697DCK-23-C-00287

Security & Performance Monitoring for UTM Ecosystems

Final Report

Matthew Synborski,[1] and Brennan Thierry[2]

ResilienX Inc., Syracuse, NY, 13202, USA

Team ResilienX's research and development effort, aligned with the Federal Aviation Administration (FAA) Uncrewed Aircraft System (UAS) Broad Agency Announcement (BAA) call 004 under contract #697DCK-23-C-00287, lays a solid foundation for an In-Time Aviation Safety Management System (IASMS) within UAS Traffic Management (UTM) and Advanced Air Mobility (AAM). Over the twelve-month execution period, the project successfully identified and analyzed key performance indicators (KPIs), failure modes, and contingency management scenarios anticipated in a typical UTM ecosystem.

This analysis was conducted with a thorough review of FAA guidance on UTM, NASA's thought leadership, and existing Air Traffic Management (ATM) systems. We derived relevant KPIs, identified potential failure modes, and down selected specific IASMS failure modes for focused testing. The results highlighted critical implications and provided insights into necessary adjustments.

Our findings suggest that a federated UTM ecosystem inherently poses risks due to its decentralized nature. The project revealed that current systems lack the capability for comprehensive, real-time checks and balances. Therefore, a standardized system, such as the IASMS, is essential for continuous safety management. This new concept, though innovative, is crucial for ensuring reliable and safe operations in a federated UTM environment.

---

[1] Chief Technology Officer

[2] Engineering Program Manager

I.Introduction

A. Background

This project, initiated through the FAA UAS BAA solicitation number 692M15-19-R-00020, aligns with the overarching goal of integrating UAS into the national airspace system. Specifically, it falls under the UAS004 topic within the BAA, focusing on UTM and demonstrating the real-time health, quality, and integrity of the UTM ecosystem. Traditional aviation systems prioritize safety based on established assurance standards and experience-backed requirements, which are not easily applicable to uncrewed aviation due to industry immaturity, scale, innovative technology, and federated service-based architectures.

A federated UTM ecosystem might have increased risks and complexities. In a federated (FAA) UTM ecosystem or centralized (EASA/EUROCAE) U-Space ecosystem there is a need for a service to provide situational awareness regarding the performance of the network between the UTM ecosystem services and components. This includes the need for standardized interfaces and data exchange protocols to ensure interoperability, and benefit from an IASMS providing a standardized approach to monitoring, managing, and mitigating these issues. The majority of UTM activities thus far have not adequately addressed these intricate safety needs, underscoring the necessity for targeted research and development efforts.

This project identified a potential path forward through the analysis of an IASMS, which provides a standardized approach to monitoring, managing, and mitigating risks within a federated UTM ecosystem. The IASMS concept is vital for ensuring robust safety and operational integrity, validating its effectiveness through rigorous testing and alignment with FAA guidelines and industry best practices.

B. Project Objective

The goal of the project was to enhance, verify, validate, and quantify the effectiveness of a system used to monitor the performance and security of a UTM ecosystem. Team ResilienX accomplished this by bringing together key ecosystem technologies. This integration included monitoring, in near-real-time, associated elements (AEs), analyzing the data, demonstrating how the monitoring system enables validation of performance, real-time detection of off-nominal issues, and the ability to impact contingency plans. The associated elements (services provided by a third party) and respective industry team members providing those capabilities are listed below:

- IASMS: The ResilienX Fault Recovery and Isolation, Health Monitoring frameWORK (FRAIHMWORK®) software platform which monitors the health, integrity, and performance of the various AEs involved with complex UAS operations. It provides user-driven and automated mitigation capabilities. In the FAA UTM Concept of Operations (ConOps) [1] as they are written today, FRAIHMWORK would be considered or align to a Supplemental Data Service Provider (SDSP). The focus of this project is to provide the substantiation that the IASMS scope and function in a UTM ecosystem reaches beyond that of a SDSP. The sections that follow provide justification for that claim.
- UAS Service Supplier (USS): OneSky Systems (OneSky) provides a comprehensive UTM capability which allows operators to avoid risks strategically, tactically and alerts within the airspace, conformance monitoring, and constraint management. Combined with FRAIHMWORK, these capabilities monitor the health, integrity, performance, and security of the various data and AE and provide a means of direct communications with operators to act, maintaining a high level of safety within the airspace.
- IASMS Cybersecurity Plugin: Assured Information Security (AIS) provides their Artemis software which acts as a cyber security plug-in to FRAIHMWORK and monitors the cyber posture (e.g., vulnerabilities and signs of compromise by malicious actors) of federated system of systems. Artemis encapsulates and extends a TRL-9 cyber-security product called Metasponse which is used in operations across the Department of Defense (DoD) and in several federal agencies as well as the National Guard.

The results of this project benefit the public interest and the FAA by expanding on the requirements needed for UAS ecosystem automation, as well as demonstrating a means of compliance. Team ResilienX believes that these results will drive additional standards and inform in-work means of compliance being developed within the standards community as referenced in section 2 of the FAA UTM Implementation Plan, Development of Performance and Safety Standards [1].

C. Team ResilienX Partners

Contract 697DCK-23-C-00287 consisted of the organizations listed and described in Table 1.

Table 1 Project Organizations and Contributions

Teammate	Name and Description	Key Contributions
RESILIENX	ResilienX is a software company productizing safety assurance solutions for highly automated and autonomous ecosystems, and leading design and development efforts of key infrastructure for AAM operations management. They've been integrating uncrewed systems of all shapes and sizes into the US National Airspace System (NAS) since 2008. ResilienX key personnel have keen experience in AAM airspace solution design and previously filled the roles of lead system architect and systems integration lead for the US Army's Ground Based Sense and Avoid (GBSAA) system.	Project prime contractor, lead designer, and System of Interest (SoI) provider. Provided the FRAIHMWORK software platform monitors the heath, integrity and performance of the systems involved in scaled, autonomous uncrewed operations, enabling organizations to meet regulatory safety requirements.
OneSky	OneSky is a global UTM company developing airspace assessment, operations, and traffic management solutions for the aviation industry. OneSky has validated its technology in numerous UTM programs globally, including projects with the FAA, NASA, and the Civil Aviation Authority of Singapore (CAAS).	Operations and contingency management expertise, design, integration test, demonstration and analysis of the USS, OneSky UTM. Provide domain expertise, modeling & simulation capability, and UTM to support Test & Evaluation (T&E) planning, execution, and reporting
ais	Established in 2001 and headquartered in Rome, New York, Assured Information Security (AIS) is a leading cyber and information security company. They play a pivotal role in advancing critical cyber operations for the federal government, intelligence community, and the commercial sector.	Cyber security subject matter expertise for all aspects of the project. Performed integration, test, demonstration, and analysis of their cyber IASMS plugin, Artemis. The Artemis platform is modular and adaptable, ensuring robust defense against an extensive range of sophisticated cyber threats within complex network systems.
NUAIR	As a proven and credible industry leader, Northeast UAS Airspace Integration Research Alliance (NUAIR) delivers the next generation of UAS and AAM solutions for the safety, societal, and economic benefit of New York State and beyond. NUAIR received its civil flight authority BVLOS waiver for 240 square miles of operational airspace in upstate New York, leveraging the Center of Excellence at the Syracuse Airport, nearby Operations Center, and associated assets for UAS/AAM advancements.	Support to system conceptualization, integration assistance with infrastructure components, live test events and flight operations at NUAIR airspace, and functional architecture development and support

D. System of Interest Context

At the highest level the project SoI is an IASMS. The SoI monitors the health, integrity, and performance of the various AEs involved with complex UAS operations. It provides user-driven and automated mitigation capabilities.

