurity risk mitigation pursuits.

In the NIST profile five common business/mission objectives were identified as follows: Maintain Human Safety, Maintain Environmental Safety, Maintain Quality of Product, Maintain Operational technology Goals, and Maintain Trade Secrets.

The AIA Civil Aviation Cybersecurity Subcommittee recommends our industry adopt these business/mission objectives, which are described in NIST IR 8183r1 as follows;

OT Business/Mission Objectives	Descriptions
Maintain Human Safety	Manage cybersecurity risks that could potentially impact human safety. Cybersecurity risk on the manufacturing system could potentially adversely affect human safety. Personnel should understand cybersecurity and safety interdependencies.
Maintain Operational Technology Goals	Manage cybersecurity risks that could adversely affect operational technology goals. Cybersecurity risk on the Civil Aviation operational systems, including asset damage, could potentially adversely affect operational technology goals. Personnel should understand cybersecurity and operational technology goal interdependencies.
Maintain Environmental Safety	Manage cybersecurity risks that could adversely affect the environment, including both accidental and deliberate damage. Cybersecurity risk on the manufacturing system could potentially adversely affect environmental safety. Personnel should understand cybersecurity and environmental safety interdependencies.
Maintain Quality of Product	Manage cybersecurity risks that could adversely affect the quality of aviation products and services. Protect against compromise of integrity of the operational processes and associated data.

Maintain Trade Secrets	Manage cybersecurity risks that could lead to the loss or compromise of the organization's intellectual property and sensitive business data.

2.2 Technical Objectives for Securing OT Systems and Networks

While the IEC 62443 series of standards provides a comprehensive framework for securing industrial automation and control systems (IACS) against cyber threats, recently updated guidance from NIST Special Publication 800-82r3 (2023), "Guide to Operational Technology Security" identified the following technical security objectives for OT implementation:

- Restrict logical access to the OT network, network activity, and systems.
- Restrict physical access to the OT network and devices.
- Protect individual OT components from exploitation.
- Restrict unauthorized modification of data.
- Detect security events and incidents.
- Maintain functionality during adverse conditions.
- Restore and recover the system after an incident.

2.3 OT Components with Legacy and/or Non-Secure Protocols or Software

Per the AIA Civil Aviation Cybersecurity Subcommittee Supply Chain Recommendations Report, components with legacy non-secure protocols or software should be avoided.

The U.S. Department of Homeland Security (DHS) provides guidance for language to be used in procurement which includes suggested clauses to avoid such a situation and to require reporting by the supplier of any known instances. This guidance may be found at following DHS website: https://www.us-cert.gov/sites/default/files/documents/Procurement_Language_Rev4_100809_S508C.pdf.

If such protocols or software cannot be avoided, for legacy equipment and software, aviation industry organizations must apply security engineering principles to system upgrades and modifications to the extent feasible, given the current state of hardware, software, and firmware within those systems.

Security engineering principles for legacy systems and components include:

- Developing layered protections;
- Establishing sound security policy, architecture, and controls as the foundation for design;
- Incorporating security requirements into the system development life cycle;
- Delineating physical and logical security boundaries;
- Ensuring that system developers are trained on how to build secure software;
- Tailoring security controls to meet organizational and operational needs;
- Performing threat modelling to identify use cases, threat agents, attack vectors, and attack patterns as well as compensating controls and design patterns needed to mitigate risk; and
- Reducing risk to acceptable levels, thus enabling informed risk management decisions.

3 Risk Assessment and Management for Civil Aviation OT Systems

DO-178C, Software Considerations in Airborne Systems and Equipment Certification is the primary document by which the certification authorities such as FAA, EASA and Transport Canada approve all commercial software-based aerospace systems.

To determine the level of potential safety risks to aviation systems and components, DO-178C continued the concept of the Design Assurance Level (DAL) identified under the prior DO-178B. DAL categorization determines the amount of rigor required by the design assurance process. DAL categorization itself is determined by the impact, in this case that a specific OT system's failure could

have in terms of Aircraft Safety. The more critical the DAL, the more activities and objectives are required. DAL categorization continues to be used in DO-178C.

Design Assurance Levels – Per DO-178C			
DAL A Condition: Catastrophic Failure rate: ≤ 1x10-9 Objectives: 71	DAL B Condition: Hazardous Failure rate: ≤ 1x10-7 Objectives: 69	DAL C Condition: Major Failure rate: ≤ 1x10-5 Objectives: 62	DAL D Condition: Minor Failure rate: 1x10-5 Objectives: 26
**The final DAL is DAL E, which confers no failure rate condition or objectives.*			

EASA's recently approved (2023) Part-IS is a set of aviation industry rules that aims to address information security risks at the entity level by establishing processes to ensure the protection of all elements identified as part of its scope. The use of the term 'information security' in Part-IS, as opposed to 'cybersecurity', is deliberate and significant.

Unlike 'cybersecurity', which primarily focuses on protecting data from digital threats in cyberspace, 'information security' is extended beyond the digital realm to include analogue threats. This comprehensive approach acknowledges that vulnerabilities and threats to information systems can arise in both digital and physical formats, which may cause potential risks to aviation safety.

As mandated, Part-IS will go into regulatory effect in October 2025.

