TLP:CLEAR

DOT/FAA/TC-693KA8-19-F-00190/TO 26

Federal Aviation Administration
William J. Hughes Technical Center
Aviation Research Division
Atlantic City International Airport
New Jersey 08405

Part 1: Cybersecurity Data Science (CSDS) Aviation Architecture Framework (AAF) - Overview & Value Proposition

August 23, 2024

Version 1.2

U.S. Department of Transportation
Federal Aviation Administration

NOTICE

This document is disseminated under the sponsorship of the U.S. Department of Transportation in the interest of information exchange. The U.S. Government assumes no liability for the contents or use thereof. The U.S. Government does not endorse products or manufacturers. Trade or manufacturers' names appear herein solely because they are considered essential to the objective of this report. The findings and conclusions in this report are those of the author(s) and do not necessarily represent the views of the funding agency. This document does not constitute FAA policy. Consult the FAA sponsoring organization listed on the Technical Documentation page as to its use.

This report may be available upon request to the FAA Aviation Research Division.

Technical Report Documentation Page

Form DOT F 1700.7 (8-72) Reproduction of completed page authorized

1. Report No.

DOT/FAA/TC-693KA8-23-F-00190/TO 26

2. Government Accession No.

3. Recipient's Catalog No.

4. Title and Subtitle

Title of Report: Cybersecurity Data Science Aviation Architecture Framework
Subtitle of Report: Overview & Value Proposition

5. Report Date

August 2024

6. Performing Organization Code

7. Author(s)
Center for Aerospace Resilient Systems (CARS)
Daniel Diessner
Dr. M. Ilhan Akbas
Isidore Venetos

8. Performing Organization Report No.

9. Performing Organization Name and Address

Embry-Riddle Aeronautical University
Center for Aerospace Resilient Systems (CARS)
1 Aerospace Blvd. Daytona Beach, Florida, 32114

10. Work Unit No. (TRAIS)

11. Contract or Grant No.

DOT/FAA/TC-693KA8-19-D-00190/TO 26

12. Sponsoring Agency Name and Address

The William J. Hughes Technical Center Aviation Research Division ANG-2
Federal Aviation Administration - FAA.
Atlantic City International Airport, Egg Harbor Township, NJ 08405

13. Type of Report and Period Covered

14. Sponsoring Agency Code
ANG-271

15. Supplementary Notes

16. Abstract

This is the first part of a series of four (4) core documents to provide an overview of the top-down output from the FAA Cybersecurity Data Science Aviation Architecture Framework (CSDS AAF) research program. The intent of this utili is to provide an ontology for the CSDS AAF. It also provides a narrative to describe and explain all of the key AAF components and functions, coupled with diagrams to illustrate the overall AAF structure. The four (4) core CSDS AAF documents are:

- **Part 1 CSDS AAF – Overview & Value Proposition**: The primary purpose is to communicate aviation stakeholders the vision and potential value of the FAA CSDS research and generally how it could potentially be leveraged to address key aviation cybersecurity challenges.
- **Part 2 CSDS AAF – Technical Definition**: As an ontology for the CSDS AAF, this document provides a narrative to describe and explain all of the key AAF components and functions, coupled with diagrams to illustrate the overall AAF structure.
- **Part 3 CSDS AAF – Implementation Guidance**: This document provides guidance for the implementation of the CSDS AAF, which is defined in the AAF Technical Definition.
- **Part 4 CSDS AAF – Glossary & Acronyms:** This document provides the Glossary and Acronym material for all parts of the CSDS AAF documentation.

17. Key Words

AAF, Aviation, Artificial Intelligence, Cybersecurity, Data Science, Machine Learning, Strategy

18. Distribution Statement

This report may be made available upon request to the FAA Aviation Research Division.

19. Security Classif. (of this report)

Unclassified

20. Security Classif. (of this page)

Unclassified

21. No. of Pages

22. Price

Contents

Figures

Acronyms

See Part 4: Cybersecurity Data Science (CSDS) Aviation Architecture Framework (AAF) – Glossary & Acronyms.

Executive Summary

The Federal Aviation Administration (FAA) Next Generation Air Transportation System (NextGen) Organization has established the FAA Cybersecurity Data Science (CSDS) research program 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 maintain the highest safety standards and increase resilience. This document defines the aviation challenges FAA CSDS attempts to address and why FAA CSDS might address these specific aviation problems/challenges.

Recent cyber-attacks and existing cyber-threats to critical infrastructure exemplify the complexity of securing operational technology (OT) driven industries such as aviation, including potential aviation safety and efficiency cyber-risks. Aviation systems present unique and different constraints and challenges compared to the mostly IT-based current cybersecurity approaches. Hence, there is a need for additional research to safeguard the cyber safety and cyber-resilience of the aviation ecosystem.

CSDS is the application of advanced data analytics and data science techniques, including AI/ML, for solving cybersecurity problems. The CSDS Aviation Architecture Framework (AAF) is defined using a system-of-systems approach for establishing a top-down framework across the entire aviation ecosystem, with a reference model supporting cross-domain and cross-stakeholder sharing. CSDS AAF provides structure and criteria for applying CSDS methods to address the cybersecurity challenges through the development of practical Aviation Domain environment Use Cases.

Stakeholder engagement is critical for the CSDS AAF research program to develop relevant use cases and identify future CSDS program stakeholder collaboration candidates. CSDS AAF will benefit stakeholders to enhance proactive cyber defense as it enables the adaptation of select methodologies, integration of them into relevant operational environments, and transfer of findings through shareable artifacts and use cases. The stakeholder engagements strategically have focused on building relationships with strong US-based industry organizations. This is an efficient approach for stakeholders since there is no need for individual logistics, and the engagements can focus on industry-wide issues that can be addressed in non-proprietary ways.

1 Introduction

This is the first part of a series of four (4) documents to provide an overview of the top-down output from the FAA Cybersecurity Data Science Aviation Architecture Framework (CSDS AAF) research program. Specifically, this document defines the aviation challenges FAA CSDS attempts to address and why FAA CSDS might address these specific aviation challenges. The four (4) core CSDS AAF documents are:

- **CSDS AAF – Part 1: Overview & Value Proposition**: The primary purpose is to communicate to aviation stakeholders the vision and potential value of the FAA CSDS research and generally how it could potentially be leveraged to address key aviation cybersecurity challenges (Embry-Riddle Aeronautical University Center for Aerospace Resilient Systems, 2024).

- **CSDS AAF – Part 2: Technical Definition**: As an ontology for the CSDS Aviation Architecture Framework, this document provides a narrative to describe and explain all of the key AAF components and functions, coupled with diagrams to illustrate the overall AAF structure (Embry-Riddle Aeronautical University Center for Aerospace Resilient Systems, 2024).

- **CSDS AAF – Part 3: Implentation Guidance**: This document provides guidance for the implementation of the CSDS AAF, which is defined in the AAF Technical Definition (Embry-Riddle Aeronautical University Center for Aerospace Resilient Systems, 2024).

- **CSDS AAF – Part 4: Glossary & Acronyms**: This document provides the Glossary and Acronym material for all parts of the CSDS AAF documentation (Embry-Riddle Aeronautical University Center for Aerospace Resilient Systems, 2024).

2 Problem Statement

The purpose of the Federal Aviation Administration (FAA) 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. The primary purpose of this document is to communicate to aviation stakeholders the vision of the FAA CSDS research program and the value of leveraging that research in addressing aviation cybersecurity challenges.

The recent cyber-threats to critical aviation ecosystem infrastructure highlight aviation safety and efficiency risks (Ukwandu, et al., 2022). The exponentially growing quantity of data in aerospace systems also drives the need for new techniques to address the ability to analyze this data and to address potential cyber-attacks. CSDS 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.

The CSDS Aviation Architecture Framework (AAF) is defined using a system-of-systems approach for establishing a top-down CSDS framework across the entire aviation ecosystem, with a reference model supporting cross-domain and cross-stakeholder sharing of the framework (See Figure 1). From a bottom-up perspective, AAF considers the application of CSDS in specific aviation environments of operation by industry stakeholders and will address the cyber resiliency needs of the Airlines, Original Equipment Manufacturers (OEMs), Airport Operators, Maintenance, Repair, and Overhaul, Service Providers, and Airspace Management.

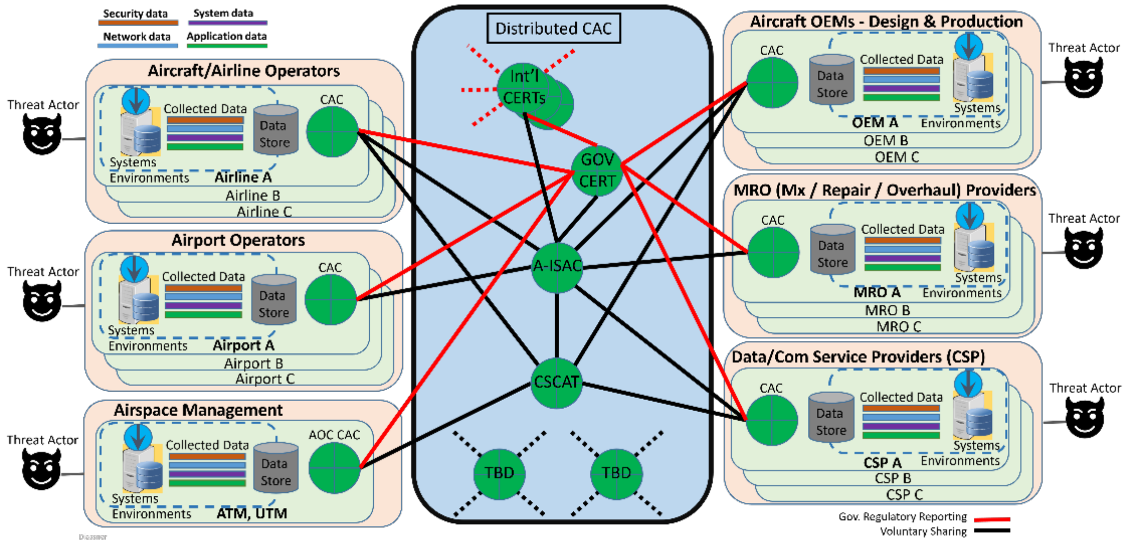


Figure 1. OV-1 Diagram for CSDS AAF.

