Developing a Cybersecurity Architecture for Extensible Traffic Management (xTM)

Terrence D Lewis[1]
NASA Ames Research Center, Moffett Field, CA 94035

Hassan Ali[2]
Science & Technology Corporation, Moffett Field, CA 94035

Kenneth Freeman[3]
NASA Ames Research Center, Moffett Field, CA 94035

This paper explores the development of a cybersecurity architecture tailored for Extensible Traffic Management (xTM) to address emerging challenges in managing diverse aerial vehicles within the National Airspace System (NAS). Driven by technological advances and the rise of uncrewed aerial systems (UAS), urban air mobility (UAM), and high-altitude traffic (ETM), the NAS is undergoing a paradigm shift. Traditional air traffic management, reliant on traditional Federal Aviation Administration (FAA) control, will give way to decentralized coordination among autonomous and semi-autonomous systems. The proposed xTM Security Architecture, designed as a high-level framework, focuses on ensuring the confidentiality, integrity, and availability of data and operations in this evolving ecosystem. Utilizing threat modeling, the research identifies potential risks across key flight phases, operations and use cases to offer security control recommendations. Key objectives include analyzing interactions between novel airspace entrants and existing NAS traffic, cataloging vulnerabilities, and developing mitigative strategies to ensure safety, operational stability, and secure data exchanges. This research lays the groundwork for regulatory and industry adaptation, providing critical insights into managing cybersecurity risks in this complex, multi-domain environment.

[1] IT Specialist, Secure Airspace Technology Group, Aeronautics Projects Office, NASA Ames Research Center
[2] Security Architect, Science & Technology Corporation
[3] Lead, Secure Airspace Technology Group, Aeronautics Projects Office, NASA Ames Research Center

I. Introduction

A. Background

In the not-too-distant future, the skies above us will look vastly different than they do now. More specifically, the change will occur with the traffic that makes up the National Airspace System (NAS); consequently, the cybersecurity that protects it must change too. Currently, the bulk of the NAS is made up of crewed traditional fixed wing aircraft and rotorcraft, from both the public and private sectors. Technology has allowed for the proliferation of cheaper and more advanced methods of flying vehicles, this in combination with the expanse and prevalence of aircraft that were traditionally utilized by governments becoming more readily available to private industry, is contributing to creating a new economy. This new economy will attract new entrants and create a paradigm shift in the way air traffic is utilized both in function and its makeup. Part of how this environment will change will be the types of vehicles that people will see and use. Some of these vehicles will take the form of an uncrewed aerial system (UAS), also known as drones, changing how people interact with businesses in their everyday life. The planned increased usage of these aircraft is also being born out of the fact that modern roadways are increasingly becoming denser and more congested, causing increased wait times and bottlenecks with the movement of people, goods, and services. To alleviate this, UASs have the expected interactions and changes with the public, initially through two main methods - drone package delivery and Urban Air Mobility (UAM) or air taxis. With UAM being a concept that proposes to develop short-range, point-to-point transportation systems in metropolitan areas using vertical takeoff and landing (VTOL) or short takeoff and landing (STOL) [1]. Additionally, Upper Class E airspace operations have historically been limited due to the challenges conventional fixed wing aircraft face. These challenges include reduced atmospheric density in the upper stratosphere and mesosphere. Recent advances in technologies, however, relating to power and propulsion, aircraft structures, flight automation, and aerodynamics have led to an increase in the number of vehicles that can operate in low atmospheric density airspace [2]. Each of these new vehicle interactions will transform how traditional airspace operates.

B. Operating Environment

Currently traditional aircraft, unless under certain areas or classes of airspace, communicate with a Federal Aviation Administration (FAA) air traffic controller (ATC) for various permissions and directions the entire time the aircraft is operated. Under this future environment, UAM vehicles and various UASs, unless under special circumstances within specific FAA controlled airspaces i.e., in and around airports, are expected to not have direct communication with FAA ATC. This lack or limited communication with the FAA brings with it the entrance of third-party services that will supplement this coordination - further discussed below. To add to this new air traffic model, in addition to the other vehicles that will be flying (mentioned above), a lesser used portion of the NAS which operates above the traditional commercial airspace (60,000 ft above ground level and above), one that is currently mainly used for military and weather services, is planned to be more readily utilized [2]. This airspace has the intended function of accommodating a new generation of high-altitude aircraft meant to efficiently satisfy research objectives, demands for broad coverage services, and supersonic passenger flight [3]. While each of these components already pose a clear challenge for coordination efforts, the difficulty compounds with the fact that all of these different and novel aircraft will be flying amongst each other. Consequently, it reveals the desperate need for these vehicles to be able to coordinate amongst each other. Given this need for coordination and the fact that it will be done mostly in absence of FAA ATC coordination, NASA has decided to research this emerging area with two major objectives, each converging to the understanding of interactions with traditional airspace traffic. One of the objectives involves developing and testing cooperative operating practices aimed at studying conflict and flow management of air traffic. The second objective is to identify requirements for a secure digital integrated operational picture that supports diverse and increasingly autonomous operations. Taken altogether, the novel vehicle concepts described above can be divided into three traffic management categories. Package delivery drones or UAS, is to be categorized as Unmanned Aircraft System Traffic Management (UTM) that is 400 ft above ground level (AGL) and below [4]; VTOL and similar “air taxi” type aircraft designed to fly over urban centers is categorized as Urban Air Mobility (UAM) that is up to 4,000 ft AGL [5]; and lastly Upper Class E Traffic Management (ETM) that is 60,000 ft AGL and above. With traditional airspace operations sandwiched between the UAM and ETM operating environments. When referring to these three environments, the term Extensible Traffic Management (xTM) is used for the overarching term of traffic management approaches and/or associated services that address the operation of select new entrants within flexibly allocated, designated airspace [6]. To illustrate the connectedness of xTM and its various entities and actors, figure 1 provides a high-level architecture of a potential xTM environment.