3.1 Civil Aviation OT Security Impact Analysis

The NIST IR 8183r1 Cybersecurity Framework Manufacturing Profile defined potential system security impacts across categories as follows:

OT System Security Impacts Across Categories (from NIST SP 800-82r3)			
Categories	Low-Impact	Moderate-Impact	High-Impact
Injury	Cuts, bruises requiring first aid	Requires hospitalization, burns, deep cuts.	Loss of life or limb, eyesight
Financial Loss ($)	Tens of thousands	Hundreds of thousands	Millions
Environmental Release	Temporary damage	Lasting damage	Permanent damage, off-site damage
Interruption of Operational technology	Hours	Days	Weeks
Public Image	Temporary Damage	Lasting Damage	Permanent Damage

Further recommendations may be established to increase security including segregating OT and supplier sites into zones with separate access rights and using color coding for zone and uniform or badges of staff as well as providing separate wired and wireless network access for each organization.

NIST also recommends OT system users (such as AIA Civil Aviation Operations Organizations, OEMs, and Equipment Providers) should develop proposed industry standards for OT security into contracts with companies who install equipment, at least until such standards become part of regulatory material.

4 Performing Civil Aviation Security Across OT System Lifecycles

4.1 Overview

This section establishes the objectives for the lifecycle of Operational Technology systems. The objectives describe the requirements an operational technology system must meet throughout its lifecycle to ensure the security and effectiveness of the system. Additionally, the roles, inputs, and outputs for each step of the system lifecycle are defined within the methods and guidance of this section.

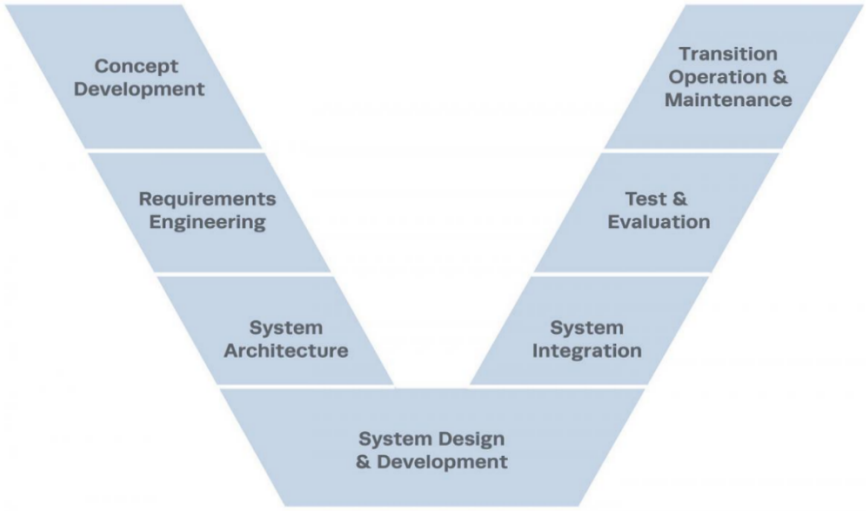

Figure 3: Operational technology System Lifecycle (per ISO/IEC/IEEE 15288)

4.2 OT Security Process Objectives

The following process objectives (aligned to IEC 15288 and IEC/ISO 62443) may be used to establish Civil Aviation system security across OT system and network design, development, and operational lifecycles.

Operational Technology system designs and requirements must include protections to ensure:

- OT systems are secure, resilient, and survivable to detect, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or system compromises.
- OT system information and data processed, stored and managed by the operational technology system and other operational technology system databases are protected from unauthorized access, manipulation, and disclosure.
- Intellectual property related to Civil Aviation systems and components are protected from disclosure to third parties.
- OT system integrity and functionality of the OT system are ensured.
- Data in transit, at rest, or in use, are secured commensurate to the information type and its functional security requirements.

4.2.1 Concept Development

- Inputs: Identify and plan for security requirements in concept development phases depending on the criticality of the operational technology System and how the equipment is deployed and managed in operations.

- Outputs: The assessment of alternatives can include modelling and simulation, or analysis techniques.
    - Initial Concepts of Operation are developed
    - Stakeholders identified
    - Sets Program/System Supply Chain Cybersecurity Risk Management objectives to encompass activities spanning the entire System Development Life Cycle (SDLC)

4.2.2 Requirements Engineering

- Inputs: Stakeholder functional and security requirements (e.g. Program, Operational technology Engineering, Quality Engineering, Security throughout the lifecycle of the Operational technology System)
- Outputs: Security requirements are captured in a central requirements repository according to various Organization program and functional policies and procedures.
    - Interfaces between subsystems are defined, as well as overall test and evaluation requirements, per OT Operational technology System Requirements and Specifications.
    - Requirements shared with Suppliers are consistent including system level protections for data stored both onsite, and in Supplier support and development environments.

4.2.3 Systems Architecture

- Inputs: Concepts of Operations, OT System Development Plans, Threat Analysis, Design Data, Lessons Learned, Program Security and Mission Assurance Requirements
- Outputs: Security Requirements and Objectives for Operational Technology, Functional or Architectural Design Recommendations will be verified through system reviews and test plans for security aspects of the Operational Technology equipment including any dependencies and design tradeoffs for Operational technology Systems and related Operational technology Assets.

4.2.4 Systems Design and Development

- Inputs: Design Concepts, Threat Assessments, Risk Assessments, initial System Requirements and Objectives

a) Outputs: Operational technology System Design and Systems Security Plans and Architecture Definitions.
    - Operational technology System Requirements: including Functional, Logical, and Physical Interfaces and Security Architectures are defined
    - Security arrangements for Suppliers should be determined in this phase to protect the organizations critical and sensitive information, per Organization Operational Technology System Requirements and Supplier contract provisions.