The AAF has been developed through open industry engagements. The top-down objective of the industry engagement is to help define guidelines for the application of CSDS AAF. The bottoms-up objective is to demonstrate how the application of CSDS AAF to various environments of operation could provide value in addressing aviation cybersecurity risks. The effort also includes developing tools and techniques for application across various aviation environments.

2.1 Challenges of the Aviation Ecosystem

The potential cybersecurity risks in aviation must be carefully assessed, as they can have far-reaching consequences for all stakeholders within the aviation industry. The recent aviation cybersecurity research indicates the existence of significant cybersecurity challenges in U.S aviation industry and need for a proactive new approach (Corretjer, 2018). The contemporary cybersecurity measures become insufficient against the modern attacks which range from traditional Information Technology (IT) threats to the attacks utilizing Operational Technology (OT) data or data-rich technologies such as Internet of Things (IoT) (Kagalwalla & Churi, 2019). The International Civil Aviation Organization (ICAO) indicates that the potential impact of attacks is extremely dangerous as the systems rely increasingly on the integrity and confidentiality of data for the optimization of daily business transactions. There are key elements of aviation industry that are considered to be vulnerable to cyber-attacks such as access and departure systems, cargo handling and Airplane Information Management System (AIMS) (Monteagudo, 2022). The recent cyber-attacks highlight the significance of challenges:

- 2018: McAfee Labs reported that hackers were selling remote access to a "major airport" on the Dark Web. It is reported that the underground forums contain IP addresses for remote desktop protocol access to hundreds of compromised systems (Kessler & Craiger, 2018).
- 2019: Albany International Airport experienced a cyber-attack that forced the authorities to pay a ransom in exchange of the decryption key to a threat actor (Goud, 2019). This attack shows how critical data can be compromised without sufficient cybersecurity measures.
- 2019: Cyberbit researchers discovered a network infection in over half of the European airport workstations by a malware (Team, 2019). The infection escalated privileges of the attacker over any other application, which may include critical systems.
- 2023: Chainanalysis reported that ransomware payments more than $1 billion globally which is the highest level ever recorded as of this report (Greenberg, 2024).
- 2023: The LockBit ransomware gang attempted to extort Boeing for $200 million for the theft of 43 gigabytes of company data. The ransom was not paid (Vicens, 2024).
- 2024: Operations at Seattle-Tacoma International Airport were disrupted to some degree by ransomware attack, to include disruption luggage delivery, for about three weeks (Girgis, 2024).

The cyber-attacks listed above demonstrate the complex approach that threat actors take and show how deep into the supply chain an attack may manifest. Within this context, the industry stakeholders were engaged and critical areas of concern regarding cybersecurity were identified: 1) Factory Cybersecurity, 2) Maintenance, Repair, and Overhaul (MRO) Systems Cybersecurity, 3) Parts and Supply Chain Integrity, 4) Aircraft Supply Chain Cybersecurity, 5) Avionics Network Interfaces, 6) Airport Networks, 7) Automated Operations for Commercial Aircraft and Advanced Air Mobility (AAM), 8) Position Navigation & Timing (PNT).

The current aviation cyber-defense approaches in place are mainly designed for IT systems. However, aviation systems often present different constraints, challenges, and designs compared to IT systems. When applying CSDS within the AAF, the OT nature of aviation systems as well as the unique aviation ecosystem constraints, design elements, and non-standard IT data types must be considered. In addition, a firm grasp of aviation use cases, threat scenarios, and the involved operational networks involved is required.

2.2 Cybersecurity Data Science for Aviation Ecosystem

CSDS AAF is proposed to facilitate the development and collaboration of CSDS techniques, tools, and processes in a systematic approach to assist cybersecurity analysts in answering three (3) key questions for aviation architectures: 1) Is there a cyber-event pending? (Initial Foothold) 2) Is there an attack occurring now? (Network Propagation) 3) Was an incident/event caused by cyber activity? (Action on Objectives). These questions can be directly mapped to the Cybersecurity Unified Kill Chain model (Pols P. , n.d.) given in Figure 2.

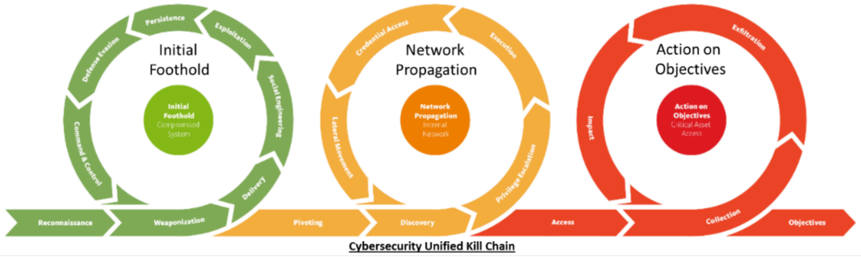


Figure 2. Cybersecurity Unified Kill Chain.

CSDS AAF functionally decomposes the overwhelmingly large aviation ecosystem into analyzable environments of operations that align with aviation business structures and the regulatory framework to accelerate the adaptation of CSDS, including AI/ML techniques, for greater resilience against cyber threats and attacks. AAF also allows utilization of all relevant digital artifacts across the aviation domains, which supports the definition of right requirements and integration of them into the businesses for cybersecurity needs.

2.3 Need for Change in Aviation Ecosystem Cybersecurity

The aviation ecosystem is composed of a multitude of stakeholders, each of which has a unique business case to support their slice of civil air transportation. To fulfill their interests and responsibilities, stakeholders control and monitor merged enterprise IT/OT systems during daily operations and act as backbone technologies throughout the aviation ecosystem. The automated systems and data science concepts within the civil aviation industry have their roots in the relatively recent deployments embodying the digitalization of the industry, such as integrating IoT, big data and AI/ML to sustain quality-of-service delivery.

The migration to increasing efficiencies through the integration of new technology also spawns new cyber-attack surfaces. The increasing amounts of data in the form of network traffic, system logs, and operational logs require the utilization of novel techniques. Hence, existing cybersecurity implementations need to be reconsidered, and the ramifications of the evolving threats must be assessed to update both the risk scenario analysis and resilience measures.

Digital technologies are reshaping the aviation industry and creating a highly interconnected ecosystem. This increased interconnectivity necessitates a shift from protections enacted on a company-by-company basis to an industry wide, coordinated approach for managing shared cyber risks across the breadth and depth of the ecosystem with an emphasis on data transmissions. However, the aviation industry currently lacks a cohesive and collaborative framework for defining and managing the risks inherent to the growingly interconnected aviation ecosystem in which products are developed, manufactured, and operated.

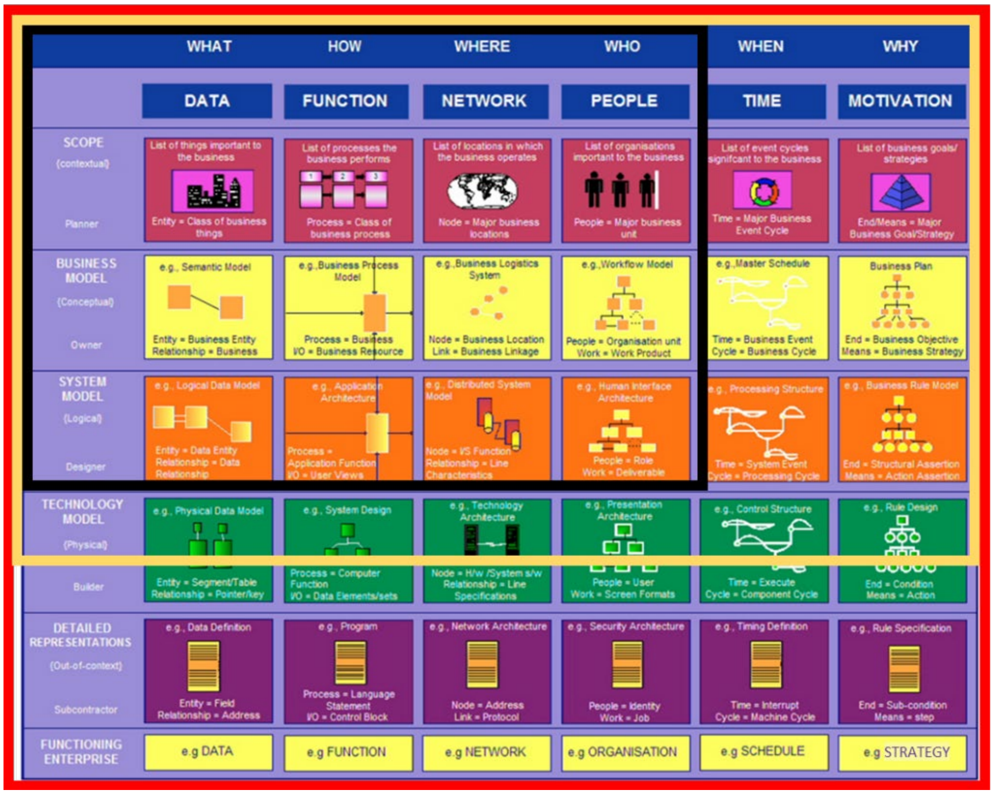
3 Background

Cybersecurity is often described as a set of technologies and processes designed to protect computers, networks, programs, and data from attacks, damage, or unauthorized access. However, this is a heavily IT-oriented definition and misses key aspects of cybersecurity needs in any other domain of critical infrastructures including aviation. Nevertheless, in recent years, there has been a heightened awareness of threats and the recognition of the unique needs of critical infrastructure OT segments to be protected against cyber-attacks. In addition, the expansive growth of interconnectivity and data generation within these OT environments supports an apparent need for a cybersecurity effort specifically aimed at aviation, where data science may play a vital role in discovering valuable cyber insights from the data.