The top-level system functionality is depicted in a context diagram shown in Fig. 1. In most cases, a computer system is the main actor that interacts with the system for receiving data via streamed data services, and via responses to API requests to service-based functions, however the utility and scope of this project and specifically the contingency management standard operating procedure (SOP) developed extends beyond just the SoI. The scope includes other human actors in the ecosystem that might be operating systems that are data consumers or users of the SoI (Fig. 1 shows this extended applicability by providing a boundary for the SOP applicability in BLUE). Several of these functions are depicted using directed flows. For these flows, they are intended to be read from the entity that is closer to the label, for example: *IASMS - monitors components health of Monitored Hardware*

The purpose for the distinction and inclusion of this information on the context diagram is to provide relevant association of the IASMS and the project objectives to the larger community. The failure modes investigated, and contingency scenarios encompass functionality from multiple ecosystem entities and necessitate actors with various roles to respond.

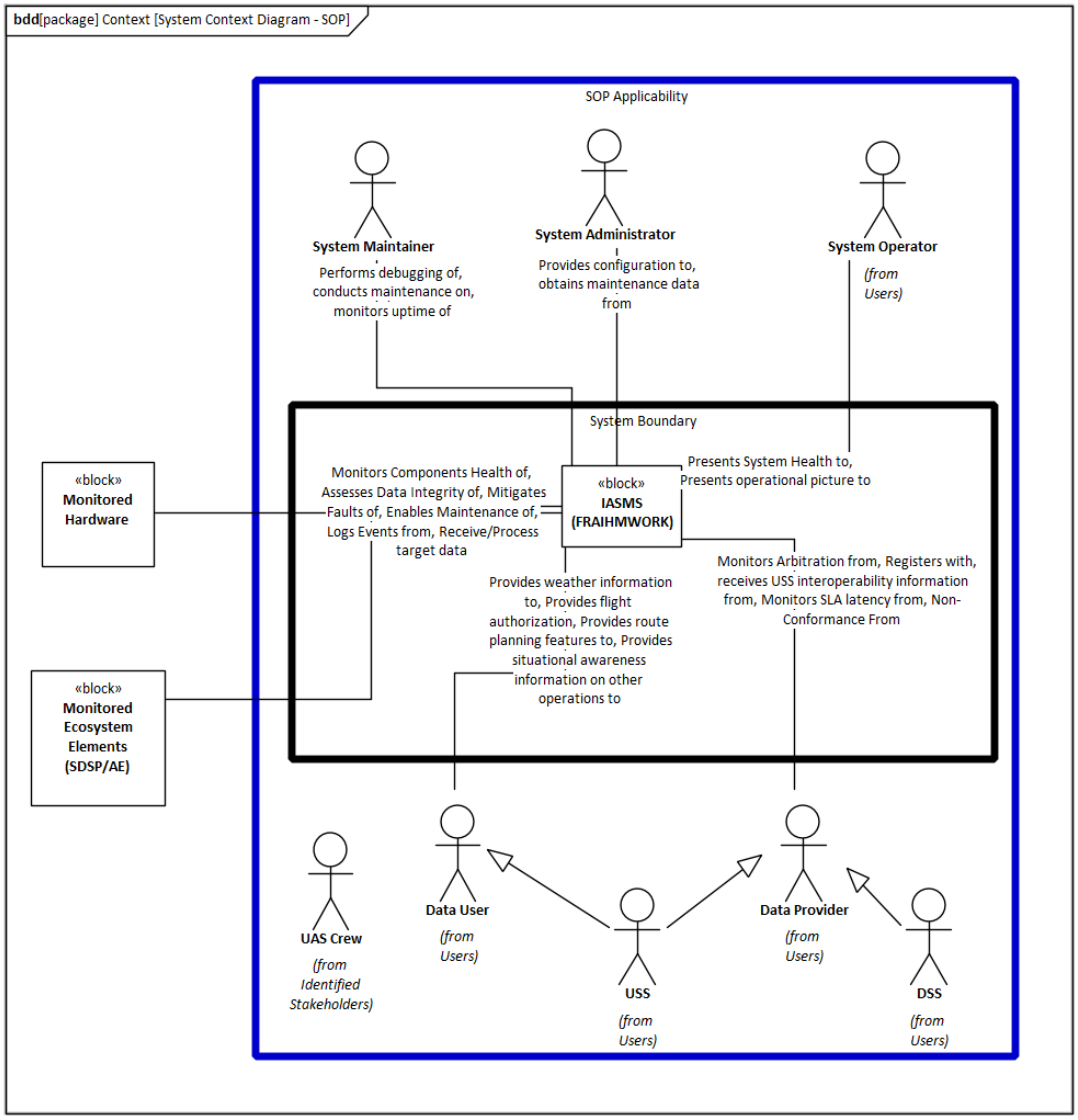

Fig. 1 Project System of Interest Context Diagram with SOP Context

E. Referenced Documents

Table 2 Referenced Documents

Document	Version
National Academies of Sciences, Engineering, and Medicine. 2018. In-Time Aviation Safety Management: Challenges and Research for an Evolving Aviation System. Washington, DC: The National Academies Press. https://doi.org/10.17226/24962	2018
Standard Specification for Detect and Avoid System Performance Requirements	ASTM 3442/F3442M – 23, Feb 28, 2023
Standard Specification for UAS Traffic Management (UTM) UAS Service Supplier (USS) Interoperability	ASTM F3548-21, Mar 08, 2022

Standard Terminology for Unmanned Aircraft Systems	ASTM F3341M-24
Standard Specification for Surveillance Supplementary Data Service Providers	ASTM F3623 − 23
Standard Specification for Performance for Weather Information Reports, Data Interfaces, and Weather Information Providers (WIPs)	ASTM F3673 – 23, Jan 09, 2024
Global UTM Association (GUTMA) Secure and Resilient UTM Task Force Report	2024

F. Acronyms and Abbreviations

Table 3 lists the acronyms and abbreviations used in this document

Table 3 Acronyms/Abbreviations

Term/Acronym	Definition/Full Name
AAM	Advanced Air Mobility
AE	Associated Element
AIP	Aeronautical Information Publication
AIS	Assured Information Security
ATM	Air Traffic Management
AUS	FAA UAS Integration Office
BAA	Broad Agency Announcement
CAAS	Civil Aviation Authority of Singapore
DSS	Discovery and Synchronization Service
FAA	Federal Aviation Administration
FRAIHMWORK	Fault Recovery and Isolation, Health Monitoring frameWORK
GBSAA	Ground Based Sense and Avoid
GUTMA	Global UTM Association
IASMS	In-Time Aviation Safety Management System
INCOSE	International Council on Systems Engineering
IMS	Integrated Master Schedule
KPI	Key Performance Indicators
MBSE	Model Based Systems Engineering
NAS	National Airspace System
NUAIR	Northeast UAS Airspace Integration Research
NYUASTS	New York Unmanned Aircraft System Test Site
PMR	Program Management Review
PUI	Program-Unique Identifier
SDSP	Supplemental Data Service Provider
SME	Subject Matter Expert
SOI	System of Interest
SOP	Standard Operating Procedures
SOS	System of Systems
T&E	Test and Evaluation
TMI	Tiered Maintenance Interface
UAS	Unmanned Aircraft System
USS	UAS Service Supplier
UTM	Unmanned Aircraft System Traffic Management
WIP	Weather Information Provider

II.Approach

Team ResilienX leveraged our collective expertise to identify the need for this project and establish the approach to help articulate and quantify the effectiveness of an IASMS to increase robustness, resiliency, and fault tolerance of a federated system of systems in the UTM ecosystem. Fig. 2 below depicts the simplified, high-level view, of the project approach. The subsections below provide further detail for the major execution items. The delivered Integrated Master Schedule (IMS) provides the detailed schedule for reference that was used to execute this program.