4.2.5 Systems Integration

- Inputs: OT System & Network specifications and drawings, Key Stakeholder Needs, Assumptions
- Outputs: Operational Technology System Engineering Analysis Results (Evidence), Decision Trade Study Report, System Integration plans

4.2.6 Testing & Evaluation

- Inputs: OT System Information, System requirements definition, Systems design definition, Supplier inputs, Key stakeholder needs
- Outputs: Operational Technology System & Configuration Verification - Update Requirements Traceability and Verification Matrix (RTVM), and Test Plan Reviews (Evidence)
    - Protections will be verified to meet all applicable Security requirements

- Outputs: Normal/expected behavior and parameters of an OT system

4.2.7 Operations and Maintenance

- Inputs: OT System security plans (e.g.: monitoring, anti-malware scanning, etc.), System Requirements and Specs, System Manuals, Maintenance manuals, and Training materials
- Transition to Operations Outputs: Certification to transition to operational technology operations
    - Test reports verifying system security requirements for the operating environment are met; and any anomalies identified
    - Problem resolution of any anomalies identified is completed and recorded
    - Training materials for System Operators covering security aspects such as asset management, access control, incident response, other cybersecurity best practices, etc.
- Operations Outputs: Manage and control both internal and external systems interfaces impacting security
    - Monitor and analyze system security activities and logs for anomalies
    - Monitor and analyze system operational status for behavioral based anomalies
    - Supply chain information risk management should be embedded within existing procurement and vendor management processes
    - Operational technology System risk and issue/incident response and recovery planning and testing should be conducted on a recurring basis
- Maintenance Outputs: Operational technology System maintenance issues and source of anomalies are identified and fixed.
    - Additional corrective and preventative actions or security controls are performed.

4.2.8 Decommission Procedures

- Decommission Inputs: Decision to retire/decommission OT systems and networks (for variety of business and/or functional reasons).
- Decommission Outputs: If identified for replacement and disposal, the operational technology system elements or components are destroyed, stored, reclaimed or recycled in accordance with safety and security requirements.

5 Enhancing the Posture of Civil Aviation OT System Security

5.1 Securing Civil Aviation OT Components and Software in Design

As OT system and component buyers are checking for security of these systems and equipment, they should ensure their manufacturers are familiar with the Secure by Demand/Design (see "Secure by Demand: Priority Considerations for Operational Technology Owners and Operators when Selecting Digital Products") guiding principles in taking ownership of their customers' security outcomes, embracing transparency and accountability with their own security progress, and business leadership for integrating cybersecurity from

As prescribed by DHS CISA in, Civil Aviation organizations should look for the following key "Secure by Demand" (Source: DHS CISA "Secure by Design/Demand website) principles when selecting OT products:

Secure by Demand Principles for Civil Aviation in selecting OT Products	
Configuration Management	Logging in the Baseline Product
Open Standards	Ownership
Protection of Data	Secure by Default
Secure Communications	Secure Controls
Strong Authentication	Threat Modeling
Vulnerability Management	Upgrade and Patch Tooling

	*Note: OT patches must be tested prior to updates

In addition to these security elements, "Buyers should look for OT system and network manufacturers that demonstrate their adoption of Secure by Design and Demand principals", and alignment with International Society of Automation (ISA) 62443 standards. Organizations may then demonstrate their adoption of Secure by Design by publishing roadmaps that detail how they are adopting these practices, including both system security requirements and contract terms if applicable to OT system supplier support.

5.2 Developing OT Inventories and Defenses in Depth for Civil Aviation

5.2.1 Collecting and Maintaining OT System and Network Configurations

Civil Aviation industry partners need to develop more effective means to collect and maintain OT System and Network Configuration inventories, including internal details on hardware, firmware, and software used in OT systems and networks that may also be used for system maintenance, vulnerability response, and obsolescence management.

As advocated in our prior AIA Recommendations on the Use of Software Bill of Materials (SBoM) in Aviation (2023), AIA indicated the effective use of SBoMs by the various stakeholders is predicated on the establishment of the detailed system and configuration inventories, along with robust vulnerability management processes. This vulnerability management process should work independently of the use of SBoMs and incorporate mechanisms for ingesting vulnerability information for their components (hardware, software, etc.), performing a risk assessment and criteria for remediation efforts.

In this report, AIA recommended organizations at every level deploy a vulnerability management process for products with documented methodologies for:

- Defining and cataloging the assets (products)
- Collecting vulnerability information about the assets
- Establishing a risk assessment methodology, the drives the urgency around a given vulnerability based of applicability, accessibility/exploitability, and impact.
- Establishing the criteria for notifications to the customers and regulatory authorities (as applicable)
- Triggering the process for updates as required based on the urgency.

5.2.2 Improving Defenses in Depth Strategies for OT Systems

The AIA Civil Aviation Cybersecurity Subcommittee has long recommended in depth cybersecurity strategies for civil aviation, that should also be applied to the use Operational Technology in design, production, testing, and operations. This also includes threat activity that may be shared by government cybersecurity monitoring organizations or industry partners, such as information provided through the Aviation Information Sharing and Analysis Center (Aviation ISAC).