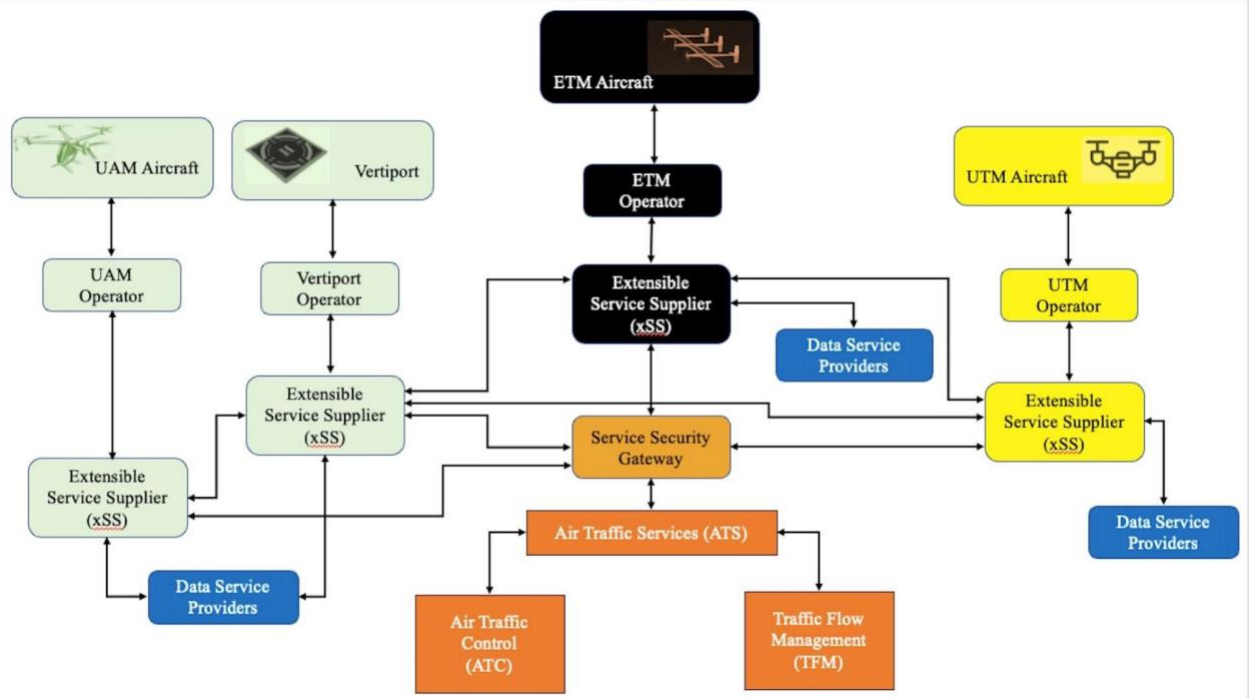

Fig. 1 Notional xTM Architecture

The elements highlighted in orange in the lower part of Figure 1 represent FAA-managed air traffic services. These services, known as Air Traffic Services (ATS), include Air Traffic Control (ATC) and Traffic Flow Management (TFM). ATC oversees traffic around airports as well as in the terminal and enroute airspace connecting them. TFM is a collaborative process designed to plan air traffic flow and prevent airport capacity from being exceeded. Additionally, the Service Security Gateway serves as an interface between the FAA and external xTM entities, ensuring that xTM stakeholders do not have direct access to FAA systems and data [7].

A new Air Traffic Management (ATM) architecture that utilizes industry's ability to supply industry-developed, third-party services that work complementarity with the FAA provided Air Traffic Service (ATS) to exchange relevant air vehicle information among the UAS operations and between the UTM systems and the conventional ATM system has been introduced. Following the success and early adoption of UTM architecture, the foundational UTM requirements and core properties were generalized to become Extensible Traffic Management (xTM) requirements to support operations of new entrants beyond small UAS, such as operations in high altitudes in upper-Class E in the United States National Airspace System (NAS) [8]. The core properties from the UTM architecture includes the concepts of service suppliers and third-party services for xTM. The architecture, in Figure 1, reflects the UAM domain, in addition to UTM and ETM. In these three domains, vehicle operators leverage service suppliers for operation planning, which allows for flight intents to be compared with others to avoid conflict. For UTM, these service suppliers are referred to as UTM service suppliers (USS). ETM refers to them as ETM service suppliers (ESS). And UAM refers to them as providers of service for UAM (PSU). Data such as vehicle surveillance, discovery and synchronization service (DSS), weather and terrestrial obstacle locations, is furnished by the Supplemental Data Service Providers (SDSP) to support xTM operators and service suppliers. This supplemental information is auxiliary to the data provided by the FAA's NAS.

II. Goals and Objectives

Since the cyber threat landscape changes daily, cybersecurity awareness and cyber threat mitigation must be systemic to the emerging xTM environments and a continuous presence in all its stakeholders and participants. To realize the potential of UAM, UTM and ETM, an assurance of cybersecurity is critical for public acceptance [9]. Through the lenses of the notional xTM Architecture (Figure 1), the goal of this paper is to provide a security architecture to establish a high-level framework that uses a combination of cybersecurity principles and methods to protect xTM operators, service suppliers or service providers' assets from cyber threats. By decoupling design from execution, the goal of outlining an architecture is to provide flexibility, scalability and adaptability, enabling future

implementers to select and implement the most effective solutions within a consistent, secure framework. The objectives of this paper are to (1) present key cybersecurity concepts and definitions applicable to xTM, (2) present an xTM ecosystem risk analysis, with associated assumptions and (3) provide a set of foundational security controls that can be leveraged to secure an xTM ecosystem.

III. Key Concepts, Definitions & Assumptions

To start, a distinction and understanding should be made between that of a threat, vulnerability, risk incident and mitigative control.

Fig. 2 Threat, Vulnerability & Risk Cycle

A threat can best be defined as a circumstance or event that has the potential to cause an unwanted incident that may result in harm to a system or organization [10]. In the cybersecurity sense, for instance, this could be intentional (malicious) being a "hacker" or unintentional errors. A vulnerability is a weakness in a system that can be exploited by a threat to cause damage or perform unauthorized actions [11]. Continuing with looking at this through the lens of cybersecurity; an example of this would be a piece of software that contains security flaws that have not been patched yet. A risk can be defined as the potential for loss or damage when a threat exploits a vulnerability, evaluated in terms of likelihood and impact [12]. For example, a hacker can utilize a software flaw and gain access to a company's system. The risk would be understanding which system and how much the exposure of that information would be impactful or hurtful to the company and/or its customers. A security incident is a compromise in a system's confidentiality, integrity and/or availability and is the actual event that has happened vs a risk is the potential [13]. Finally, a mitigative control seeks to provide actions or steps to take to minimize impact of risk.

To aid with identifying the threats and vulnerabilities and outlining the risks therein, the research team needed to lay out a format for representing these for the xTM environment. To do this, a security analysis of the xTM environment was designed, captured and outlined into a security architecture. This security architecture design differs from a traditional security architecture in that it resides between high-level generality and technical specificity. With the overall intent from the research team to be less prescriptive of specific technologies and actions and instead to more generally identify possible security holes through the lens of the xTM environment and its interactions.

As the research team developed the security architecture in understanding the risks that were involved with each component of the xTM environment, the weight of these risks needed to be put in a format to show a level of importance and overall impact to the xTM environment. Because not all risks are weighted evenly, they need to be quantified. Not only was there a need to quantify the risk but this in accordance with the impact needed some sort of rating or assessment of possible impact. In figure 2 a risk assessment matrix can be found. This matrix that was used was an adaptation of the International Civilian Aviation Organization (ICAO)/FAA Safety Management System (SMS) for Risk Assessment [14]. Further modifications to the matrix also included additional adaptations from work that Philadelphia International Airport (PHL) had done looking at SMS for risk assessment [15].

Severity / Likelihood	Minimal 5	Minor 4	Major 3	Hazardous 2	Catastrophic 1
Frequent A					
Probable B					
Remote – C					
Extremely Remote - D					
Extremely Improbable - E					

Fig. 3 Risk Assessment Matrix

Figures 4a & 4b show the breakdown of severity and probability used with severity utilizing FAA Airport Internal Order 5200.11 [16]. This order describes the roles and responsibilities of FAA's office of Airports (ARP) management and staff as well as other lines of business that will contribute to the ARP SMS. SMS helps ARP identify and address safety issues before they become hazards or accidents. It should be noted that ARP will not be the only FAA office to oversee xTM actions and instead was used by the research team as a reference. This utilizes the following indices:

A) How many injuries could occur or lives lost?
B) What is the environmental impact?
C) What is the impact of the property or financial damage?
D) What operational closures or constraints could occur?
E) What are the likely political implications and/or media interest?

Figure 4b incorporates ICAO's Safety Management Manual (SMM) in column 3 which is defined in their safety risk probability table (this is inverted from the matrix). The first column, described by *likelihood,* details the frequency that a vehicle will possibly experience this risk with the actual number or probable occurrences. An assumption was made with the *likelihood* column with the number of specifically with the number of vehicles. Due to the fact that UTM, UAM and ETM vehicles are not readily on the market the actual numbers for likelihood were assumed based on FAA numbers of traditional aircraft. The severity is broken down based on the possible impact to aircraft, any injury to passengers/workers or airport/surrounding facilities or equipment, and further impacts to operations - these details are outlined in figures 4a & 4b.