The FAA CSDS research is intended to provide a catalyst for the industry to pick up and leverage the CSDS concept, support the development of recommendations for standards efforts and show the value of CSDS by applying it to aviation-specific use cases. The primary purpose of this report is to identify the aviation challenges, and to communicate to aviation stakeholders the vision and potential value of the FAA CSDS research.

3.1 CSDS AAF Scope

The scope of CSDS AAF can be illustrated using the Zachman Framework (Zachman, 2008), which provides a systematic way of defining an enterprise architecture (See Figure 3). The early more generic version of the Zachman Framework is used for CSDS AAF since it provides a useful construct for OT-heavy aviation environments of operation. The newer versions of the Zachman Framework are honed with a representation more specifically addressable to the intricacies of the IT industry. This systematic view will allow the aviation community to leverage CSDS AAF at multiple highly networked environments of operation in various domains across the aviation ecosystem.



	WHAT	HOW	WHERE	WHO	WHEN	WHY
	DATA	FUNCTION	NETWORK	PEOPLE	TIME	MOTIVATION
SCOPE (contextual) Planner	List of things important to the business Entity = Class of business things	List of processes the business performs Process = Class of business process	List of locations in which the business operates Node = Major business locations	List of organisations important to the business People = Major business unit	List of event cycles signifcant to the business Time = Major Business Event Cycle	List of business goals/ strategies End/Means = Major Business Goal/Strategy
BUSINESS MODEL (Conceptual) Owner	e.g., Semantic Model Entity = Business Entity Relationship = Business	e.g.,Business Process Model Process = Business I/O = Business Resource	e.g.,Business Logistics System Node = Business Location Link = Business Linkage	e.g.,Workflow Model People = Organisation unit Work = Work Product	e.g.,Master Schedule Time = Business Event Cycle = Business Cycle	Business Plan End = Business Objective Means = Business Strategy
SYSTEM MODEL (Logical) Designer	e.g., Logical Data Model Entity = Data Entity Relationship = Data Relationship	e.g., Application Architecture Process = Application Function I/O = User Views	e.g., Distributed System Model Node = I/S Function Relationship = Line Characteristics	e.g., Human Interface Architecture People = Role Work = Deliverable	e.g., Processing Structure Time = System Event Cycle = Processing Cycle	e.g., Business Rule Model End = Structural Assertion Means = Action Assertion
TECHNOLOGY MODEL (Physical) Builder	e.g., Physical Data Model Entity = Segment/Table Relationship = Pointer/key	e.g., System Design Process = Computer Function I/O = Data Elements/sets	e.g., Technology Architecture Node = H/w /System s/w Relationship = Line Specifications	e.g., Presentation Architecture People = User Work = Screen Formats	e.g., Control Structure Time = Execute Cycle = Component Cycle	e.g., Rule Design End = Condition Means = Action
DETAILED REPRESENTATIONS (Out-of-context) Subcontractor	e.g., Data Definition Entity = Field Relationship = Address	e.g., Program Process = Language Statement I/O = Control Block	e.g., Network Architecture Node = Address Link = Protocol	e.g., Security Architecture People = Identity Work = Job	e.g., Timing Definition Time = Interrupt Cycle = Machine Cycle	e.g., Rule Specification End = Sub-condition Means = step
FUNCTIONING ENTERPRISE	e.g DATA	e.g FUNCTION	e.g NETWORK	e.g ORGANISATION	e.g SCHEDULE	e.g STRATEGY

Figure 3. Early Zachman Framework for Defining an Enterprise Architecture.

In Figure 3, the elements within the black box provide a map to the initial scope of the CSDS AAF. These elements address the "Contextual," "Conceptual and "Logical" layers top to bottom for the "Data," "Function," "Network" and "People" considerations. When creating a generic

CSDS Use Case, all areas in the yellow box must be applied, incorporating the “Time” and “Motivation” aspects of the Use Case, as well as considering appropriate technologies. For a stakeholder specific Use Case, the entire Zachman Framework must be implemented to address the aviation stakeholder’s specific functioning environment of operation.

3.2 CSDS AAF Overview

CSDS AAF uses the reference architecture shown in Figure 4 for the aviation ecosystem. The architecture is composed of multiple aviation domains, which form the civil aviation infrastructure. Each aviation domain contains the domain stakeholders, and the organizations of the aviation domain. Each domain stakeholder owns and maintains multiple environments of operation, each of which is composed of several Interconnected Individual Systems (IIS).

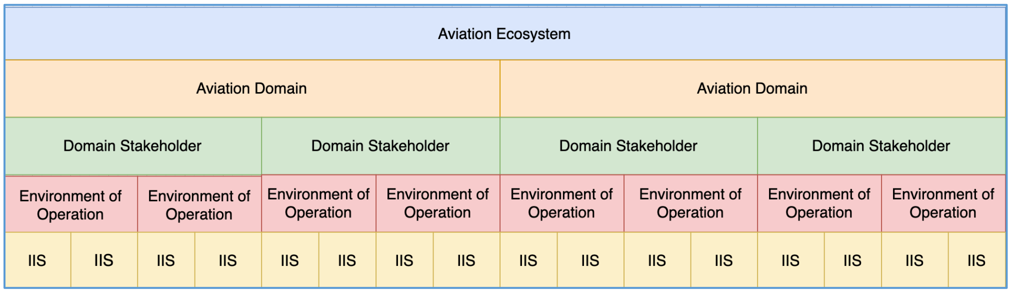


Figure 4. Top Level Aviation Ecosystem Reference Model from a CSDS AAF Perspective.

Aviation Domains are the major, functional segments based on the typical aviation structure of core business operations. The CSDS AAF currently identifies six (6) domains of interest: Aircraft OEMs, Aircraft/Airline Operators, MRO Providers, Data / Communication Service Providers (CSPs), Airspace Management / ANSP (ATM, UTM) and Airport Operators. These domains align with the Aviation Stakeholder Framework of DO-391, which identifies the stakeholders as maintainers, manufacturers, operators, product suppliers, and service providers.

A Domain Stakeholder is a stakeholder of a specific Aviation Domain, which is defined in DO-391 (ISO, 2015) as an organization having a right, share, claim, or interest in the aviation system or in its possession of characteristics that meet their needs and expectations. Examples of these include Airline Operators – Part 121, Aircraft OEM – Part 21, Airport Operator and MRO – Part 145. It is important to note that a business such as an airline may be a Domain Stakeholder in multiple Aviation Domains. Figure 5 shows how such an airline can be structured using the CSDS AAF reference model.

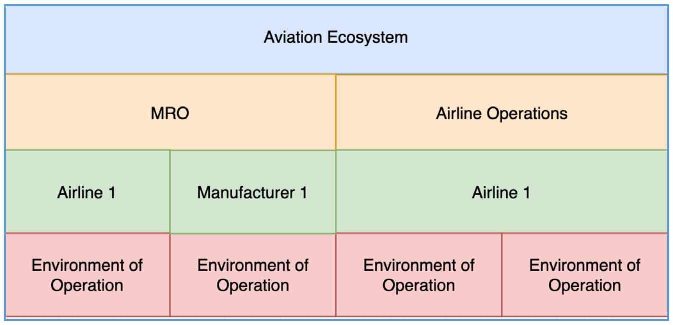


Figure 5. Example of CSDS AAF Reference Model applied to an Airline.

The Interconnected Individual Systems (IIS) within the environment of operation include hardware and software that provide its operational capabilities. These systems acquire diverse types of raw data and perform pre-analyzing processes before storing data determined to be relevant per the programmed system data collection instructions. Each IIS includes data acquisition sensors, processors that pre-process and store/forward the raw data and local storage.

4 Present and Future Aviation Condition and CSDS AAF

After briefly describing the scope and overview of AAF in Section 3, the cybersecurity considerations in the present aviation ecosystem and the expected future conditions are discussed in this section. These descriptions are used to set the stage for the reader to clearly see the differences between the current and future aviation cybersecurity needs before moving on to the CSDS AAF utilization discussion in Section 5.

4.1 Present Aviation Condition

4.1.1 Background

The assurance of cybersecurity in aviation is imperative to maintain safety and preserve valuable resources within the industry. The rapid pace of advancements in the IT sector demands increased attention to security and protection. Failure to prioritize security measures renders these advancements vulnerable to cyber-attacks, with potentially devastating consequences for both human life and economic resources. The current state of the aviation industry in terms of cybersecurity and the main challenges can be summarized as follows:

- Given the unique OT nature of the aviation ecosystem as a system-of- “Integrated Control Systems (ICSs), the contemporary cybersecurity measures that are typically developed for IT systems encounter difficulties for aviation systems (Kagalwalla & Churi, 2019).

- The danger of cyber-incidents has increased due to the increased reliance on the integrity and confidentiality of data for the optimization of daily business transactions (ICAO). Increased levels of automation enlarge the attack surface and allow attackers to disrupt businesses and steal information for political and financial gain.
- A more proactive implementation for cybersecurity is found necessary based on the analysis of cybersecurity procedures within the U.S. aviation industry (Corretjer, 2018).
- There is a lack of resources, funds, and skilled staff specialized in aviation cybersecurity. In addition, insider threats are becoming more complex continuously and the cyber structure is unprepared for modern-day operational technologies (Kagalwalla & Churi, 2019).
- Available datasets for research on using data science in aviation cybersecurity are not large enough to be meaningful and/or do not cover all domains within the whole ecosystem.
- The aviation ecosystem lacks testbeds for research on the utilization of data science in cybersecurity, often due to cost or regulations (Garcia, Babiceanu, & Seker, 2021).