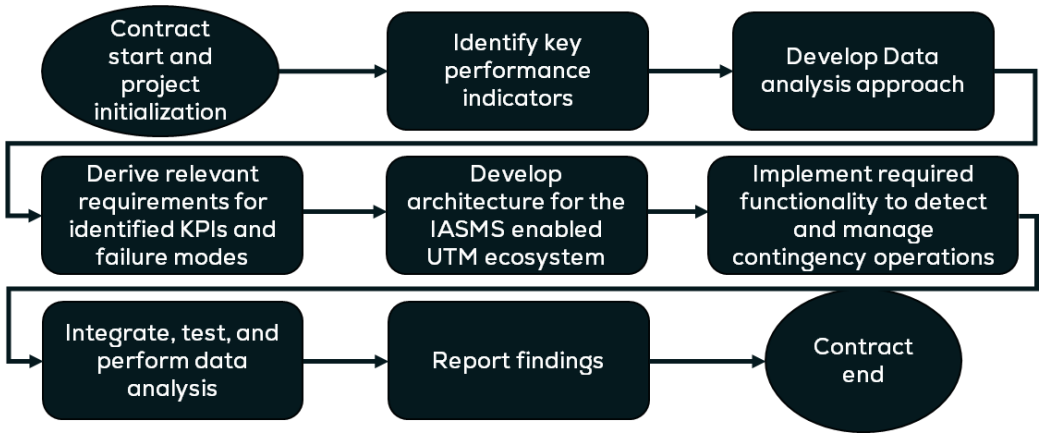

Fig. 2 Simplified Contract Execution Approach

A. Project Phases

The project work breakdown structure was broken into 6 major elements aligning to the contract tasks and included the following tasks and subtasks:

1. Task 1: Project Initiation
   - 1.1 Project Kickoff
   - 1.2 IMS Development
   - 1.3 FAA Deliverable Submittal Tool Training
2. Task 2: Research, Design, and Planning
   - 2.1 Failure Mode Identification
   - 2.2 Condition Research
   - 2.3 Data Analysis Plan
   - 2.4 Detailed Design
3. Task 3: Integration
   - 3.1 Software Integration
   - 3.2 Infrastructure Integration
4. Task 4: Development and Implementation:
   - 4.1 Feature Development/Implementation
   - 4.2 Contingency Management Development
   - 4.3 SOP Development
5. Task 5: Test and Demonstration (Flight Testing and Analysis)

5.1 T&E Plan
5.2 Test Procedure Development
5.3 Test and Demonstration Execution
5.3.1 Phase 1 Contractor Lab Test
5.3.2 Phase 2 Contractor Live Flight Test
5.3.3 Phase 3 Formal Test Site Live Flight Test and Demonstration
5.4 Test Report

6. Task 6: Program Management and Reporting to FAA UAS Integration Office (AUS)
6.1 Monthly Project Progress Reports
6.2 Quarterly Program Management Review (PMR) Briefings
6.3 Final Report
6.4 Final Presentation

The following subsections elaborate on key tasks and subtasks for this project.

B. Research, Design, and Planning

Task 2 was pivotal for the project's success, focusing on deriving KPIs, developing a comprehensive data analysis approach, and completing detailed design activities. The team selected KPIs aligned with specific IASMS-enabled failure modes to ensure relevant analysis throughout the project. The data analysis plan served as the foundation for data collection and analysis, guiding the team's execution. Additionally, the detailed design subtask, grounded in rigorous systems engineering practices, involved defining use cases, functional and performance requirements, and system architecture. Overall, this task was crucial for establishing a clear and accurate foundation for the project and creating a definitive reference for design and objectives. The following subsections provide further details on key subtasks.

1. Key Performance Indicators

As part of this project, Team ResilienX applied model-based systems engineering (MBSE) principles and methods, across the project's lifecycle. A crucial aspect of our design effort, particularly in defining, testing, and validating failure modes, is the establishment of KPIs to gauge and evaluate the system's performance, effectiveness, and success throughout its lifecycle. In task 2.1, Team ResilienX delivered the Data Analysis Plan that included 21 KPIs aligned to the following categories:

- **Data Integrity:** Measures the accuracy, consistency, and reliability of the data collected and processed by the system. KPIs in this category assess how well the system maintains the correctness of data throughout its lifecycle and identifies any discrepancies or errors in data handling.

- **Information Assurance and Cybersecurity:** Evaluates the system's ability to protect data and ensure privacy and security against unauthorized access, breaches, or cyber threats. KPIs here focus on the effectiveness of implemented security measures and protocols in safeguarding sensitive information.
- **Surveillance Tracking:** Assesses the system's capability to accurately monitor and track entities within the operational environment. KPIs in this category measure the precision and reliability of surveillance data, including the system's performance in real-time tracking and reporting.
- **Ecosystem Component Health and Status:** Monitors the operational condition and performance of various components within the system ecosystem. KPIs assess the health, status, and reliability of components to ensure they function correctly and contribute effectively to the overall system performance.

Throughout the project, Team ResilienX undertook the critical task of quantifying these KPIs. Given the complexity of defining and validating these indicators within the project's timeframe, this proved to be a highly challenging endeavor. The tables below details the KPIs and their target values as determined during this phase of the project. To further refine these values, additional empirical testing and stakeholder engagement with larger datasets and related elements will be necessary for formalization and comprehensive validation. An asterix (*) in the substantiation denotes a recommendation for further investigation via future work.

Table 4 Data Integrity KPIs

Data Integrity				Substantiation
KPI #	**Indicator**	**Detail**	**Derived Value**	
1	Data Accuracy Rate	Percentage of data records that are free from errors or discrepancies	99.9% System can effectively handle critical operations, maintain high data quality, and support safety and operational objectives	TC04
2	Data Completeness	Percentage of expected data records that are present and complete.	99.9% System can effectively handle critical operations, maintain high data quality, and support safety and operational objectives	TC04, TC04.2
3	Data Timeliness	Average time taken to update or process data.	<1s Supports the system's ability to function effectively in high-speed and high-demand environments	TC04, TC04.1
4	Data Consistency	Measurement of data consistency across different parts of the system.	99.9% System can effectively handle critical operations, maintain high data quality, and support safety and operational objectives	TC04
5	Data Validation Failures	Number of data validation failures or anomalies detected	<1 / 10,000 records Provides reliable and accurate information for operational decisions	TC04