The intersection of severity and likelihood allowed the team to then do grouping of acceptance – demonstrated by the colors categorizations as defined as the following: Green: This safety risk acceptable without restriction or limitation; hazards are not required to be actively managed but must be documented. Yellow: these risks are acceptable with mitigation – This safety risk is acceptable; however, documentation, tracking, monitoring, and management are required. Red: This safety risk is either unacceptable or short-term acceptable. If it is simply not acceptable then it cannot be accepted by any level of management until it has been mitigated to an acceptable level. If it is short-term acceptable - This safety risk is higher than would have been initially acceptable but is allowed to exist while new safety risk controls are developed and implemented. Each of the two sections has either an alpha or numeric value associated with it. The final "risk score" is attributed to the combination of these two scores and when placed on the matrix it is accompanied by the risk color.

Value	Severity	FAA ARP Internal Order 5200.11
A	CATASTROPHIC	- Complete loss of aircraft and/or facilities or fatal injury in passenger(s)/worker(s); - or Complete unplanned airport closure and destruction of critical facilities; or - Airport facilities and equipment destroyed
B	HAZARDOUS	- Severe damage to aircraft and/or serious injury to passenger(s)/worker(s); or - Complete unplanned airport closure, or - Major unplanned operations limitations (i.e. runway closure), or - Major airport damage to equipment and facilities
C	MAJOR	- Major damage to aircraft and/or minor injury to passenger(s)/worker(s), or - Major unplanned disruption to airport operations, or - Serious incident, or - Deduction on the airport's ability to deal with adverse conditions
D	MINOR	- Minimal damage to aircraft or - Minor injury to passengers, or - Minimal unplanned airport operations limitations (i.e. taxiway closure), or - Minor incident involving the use of airport emergency procedures
E	NEGLIGIBLE	No damage to aircraft but minimal injury or discomfort of little risk to passenger(s) or workers

Fig. 4a Severity Categorization

Value	Probability	ICAO SMM	FAA ARP Internal Order 5200.11
1	EXTREMELY IMPROBABLE	Almost inconceivable that the event will occur	Expected to occur < every 100 years
2	IMPROBABLE/ Extremely Remote	Very unlikely to occur (not known to have occurred)	Expected to occur once every 10-100 years or 25 million departures, whichever occurs sooner
3	REMOTE	Unlikely to occur, but possible (has occurred rarely)	Expected to occur about once every year or 2.5 million departures, whichever occurs sooner
4	OCCASIONAL	Likely to occur sometimes (has occurred infrequently)	Expected to occur about once every month or 250,000 departures, whichever occurs sooner
5	FREQUENT	Likely to occur many times (has occurred frequently)	Expected to occur more than once per week or every 2500 departures, whichever occurs sooner

Fig. 4b Probability Categorization

The research team studied the xTM environments to understand where commonalities and differences may exist for flight operations. To be able to properly study the flow of information and any possible security flaws therein, there was a need to decompose and understand, from an operational perspective, how a vehicle flies. To do this a standard flight was broken into five separate phases. These phases were derived through interviewing a former FAA air traffic controller. This allowed the research team to gain real-world understanding of how flights are broken up and in doing so be able to conduct a better analysis. These phases of flight, as defined below, were combined with an understanding of the xTM environment yielding the below phases of flight:

1. Pre-flight
2. Departure Phase
3. Enroute
4. Arrival
5. Post flight

This will be outlined further down in the paper, but the research team outlined and defined the users, operators and service suppliers, or as expressed here - "actors" as well as outlining use cases. These actors were pulled from the xTM understanding and combined with the use cases. The phases of flight as mentioned above, were used to reach common themes of flight actions and maneuvers that were shared across UTM, UAM and ETM. These commonalities were taken at a high level and used to aid with the development of use cases. The use cases were developed as most likely scenarios that would happen during vehicle operations should a security incident were to occur and worked to define all interactions in the system. The use cases include operations intent, identity services and replanning for operators, two (Identity Service, Ops Intent) of these falls in the pre-flight phase and one (Replanning) in the enroute phase. Through the lens of the different phases of flight, superimposed with actors these use cases yielded a foundation for the team's analysis. Given now that there is a system which constraints can be bound and the operating structure of the xTM environment is defined. Once that had been defined a security analysis could then be conducted. To efficiently breakdown and study possible security flaws throughout, a threat model analysis was to be conducted. The

research team opted to leverage STRIDE as the base threat modeling technique. STRIDE was selected as the threat modeling technique due to its structured and comprehensive approach, which aligns well with identifying and categorizing the broad range of security threats relevant to xTM's complex environment. STRIDE systematically addresses common threat categories—Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege—each of which is crucial for understanding potential risks in a distributed system like xTM. By categorizing threats across these dimensions, STRIDE enables a detailed analysis of how specific vulnerabilities might compromise critical aspects such as confidentiality, integrity, and availability. Additionally, STRIDE's straightforward framework allows for consistent identification of risks and actionable insights across multiple use cases, ensuring a robust foundation for designing effective, targeted security controls.

Threat Category	Violates	Examples
Spoofing	Authenticity	Threat action aimed at accessing and use of another user's credentials, such as username and password
Tampering	Integrity	Threat action intending to maliciously change or modify persistent data, such as records in a database, and the alteration of data in transit between two computers over an open network, such as the Internet
Repudiation	Non-Repudiability	Threat action aimed at performing prohibited operations in a system that lacks the ability to trace the operations
Information Disclosure	Confidentiality	Threat action intending to read a file that one was not granted access to, or to read data in transit
Denial of Service	Availability	Threat action attempting to deny access to valid users, such as by making a web server temporarily unavailable or unusable
Elevation of Privileges	Authorization	Threat action intending to gain privileged access to resources in order to gain unauthorized access to information or to compromise a system

Fig. 5 STRIDE Categorization [17]

As mentioned previously, the research team had to make assumptions in understanding how to go about the security analysis. Given the complexities that are inherent within an architecture such as this the level of detail that this work could go into is vast. As such, there were various assumptions made in tackling the challenge of outlining possible security flaws within the xTM environment. The assumptions listed will include scope, audience and foundational understating of the environment. Further, many of these concepts are future oriented and focused so the exact landscape and implementation is still being developed and as a result uncertain.

When seeking to develop and design the security architecture the team wanted to keep the document to a high enough level where it was agnostic to the environment i.e., UTM, UAM or ETM and to instead highlight what was common across each operating environment.

Assumptions:

- When looking at the xTM architecture in figure 1 a vertiport is listed - ground operations were excluded from this analysis
- The phases of flight were based off traditional flight profiles
- The FAA's security gateway and systems were out of scope
- In the event a vehicle enters controlled airspace that would be in and around an airport, it is assumed that there will be some direct communication between ATC and the XSS
- Throughout the analysis there are security control recommendations that are made for a singular actor or entity within the xTM architecture. However, there may exist different permutations that would be applicable in other scenarios or use cases. In an effort for concision, these are not all listed. With the assumption that duplicates do not help identify new classes of vulnerabilities or identify classes of control

- The recommended security controls for risk mitigation below are not stated for all scenarios to minimize redundancy
- There was no assumption that the DSS would be available across xTM domains
- For each risk scenario a worst case selected where for each of the risk categorization is collision, no matter the operating environment
- When referencing logging - FAA collection and storage requirements were cited [18]
- For the connection "Public" outlined in the UAM ConOps [7] the team opted towards merging public and public safety organizations
- There will be a set of trusted identity providers that will provide authentication services for actors per domain
- There exists a communications and internet network for actors to communicate over
- Ability for actors to log and store events and decisions
- Actors have the ability to respond to inquiries

Out of Scope:

- Specific protocols, ports or specific technology recommendations for mitigation
- What happens in the event of failure of deconfliction e.g., no PSU gives/agrees to a new flight path
- The method or technology utilized by which a vehicle receives its flight plan
- Approval of flight plan process
- Service Level Agreements for response – ability to take action, for listening and processing, how long you can wait
- Specific governance of systems
- Giving specific examples as that will require making beyond necessary assumptions about future system implementation

IV. Security Architecture: Use Cases, Risk Analysis & Control Recommendations

In defining the security architecture for xTM, our approach is centered on safeguarding the **Confidentiality, Integrity, and Availability** (CIA triad) of xTM's vehicles, services and operators. Our strategy is methodical and phased, ensuring each element of the architecture aligns with these foundational principles of information security.