Hence, there is a need for an community-wide research effort in aviation that will help identify threats and protect aviation systems using a modern, data-centered approach.

4.1.2 Operational Policies and Constraints

Aviation policy, guidance, and standardization from a regulatory perspective begins at the United Nations world government level via the International Civil Aviation Authority (ICAO). The purpose of this guidance is to enhance and revise cybersecurity regulations, standards, and principles across the entire ecosystem, including avionics, airlines, and airports. For the US, RTCA produces minimum performance standards and guidance materials that become a partial basis of FAA regulations for aviation systems and equipage. This function is served in Europe through EUROCAE. There are also industry standards bodies that the industry relies upon to develop non-regulatory based standards such as AEEC ARINC, ISO, ATA, SAE and AIA.

The industry implements new technologies and tools as they experience the positive effects of these on aircraft control systems, aviation operations quality, safety, and performance. Every aspect of aviation is increasing the amount of data produced by these technologies. This trend leads to an increase in cybersecurity vulnerabilities, potentially resulting in breaches that could threaten human life and business continuity. The present cybersecurity practices have difficulty managing the volume of data and alerts that are produced by modern systems (Shimeall, 2021). There is also no standard way to share the data produced in different systems, which causes a lack of available datasets for research or information sharing. Even though data science provides significant methodologies and toolsets for potential solutions to these challenges, there are existing operational constraints to implementing data science solutions for cybersecurity in aviation. Some of the main operational and policy constraints can be listed as follows:

- The cybersecurity concern for aviation grows with the continuous integration of technology and progressive innovation without a standardized operational policy (Cooper, 2017). The lack of standardized cybersecurity practices may increase susceptibility of aviation to cybersecurity incidents (Nobles, Burrell, & Waller, 2022).
- Cybersecurity in aviation is typically approached through the segmentation of cyberspace networks into distinct sectors. While this division enables security controls to be isolated at individual sector nodes, it also creates vulnerabilities that may be exploited by attackers.
- There is value in existing research efforts on standardization that map out their various appropriate activities. Additional research activities are needed to use these to determine optimal engagement opportunities for best value to the industry as a whole.

The CSDS AAF provides a response to the existing policy challenges by defining a framework for cybersecurity data science implementation across the aviation ecosystem which involves both IT and OT with various stakeholders such as airlines, airports, and OEMs. The research effort supports development of guidance and recommendations by defining an aviation ecosystem taxonomy and reference model, which is briefly introduced in Section 5. The “Part 2 CSDS AAF - Technical Specification Document” provides the details of the taxonomy and reference model with the system architecture and the data life cycle. The system architecture applies the framework in different Environments of Operation and involves Stakeholder Data-Stores, CACs, and IIS. The AAF data life cycle describes the perspective of the architecture for collecting the appropriate data.

4.2 Future Aviation Condition

4.2.1 Background

The migration to increasing automation levels through operational systems integration spawns new cyber-attack surfaces in the Aviation Domain, which in turn mandates the revision of existing cybersecurity implementations, assessment of the ramifications of the latest evolving threats, and updating both the risk scenario analysis and resilience measures.

The AI/ML, IoT, Radio Frequency Identification (RFID), geolocation, immersive realities, biometric systems, and robotics are considered core elements of transformative technologies (Zamorano, Fernández-Laso, & de Esteban Curiel, 2020). The scope of threats against infrastructures using these technologies and applications within these systems can be broadly grouped into network attacks, malicious software, and tampering with smart devices. The scenario analysis of likely malicious attacks also includes the misuse of authorization, social engineering, and phishing with consideration of smart applications, mitigating actions, and resilience measures. It is also shown that data collection systems and devices are prone to advanced persistent threats due to hardware constraints, software flaws, or misconfigurations. AI/ML based techniques are suggested as the potential solution that will address this challenge (Koroniotis, Moustafa, Schiliro, Gauravaram, & Janicke, 2020).

The use of electronic data exchange and digital network connectivity are important parts of the approach adopted by the industry to increase the efficiency of aviation operations, and data collectors will play an essential role in this respect (Wolf, Minzlaff, & Moser, 2014). Hence, it is important to review the role of e-enabled devices (composed of highly integrated interconnected software and firmware driven computer systems with computing and control tasks) in enhancing digital network connectivity and electronic data exchange, together with the vulnerabilities, attack surfaces, and mitigating factors. It is shown that the design of an adaptive security architecture is needed for future network-connected aircraft and a secure system topology for the embedded aircraft system network (Mahmoud, Larrieu, Pirovano, & Varet, 2010). There is also evidence that the efficiency of e-enabled systems will be highly dependent on the security capabilities of the cyber-physical systems (Sampigethaya, Poovendran, & Bushnell, 2008).

The consequence of deploying advanced sensing, extensive computerized systems, enhanced communication channels between on-ground and on-board systems, on-board system integration, and smart software-enabled interfaces is a proliferation of attack surfaces. Such surfaces present opportunities to exploit on-board cyber-physical systems remotely through radio frequency jamming, node impersonation, and passive eavesdropping. The relatively recent harnessing of AI by cyber-attackers to automate attack processes stimulates a response strategy founded on using AI-enabled cyber-defense frameworks to safeguard e-enabled aircraft.

The team for traditional cyber security services within any given industry stakeholder will likely have a minimal number of employees (Shimeall, 2021). With a large amount of cyber-attack surfaces and the additional number of attack methods, the number of “hands on deck” leads to the question of responsive capability from the cybersecurity team. Even with more professionals hired, a team could not feasibly address every threat. The data science based cybersecurity solution would always have a more responsive capability with the high speed of data exchange. The cyber security team would then be free to address the lower number of attacks.

4.2.2 Application of the CSDS AAF

The businesses need to follow the data life cycle model given in Figure 6 to apply CSDS AAF in their environment of operation.

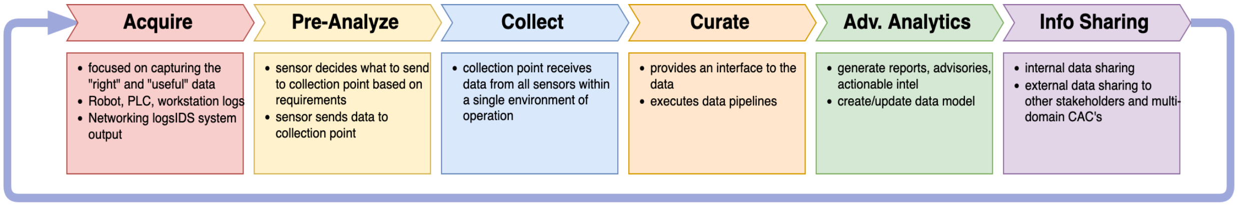

Acquire
• focused on capturing the "right" and "useful" data
• Robot, PLC, workstation logs
• Networking logsIDS system output
Pre-Analyze
• sensor decides what to send to collection point based on requirements
• sensor sends data to collection point
Collect
• collection point receives data from all sensors within a single environment of operation
Curate
• provides an interface to the data
• executes data pipelines
Adv. Analytics
• generate reports, advisories, actionable intel
• create/update data model
Info Sharing
• internal data sharing
• external data sharing to other stakeholders and multi-domain CAC's

Figure 6. CSDS AAF Life Cycle.

Businesses will integrate/configure selected IIS with Data Acquisition Sensors, to acquire and pre-analyze data. Sensors monitor and capture data from hardware components or software processes of the IIS across the environment of operations. The potential impact of large data on the performance of sensors is also assessed as the data is acquired. The pre-analyze phase includes software-based logic that evaluates whether the data being acquired and the automation to filter and extract data features. In the Collect Phase, relevant data is stored on various non-volatile memory storage devices within an environment of operation. A primary objective of the Collect Phase is to ensure local storage devices are installed, connected, and configured correctly to manage data velocity requirements and remote storage. The Curate Phase aims to extract cyber-relevant data from the Data-Store and create data sets and models from it, depending on specific needs and interests. In the Advanced Analytics phase, the curated data is taken to produce meaningful artifacts that include insights and actionable information. In terms of insights, analytical toolsets provide enhanced capabilities for human analysts to visualize and interpret data in numerous ways. In terms of actionable information, AI/ML solutions function as an expert advisory system that provides suggestions to the business, such as the recommendation of disabling specific network ports on an aircraft network as they may not be currently in use. In the Information Sharing phase, the data analytics results are prepared for internal notifications and disclosure to other stakeholders within the aviation community. This process ensures proper handling of confidential or sensitive data such as personally identifiable information of customers or International Traffic in Arms Regulations (ITAR) / Export Administration Regulations (EAR) data. More details on the data flow, its relation to AAF Systems in CSDS operational concept and the main steps to create a use case are given in Section 5.

5 CSDS Aviation Architecture Framework Utilization

This section includes the fundamental concepts of the CSDS AAF, brief descriptions of these concepts, involved personnel, the operational scenario, and practical applications of CSDS AAF concepts in aviation systems design, implementation, and operation.

5.1 CSDS AAF Introduction

The utilization of CSDS AAF requires the understanding of three (3) conceptual elements given in Figure 7: Data Acquire Elements, Data Categories, and Analytical Functional Elements.