Table 5 IA and Cybersecurity KPIs

Information Assurance / Cybersecurity				Substantiation
KPI #	**Indicator**	**Detail**	**Derived Value**	
6	Access Control Effectiveness	Percentage of unauthorized access attempts prevented.	99.9% High percentage of unauthorized access attempts prevented, organizations can significantly enhance their cybersecurity posture and protect against potential security breaches. Note: This is a very difficult one to measure post deployment but can be achieved through controlled testing.	TC06, TC06.1, TC06.3
7	Security Policy Compliance	Percentage of system components and users in compliance with security policies.	95% Essential to ensure that the majority of system components and users adhere to established security policies. Best practices from ISO/IEC 27001, NIST 800, NIST CSF, etc. No KPIs are listed in those standard but the basis for understanding is derived. This is a KPI that is established and managed by the security team and one that needs further testing and deliberation.	*
8	Incident Response Time	Average time taken to detect and respond to security incidents.	<30 minutes for critical incidents, <4 hours for medium severity, and <24 hours for low severity Monitoring these times helps organizations ensure their incident response capabilities are effective and efficient.	*
9	Number of Security Incidents	Count of security incidents, including breaches, attacks, and vulnerabilities discovered.	This is a KPI that is established and managed by the security team and one that needs further testing and deliberation. Team ResilienX can propose based on a target ecosystem but it is subject to the final system of system architecture and system security plan.	*
10	Vulnerability Assessment	Frequency of vulnerability assessments and their findings.	Quarterly Regular assessments help in identifying and addressing vulnerabilities before they can be exploited.	TC06
11	Patch Management	Percentage of critical patches applied within a specified timeframe.	This is a KPI that is established and managed by the security team and one that needs further testing and deliberation.	TC06, TC06.2
12	Antivirus Effectiveness	Percentage of malware blocked by antivirus software.	99% Indicates that the antivirus software is highly effective in preventing malware infections. Note: This is a very difficult one to measure post deployment but can be achieved through controlled testing.	TC06

Table 6 Surveillance KPIs

Surveillance Tracking				Substantiation
KPI #	Indicator	Detail	Derived Value	
13	Probability of Detection (Pd)	Percentage of (a) cooperative and (b) non-cooperative tracked objects accurately identified and monitored.	0.90 to 0.95 High Pd ensures that all vehicles and potential hazards are detected accurately, essential for preventing accidents and maintaining safe traffic flow.	TC02, TC02.1
14	(a) False Positive and (b) False Negative Rate	Percentage of false alarms or erroneous tracking reports.	<5% Ensures reliable system performance, effective decision-making, and increased confidence from users and stakeholder	TC02, TC02.1
15	Tracking Sensitivity	Percentage of the surveillance volume covered effectively.	95% Ensures that the surveillance system performs effectively and supports the safe and efficient management of air traffic	*
16	Tracking Latency	Average delay in tracking and reporting changes in surveillance data	<2s Supports the need for rapid response and accurate situational awareness in the management of air traffic	*

Table 7 Health and Status KPIs

Health and Status				Substantiation
KPI #	Indicator	Detail	Derived Value	
18	System Uptime	Percentage of time the system is operational and available.	99.9% Ensures that the system is consistently operational, providing reliable service and support to users and maintaining trust in its performance.	TC03, TC04,
19	Resource Utilization	Usage levels of system resources (CPU, memory, storage).	<80% CPU, <75% memory, <85% storage Ensures storage and performance is adequate for peak demand and future expansion	*
20	Maintenance Downtime	Total time spent on scheduled maintenance or upgrades.	<5% Ensures that system availability is maximized while still allowing for necessary updates and improvements.	TC02, TC02.1
21	System Availability	Measurement of system availability during peak and off-peak hours.	99.9% peak, 99.5% off-peak Maintaining high system availability across different usage periods is essential for ensuring that the system meets the needs of its users and remains reliable	*

2. Failure Modes and Data Analysis Approach

As described in preceding sections, this project's primary objective is to validate and quantify the efficacy of a system dedicated to monitoring UTM ecosystem performance and security. Given the intricate nature of this task, the

project's scope sharply focuses on specific failure modes aligned with identified KPIs. Team ResilienX has concentrated its efforts on ten distinct failure modes closely aligned with KPIs, laying a solid foundation to achieve the project's goal, with anticipation of subsequent efforts to further refine and expand upon this groundwork. The detailed breakdown of these ten failure modes, along with their high-level risk impact and association with KPIs is provided in the submitted Data Analysis Plan. The failure modes were first identified in the data analysis plan however were matured through the iterative design process and refined through the project. The ten failure modes for investigation and analysis for this project were down selected to be:

1. **USS lack of availability (USS arbitration failure):** Failure arising from a connected USS being, unavailable or unresponsive, occurs when the interconnected components experience delays or become non-responsive, hindering the overall ecosystem's performance, or a USS that is connected being intentionally removed or taken offline for a period of time.
2. **Surveillance sensitivity degradation:** A deviation or failure in the system's ability to accurately and reliably detect and track intended targets.
3. **Network Loss of Link:** A failure due to a loss of liveliness for a network component occurs when the component becomes unresponsive or inactive, leading to a breakdown in its expected functionality.
4. **Network degradation (e.g. high latency):** A failure resulting from network degradation occurs when the network experiences a decline in performance, leading to slower data transfer, increased latency, or intermittent connectivity issues.
5. **SDSP becomes slow or unresponsive (SDSP Latency):** Failure arising from a connected SDSP being latent or unresponsive, occurs when the interconnected components experience delays or become non-responsive, hindering the overall ecosystem's performance
6. **SDSP Loss of Liveliness:** A failure due to a loss of liveliness for a SDSP occurs when the SDSP becomes unresponsive or inactive, leading to a breakdown in its expected functionality or provided service.
7. **Aircraft tracking is unreliable or out of performance**: A failure arising from unreliable telemetry from a craft occurs when the transmitted data, crucial for monitoring the aircraft's status and performance, becomes inconsistent or inaccurate.
8. **Security vulnerability on a device:** A failure from a determined security vulnerability on a device occurs when a security control is not implemented, or other vulnerability is discovered on a device.

9. **Unauthorized or malicious device detection:** A failure resulting from an unauthorized or malicious device occurs when an external device gains unauthorized access to the ecosystem.

10. **Unknown or malicious system account:** A failure from a determined security vulnerability on a device occurs when malicious actors exploit weaknesses in the device's cybersecurity defenses, gaining unauthorized access or compromising sensitive data.

3. Detailed Design

Team ResilienX understands the critical role that requirement and architecture development play in ensuring the success of a project, especially when dealing with systems of systems (SoS). The intricate interplay of multiple systems necessitates a robust and comprehensive approach to defining requirements and establishing architectures that can seamlessly integrate and interact in a predictable manner and can be used to assure safe operations. By adhering to INCOSE (International Council on Systems Engineering) Systems Engineering Handbook [3], Team ResilienX ensures that the requirements document (provided in task 4.3) captures the detailed specifications and functionalities required of the system of interest. Likewise, the architecture document (provided in task 2.6) delineates the structural framework, interfaces, and interactions among system components, providing a clear blueprint for system integration and operation within the larger SoS context. This meticulous approach not only facilitates effective communication and collaboration among stakeholders but also lays a solid foundation for system performance, reliability, and scalability.

C. Integration

Task 3 focused on realizing the SoI for the project through integration of the identified AEs and infrastructure at the NUAIR Area of Regard and NY UAS Test Site (NYUASTS). Fig. 3 displays the project’s physical architecture and interfaces that were integrated during this effort.