The process begins with *Scope Definition*, where we utilize the Concept of Operations (ConOps) as the baseline. This phase involves comprehensive data gathering across various phases of flight and applicable use cases. These use cases are instrumental in delineating the scope for subsequent assessments, forming a structured foundation that guides threat modeling and subsequent risk analysis.

Next, we proceed to the *Risk Assessment* phase, in which we systematically identify and evaluate potential security threats and vulnerabilities that could compromise the CIA of the xTM system. Using threat modeling on the defined use cases, we examine how specific threats and vulnerabilities could impact the system. This process results in a detailed catalog of risks, each categorized to offer a clear view of the system's exposure and resilience.

The final phase, *Security Architecture Design*, involves specifying and prioritizing the necessary controls to address the identified risks. Here, we classify the controls and assess their effectiveness, ensuring that each critical and high-level risk is mitigated through layered security measures. These controls, aligned with the CIA triad, form a robust security framework, safeguarding xTM's operational integrity across all phases.

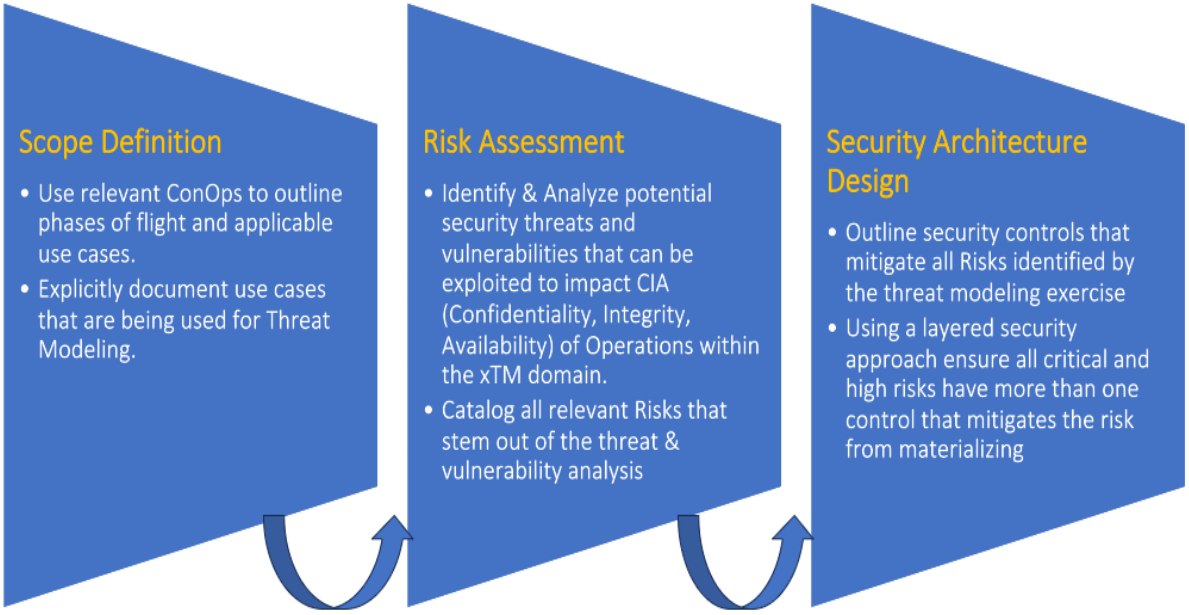

Fig. 6 Scope, Assessment & Design Breakdown

A. Use Cases & Risk Analysis

The security architecture for xTM is built upon targeted threat modeling and risk analysis of three core use cases, most commonly used: *Identity Service*, *Operations Intent*, and *Replanning*. These use cases were selected to serve as the foundation for security control recommendations, given their critical role in ensuring secure interactions and coverage of operations within xTM.

Each use case is carefully analyzed to identify potential vulnerabilities and assess the impact should these vulnerabilities be exploited. By systematically evaluating these use cases for severity and likelihood of risk, we prioritize controls to address the most significant threats, ensuring the confidentiality, integrity, and availability of critical xTM operations.

1. Identity Service

This use case focuses on ensuring that each entity within the xTM environment—such as vehicles, operators, and services—can authenticate securely and reliably. This use case involves the management and verification of digital identities to establish trusted communication between entities, preventing unauthorized access and impersonation. The Identity Service is a foundational trust layer that is essential for safeguarding sensitive interactions and enabling secure, seamless coordination across the xTM ecosystem.

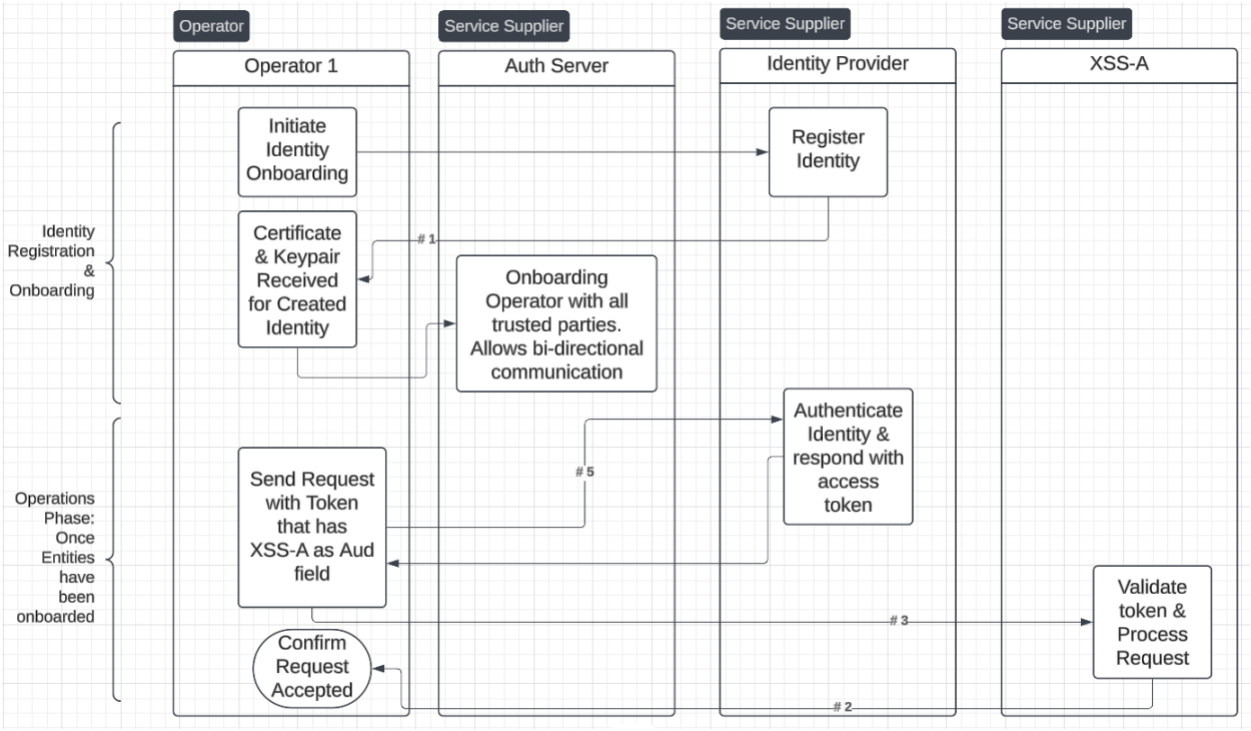

Fig. 7a Identity Service Diagram

The table below captures the outcome of threat modeling, risk analysis performed on the threats and vulnerabilities and control mitigations recommended to mitigate the Risks identified for the Identity Service. The class of controls and frameworks will reference the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) [19] and the Center for Internet Security (CIS) framework [20].