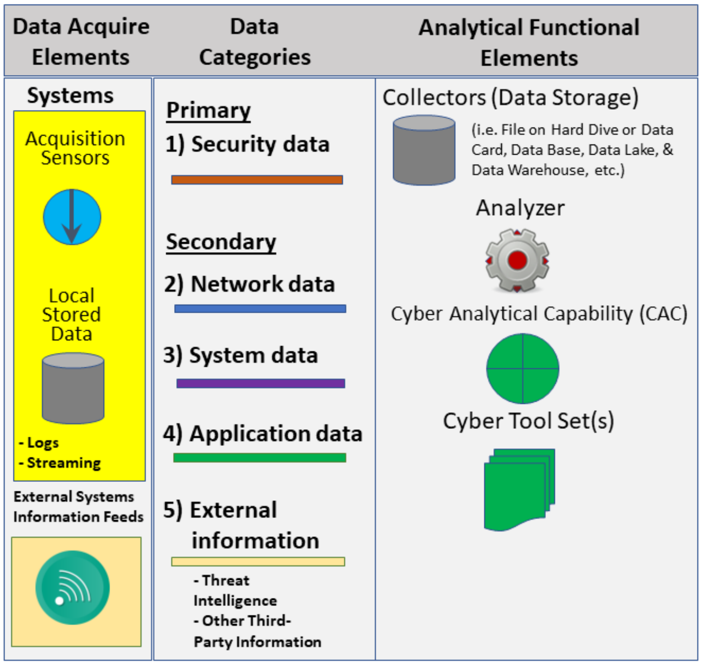


Figure 7. CSDS Conceptual Elements.

Data Acquire Elements refer to the IIS components essential for acquiring data. The data acquisition sensors monitor data generated on systems and evaluate data relevancy. Once data is determined as relevant, it is encoded and often stored in Local Storage.

Data Categories include security data as the primary category as well as Network, Systems, and Application Data, as discussed earlier. Security data is typically a subset of network, systems, and application data that is cybersecurity relevant. For example, a login attempt into a system on the network is considered security-related, but it can be a network, system, or application-type log. Data from all external sources are collectively categorized as external data.

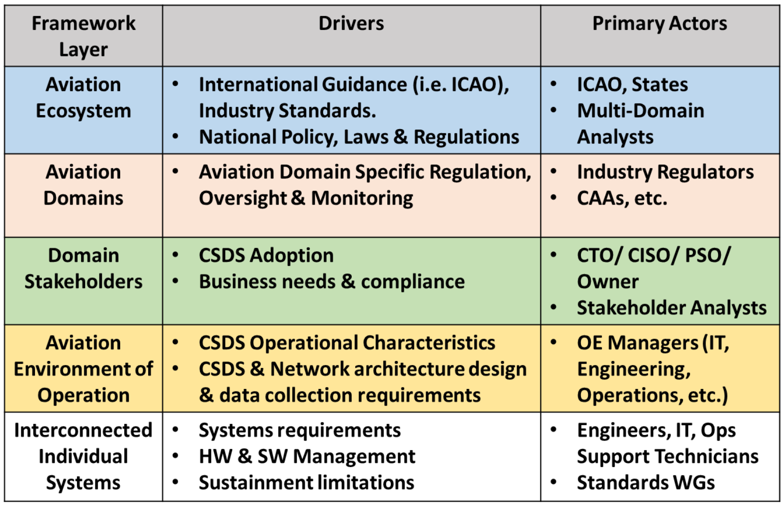
Information generated outside the EOO but used within the CSDS process is categorized as external information. Examples of external information include threat intelligence and other third-party data. Threat intelligence can include disclosed vulnerabilities and security bulletins from both private and public sources.

The Analytical Functional Elements include Data Collector, Analyzer, Cyber Analytical Capability (CAC) and Cyber Tool Sets. CSDS Collectors are storage devices that can be located throughout an Environment of Operation and provides basic data storage and retrieval capabilities. Collectors can be embedded into an IIS or can be an IIS itself that specializes in data storage such as a network attached storage server. The Analyzers choose to retain or discard the collected data. CACs are represented by a collection of Human Analysts using software-based Tool Sets to perform analytics on data to produce cyber-analytical information.

The overall CSDS AAF architecture includes the Distributed CACs that have vested interests in the cyber analytical information generated and shared by Domain Stakeholders (See Figure 1). The architecture is segmented into multiple aviation domains, each containing numerous domain stakeholders that own, maintain, and manage various Systems and Environments of Operations.

5.2 CSDS AAF Users

The CSDS AAF layers, their primary drivers and actors are given in Figure 8. The drivers represent the key roles that each layer plays in supporting the CSDS AAF.



Framework Layer	Drivers	Primary Actors
Aviation Ecosystem	• International Guidance (i.e. ICAO), Industry Standards. • National Policy, Laws & Regulations	• ICAO, States • Multi-Domain Analysts
Aviation Domains	• Aviation Domain Specific Regulation, Oversight & Monitoring	• Industry Regulators • CAAs, etc.
Domain Stakeholders	• CSDS Adoption • Business needs & compliance	• CTO/ CISO/ PSO/ Owner • Stakeholder Analysts
Aviation Environment of Operation	• CSDS Operational Characteristics • CSDS & Network architecture design & data collection requirements	• OE Managers (IT, Engineering, Operations, etc.)
Interconnected Individual Systems	• Systems requirements • HW & SW Management • Sustainment limitations	• Engineers, IT, Ops Support Technicians • Standards WGs

Figure 8. Drivers and Primary Actors with respect to the CSDS AAF.

Aviation Ecosystem: This layer is primarily driven by International and National Policies set forth by governing bodies to ensure a safe and secure aviation environment. Examples of these include ICAO guidance, as well as the National Strategy for Aviation Security.

Aviation Domains: CSDS-specific regulations, guidance and oversight must be in place in this layer so that stakeholders implement CSDS correctly within their organizations. Primary actors at this layer are the Civil Aviation Authorities and National or Regional Airspace Operators.

Domain Stakeholders: The primary driver at this layer is starting the process and approving security business changes concerning CSDS. C-Suite leaders such as Chief Technology Officers and Chief Information Security Officers and the subservient organization owners must be able to approve and facilitate the development of CSDS programs/activities.

Environments of Operation: Each Environment of Operation will be responsible for the Design and Operations of its CSDS activities. Since each will have a unique structure, IT and OT Managers must design, implement, and operate CSDS consistent with the rest of the ecosystem.

Interconnected Individual Systems: Within IIS, Engineers must identify the networked operational elements and data-rich networks with respect to CSDS activities and implement methods for raw data collection. Technicians are responsible for the configuration of networked operational elements to support CSDS raw data acquisition activities and verify that the appropriate network traffic is being transmitted and the correct log files are being produced.

5.3 CSDS AAF Operational Scenario

The system components in the CSDS AAF Operational Scenario are interconnected to share cyber analytical data amongst Domain Stakeholders and develop real-time cyber threat intelligence capabilities. The AAF Operational Concept Diagram (Figure 9) shows the AAF structure for the connection of Domain Stakeholders and Multi-Domain CAC.

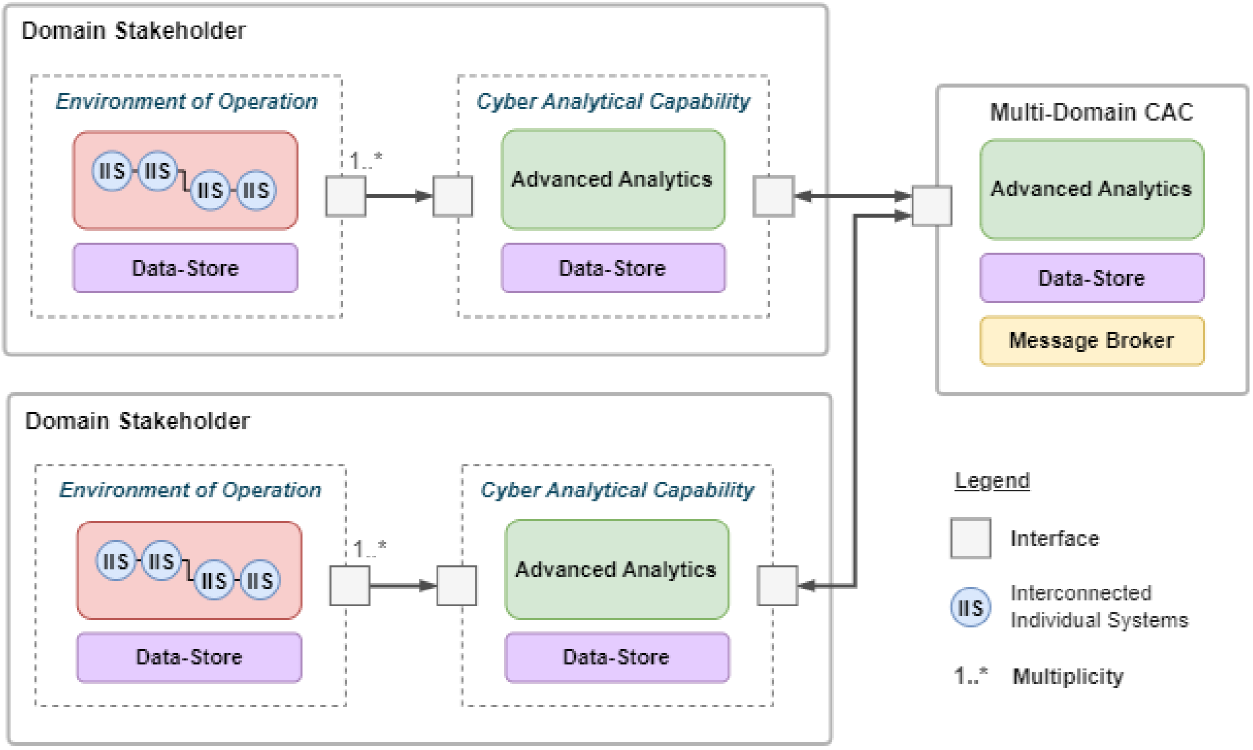


Figure 9. CSDS AAF Operational Concept Diagram.

CACs must work closely with the primary actors at the Environments of Operation layer to identify all Data-Store elements that make up the Data-Store and implement strategies to extract the right CSDS data. From a systems perspective, this would involve configuring/re-configuring the data acquisition sensors within IISs. Human Analysts and Data Scientists at CAC extract data from the Data-Store to conduct preliminary analysis on the data, and develop various analytical Tool Sets and AI/ML automation software that can perform real-time analytics.