Per NIST SP 800-82r3, an effective defense-in-depth strategy for OT systems should include (among other features):

- Developing more effective security policies, procedures, training, and materials that apply specifically to OT systems and networks
- Employing consistent OT security policies and procedures and deploying increasingly heightened security postures commensurate with Threat Level increases
- Addressing security throughout the life cycle of the OT system, including architecture design, procurement, installation, operations, maintenance, and decommissioning
- Designing critical systems for graceful degradation (fault tolerant) to prevent catastrophic cascading events
- Restricting OT user privileges to only those that are required to perform each user's function (e.g., establishing role-based access control, configuring each role based on the principle of least privilege)
- Implementing security controls (e.g., intrusion detection software, antivirus software, file integrity checking software) where technically feasible to prevent, deter, detect, and mitigate the introduction, exposure, and propagation of malicious software to, within, and from the OT system
- Expeditiously deploying security patches after testing all patches under field conditions on a test system, if possible, before installation on the OT system

- Employing reliable and secure network protocols and services (where feasible)

5.3 Investing in Future OT System Security Capabilities

5.3.1 Establishing Civil Aviation OT Cyber Testing and Evaluation Capabilities

AA recommends Civil Aviation industry partners consider developing dedicated OT Cyber Testing and Evaluation capabilities to assess risks and test/validate options for operational technology systems. These efforts should be guided by our earlier AIA Civil Aviation Cyber Security Subcommittee – Testing White Paper 2021 that may be used to emulate, but not actually test on OT systems and networks that are in operational use.

AIA proposes the following related to planning and implementing OT cybersecurity capabilities

Civil Aviation organizations should make direct correlation to Civil Aviation Product Safety and Quality regulations and industry standards as the basis for developing OT testing and other technical evaluation solutions.

- Develop functional plans to develop the types of capabilities and features to be used in OT Cyber Testing and Evaluation facilities; including the use of Digital Twins, to demonstrate capabilities to identify, characterize, test, and validate system performance prior to implementing on real world operational technology systems and assets.
- Establish means to allow OT system engineering, design, and R&D orgs to connect to OT cyber labs for cross team evaluations and for pre-implementation testing of new capabilities on existing OT systems.

5.3.2 FAA/AIA Cyber Security Data Science (CSDS) Research Projects

AIA recommends continuing development the Federal Aviation Administration's (FAA) and AIA's ongoing Cybersecurity Data Science (CSDS) program is to accelerate the aviation industry's timely adoption and adaptation of novel CSDS and Artificial Intelligence (AI) / Machine Learning (ML) technologies for the enhancement of cybersecurity for the airline, airport, and aircraft elements of the national aviation ecosystem to increase safety and resilience.

Cyber AI/ML Application can be applied across the entire aviation product life cycle with primary and secondary roles as illustrated below. By taking advantage of AI/ML in early phases, this will benefit the security of the system and its architecture throughout the lifecycle, and this will improve product resiliency and reduce integration costs of these advanced technology methods. Model based System Engineering (MBSE) may be used early in the product lifecycle to determine the most useful/efficient approaches for sensors, preprocessing, data curation, along with processing and information flow loads across the OT system and its architectures.

Aviation Development and Operational Lifecycles with Cyber AI/ML Applications (Showing Prime and Secondary Roles)				
Product Life Cycle Phases	**Functionality**			
	MBSE	Vulnerability Management	Anomaly Detection	Cyber Event Detection
Planning and Requirements	Prime			
Concept Design	Prime	Secondary		
Product Design	Prime	Prime		
Simulation & Validation	Secondary	Secondary		
Manufacturing Engineering	Secondary	Secondary	Prime	Secondary
Build and Produce		Prime	Prime	Prime
Test and Quality		Prime	Prime	Prime
In-service Operations		Secondary	Prime	Prime
Maintenance and Repair		Secondary	Prime	Prime

The ability to generate simulation data sets and synthetic data sets that complement operational (real) data sets is critical for researching AI/ML as these methods relate to Civil Aviation Operational Technologies. As such the focus of the CSDS project is on using the right contextual data for the manufacturing environment (for factory cyber use case) which includes machine specific attributes, and part quality attributes. CSDS also offers methodologies that have a greater ability to detect cyber-attacks and may someday provide the ability to dynamically evolve cyber protection systems to learn and adapt to cyber threats.

Recommendations for use of the Cyber Security Data Science (CSDS) methodologies in applying AI & Machine Learning for the AIA community includes the following:

1. Understanding what AI-readiness data means for the specific systems of interest and the analytics goals
2. For new system development, build AI-ready data collection and access into the system from the beginning. This would require that the system integrators understand what AI-readiness means the goals of future analytics development. Equipment/sensor/parts vendors will need to make their data accessible to integrators for this purpose.
3. For existing systems, an assessment will have to be made on the cost of acquiring AI-ready data and the potential benefits of AI-based analytics capability. This level of costs for this analysis will need to be made on a case by case basis.

Additionally, Embry-Riddle Aeronautical University (ERAU) has developed the CSDS Aviation Architecture Framework (AAF), defined using a system-of-systems approach for establishing a top-down CSDS framework across the entire aviation ecosystem, including a reference model supporting cross-domain and cross-stakeholder sharing of the framework. From a bottom-up perspective, AAF considers the application of CSDS in specific aviation environments of operation by industry stakeholders.

5.4 AIA Civil Aviation Subcommittee Strategic Recommendations for OT Security

The AIA Civil Aviation Subcommittee provides the following as strategic recommendations for enhancing the cybersecurity posture in the use of OT in Civil Aviation:

• Governance and Industry Standards: Advocate for more greater clarity in governance across multiple regulatory organizations and industry standards specific to cybersecurity for Civil Aviation OT systems and networks (including aircraft production, energy & facility management, testing/labs, and air traffic control systems).

• Community Engagement: Increase Civil Aviation sector engagement with NIST, DHS CISA, and other industry sectors and communities of interest related to OT Hardware and Software Security.

• OT Asset and Configuration Inventories: Develop and implement new methods to identify and maintain cybersecurity relevant OT asset and configuration inventories, including levying supplier requirements for Hardware and Software Bill of Materials (see link) details for Civil Aviation OT, including data fields, data exchange formats, and vulnerability management processes software and firmware used in Civil Aviation OT systems and components.