ID	Context	Threat & Vulnerability	Impact & Risk Analysis	Risk Score	Mitigative & Compensating Controls	Class of Controls & Frameworks
1	Operator-1 insecurely stores the certs & credentials for communications to other entities, an attacker compromises the certificate to impersonate the identity of Operator1	An attacker gets unauthorized access to identity certificate exploiting insecure storage of credentials and is able to authenticate with the Identity service as Operator-1	XSS-A receives a request from the attacker that is impersonating Operator-1, this allows the attacker to execute any number of actions such as changing flight path registered with DSS, potentially causing a scenario where two vehicles are put on a collision path.	Sev1 / Red (Hazardous * Remote) C2	Secure storage of credentials & certificates (including physical security controls)	1. Credential Management 2. Physical Security Framework References: - **NIST CSF PR.AC-5**: Access permissions are managed, incorporating secure storage. - **CIS Control 16.4**: Protect credentials with encryption.

2	XSS-A communicates with Operator-1 over an insecure communications channel, an attacker captures the insecure traffic to get access to token	An attacker gets unauthorized access to access token exploiting insecure transmission of token and can send requests to DSS pretending to be XSS-1	DSS receives a request to update flight plan for its vehicles by an attacker that has assumed the identity of XSS-A, potentially causing a scenario where two vehicles are on a collision path.	Sev1 / Red (Hazardous * Remote) C2	Transmission of requests over a secure communications channel	Secure communications Channel Framework References: - **NIST CSF PR.DS-6**: Integrity checking mechanisms are used. - **CIS Control 12.11**: Ensure critical services have failover capabilities. - **NIST CSF PR.DS-4**: Communications and control networks are protected. - **NIST CSF PR.DS-5**: Protect data in transmission.
3	XSS-A receives a request from an attacker with an access token spoofed to be from Operator1, XSS-A does not perform token validation	An attacker sends an event to DSS via XSS-A pretending to be Operator1 by using an access token that is not minted by the authoritative Identity provider exploiting lack of token validation	DSS receives a request to update flight plans for its vehicles by an attacker that is using an access token to spoof the identity of XSS-A, potentially causing a scenario where two vehicles are on a collision path.	Sev1 / Red (Hazardous * Remote) C2	Validation of access tokens to have integrity and authenticity	Input Validation Framework Reference: - **CIS Control 18.1**: Validate all input from users, systems, and APIs to prevent malicious data injection. - **NIST CSF PR.DS-8**: Data integrity verification mechanisms are used.
4	Operator-1 sends authentication request to Identity provider, but an attacker conducts a DOS attack against Identity provider service	An attacker targets Identity Provider's service that is to receive events from Operator-1 with a DOS attack, the attack	Operator-1 is not able to receive an access token that prevents it from communicating securely with its Vehicle to reroute to avoid being on a	Sev1 / Red (Hazardous * Remote) C2	Identity Service must limit/block requests from unauthorized sources and ensure availability of its	**Availability** (of service to receive events) Framework References: - **NIST CSF PR.DS-4**: Communications and control

	and authentication event is not received.	takes advantage of weak availability controls for the Identity service.	collision path with another vehicle, resulting in a hazardous situation.		service to receive critical events.	networks are protected.
5	XSS-1 receives an event from XSS-2 and it uses the access token received to assume XSS-2's identity and send requests to DSS exploiting token replay vulnerability	XSS-1 acts as an attacker and assumes the identity of XSS-2 by performing a token replay attack exploiting a weakness in token attributes available for validation	DSS receives a request from XSS-1 that is acting maliciously and assuming the identity of XSS-2, DSS updates the routes for vehicles associated with XSS2, potentially causing a scenario where two vehicles are on a collision path.	Sev1 / Red (Hazardous * Remote) C2	Access tokens must have an Audience field, preventing token replay attacks	1. Token Integrity 2. Secure Authentication Framework References: - **NIST CSF PR.AC-7**: Mechanisms are in place to validate credentials and tokens. - **CIS Control 6.3**: Use strong authentication mechanisms.

Fig. 7b Identity Service Security Analysis

2. Operations Intent

This use case captures the workflow in which an operator initiates and manages a flight plan request within the xTM environment. This process begins with the operator filing the flight plan through a designated service supplier, which then communicates with DSS to obtain approval. The DSS is an SDSP that provides a common operational picture related to operational intent for vehicles operating in a collaborative area. Upon receiving flight plan approval, the operator securely transmits the confirmed plan to the vehicle and notifies other relevant service suppliers in the xTM ecosystem. This coordinated communication ensures that all entities are informed and aligned on the flight path, enabling safe and efficient airspace management across the xTM network.

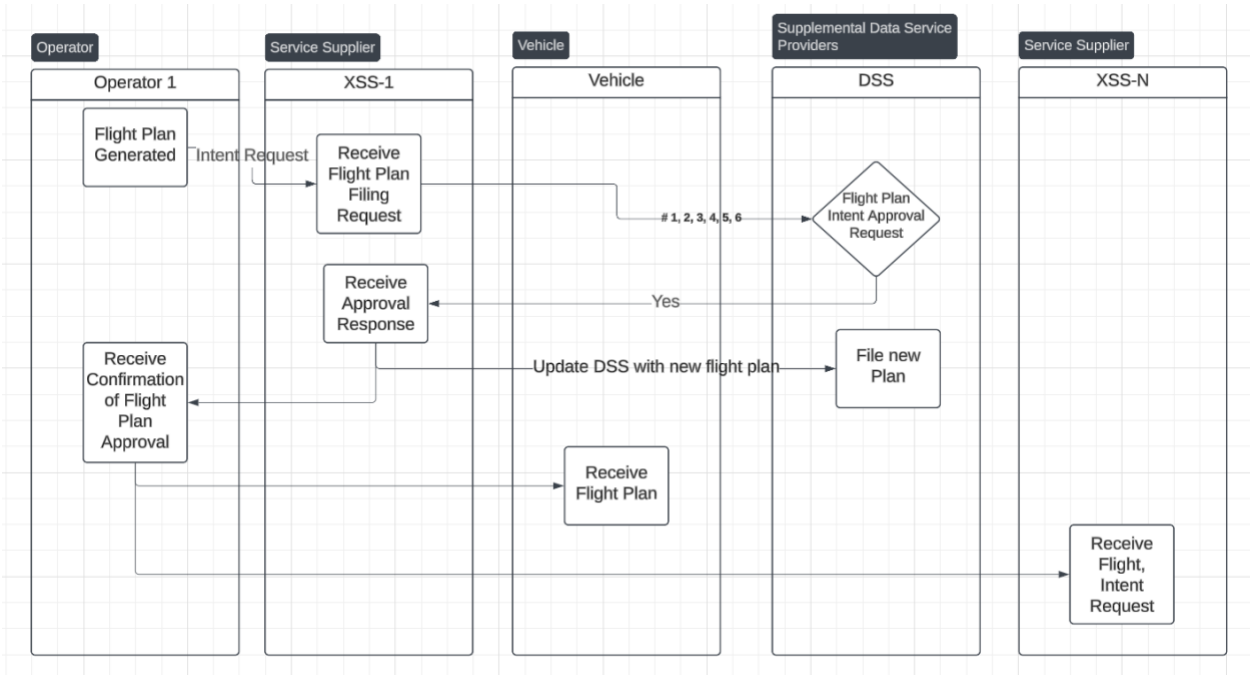

Fig. 8a Operations Intent Diagram

The table below captures the outcome of threat modeling, risk analysis performed on the threats and vulnerabilities and control mitigations recommended to mitigate the Risks identified for the Operations Intent use case. The class of controls and frameworks will reference the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) [19] and the Center for Internet Security (CIS) framework [20].