The Data-Store is not a single system, but a collection of storage elements scattered throughout an environment of operation that each contributes to making up the Data-Store. The Data-Store will usually store sensitive and confidential data. This includes uniquely identifiable data that should be kept undisclosed within the Domain Stakeholder itself. Therefore, the AAF requires that no data shall be shared with external entities directly from the Data-Store but must instead always be shared through the CAC.

Figure 10 shows the Data Flow in the CSDS operational scenario with AAF systems, which encompasses all phases of the CSDS Data Life Cycle with an operational scenario focus. It also shows what phases are under the jurisdiction of a business's engineers or the CAC team.

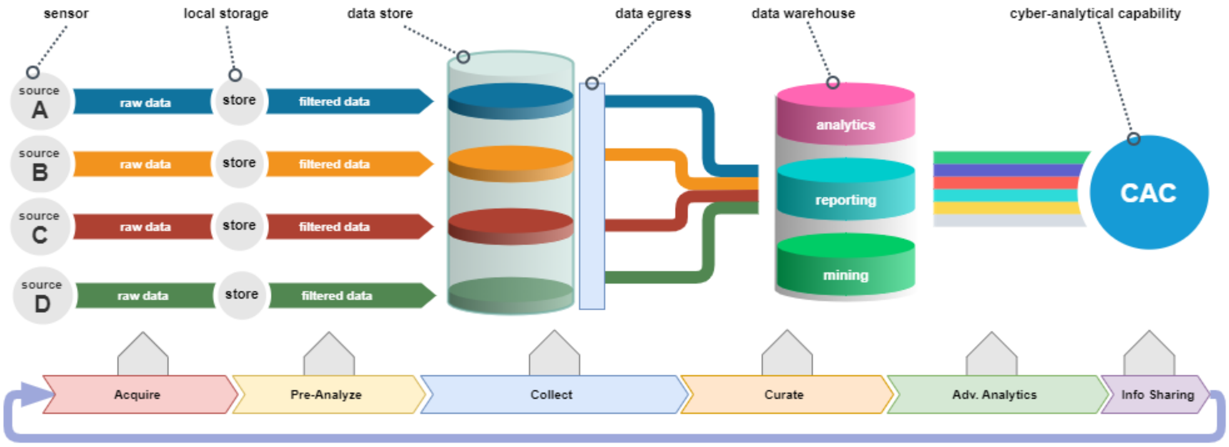


Figure 10. Data Flow and AAF Systems in CSDS Operational Concept.

The first phase of the data flow is the Acquire Phase, which is used to integrate/configure Data Acquisition Sensors into IISs so that processes running on those systems can be monitored and pre-analyzed.The Pre-Analysis Phase first uses a Data Type Detection process where Human Analysts or automated software try to determine the data type and execute a set of pre-analysis tasks. The Collect Phase aims at storing Data Sets in various Data-Store elements where they can be accessed by Human Analysts, Data Scientists and automated toolsets. AI/ML tools would be instrumental in managing the data across all the Data-Store elements.

The Curate Phase is the where the strategies are implemented to extract the Desired Relevant Data from the decentralized Data-Store elements. A data management strategy is required to organize the data and ensure that each piece of data is traceable back to a single origination point and system characteristics can be measured accurately over time. There are many opportunities for applying AI/ML, particularly data mining, to the Curation Phase.

The Advanced Analytics Phase uses Data Models generated from the curation process and generates cyber analytical information. This phase also provides visualization for executives, which may include comparison charts, maps, density plots, histograms, or network diagrams. Advanced Analytics may also generate security recommendations and alerts for analysts. The Information Sharing Phase uses cyber analytical information to create Shareable Artifacts. This is governed primarily based on information-sharing policies and regulations put in place by national regulators or the domain stakeholders themselves. Shareable Artifacts are also constrained by a specific specification that information must conform to be valid.

The results that have been generated throughout the CSDS AAF Data Life cycle will be stored in the Data Warehouse. The result artifacts may be owned by the domain stakeholder or come from other domain stakeholders and multi-domain CAC. Data warehouses shall be designed with resiliency and fault tolerance in mind to ensure data is not corrupted or lost. An example for the utilization of external domain stakeholder information is the comparative analysis of specific environments of operation. If a domain stakeholder can compare their operational metrics to the rest of the community, it may help to detect abnormal activity within their environment.

5.4 Practical Applications of CSDS AAF

CSDS AAF provides structure, key considerations, and criteria for applying CSDS methods to address the cybersecurity challenges through the development of practical aviation domain environment Use Cases. Use Cases represent the missions and goals associated with a Stakeholder's specific Environment of Operation. Use Cases will be used as the basis for implementing CSDS capabilities into the associated Environments of Operation.

The development process for a CSDS Use Case involves selecting and defining the Environment of Operation intended for applying, identifying Threat Scenarios, and documenting the Use Case in the context of CSDS AAF. This will need to include involving Stakeholders, locating available relevant data, identifying optimal Data Acquisition Sensor placement, and defining Data Extraction processes. Applying the CSDS AAF within a use case also includes identifying or considering requirements for Data-Store elements, CAC, Data Warehouses, and potential multi-domain CACs. A use case follows the lifecycle of the environment(s) of operation it describes, which includes the associated systems and/or products. This Use Case is the primary systems engineering tool for defining, verifying, and re-defining the CSDS requirements that need to be implemented within the target environment(s) of operation.

Figure 11 illustrates the high-level overview of the use case 5-stage lifecycle process as well as the primary activities that occur in each stage. This lifecycle shows how a use case lives for a long time as it gets implemented and continues to provide feedback over time through the Evaluate Effectiveness phase.

The Domain Stakeholders will either generate and lead their own business-specific CSDS Use Cases or participate in developing a general Community CSDS use case, possibly one being led by a multi-domain CAC. In either case, the structure of the generated CSDS use case document will be important. The documented use case needs to identify or define all relevant aspects of the AAF needed for CSDS methodology from the systems and the data architecture perspectives.

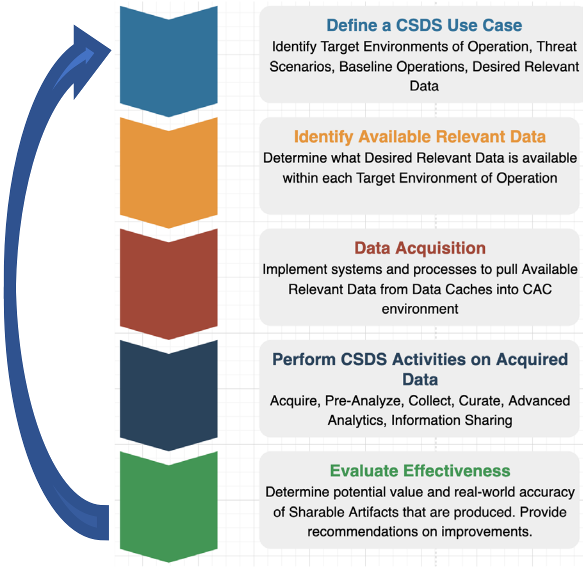

Define a CSDS Use Case
Identify Target Environments of Operation, Threat Scenarios, Baseline Operations, Desired Relevant Data
Identify Available Relevant Data
Determine what Desired Relevant Data is available within each Target Environment of Operation
Data Acquisition
Implement systems and processes to pull Available Relevant Data from Data Caches into CAC environment
Perform CSDS Activities on Acquired Data
Acquire, Pre-Analyze, Collect, Curate, Advanced Analytics, Information Sharing
Evaluate Effectiveness
Determine potential value and real-world accuracy of Sharable Artifacts that are produced. Provide recommendations on improvements.

Figure 11. CSDS AAF Use Case Lifecycle.

The generic use case development allows the aviation community to work together in a non-proprietary fashion to develop useful top-level use cases applicable to generic aviation environments of operation. This approach provides a representative environment of prototype value demonstrations, provides a technical basis for developing industry standards, and forms the core effort for Stakeholders to build off for developing detailed Use Cases of their specific internal proprietary implementations.

CSDS is a multi-disciplinary process to generate actionable insights from large and ever-increasing volumes of cybersecurity data. Therefore, Aircraft Original Equipment Manufacturer (OEM) presents a good example where CSDS would offer a comprehensive cybersecurity solution. Aircraft OEM is the source of aircraft components, and it is a factory setting in which many systems collaborate in the production of aircraft components. The organization of systems primarily consists of management, executive control, and physical hardware. It is a data-rich environment that includes factory floor level, PLCs, SCADA system, MES system, and ERP system. The utilized data ranges from sensor data carried through serial communication to business analytical data. Therefore, there is a large volume and variety in the collected data. Velocity of data is also especially high in the factory floor level due to real-time data usage.

Another important example of CSDS implementation can be the airport networks. An airport network involves multiple domain stakeholders. It is a data-rich environment with a large variety as it includes data from cloud infrastructure (OS system, virtualization, servers, firewalls), databases, on-premises hardware, software applications, network activities, mobile devices. Additionally, airports such as Warsaw airport in Hungary, Boryspil airport in Ukraine, Heathrow airport in UK, two (2) San Francisco airports, and the Seattle-Tacoma airport have been cyber-attack victims.

6 Expected Benefits and Industry Engagement Strategy

6.1 Anticipated Outcomes

The current cybersecurity challenges in aviation show the importance of the emerging opportunities for developing data science-based solutions and sharing experiences and lessons learned to address the significant cyber threats to the operational integrity of the aviation industry. Hence, the outcomes, such as sharable artifacts and use cases, will be valuable for the aviation stakeholders in working together to mitigate shared cyber risks. Another important outcome of the CSDS AAF will be the multi-domain CACs. Today, CACs mostly exist at the domain stakeholder level. However, multi-domain CACs will enable collaboration and drive new and integrated requirements to address the shared aviation community cyber risks. Working together with the aviation industry to develop key example use cases for the application of CSDS via the AAF will highlight the benefits it can provide.