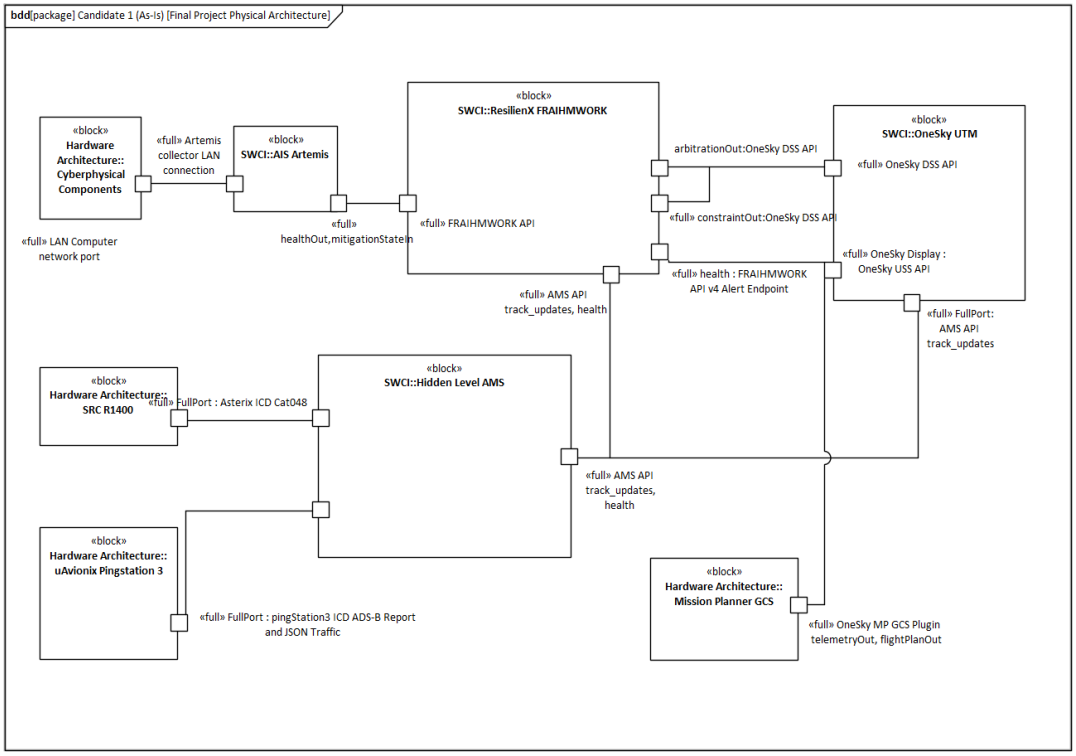

Fig. 3 Project Physical Architecture – Simplified

Table 8 provides the version and interface detail for the major AEs and other components used during this project for Team ResilienX.

Table 9 provides information for the test equipment and enabling systems used for the test, demonstration, and analysis.

Table 8 SoI and Technology Partner Software and Hardware Version Information

Component/AE	Version
ResilienX IASMS, FRAIHMWORK	v2024.08.06
OneSky UTM	v2472
OneSky DSS	v0.3.17
AIS Artemis	v1.0.0.0

Table 9 Test Equipment and External System Information

Item	Information
Cooperative Sensor	uAvionics pingStation 3
Non-Cooperative Radar	SRC R1400, spiral 2
NUAIR UAS	Carrier HX8
NYUASTS UAS	Faw Astro, Inspired Flight IF800
GCS	Mission Planner 1.3.77

D. Development and Implementation

Task 4 focused on finalizing the implementation by addressing failure mode identification, integration requirements, and developing essential documentation for contingency management within the UTM context. Thanks to the high TRL products provided by Team ResilienX, there was no need to develop new technologies; instead, the task concentrated on collaborating with Subject Matter Experts (SMEs) to investigate specific failure modes and the capabilities of the existing UTM AEs. This collaboration led to the creation of an exemplar SOP for relevant stakeholders. SMEs were interviewed, providing personas, context, and real-world and regulatory examples (e.g., United States of America Aeronautical Information Publication (AIP) Enroute Procedures [4]). The resulting Contingency Management SOP was developed and delivered as part of Task 4.4.

E. Test, Demonstration and Analysis

Task 5 was the culmination of the project, taking the integrated system and testing it utilizing the test and evaluation plan and procedures that were developed to verify the IASMS performance in monitoring and mitigating the failures identified. For this project, testing was strategically structured in three distinct phases to allow for incremental testing that validated integration and test approaches while reducing schedule risk. Although testing was completed in three phases, requirement verification and signoff was only performed in the final test and demonstration phase. Generally, the ResilienX incremental test approach would include testing and verifying requirements in earlier phases; however, the team decided to tailor the process for this project for efficiency. The three phases of test execution were:

- **Phase 1: Contractor simulated testing;** This phase involved using simulated data feeds and failure scenarios to validate the integration of system components (i.e., associated elements) and develop a robust test strategy. It was successful in identifying integration issues and aided in refining the test approach before proceeding to live testing.
- **Phase 2: Contractor live flight testing;** In this phase, testing was conducted with contractor-owned UAS to verify functionality, identify bugs, and validate procedures through real-world scenarios and in a relevant environment. It served as a dry run to ensure system readiness and functionality prior to formal evaluation.
- **Phase 3: Formal test and evaluation;** This final phase employs NUAIR and NYUASTS and contractor pilots and live data feeds to conduct formal testing. The focus was on verifying requirements and demonstrating the system's capabilities. It provided a comprehensive assessment of system performance under operational conditions and results are detailed in the Test Results section of this summary report.

The only phase of testing that resulted in formal test results for this project was phase 3. The other phases were valuable in identifying issues and preparing the products and team for formal verification. Phase 1 and 2 resulted in 8 identified bugs, two test procedure revisions, and proved valuable in crafting live flight scenarios necessary to showcase IASMS functionality. Phase 2 had a total of 4 live flights and utilized contractor owned UAS with live SDSP and sensor feeds.

III.Demonstration / Verification Results

Phase 3 of Task 4 (Test, Demonstration and Analysis) was conducted at multiple sites in Central New York on August 8th, 2024. The primary execution was concentrated at the NYUASTS in Rome, NY, and additional test personnel were distributed in Syracuse, Verona, and Canastota. Live flights were executed at both the NUAIR operation center in Canastota (9 flights) and at the NYUASTS by test site manager personnel (12 flights), a total of 21 flights were performed in Phase 3 meeting the contract required minimum number of flights (20 total for the contract, 25 were performed when including all phases). Fig. 4 depicts the geographic locations of the test personnel.