ID	Context	Threat & Vulnerability	Impact & Risk Analysis	Risk Score	Mitigative & Compensating Controls	Class of Controls & Frameworks
1	XSS-1 checks with DSS if the new flight plan can be approved, an attacker impersonates the identity of DSS.	An attacker impersonates the identify of DSS exploiting weak authentication controls and XSS-1 receives approval for a flight path that should not be approved.	XSS-1 receives an approved flight path from the attacker that is impersonating DSS and the path that is approved puts the Vehicle on a collision course with another vehicle leading to a hazardous situation	Sev1 / Red (Hazardous * Remote) C2	Strong authentication mechanism to ensure an attacker cannot impersonate the identity of an entity within xTM.	**1.** Identity and Access Management **(IAM)** Framework References: **- CIS Control 6.3**: Use strong authentication mechanisms. **- NIST CSF PR.AC-1**: Identities and credentials are managed.
2	XSS-1 checks with DSS if the new flight can be approved by DSS, an attacker compromises the integrity of the message.	An attacker compromises the integrity of the message being sent by XSS-1 to DSS by exploiting an insecure communications channel between XSS-1:DSS	DSS approves an incorrect flight path, as the flight path was changed by the attacker. Such an unauthorized change to the message can cause a hazardous situation as the flight path that is approved puts the Vehicle on a path that overlaps with another vehicle's flight path	Sev1 / Red (Hazardous * Remote) C2	Only allow communications of priority events over secure communications channels that provide integrity 2. secure communications channel (availability within a SLA)	**Secure Communications Channel - Integrity** Framework References: **- NIST CSF PR.DS-6**: Integrity checking mechanisms are used.
3	XSS-1 checks with DSS if the new flight path can be approved by DSS, XSS-1 does not log the flight path being approved.	No logging of planning event takes place due to weak logging control for all events received by XSS-1	FAA is unable to do proper root cause analysis for possible incidents that take place, due to lack of event data. This leads to a setup where appropriate mitigative actions cannot be taken to ensure incident recurrence does not take place.	Sev2 / Yellow (Minor * Probable) B4	Log all events so that post event analysis can be conducted.	**Logging** Framework References: **- CIS Control 8.1**: Ensure logging of all events.

4	XSS-1 checks with DSS if the new flight path can be approved by DSS, XSS-1 logs the flight path but then changes the logs as an incident occurs.	XSS-1 can modify logs of planning event to cover up mistakes made by XSS-1 to avoid repercussions.	FAA is unable to do proper root cause analysis for possible incidents that take place, due to modification of event data. This leads to a setup where appropriate mitigative actions cannot be taken to ensure incident recurrence does not take place.	Sev2 / Yellow (Minor * Probable) B4	Log all events in an immutable system so that post event analysis can be conducted properly.	**Logging** (of events in a secure immutable system for RCA) Framework References: **- NIST CSF PR.DS-1**: Protect data at rest and in use.
5	XSS-1 checks with DSS if the new flight path can be approved by DSS, an attacker is able to eavesdrop on the flight path confirmation.	An attacker can get flight path information for sensitive flights by exploiting an insecure communications channel between XSS-1 and DSS.	An attacker is able to get unauthorized access to sensitive flight plans that can lead to a breach of security for VIPs.	Sev1 / Red (Hazardous * Remote) C2	XSS-1 must communicate over a secure communications channel to prevent a malicious actor from eavesdropping	Secure Communications Channel Framework References: **- NIST CSF PR.DS-5**: Protect data in transmission.
6	An entity other than XSS-1 logs the flight path with DSS, DSS files the path as if XSS-1 has submitted the flight path.	An attacker leverages weak authorization checks for logging flight paths for Vehicles to log an invalid flight path for a Vehicle managed by XSS-1	Due to an attacker filing an incorrect flight path, DSS has incorrect flight paths in its datastore leading to a scenario where multiple vehicles have overlapping flight paths, leading to a hazardous scenario.	Sev1 / Red (Hazardous * Remote) C2	DSS must keep a mapping of Vehicles and their corresponding approved XSS (service supplier) and only allow approved entities to log flight paths for a Vehicle.	**Authorization / Elevation of Privilege** Framework References: **- CIS Control 6.3**: Ensure Role-Based Access Control is enforced.

Fig. 8b Operations Intent Analysis

3. Replanning

This use case addresses scenarios where an existing flight plan requires modification due to inputs from external entities, such as CFM (Conformance Monitoring) or the weather service. The service supplier coordinates to file an alternative flight path, this modified plan is submitted to the DSS for approval. Once approved, the service supplier, via the operator, communicates the updated flight path to the vehicle and informs other relevant service suppliers within the xTM ecosystem. This process mirrors the Operations Intent use case, ensuring real-time adaptability and safe navigation adjustments.

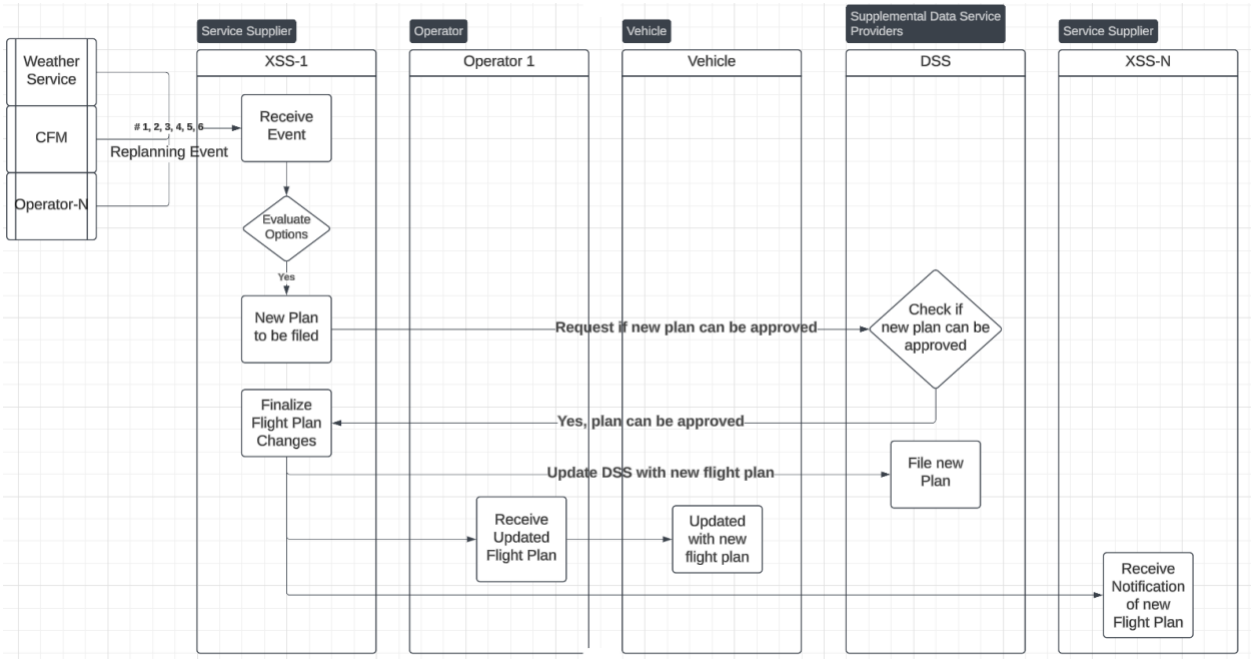

Fig. 9a Replanning Diagram

The table below captures the outcome of threat modeling, risk analysis performed on the threats and vulnerabilities and control mitigations recommended to mitigate the Risks identified for the Replanning use case. The class of controls and frameworks will reference the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) [19] and the Center for Internet Security (CIS) framework [20].