•Secure Development Practices: Develop new Civil Aviation OT secure coding standards (see DHS CISA Security by Design/Demand) and security testing methods reduce risks to OT systems and networks. (in alignment with AIA Civil Aviation Cybersecurity Recommendations Report)

•Risk Management and Resilience: Establish new Civil Aviation OT safety and security risk management frameworks to enhance OT system resilience to withstand and recover from cyberattacks.

•Workforce Development and Training: Develop roadmaps and industry resources to address lack of Operational Technology-specific cybersecurity skills and training across many Aviation organizations, including detect, protect, respond, and recover functions across the NIST Cybersecurity Framework.

•Advanced Threat Detection and Response: Continue to develop and integrate AIA/FAA Cyber Security Data Science AI and Machine Learning enabled technologies and methods to enhance OT system and network monitoring, including threat detection and automation of responses.

By incorporating these additional recommendations, our Civil Aviation industry can further strengthen its cybersecurity posture and better protect its critical operational technology systems from evolving threats

6 Conclusions

Civil Aviation, as a vital segment of the Transportation Sector, is now at a unique juncture to move to a more secure future in protecting and defending its most vital Operational Technology systems and networks.

As required for all else in Aviation, Operational Technologies used in Civil Aviation must ensure aviation operations and products remain safe and secure both for the flying public as well as for aviation industry partners and their workforce employees that make use of these technologies every day.

Growing threats to OT present both increased aviation industry risks, and an opportunity to develop and clarify more effective global cybersecurity regulations and industry standards specific to the use of Operational Technologies in Civil Aviation.

Additionally, ongoing efforts to develop improvements to OT in secure coding practices along with the development of Hardware/Software Bill of Materials baseline elements will enable Civil Aviation better understand the software and firmware within aviation OT systems, which will enable Civil Aviation to develop longer term solutions for securing and reducing risks to these vital OT systems and components.

As such, AIA industry partners should also begin now to address Operational Technology cybersecurity skills across Civil Aviation industry organizations. This includes OT specific training and workforce development.

Finally, AIA must continue to support efforts such as the ongoing AIA/FAA Cyber Security Data Science AI and Machine Learning and other related technologies to enhance OT threat detection and automated security protections for the expected broader use of aviation OT systems and networks going forward into the future of Civil Aviation.

Appendices

Mapping OT Improvements to Civil Aviation Regulations & Industry Standards

The following specific recommendations are intended to guide AIA and its partners towards developing more comprehensive long-term solutions to improve the Security of Operational Technologies used across the Civil Aviation industry.

NIST CSF Ver 2.0 Mapping	AIA Civil Aviation Subcommittee Recommendations	Target Group(s)	Regs & Standards
Govern	Conduct analysis to determine potential conflicts between multiple global regulations and industry standards related to OT system and network security in Civil Aviation	FAA, IEC, ISO, IAQG	14 CFR Parts 20, 21, 25, IEC 15288, IEC 62443, NIST SP 800-82r3
Govern	Increase Civil Aviation engagement with NIST and DHS CISA OT, HW/SW Bill of Materials, and Manufacturing Communities of Interest	NIST/DHS CISA	NIST SP 800-82r3, NISTR 82866
Protect	Develop new Hardware and Software Bill of Materials (H/SBOM) standards and approved data fields and formats for Civil Aviation OT systems and components	SAE G-32 RTCA SC-216 EUROCAE WG-72 IAQG	DO-/ED-ISMS, JA6801, JA7496 JA6678, IAQG AS 9115, AS 9125
Govern	Create new Aviation Circular level guidance to meet IEC 15288 and IEC 62443 security principles for OT used in Civil Aviation	ISO / IEC / IECQ	FAA ACs, IEC/ISO 15288, IEC 62443 (Series)
Govern	Establish an OT Specific Guidance for Civil Aviation in new RTCA/EUROCAE Report on Information Security Management System for Aviation Organizations	AIA / ASD ISO / IEC / IECQ	Updates to RTCA/EUROCAE ISMS
Protect	Develop recommendations for securing the Civil Aviation OT Supply Chain through common contractual language, specification requirements, and auditing/verification approaches	AIA / ASD	FAA ACs, IEC/ISO 15288, IEC 62443 (Series), AS 9125
Protect	Develop new baseline requirements and roadmap for introducing new "Secure by Demand/Design" standards for Civil Aviation OT System Components and Software	FAA, DHS CISA, IAQG	AS 9125
Protect	Develop common scoring and vulnerability assessment methods for Operational Technology systems and networks used in Civil Aviation.	RTCA SC-216 EUROCAE WG-72AIA / ASD	DO-392/ED-206 and/or JA6801, JA7496, JA6678
Detect, Respond	Develop a roadmap to address a general lack of Operational Technology-specific cybersecurity skills and training across Civil Aviation industry organizations.	AIA, FAA, DHS CISA	IEC 62443 (Series)
Detect, Respond	Develop Civil Aviation-level guidance and prescribed methods for OT Cybersecurity Testing (in alignment with AIA Civil Aviation Cybersecurity Recommendations Report) testing	AC 20-152A / AMC 20-152A, RTCA SC-216, EUROCAE WG-72, SAE G-32	Update FAA Aviation Circular and Orders, and/or Industry Standards
Detect, Protect, Respond	Continue efforts to expand AIA/FAA Cybersecurity Data Science (CSDS) program is to accelerate the aviation industry's timely adoption and adaptation of	FAA, Industry Partners	New cyber security data science capabilities and standards for

	novel CSDS and Artificial Intelligence (AI) / Machine Learning (ML)		testing OT security features