CSDS AAF identifies two levels regarding the artifacts and use cases: community and stakeholder proprietary. Stakeholder proprietary is internal to a particular business and is specific to the stakeholder's respective internal proprietary system implementations. So, while two stakeholders in a specific domain may have very compatible systems and learn regarding CSDS, sharing proprietary details of those implementations is not practical as they are direct industry competitors. Therefore, the strategy is to engage via industry organizations such as AIA, CSCAT, and A-ISAC to work on domain-specific but operational environment generic use cases, which can inform the development of aviation industry CSDS guidance that each stakeholder can apply to their unique and proprietary implementations. This will include efforts to define aviation community sharable artifact guidance. The aviation community shared and collaborated artifacts between different stakeholders through organizations like A-ISAC, CSCAT, and nation-state Certs such as US DHS's CISA Central.

Stakeholders and multi-domain CACs will develop and maintain a collection of CSDS artifacts, both Stakeholder Proprietary and Community shareable artifacts. This includes potential use cases of interest that may be selected based on some prioritization method, such as a cost-benefit analysis. Each Use Case, either Community or Stakeholder Specific, defines required CSDS Artifacts for the specific environment of operation. As CACs define and produce artifacts associated with various use cases, it is envisioned that they will ensure that each artifact conforms to a particular CSDS artifact guidance. It is recognized that this research effort can only act as a catalyst in engaging the industry to begin CSDS guidance development. These guidance efforts are important as they provide the data governance required for effective collaboration within the business and across the aviation community. At a stakeholder proprietary level, these artifacts will be used to drive internal business decisions, whereas the community artifacts will be used to drive decisions at the multi-domain level.

It is essential to understand that a direct relationship is created only between a domain stakeholder CAC and the environments of operation. A multi-domain CAC may only use the shareable artifacts that domain stakeholders produce. In other words, shareable artifacts become the common communication channel among stakeholders. Thus, working with organizations like the A-ISAC to begin the creation of sharable artifact guidance materials will be a critical industry engagement for the CSDS efforts.

6.2 Expected Benefits

AAF will be beneficial for stakeholders to enhance proactive cyber defense as it enables the adaptation of select methodologies, integration of them into relevant operational environments and transfer of findings through shareable artifacts and use cases. CSDS AAF provides structure, key considerations, and criteria for applying CSDS methods to address the key cybersecurity challenges. This includes an aviation ecosystem taxonomy and reference model including conceptual elements, a systems perspective with a reference model and a data perspective. The scope and reference model of the framework are introduced in Section 3. The conceptual elements, data flow and use case development are introduced in Section 5. The detailed discussions of these are provided in “Part 2 CSDS AAF - Technical Definition” and “Part 3 CSDS AAF – Implementation Guidance.”

The CSDS AAF research will provide a catalyst for the aviation industry to pick up and leverage CSDS. This will support the ability to effectively communicate with industry stakeholders such as airlines, aircraft OEMs, and airports to facilitate FAA-industry CSDS AAF collaboration and standardization efforts. It is expected that other portions of the aviation ecosystem will also contribute to, and benefit from, the products of CSDS AAF. CSDS industry-wide guidance and recommendations will be the end goal of the FAA CSDS Program efforts.

As an initial step to understanding how the AAF and guidelines could be applied to the aviation ecosystem, Aircraft OEM Manufacturing Environment of Operations Use Case Area was executed at the Analytical Exercise (AE) held in February 2023. The AE was placed industry knowledgeable personnel into modeled situations of cyber events to identify potential design deficiencies and opportunities for refinement and enhancement of the Aviation Architecture Framework (AAF). The analytical exercise was beneficial for the pariticipants as it created an environment that prompted open and meaningful discussion in relation to the AAF and its supporting documentation. Many discussions focused on AI/ML and how it can be trained to handle the issues presented within the AE. AE also created discussion points around general CSDS topics such as the vulnerability of wireless networks and the importance of explainability in AI/ML applications. Additionally, most participants agreed that the event itself was a good use of their time and overall improved their understanding of the AAF and its related principles to some degree.

CSDS AAF is intended to be applied across multiple stakeholders and domains to share actionable data. Shareable artifacts will allow for faster collaboration and progress within the aviation community to accomplish mutual CSDS objectives. Traditionally, domain stakeholders would only have access to their data when doing data analytics. Shareable artifacts will allow domain stakeholders to work together and build on each other's progress to form a common body of knowledge. Domain stakeholders may not have the cyber capability to establish a full-fledged CSDS program. The Shareable artifacts concept is developed considering this fact and it allows stakeholders to share "what they can."

Some of the Shareable artifacts would include meaningful data sets that could be used to assess the utilization of data science in cybersecurity. The lack of meaningful data sets is one of current limitations of implementing data science in aviation cybersecurity as identified in Section 4.1.1.

The multi-domain collaboration requirement of the CSDS AAF will necessitate data governance, which is defined as "everything you do to ensure data is secure, private, accurate, available, and usable. It includes the actions people must take, the processes they must follow, and the technology that supports them throughout the data life cycle" (Google Cloud). For the purpose of the AAF, data governance is a crucial prerequisite for multi-domain collaboration. Hence, the definition of data governance concepts will be beneficial for both individual stakeholders and also for the whole aviation domain.

6.3 Industry Stakeholder Engagement

The industry stakeholder engagement has been conducted to identify multiple industry candidates from three specific elements of the aviation ecosystem for potential participation in CSDS research: Airlines, Airports, and Aircraft. The industry stakeholders mostly expressed an interest in working with the CSDS program through larger industry forums, which make it easier to collaborate by keeping the engagements focused on industry-wide issues and solutions that can be addressed in non-proprietary ways via open recommendations and standards. Three (3) key industry organizations were targeted initially for use case development engagement (AIA, A-ISAC, CSCAT), with each having certain value propositions:

- **Aerospace Industries Association (AIA) – Civil Aviation Cybersecurity Subcommittee:** AIA represents the interests of US Aerospace OEM community, leading the US Aerospace OEM position globally. AIA provides a single point of engagement to work together with all US based Aerospace OEMs that are dedicated and committed working specific topics of priority for the US Aerospace OEM community. The Aircraft OEM Factory Cybersecurity Use Case was the focus of ERAU Analytical Exercise, in which the OEM community via AIA has been a strong supporter. Thus, following the successful complete of the Aircraft OEM Factory Cybersecurity Use Case, there will be good potential to address one of the other high priority use cases areas of interest to the OEM Community
- **Aviation Information Analysis & Sharing Center (A-ISAC):** A-ISAC comprises aviation industry members and is the only international cyber-threat sharing organization providing aviation-specific threat information to the aviation community. A-ISAC provides a single point of engagement for a cross-section of the aviation cybersecurity community, including Aircraft OEMs, Airlines, and Airports. The A-ISAC area for CSDS engagement is focused on A-ISAC as a global cross-domain Cyber Analytical Capability (CAC) for the sharing and analysis of threat intelligence. Hence, Multi-Domain CAC is a suitable candidate for a CSDS Program Use Case to work on with A-ISAC.
- **Cyber Safety Commercial Aviation Team (CSCAT):** CSCAT provides a single point of engagement with a cross-section of key aviation stakeholders from both the aviation industry (primarily OEMs and Airlines) and government agencies (primarily within the FAA). Through engagements, CSCAT selected the " Aircraft SW Security Use Case." Following the successful complete of the SW Security Use Case, there will be good potential to address one of the other high-priority use cases on the CSCAT use case list.

The stakeholder engagements strategically have focused on building CSDS engagements with strong US-based industry organizations. Building on top of existing industry stakeholder relationships, the initial future plan is to build relationships with the airport and airline stakeholders such as Airlines For America (A4A), International Air Transport Association (IATA), Airports Council International (ACI) and Airports Council International - North America (ACI-NA), Daytona Beach International Airport (KDAB). The longer-term goal is to leverage the initial engagements into further US and international industry engagements. This specifically includes engaging with the A-ISAC to address the multi-domain stakeholder CAC use case, but also to build broader Airline and Airports contacts for future industry engagement.

The domain stakeholders have different amounts of technical capabilities, expertise, and workforce regarding CSDS and other parts of the AAF. Therefore, there are various ways or levels a domain stakeholder can participate in data and information sharing: 1) Share cyber-relevant data "as-is" that has been captured from Environments of Operation, 2) Share cyber-relevant data after it has been conformed, 3) Share cyber-relevant data after it has been modeled, 4) Share advanced analytical results on modeled data, 5)Share custom toolsets used to produce analytical results, 6) Share AI/ML algorithms developed to produce analytical results, 7) Share data mining results on modeled data.

7 References

American Psychological Association. (2009). *Publication manual of the American Psychological Association.* Washington, D.C.: American Psychological Association.

Cabridge Technical Communications. (2007). *The Zachman Enterprise Framework.* Retrieved January 2021, from technical-communicators.com: http://www.technical-communicators.com/articles/zachman_framework.pdf

Chandrasekaran, R., Payan,, A., Collins,, K., & Mavris, D. (2019). *A Survey of Wire Strike Prevention and Protection Technologies for Helicopters.* Technical Report, U.S. Department of Transportation, Federal Aviation Administration. Retrieved from http://actlibrary.tc.faa.gov

Chua, A. (2020). *Ransomware Attack hits ST Engineering's USA Aerospace Unit.* Retrieved from Flight Global: https://www.flightglobal.com/

Claburn, T. (2021). *Airline Software Super-Bug: Flight Loads Miscalculated Because Women Using 'Miss' Were Treated as Children.* Retrieved from The Register: https://www.theregister.com/2021/04/08/tuisoftwaremistake/

Cooper, P. (2017, November). *Aviation cybersecurity: Finding lift, minimizing drag.* Retrieved from Atlantic Council In-Depth Research Reports: https://www.atlanticcouncil.org/in-depth-research-reports/report/aviation-cybersecurity-finding-lift-minimizing-drag/

Corretjer, P. J. (2018). A Cybersecurity Analysis of Today's Commercial Aircrafts and Aviation Industry Systems. *Masters Thesis*.