ID	Context	Threat & Vulnerability	Impact & Risk Analysis	Risk Score	Mitigative & Compensating Controls	Class of Controls & Frameworks
1	CFM sends Re-Planning event to XSS-1, Attacker impersonates identity of CFM	XSS-1 receives re-planning event from CFM, but an attacker is impersonating the identity of CFM by exploiting weak authentication controls.	XSS-1 replans the flight path unnecessarily as it assumes the request has come from CFM, this can lead to overburdening of XSS-1's resources that can prevent it from responding to an actual request from CFM that needs urgent response from XSS-1 to avoid an incident, this can lead to a hazardous situation.	Sev1 / Red (Hazardous * Remote) C2	Strong authentication mechanism to ensure no entity other than CFM can assume the identity of CFM.	**Authentication** - Identity and Access Management **(IAM)** Framework References: - **CIS Control 6.3**: Use strong authentication mechanisms. - **NIST CSF PR.AC-1**: Identities and credentials are managed.
2	Attacker sends Re-Planning event to XSS-1, where attacker is	XSS-1 receives re-planning event from an entity and processes the	XSS-1 replans the flight path unnecessarily as it assumes the request	Sev1 / Red (Hazardous * Remote) C2	Only ATC can send Re-Planning events to XSS-1.	**Authorization / Elevation of Privilege**

	impersonating the identity of an entity other than CFM.	Re-Planning event, the attacker exploits the weakness in authorization controls where XSS-1 only allows some approved entities like CFM to send a re-planning event.	has come from an authorized entity, this can lead to overburdening of XSS-1's resources that can prevent it from responding to an actual request from ATC that needs urgent response from XSS-1 to avoid an incident, this can lead to a hazardous situation.		• Explicit authorization check for entity sending event	Framework References: - **CIS Control 6.3**: Ensure Role-Based Access Control is enforced.
3	CFM sends a Re-Planning event to XSS-1, Attacker Impersonating XSS-1.	CFM sends flight re-planning event to XSS-1, but an attacker impersonates XSS-1 by exploiting weak authentication controls and receives the request intended for XSS-1	CFM assumes the re-planning event has been received by XSS-1 (OP1). This can cause a hazardous situation where it can not be relied upon for XSS-1 to appropriately react to re-planning events and route vehicles safely.	Sev1 / Red (Hazardous * Remote) C2	1. Ability to perform strong authentication checks to establish the identity of the receiving party, I.e. XSS-1 2. Having secure communications channel available that can allow for communications to take place within an acceptable SLA	**1. Authentication - IAMM** **2. Availability** Framework References: - **CIS Control 9.2**: Limit access to services to authorized devices and entities. - **NIST CSF PR.DS-4**:Communications and control networks are protected.
4	CFM sends Re-Planning event to XSS-1, Attacker compromising Integrity of communications channel	An attacker compromises the integrity of the message being sent by CFM to XSS-1 by exploiting an insecure communications channel between CFM:XSS-1	The flight plan that is received by XSS-1 is not what was sent by CFM, this can allow for an incorrect flight plan to be charted and logged with DSS. Such an unauthorized change to the plan can cause a hazardous situation where it cannot be relied on, that the operators can receive CFM notifications and route vehicles safely.	Sev1 / Red (Hazardous * Remote) C2	Only allow communications of priority events over secure communications channels that provide integrity 2. secure communications channel (availability within a SLA)	**Integrity** Framework References: - **NIST CSF PR.DS-6**: Integrity checking mechanisms are used.
5	CFM sends Re-Planning event to	No logging of Re-Planning event takes place	FAA is unable to do proper root cause analysis for possible	Sev2 / Yellow (Minor *	Log all events in an immutable manner so that	**Logging (Immutable)**

	XSS-1. The event is not logged.	due to weak logging control for all events received by XSS-1.	incidents that take place, due to lack of event data. This leads to a setup where appropriate mitigative actions cannot be taken to ensure incident recurrence does not take place.	Probable) B4	post event analysis can be conducted properly	Framework References: **- CIS Control 8.1**: Ensure logging of all events. **- NIST CSF PR.DS-1**: Protect data at rest and in use.
6	CFM sends Re-Planning event to XSS-1, but an attacker conducts a DOS attack against XSS-1 and event is not received.	An attacker targets XSS-1's service that is to receive events from ATC with a DOS attack, the attack takes advantage of weak availability controls for the re-planning event ingestion service.	XSS-1 is not able to receive an urgent re-planning event and is not able to reroute a vehicle on a collision path and results in a hazardous situation.	Sev1 / Red (Hazardous * Remote) C2	XSS-1 must limit/block requests from unauthorized sources and can ensure availability of services to receive critical events.	**Availability** (of service to receive events) Framework References: **- NIST CSF PR.DS-4**: Communications and control networks are protected.
7	CFM sends Re-Planning event to XSS-1, the replanning event or the confirmation of re-planning of route is disclosed to an attacker.	An attacker targets a communications channel or route store datastore to get access to replanning events due to weak confidentiality controls.	The flight path or replanning events are not confidential so there is no significant impact to the information disclosure.	Sev3 / Green (Minimal * Remote) C5	Communications must occur over a secure communications channel to prevent a malicious actor from eavesdropping	Secure Communications Channel (Confidentiality) Framework References: **- NIST CSF PR.DS-5**: Protect data in transmission.

Fig. 9b Replanning Analysis

B. Security Architecture Control Recommendations

ID	Compensating Controls	Control Class
1	Strong authentication control that allows one entity to securely establish the identity of another entity, either directly or via an Identity Provider, e.g. establish the identity of the entity that is sending a replanning event.	**Authentication** (of entity's identity that is communicating)
2	Authorization verification control that allows an entity to validate if another entity has the privileges to execute a privileged function or make a privileged request e.g. require route replanning.	**Authorization** (of entity sending a 'privileged' request)
3	Integrity control provides integrity of data (messages) over communications channel and at rest.	**Secure & Trusted Communications channel (**Integrity)
4	Availability of communications channel to send messages, within a committed SLA.	**Secure & Trusted Communications channel (**Availability of channel)

5	Confidentiality of messages being communicated when required.	**Secure & Trusted Communications channel (**Confidentiality
6	Allow logging of all required events in an immutable manner so that post event analysis can be conducted properly	**Logging** (of events in a secure immutable system)
7	Availability control allows a service to be up and running in a state that allows the service to perform all activities within committed SLAs.	**Availability** (of service to receive events)
8	Secure configuration must be in place to enforce validation & integrity checks on data to ensure only trusted inputs are processed.	**Secure Configuration & State Integrity** (Validation, Data Integrity, and Security Assurance)
9	Continuously monitor critical activities across the system for anomaly detection.	**Incident Detection** (cyber-attacks)
10	Develop structured incident response processes & capabilities to address security events.	**Incident Response**

Fig. 10 Control Recommendations

As outlined earlier to define the security architecture we have utilized different FAA Concept of Operations (ConOps) for UAM, UTM, and ETM to identify all relevant scenarios and use cases that could introduce risk to the Extensible Traffic Management system (xTM). We then used representative use cases to perform threat modeling and document the risks that are present or could emerge in the environment. Following this, we led a detailed analysis to outline compensating controls designed to mitigate these risks, ensuring the system's Confidentiality, Integrity, and Availability (CIA) are safeguarded from malicious actors, both internal and external. These controls form the foundation of the security architecture, providing a robust framework to secure the system across all operational phases.