Regulatory Requirements for OT in Civil Aviation

Civil Aviation Quality and Safety Regulations for Operational Technology		
Source	**Title**	**Subject Matter**
14 CFR Part 21.137[1]	Quality System	Provides rules to require control of suppliers such that supplier-provided products, articles or services conform to operational technology approval holder's requirements and that there is a reporting process for non-conformance.
14 CFR Part 21.146[2] 14 CFR Part 21.316 14 CFR Part 21.616	Responsibility of Holder	Requires operational technology, PMA and TSO certificate holders to inform FAA of delegation of authority to suppliers.
21.A.139[3]	Quality System	Provides rules to require control of suppliers such that supplier-provided products, articles or services conform to operational technology approval holder's requirements and that there is a reporting process for non-conformance. *Note: EASA Part 21 provides Acceptable Means of Compliance and Guidance Material including more detail on surveillance of suppliers similar to the quoted FAA orders*
AC 20-152A / AMC 20-152A[4]	Development Assurance for Airborne Electronic Hardware	Requires applicants to have an Electronic Component Management Plan (ECMP). The plan identifies each commercial hardware part and identifies multiple trusted suppliers/sub-tiers for the part. EIA-STD-4899 provides industry standard for preparing plan.
FAA Order 8120.12A	Operational technology Approval Holder Use of Other Parties to Supplement Their Supplier Control Program	Provides information and guidance concerning use by FAA operational technology approval holders of other-party registered suppliers and contracted other-party supplier surveillance and assessments.
FAA Order 8120.16	Suspected Unapproved Parts Program	Describes responsibilities, policies and procedures for coordinating, investigating and processing FAA suspected unapproved parts reports. Order applies to all personnel involved in the program – including FAA Aircraft Certification Service, FAA Flight Standards Service and FAA Office of Audit and Evaluation.

[1] As current in e-CFR as of May 7, 2020 equivalent to Amendment 21-100
[2] Ibid.
[3] Ibid.
[4] AMC 20-152A has been issued but the equivalent AC 20-152A has not been issued yet but release is imminent in 2020. See https://www.faa.gov/aircraft/air_cert/design_approvals/air_software/planned/

Civil Aviation Quality and Safety Regulations for Operational Technology		
Source	**Title**	**Subject Matter**
FAA Order 8120.23A	Certificate Management of Operational technology Approval Holders	Umbrella document providing guidance on manufacturer's supplier control for all aspects of parts procurement process. It provides guidance and assigns responsibility for the implementation of the Aircraft Certification Service (AIR) certificate management of operational technology activities of manufacturers and their supplier.

Existing Civil Aviation OT Industry Standards

A number of civil aviation and other industry standards exist or are in work that support OT system security are listed in the following **Error! Reference source not found.**:

Industry Standards supporting OT use in Civil Aviation		
Identifier	**Title**	**Subject Matter**
IEC/IEEE 15288	Systems and Software Engineering — System life cycle processes	IEC 15288 provides a technical standard for systems and software engineering which covers processes and lifecycle stages
IEC 62239 (Series)	Part 1: Preparation and maintenance of an OT component management plans Part 2: Preparation and maintenance of an electronic COTS assembly management plan	Provides guidance and requirements to aviation on establishing an electronic components management plan to choose correct components for intended use and to avoid counterfeit, fraudulent and recycled components
IEC 62443 (Series)	Security for industrial automation and control systems	Specifies the process requirements for the secure development of products used in industrial automation and control systems. This specification is part of a series of standards that addresses the issue of security for industrial automation and control systems (IACS).
IEC 62668 (Series)	Managing electronic components from non-franchised sources	Provides guidance on sourcing components from non-franchised distributors.
ISO/IEC 27000	Information Security Management Systems – Overview and Vocabulary	Overview document of the ISO/IEC27000 series of documents for establishing a security management system. Series provides general guidance for securing organizations with some sector specific guidance available
NIST CSF Ver 2.0	NIST Cyber Security Framework Version 2.0	Provides functional framework and implementation tiers for enhancing Cyber Security across all organizations.
NIST SP 800-82r3	Guide to Operational Technology Security	Provides general guidance for securing industrial control systems

NIST SP 800-161	Supply Chain Risk Management Practices for Federal Information Systems and Organizations	Provides guidance for US Federal Organizations for securing supply chain based on 3 tier model and links to NIST 800-53
NIST IR 8183	Cybersecurity Framework Manufacturing Profile	Provides guidance for applying NIST 800-82 in simplified risk framework for manufacturing systems
NIST IR 8276	Key Practices in Cyber Supply Chain Risk Management	Provides key practices in Cyber Supply Chain Risk Management (C-SCRM) to manage cybersecurity risk associated with supply chains.
SAE AS 6081	Fraudulent/Counterfeit Electronic Parts: Avoidance, Detection, Mitigation, and Disposition - Distributors	Provides guidance to aviation on establishing purchasing plans for both purchasing components from distributors
SAEG 9100 (Series)	Quality Management Systems - Requirements for Aviation, Space, and Defense Organizations	Provides guidance and requirements on managing processes in a company and ensuring quality audits of adherence to process
SAE AS 9115	Quality Management Systems - Requirements for Aviation, Space, and Defense Organizations - Deliverable Software	Provides supplementary guidance to AS 9100 to ensure software is correctly managed and includes some cybersecurity considerations.
SAE AS 9125	Quality Management Systems - Requirements for Non-Deliverable Software	Provides supplementary guidance to AS 9100 for Non-Deliverable Software.
SAE EIA STD 4899	Requirements for an Electronic Components Management Plan	Provides guidance and requirements to aviation on establishing an electronic components management plan to choose correct components for intended use and to avoid counterfeit, fraudulent and recycled components