Duchamp, H., Bayram, I., & Korhani, R. (2016). Cyber-Security, a new challenge for the aviation and automotive industries. *Seminar in Information Systems: Applied Cybersecurity Strategy for Managers.*

Embry-Riddle Aeronautical University Center for Aerospace Resilient Systems. (2024). *Part 1: Cybersecurity Data Science (CSDS) Aviation Architecture Framework (AAF) - Overview & Value Proposition.* Atlantic City, NJ: FAA NextGen Cybersecurity Data Science Project.

Embry-Riddle Aeronautical University Center for Aerospace Resilient Systems. (2024). *Part 2: Cybersecurity Data Science (CSDS) Aviation Architecture Framework (AAF) - Technical Definition.* Atlantic City, NJ: FAA NextGen Cybersecurity Data Science Project.

Embry-Riddle Aeronautical University Center for Aerospace Resilient Systems. (2024). *Part 3: Cybersecurity Data Science (CSDS) Aviation Architecture Framework (AAF) - Implementation Guidance.* Atlantic City, NJ: FAA NextGen Cybersecurity Data Science Project.

Embry-Riddle Aeronautical University Center for Aerospace Resilient Systems. (2024). *Part 4: Cybersecurity Data Science (CSDS) Aviation Architecture Framework (AAF) - Glossary & Acronyms.* Atlantic City, NJ: FAA NextGen Cybersecurity Data Science Project.

Garcia, A. B., Babiceanu, R. F., & Seker, R. (2021). Artificial Intelligence and Machine Learning Approaches for Aviation Cybersecurity: An Overview. *Integrated Communications Navigation and Surveillance Conference.* Institue of Electrical and Elecetronics Engineers Xplore.

Girgis, L. (2024, September 13). Sea-Tac Airport cyberattack caused by global ransomware gang, Port says. *Seattle Times*.

Google Cloud. (n.d.). *What is Data Governance.* Retrieved 2022, from cloud.google.com: https://cloud.google.com/learn/what-is-data-governance

Goud, N. (2019). *Ransomware Attack on Albany Airport on Christmas 2019https://www.cybersecurity-inside.* Retrieved from Cybersecurity Inside: https://www.cybersecurity-inside.com

Hamutcu, U. F. (2020, June 30). *Toward Foundations for Data Science and Analytics: A Knowledge Framework for Professional Standards.* Retrieved March 2021, from hdrs.mitpress.edu: https://hdsr.mitpress.mit.edu/pub/6wx0qmkl/release/3

ISO. (2015, May). *Systems and software engineering — System life cycle processes.* Retrieved March 2022, from iso.org: https://www.iso.org/standard/63711.html#:~:text=ISO%2FIEC%2FIEEE%2015288%3A2015%20establishes%20a%20common%20framework,hierarchy%20of%20a%20system's%20structure

Kagalwalla, N., & Churi, P. P. (2019). Cybersecurity in aviation: An intrinsic review. *International Conference On Computing, Communication, Control And Automation (ICCUBEA)* (pp. 1-6). IEEE.

Kessler, G., & Craiger, J. (2018). *Aviation Cybersecurity: An Overview.* Retrieved from https://commons.erau.edu/ntas/2018

Kochhar, S., & Friedell, M. (1990). User control in cooperative computer-aided design. *UIST '90: Proceedings of the 3rd annual ACM SIGGRAPH symposium on user interface software and technology* (pp. 143-151). ACM. doi:https://doi.org/110.11445/97924.9794

Koroniotis, N., Moustafa, N., Schiliro, F., Gauravaram, P., & Janicke, H. (2020). A Holistic Review of Cybersecurity and Reliability Perspectives in Smart Airports. *IEEE Access 2020, 8*, 209802–209834.

Lehto, M. (2020). Cyber security in aviation, maritime and automotive. *Computation and Big Data for Transport*, 19-32.

Mahmoud, M., Larrieu, N., Pirovano, A., & Varet, A. (2010). An adaptive security architecture for future aircraft communications. In. *Proceedings of the 29th Digital Avionics Systems Conference* (pp. 3.E.2-1–3.E.2-16.). Salt Lake City, UT, USA: IEEE.

Mongeau, S. (2021, September). *Cybersecurity Data Science (CSDS): Emerging Trends.* Retrieved January 2022, from Resources.sei.cmu.edu: https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=739704

Mongeau, S. A. (2021). *Cybersecurity Data Science.* Springer International Publishing.

Monteagudo, J. (2022). *Aviation Cyber Security – Major Challenges.* Retrieved from Aviation Cyber Security – High Level Analysis, Major Challenges and Where the Industry is Heading: https://cyberstartupobservatory.com/aviation-cyber-security-major-challenges/

Morrison, S. (2021, June 10). *Ransomware Attack Hits Another Massive, Crucial Indistry: Meat.* (VOX) Retrieved January 2021, from Vox.com: https://www.vox.com/recode/2021/6/1/22463179/jbs-foods-ransomware-attack-meat-hackers

NIST Computer Security Resource Center. (n.d.). *CSRC: Environment of Operation.* Retrieved January 2021, from csrc.nist.gov: https://csrc.nist.gov/glossary/term/environment_of_operation

Nobles, C., Burrell, D., & Waller, T. (2022). The Need for a Global Aviation Cybersecurity Defense Policy. *Land Forces Academy Review, 27*(1), 19-26.

Pols, P. (n.d.). *The Unified Kill Chain.* Retrieved from https://www.unifiedkillchain.com/

Pols, P. (n.d.). *The Unified Kill Chain*. Retrieved from https://www.unifiedkillchain.com/

Raza, M. (2020, March 27). *TOGAF vs Zachman: What's The Difference?* Retrieved February 2021, from bmc.com: https://www.bmc.com/blogs/togaf-vs-zachman/

Russon, M.-A. (2021, May 10). *US fuel pipeline hackers 'didn't mean to create problems'*. (BBC) Retrieved 2021, from BBC.com: https://www.bbc.com/news/business-57050690

Sampigethaya, K., Poovendran, R., & Bushnell, L. (2008). Secure operation, control, and maintenance of future e-enabled airplanes. *Proc. IEEE., 96*, 1992–2007.

Scruton, R. (n.d.). The eclipse of listening. *The New Criterion, 15*(3), 5-13.

Shimeall, T. (2021). *Cybersecurity Data Science Best Practices in an Emerging Profession.* Cham: Springer Nature Switzerland AG.

Singer, W. (2007). *The Origins and Purpose of the Zachman Enterprise Framework.* Cambridge, UK: Cambridge Technical Communicators. Retrieved from http://www.tud.ttu.ee/material/enn/IDU0080_2011/12ProcessMeasurement/zachman_framework.pdf.

Souppaya, K. K. (2006, September). *Guide to Computer Security Log Management.* Retrieved December 2021, from csrc.nist.rip: https://csrc.nist.rip/library/NIST%20SP%20800-092%20Guide%20to%20Computer%20Security%20Log%20Management,%202006-09.pdf

Strunk, W., & White, E. B. (1979). *The Elements of Style* (Third ed.). New York, New York, USA: Macmillan Publishing Co., Inc.

TCNJ Information Security Program. (n.d.). *Information Security Roles & Responsibilities.* Retrieved 2022, from security.tcnj.edu: https://security.tcnj.edu/program/security-responsibilities/third-party-system-administrator-guidelines/

Team, N. (2019). *Cryptocurrency Miners Infected More than 50% of the European AirportWorkstations.* Retrieved from Cyberdefense Magazine: https://www.cyberdefensemagazine.com/cryptocurrency-miners-infected-more-than-50-of-the-european-airport-workstations/

Techopedia. (n.d.). *Data Ownership.* Retrieved March 2021, from techopedia.com: https://www.techopedia.com/definition/29059/data-ownership

The Open Group Architecture Framework Version 8.1.1, Enterprise Edition. (2006, August). *ADM and the Zachman Framework.* Retrieved January 2021, from pubs.opengroup.org: https://pubs.opengroup.org/architecture/togaf8-doc/arch/chap39.html

Torres, P. (2021, January 16). *Data Science for Cyber Security.* Retrieved March 2021, from medium.com: https://medium.com/codex/data-science-for-cyber-security-32e2f81e15d3

Ukwandu, E., Ben-Farah, M. A., Hindy, H., Bures, M., Atkinson, R., Tachtatzis, C., . . . Bellekens, X. (2022). Cyber-security challenges in aviation industry: a review of current and future trends. *Information*(13), 146-167.

Vicens, A. (2024, May 8). Boeing confirms attempted $200 million ransomware extortion attempt. *Cyberscoop*.

Welsh, W. (2013). *Phishing Scam Targeted 75 US Airports.* Retrieved from Information Week: https://www.informationweek.com/?1

Wolf, M., Minzlaff, M., & Moser, M. (2014). Information technology security threats to modern e-enabled aircraft: A cautionary note. *J. Aerosp. Inf. Syst., 11*, 447–457.

Zachman, J. A. (2008). *The Concise Definition of The Zachman Framework by: John A. Zachman* . (J. A. Zachman, Producer, & Zachman International, Inc.) Retrieved 2021, from Zachman: https://www.zachman.com/about-the-zachman-framework

Zamorano, M., Fernández-Laso, M., & de Esteban Curiel, J. (2020). Smart Airports: Acceptance of Technology by Passengers. *Cuad. Tur., 45*, 567–570.