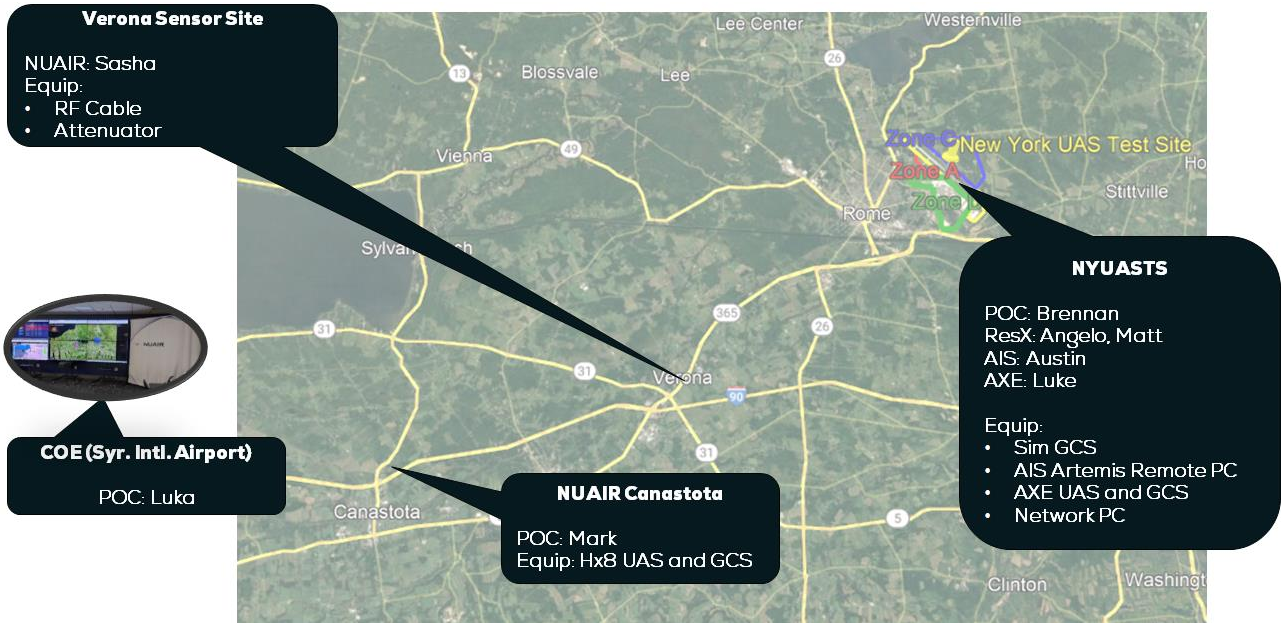

Fig. 4 Phase 3 Test Location Information

The test was structured in ten individual test cases that aligned one to one with the IASMS enabled UTM ecosystem failure modes. Four of the ten cases (some being denoted as “sub-cases”, due to the way the test plan was organized) were identified for live flights (TC02.1, TC04.1, TC04.2, and TC05.2). Fig. 5 and Fig. 6 depict the flight overlays for the live flights, these flights were repeated for the test cases as regression executions for additional analysis. The constraints depicted in Fig. 5 are associated with TC02.1 and TC05.2, the larger of the two constraints is for the surveillance sensitivity failure in TC02.1 and the smaller, circular one is for the unreliable telemetry in TC05.2.

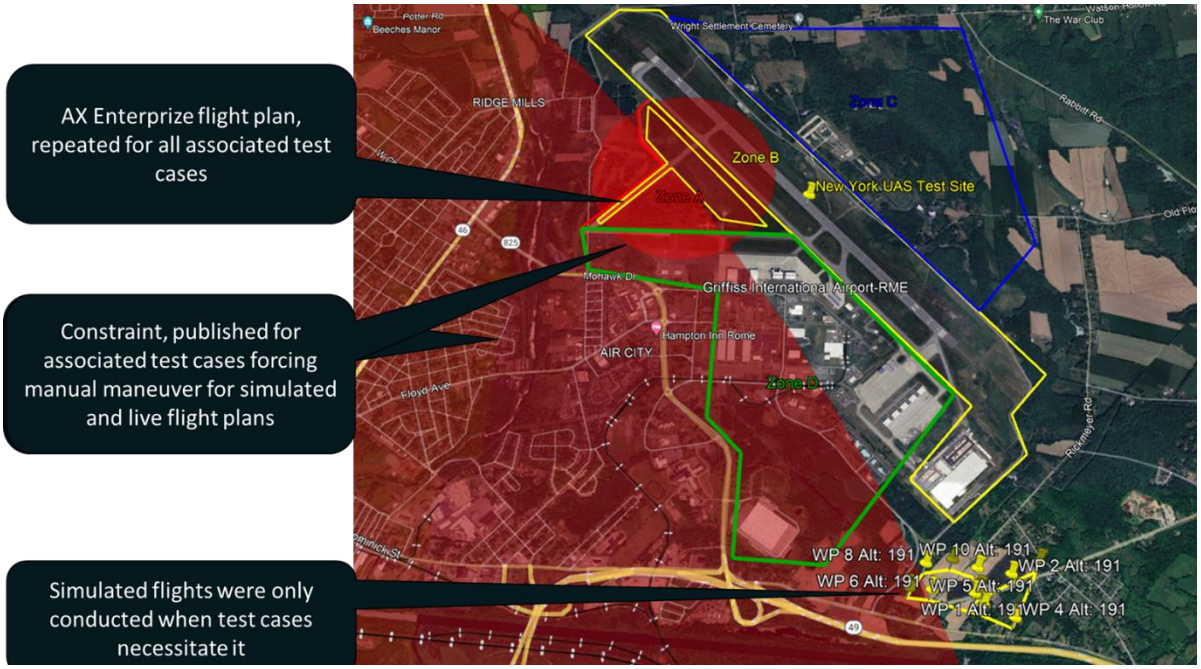

Fig. 5 AX NYUASTS Live and Simulated Flight Plan Overlay

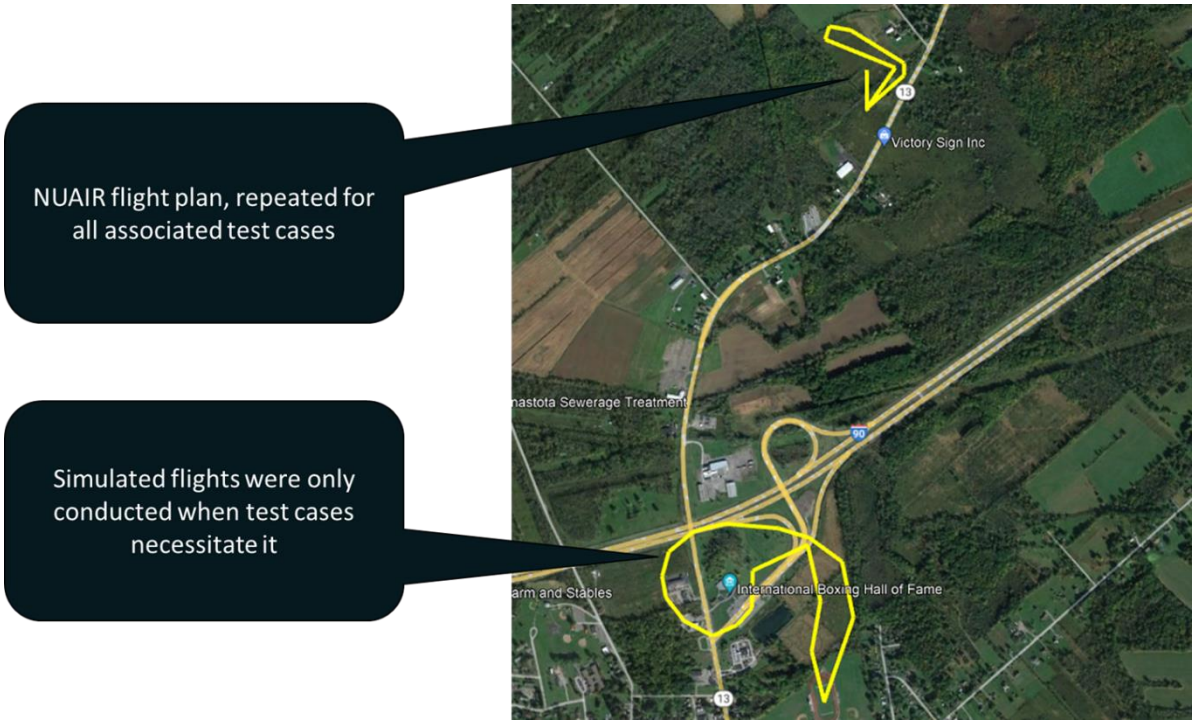

Fig. 6 NUAIR Canastota Live and Simulated Flight Plan Overlays

The test procedures were constructed such that any individual test case could be executed in any order which proved useful during execution to navigate around weather risk during the day. Fig. 7 depicts the test execute flow design.