Abbreviations

AC	Advisory Circular
AIA	Aerospace Industries Association
A-ISAC	Aviation Information Sharing and Analysis Center
AISS	Aeronautical Information System Security
AMC	Acceptable Means of Compliance
ARP	Aerospace Recommended Practice
AS	Aerospace Standard
ASD	Aerospace and Defence Industries Association of Europe
ASIC	Application Specific Integrated Circuit
BOM	Bill of Materials
CDI	Covered Defense Information
CEN	European Committee for Standardization

CENELEC	European Committee for Electrotechnical Standardization
CFR	Code of Federal Regulation
CHG	Change
CIS	Center for Internet Security
CNC	Computer Numerical Control
COTS	Commercial-Off-The-Shelf
CMMC	Cybersecurity Maturity Model Certification
CPLD	Complex Programmable Logic Device
CPSS	Cyber Physical System Security
CUI	Covered Unclassified Information
CVE	Common Vulnerability Enumeration
CVSS	Common Vulnerability Scoring System
DAL	Design/Development Assurance Level
DHS	Department of Homeland Security
DOC	Document
EASA	European Aviation Safety Agency
ECSCG	European Cybersecurity for aviation Standards Coordination Group
ECMP	Electronic Component Management Plan
EEE	Electrical, Electronic and Electromechanical
EIA	Electronic Industries Alliance
EN	European Norm
ENISA	European Union Agency for Cybersecurity
ETSI	European Telecommunications Standards Institute
EU	European Union
EUROCAE	European Organisation for Civil Aviation Equipment
FAA	Federal Aviation Administration
FMECA	Failure Mode and Effects Criticality Analysis
FPGA	Field Programmable Gate Array
GM	Guidance Material
HW	Hardware
IAQG	International Aerospace Quality Group
IATF	International Aviation Trust Framework
ICAO	International Civil Aviation Organisation
ICS	Industrial Control Systems
IEC	International Electrotechnical Commission
IECEE	IEC System of Conformity Assessment Schemes for Electrotechnical Equipment and Components
IECQ	IEC Quality Assessment System for Electronic Components
IFE	In Flight Entertainment
IR	Internal Report
IR	Industry Recommendations
IS	Information Security

ISMS	Information Security Management System
ISO	International Organization for Standardization
JIS Q	Japanese Industrial Standards, area division Q (Management System)
LRU	Line Replaceable Unit
MOTS	Modified-Off-The-Shelf
NIS	Network and Information System Security (Directive)
NIST	National Institute of Standards and Technology
NPA	Notice of Proposed Amendment
OEM	Original Equipment Manufacturer
OES	Operators of Essential Services
OpSpec	Operational Specification
OSS	Open Source Software
O-TTPS	Open Trusted Technology Provider Standard
PWB	Printed Wiring Boards
RMT	Rulemaking Task
RTCA	Radio Technical Commission for Aeronautics
SAE	Society of Automobile Engineers
SAL	Security Assurance Level
SL	Security Level
STD	Standard
SW	Software
TR	Technical Report
TS	Technical Specification
US ACCESS	US Aviation Coordination of Cybersecurity & E-enabled Standards Strategy

7 List of References

The following table provides a list of key references

Reference	Title
14 CFR Part 21 Amendment 21-100	Certification Procedures for Products and Articles
AC 20-152A (draft)	Development Assurance for Airborne Electronic Hardware
AC 25-571-1D	Damage Tolerance and Fatigue Evaluation of Structure
AC 43-216	Software Management During Aircraft Maintenance
AC 119-1A	Airworthiness and Operational Authorization of Aircraft Network Security Program (ANSP)
AIA Software and Data load Cyber Recommendations Report	Civil Aviation Cybersecurity Software Distribution and Data load Cyber Recommendations Report
AMC 20-152A	Development Assurance for Airborne Electronic Hardware
Commission Regulation (EU) No 748/2012 *(EASA Part 21)*	Commission Regulation (EU) No 748/2012 of 3 August 2012 laying down implementing rules for the airworthiness and environmental certification of aircraft and related products, parts and appliances, as well as for the certification of design and operational technology organisations
Commission Regulation (EU) 2019/881 *(Cybersecurity Act)*	Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)
CMMC Version 1.02	Cybersecurity Maturity Model Certification
CVSSv3.1	Common Vulnerability Scoring System version 3.1 Specification Document
DEF STAN 05-135 Issue 2	Avoidance of Counterfeit Materiel
DFARS 239.73	Requirements for information relating to supply chain risk
DFARS 252.246-7007 and -7008	Contractor Counterfeit Electronic Part Detection and Avoidance System
Directive (EU) 2016/1148 *(NIS Directive)*	Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union
EASA NPA 2018-09	Regular update of AMC-20:AMC 20-152 on Airborne Electronic Hardware and AMC 20-189 on Management of Open Problem Reports
EASA Part-IS [Oct 2025]	Management of Information Security Risks
ED Decision 2020/006/R	Executive Director Decision 'Aircraft Cybersecurity'