The eight foundational security controls that underpin this architecture are **Authentication**, **Authorization**, **Secure communications channels**, **Availability** of services, **Incident Detection & Response, Logging** and **Secure Configuration & State Integrity**:

- **Authentication** ensures that each entity—whether an operator, vehicle, or service provider—can be trusted by verifying their identity, ensuring that data, commands, or events are being sent from a legitimate source.
- **Authorization** ensures that once an entity is authenticated, it has the correct permissions to access only the data and perform only the actions relevant to its role. For example, within the DSS (Distributed Service System), only an authorized operator is allowed to update their own flight path, preventing unauthorized changes from other entities.
- **Secure & Trusted Communications Channel (Integrity)**: Integrity controls safeguard the integrity of messages during transit and when stored, preventing unauthorized alterations to critical data.
- **Secure & Trusted Communications Channel (Availability)**: Availability controls ensure the communications channel remains accessible within a specified Service Level Agreement (SLA), supporting critical message transmission even during high-demand periods.
- **Secure & Trusted Communications Channel (Confidentiality)**: Confidentiality controls protect sensitive messages, ensuring that communications remain secure and accessible only to authorized parties when needed.
- **Availability of services** ensures that critical services within the system remain operational and capable of processing messages and actions in a timely manner. Specific Service Level Agreements (SLAs) are established to set expectations for service uptime and performance. Redundant infrastructure and failover mechanisms are also implemented to maintain continuous operations, even in the event of partial system failures or increased load.
- **Incident Detection**: Continuous monitoring of system activities enables prompt detection of anomalies or cyber-attacks, allowing the system to respond quickly to emerging threats.
- **Incident Response**: Structured incident response capability needs to be in place to respond to incidents that span multiple entities (XSS', Operators) within the xTM environment.
- **Logging** provides an auditable trail of all actions and events performed by operators, service providers, and other entities. This audit trail is crucial for root cause analysis in the event of a security incident, allowing for quick triage and resolution of issues while ensuring accountability.

- **Secure Configuration and State Integrity** (Validation, Data Integrity, and Security Assurance)**:** Secure configuration and entity state integrity must be maintained to ensure robust validation of inputs, secure handling of data, and system-wide integrity checks. This includes automated security checks, input validation, and measures to preserve data accuracy and consistency across all system processes. Continuous monitoring, automated code scanning, and comprehensive code and design reviews for APIs and services are essential to ensure that configurations meet security standards and protect against attacks that could compromise system reliability.

These compensating controls form a multi-layered security architecture, enhancing the xTM system's resilience against malicious actors. By focusing on the essential principles of authentication, authorization, secure communications, data validation, availability, monitoring, and incident management, the xTM security architecture effectively mitigates the risks identified during threat modeling. This architecture supports the secure, reliable, and efficient operation of the xTM system across all phases, ensuring robust defense and compliance with CIA requirements.

References

[1] P. D. H. R. J. &. D. N. S. Vascik, "Analysis of urban air mobility operational constraints.," no. 26(4), pp. 133-146, 2018.

[2] Federal Aviation Administration, Upper Class E Traffic Management (ETM) Concept of Operations v1.0, May 2020, https://nari.arc.nasa.gov/sites/default/files/attachments/ETM_ConOps_V1.0.pdf

[3] FAA, "Unmanned Aircraft System Traffic Management (UTM)," 2 March 2020. [Online]. Available: https://www.faa.gov/sites/faa.gov/files/2022-08/UTM_ConOps_v2.pdf. [Accessed 2024].

[4] FAA, "FAA Issues Implementation Plan Outlining Steps to Usher in Advanced Air Mobility," 18 July 2023. [Online]. Available: https://www.faa.gov/newsroom/faa-issues-implementation-plan-outlining-steps-usher-advanced-air-mobility. [Accessed 2024].

[5] FAA, "Extensible Traffic Management (xTM)," 15 March 2022. [Online]. Available: https://www.faa.gov/sites/faa.gov/files/2022-03/508.05Spring2022REDACNASOps_XTM.pdf.

[6] H. Poston, "STRIDE-LM Threat Model," [Online]. Available: https://csf.tools/reference/stride-lm/. [Accessed 2024].

[7] Federal Aviation Administration, Urban Air Mobility (UAM) Concept of Operations v2.0, April 2023, https://www.faa.gov/sites/faa.gov/files/Urban%20Air%20Mobility%20%28UAM%29%20Concept%20of%20Operations%202.0_1.pdf

[8] Jung J., Rios J., Xue M., Homola J., Lee P., Overview of NASA's Extensible Traffic Management (xTM) Research, January 2022, *AIAA SciTech 2022 Forum*

[9] Freeman, K., Garcia, S., Cyber Threats and Security Controls Analysis for Urban Air Mobility Environments, January 2021, *AIAA SciTech 2021 Forum*

[10] C. C. Editor, "Cyber Threat - Glossary | CSRC," *csrc.nist.gov*. https://csrc.nist.gov/glossary/term/Cyber_Threat

[11] CSRC, "vulnerability - Glossary | CSRC," *Nist.gov*, 2015. https://csrc.nist.gov/glossary/term/vulnerability

[12] C. C. Editor, "cyber risk - Glossary | CSRC," *csrc.nist.gov*. https://csrc.nist.gov/glossary/term/cyber_risk

[13] C. C. Editor, "security incident - Glossary | CSRC," *csrc.nist.gov*. https://csrc.nist.gov/glossary/term/security_incident

[14]Federal Aviation Administration, "Safety Management System (SMS) | Federal Aviation Administration," *Faa.gov*, Aug. 02, 2024. https://www.faa.gov/about/initiatives/sms

[15]"QUICK REFERENCE GUIDE Safety Risk Management (SRM)." Available: https://www.phl.org/drupalbin/media/PHL%20SMS%20-%20QRG%20-%20FINAL%20REVIEW%20-%2011-22-20%20(1).pdf

[16]"Order 5200.11A - FAA Airports (ARP) Safety Management System (SMS)," *Faa.gov*, 2021. https://www.faa.gov/regulations_policies/orders_notices/index.cfm/go/document.current/documentNumber/5200.11 (accessed Nov. 12, 2024).

[17]L. Conklin, "Threat Modeling Process | OWASP," *owasp.org*. https://owasp.org/www-community/Threat_Modeling_Process#stride

[18]"Records," *Faa.gov*, 2024. https://www.faa.gov/air_traffic/publications/atpubs/foa_html/chap4_section_6.html (accessed Nov. 21, 2024).

[19]NIST, "Cybersecurity Framework," National Institute of Standards and Technology, 2024. https://www.nist.gov/cyberframework

[20]Center for Internet Security, "CIS Critical Security Controls," *CIS*, 2023. https://www.cisecurity.org/controls