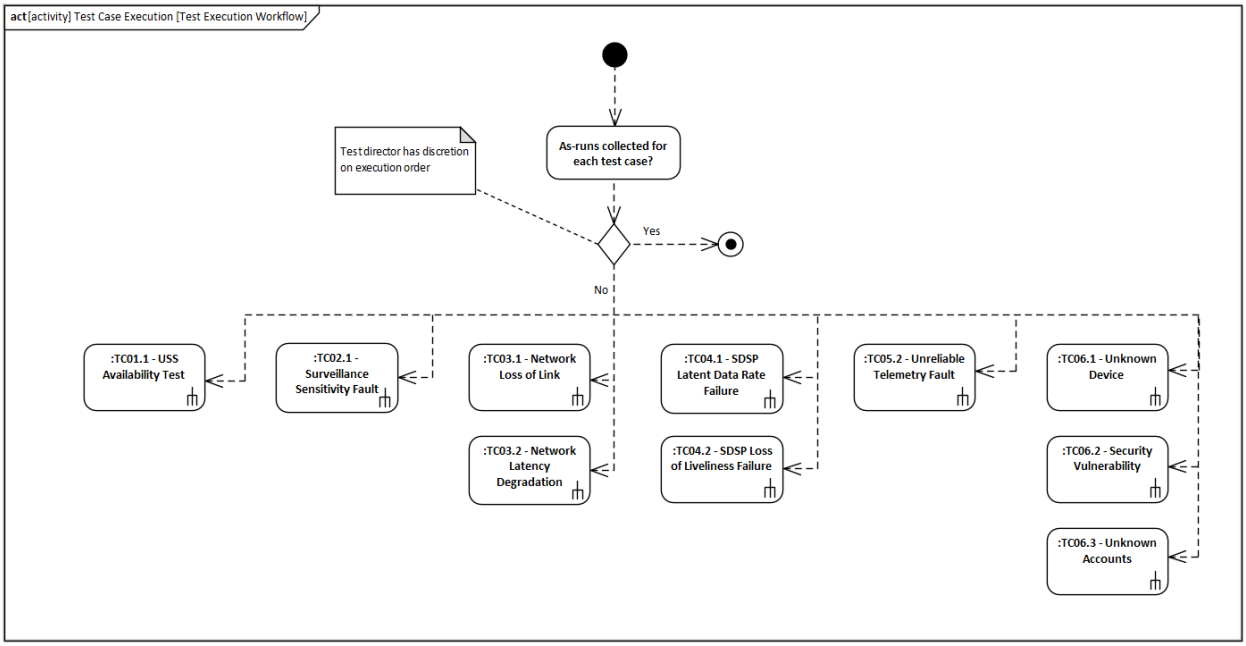

Fig. 7 Test Execution Workflow

The actual execution order during the official test was established by the test director at the start of testing, informed by current and forecasted weather and personnel availability. The sequence order for the day of execution was:

1. TC02.1
2. TC05.2
3. TC04.1
4. TC04.2
5. TC01.1
6. TC06.3
7. TC06.1
8. TC06.2
9. TC03.1
10. TC03.2

To summarize the detail in the test report, every test case that was executed was successful, showcasing the validity of an IASMS in a UTM ecosystem and verifying all 76 system level requirements. During execution there was a need

to perform redlines to the procedures, concurrence was received from all stakeholders and the test director and redlines were executed successfully.

The requirement verification trace matrix tables are included in Table 10 through Table 15, these align to the major IASMS functions under test. Fig. 8 provides the individual test case mapping to these major functions. The verdict for the associated requirement is dynamically applied to requirements traced to the individual test case within the ResilienX MBSE model. Note, that the sequence of requirements in the tables in this section are not hierarchal, these requirements should be read in their entirety for context. The tables are a result of the requirements being exported from their native format in the ResilienX MBSE model for this report. Appendix B: IASMS System Level Requirements provides the superset of requirements as well as the diagrams that provide the hierarchy and containment relationships.

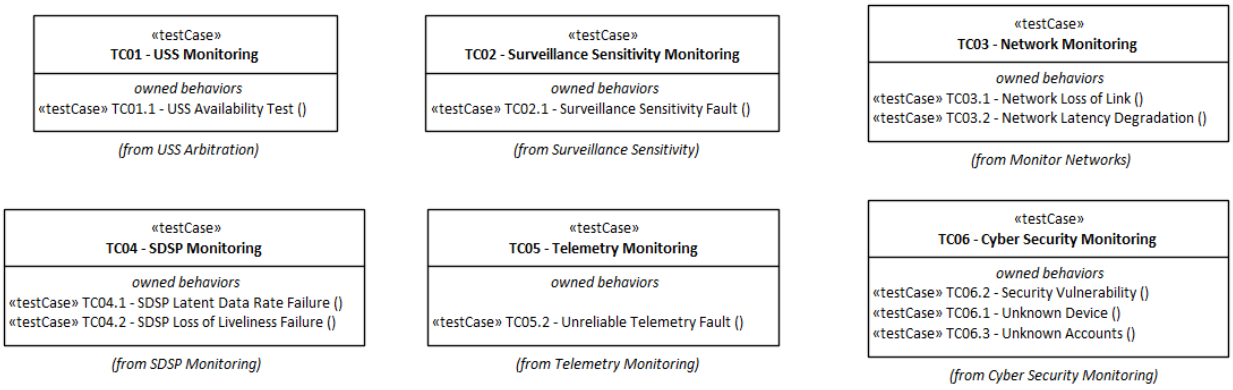

Fig. 8 Test Case Structure

A. USS Monitoring

1. Test Case Number

USS Monitoring/USS Arbitration was tested in TC01 with a single sub-case, TC01.1 – USS Availability Test

2. Test Case Description

A failure mode is induced by abruptly shutting down a USS that was last reported to a DSS as available. The DSS is notified of the faulted USS. All operational intents managed by the faulted USS are moved to a second active USS manually as indicated by the recommended mitigation. The operator is presented with a fault for the USS component with a manual mitigation to notify GCSs to transfer to a partner USS along with an automatic mitigation to set the USS's availability to DOWN.