Reference	**Title**
ETSI TR 103 305 (series) *(Equivalent to CIS Top 20 with additional guidance)*	Critical Security Controls for Effective Cyber Defence
EUROCAE ED-12B *(equivalent to RTCA DO-178B)*	Software Considerations in Airborne Systems and Equipment Certification
EUROCAE ED-12C *(equivalent to RTCA DO-178C)*	Software Considerations in Airborne Systems and Equipment Certification
EUROCAE ED-202B *(equivalent to RTCA DO-326A)*	Airworthiness Security Process Specification
EUROCAE ED-203A *(equivalent to RTCA DO-356A)*	Airworthiness Security Methods and Considerations
EUROCAE ED-79A *(equivalent to SAE ARP 4754A)*	Guidelines for Development of Civil Aircraft and Systems
EUROCAE ED-80 *(equivalent to DO-254)*	Design Assurance Guidance for Airborne Electronic Hardware
EUROCAE ED-*206*	Information Security Event Management
FAA Order 8110.105A	Simple and Complex Electronic Hardware Approval Guidance
FAA Order 8110.49 Chg. 1	Software Approval Guidelines
FAA Order 8120.12A	Operational technology Approval Holder Use of Other Parties to Supplement Their Supplier Control Program
FAA Order 8120.16	Suspected Unapproved Parts Program
FAA Order 8220.23A	Certificate Management of Operational technology Approval Holders
ICAO Doc 7300/9	Convention on International Civil Aviation
IEC 62239-1:2018	Part 1: Preparation and maintenance of an electronic component's management plan
IEC TS 62239-2:2017	Part 2: Preparation and maintenance of an electronic COTS assembly management plan

Reference	Title
IEC 62443 (series) IEC TS 62443-1-1:2009 IEC 62443-2-1:2010 IEC TR 62443-2-3:2015 IEC 62443-2-4:2017 IEC TR 62443-3-1:2009 IEC 62443-3-3:2013 IEC 62443-4-1:2018-01 IEC 62443-4-2:2019-02	Industrial communication networks – Network and system security
IEC 62668-1:2019	Avoiding the use of counterfeit, fraudulent and recycled electronic components
IEC 62668-2:2019	Managing electronic components from non-franchised sources
ISO 9001:2015	Quality management systems - Requirements
ISO 27000 (series)	Information technology — Security techniques — Information security management systems
ISO 28590:2017	Sampling procedures for inspection by attributes — Introduction to the ISO 2859 series of standards for sampling for inspection by attributes
ISO/IEC 20243-1:2018	Open Trusted Technology Provider Standard – Mitigating maliciously tainted and counterfeit products – Part 1: Requirements and recommendations
ISO/IEC 20243-2:2018	Open Trusted Technology Provider Standard – Mitigating maliciously tainted and counterfeit products – Part 2: Assessment procedures for the O-TTPS and ISO/IEC 20243-1:2018
ISO/IEC 27000	Information Security Management Systems – Overview and Vocabulary
ISO/IEC 27036-3:2013	Guidelines for information and communication technology supply chain security
ISO/IEC 29147:2014	Information technology — Security techniques — Vulnerability disclosure
ISO/IEC 30111:2013	Information technology — Security techniques — Vulnerability handling processes
NIST CSF Ver 2.0	NIST Cyber Security Framework Version 2.0
NIST SP 800-82r3	Guide to Operational Technology Security
NIST IR 8183	Cybersecurity Framework Manufacturing Profile
NIST SP 800-53r4	Security and Privacy Controls for Federal Information Systems and Organizations
NIST SP 800-171r2	Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations
NIST SP 800-171B (draft June 2020)	Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations - Enhanced Security Requirements for Critical Programs and High Value Assets
NSTAC REPORT TO THE PRESIDENT (2022)	NATIONAL SECURITY TELECOMMUNICATIONS ADVISORY COMMITTEE (NSTAC) REPORT TO THE PRESIDEN; Information Technology and Operational Technology Convergence, August 23, 2022

Reference	Title
Presidential Policy Directive 21	Critical Infrastructure Security and Resilience
RTCA DO-178B *(equivalent to EUROCAE ED-12B)*	Software Considerations in Airborne Systems and Equipment Certification
RTCA DO-178C *(equivalent to EUROCAE ED-12C)*	Software Considerations in Airborne Systems and Equipment Certification
RTCA DO-254 *(equivalent to EUROCAE ED-80)*	Design Assurance Guidance for Airborne Electronic Hardware
RTCA DO-326B *(equivalent to EUROCAE ED-202A)*	Airworthiness Security Process Specification
RTCA DO-356A *(equivalent to EUROCAE ED-203A)*	Airworthiness Security Methods and Considerations
RTCA DO-392	Information Security Event Management
SAE ARP 4754A *(equivalent to EUROCAE ED-79A)*	Guidelines for Development of Civil Aircraft and Systems
SAE AS 5553C	Counterfeit Electrical, Electronic, and Electromechanical (EEE) Parts; Avoidance, Detection, Mitigation, and Disposition
SAE AS 6081	Fraudulent/Counterfeit Electronic Parts: Avoidance, Detection, Mitigation, and Disposition - Distributors
SAE AS 6174A	Counterfeit Materiel; Assuring Acquisition of Authentic and Conforming Materiel
SAE AS 6496	Fraudulent/Counterfeit Electronic Parts: Avoidance, Detection, Mitigation, and Disposition - Authorized/Franchised Distribution
SAE AS 9100D	Quality Management Systems - Requirements for Aviation, Space, and Defense Organizations
SAE AS 9115A	Quality Management Systems - Requirements for Aviation, Space, and Defense Organizations - Deliverable Software
SAE EIA 993B	Requirements for a COTS Assembly Management Plan
SAE EIA STD 4899C	Requirements for an Electronic Components Management Plan