3. Test Case VRTM

Table 10 UTM Arbitration VRTM

PUI/Name	Body	Verdict	Allocated To
FRAIHM439 - Monitor UTM Ecosystem for Failures	The system **SHALL** monitor all DSSs and USSs in a UTM ecosystem for failures, and report on them accordingly.	pass	TC01
FRAIHM440 - Model UTM Ecosystem Entities	The system **SHALL** create components and faults within FRAIHMWORK to model the USSs and DSSs within the UTM ecosystem.	pass	TC01.1
FRAIHM430 - Perform USS Arbitration	The system **SHALL** perform USS arbitration to indicate any offline or unavailable USSs within the UTM ecosystem.	pass	TC01.1
FRAIHM431 - Monitor Non-Conformance	The system **SHALL** monitor non-conformance as reported by a craft's managing USS.	pass	TC01.1
FRAIHM438 - Monitor USS Telemetry Updates	The system **SHALL** monitor telemetry updates associated with a USS's operational intents.	pass	TC01.1
FRAIHM432 - Register as USS	The system **SHALL** register itself as a USS to one or more DSSs in the target UTM ecosystem.	pass	TC01.1

4. Test Case Summary

TC01.1 was completed successfully resulting in all requirements for TC01 having a verdict of *pass*, demonstrating that FRAIHMWORK can detect failure modes for USS Monitoring and perform USS Arbitration.

B. Monitor Craft Telemetry

1. Test Case Number

Telemetry Monitoring was tested in TC05 with a single sub-case, TC05.2 – Unreliable Telemetry Fault. TC05.1 – Performance Envelope Fault was developed, and requirements associated with it but determined to be out of the purview of this project and deferred from testing and analysis.

2. Test Case Description

To ensure effective telemetry monitoring, the source of all telemetry must be officially registered as a component during startup. The operator confirms the visibility of telemetry sources on the Tiered Maintenance Interface (TMI) display (the display interface for FRAIHMWORK) as components. After registration, a simulated telemetry feed is supplied to FRAIHMWORK, featuring values with larger than nominal variances (i.e., on the SA display, the craft appears to hop around). The operator receives a fault notification on the TMI Display, along with a recommended mitigation to establish a constraint around the craft's position and altitude. Once the system maintainer approves, the Situational Awareness display depicts the 4D constraint around the last known location of the craft. Subsequently, the

simulated telemetry returns to normal conditions, the fault is cleared from the component, and the 4D constraint on the SA display is removed.

3. Test Case VRTM

Table 11 Monitor Craft Telemetry VRTM

PUI/Name	Body	Verdict	Allocated To
FAA088 Manage Constraint Reference	The system **SHALL** create Constraint References given the Operational Intent of the Craft whose telemetry data is faulted.	pass	TC05
FAA094 - Receive Craft Telemetry Data	The system **SHALL r**eceive Craft Telemetry Data.	pass	TC05
FAA117 - Determine Constraint Shape	The system **SHALL** determine the Constraint Shape. The shape will be dependent on the behavior of the craft velocity based on TBD methods.	pass	TC05
FAA093 - Specify Preferred Data Source	The system **SHALL** be capable of determining which telemetry data source is used for monitoring by default.	pass	TC05
FAA119 - Remove Constraint Reference	The system **SHALL** remove Constraint References based on TBD methods.	pass	TC05
FAA128 - Update Component State to Faulted	The system **SHALL** update the component state to Faulted.	pass	TC05
FAA090 - Receive GCS Telemetry Data	The system **SHALL** receive GCS Telemetry Data when requested.	pass	TC05
FAA129 - Register Monitored Components	The system **SHALL** register all monitored components. This will enable functions down the processing chain to register faults and apply mitigations to these components.	pass	TC05
FAA116 - Determine Constraint Size	The system **SHALL** determine the Constraint Size via TBD methods. Some methods could include: • Bollinger Bands based on SMA and STD of position updates. • Scaling the operational intent volume	pass	TC05
FAA118 - Update Constraint Reference	The system **SHALL** update Constraint References based on TBD methods. Look through the ASTM 3548-21 Section 5.7 CSTM0080, and A1. TABLE OF VALUES for more information.	pass	TC05
FAA120 - Determine Constraint Location	The system **SHALL** determine Constraint Locations based on TBD.	pass	TC05
FAA064 - Craft Telemetry Configuration Rules	The system **SHALL** ingest Craft Telemetry Integrity Rules to detect off-nominal craft telemetry. These rules should include: • Off-Nominal Velocity. • Off-Nominal Acceleration	pass	TC05

PUI/Name	Body	Verdict	Allocated To
FAA089 - Send Constraint Reference	The system **SHALL** send Constraint References to the managing USS of the craft whose telemetry data is faulted.	pass	TC05
FAA060 - Monitor Craft Telemetry	The system **SHALL** monitor Craft Telemetry. Failure Modes: • Performance Envelope Fault: Fault initiated following the failed validation of the integrity or reliability of a craft by assessing its performance within predefined operational limits or boundaries, performance envelope (range of conditions under which a system is expected to operate safely and effectively). • A failure arising from unreliable telemetry from a craft occurs when the transmitted data, crucial for monitoring the aircraft's status and performance, becomes inconsistent or inaccurate.	pass	TC05
FAA063 - Telemetry Fault Mitigation	The system **SHALL** provide Telemetry Fault Mitigation steps.	pass	TC05
FAA065 - Register Craft Telemetry Fault	The system **SHALL** register Craft Telemetry Faults.	pass	TC05
FAA075 - Register Unreliable Telemetry Fault	The system **SHALL** register Unreliable Telemetry Faults.	pass	TC05.2
FAA116 - Determine Constraint Size	The system **SHALL** determine the Constraint Size via TBD methods. Some methods could include: • Bollinger Bands based on SMA and STD of position updates. • Scaling the operational intent volume	pass	TC05.2
FAA115 - Detect Latent Telemetry Data	The system **SHALL** detect Latent Telemetry Data when a telemetry feed or AMS is providing a lack of track updates.	pass	TC05.2
FAA062 - Detect Unreliable Telemetry	The system **SHALL** detect Unreliable Telemetry.	pass	TC05.2
FAA077 - Mitigate Unreliable Telemetry Fault	The system **SHALL** mitigate Unreliable Telemetry Faults.	pass	TC05.2

4. Test Case Summary

TC05.2 was completed successfully, resulting in all requirements for TC05.2 and relevant requirements in TC05 having a verdict of *pass* (not executing TC05.1 doesn't affect verification status of requirements allocated to TC05). This demonstrated that FRAIHMWORK can detect failure modes for unreliable telemetry faults.

C. Monitor Surveillance

1. *Test Case Number*

Surveillance sensitivity monitoring was tested in TC02 with a single sub-case, TC02.1 – Surveillance Sensitivity Fault

2. *Test Case Description*

In this test case, an administrator configures specific surveillance sensors such that they are registered as components on the system display. Surveillance data with overlapping coverage areas is used to induce a surveillance sensitivity fault. The operator is alerted of the fault associated with the surveillance sensor. As a mitigation, the operator can add a constraint suggested by the system. Once the sensor's sensitivity is addressed, the fault and constraint is removed from the component.

3. *Test Case VRTM*

Table 12 Surveillance Monitoring VRTM

PUI/Name	Body	Verdict	Allocated To
FAA012 - Monitor Surveillance Service	Failure Mode: • A deviation or failure in the system's ability to accurately and reliably detect and track intended targets. The system **SHALL** monitor surveillance sensitivity data from available surveillance sources.	pass	TC02
FAA128 - Update Component State to Faulted	The system **SHALL** update the component state to Faulted.	pass	TC02.1
FAA089 - Send Constraint Reference	The system **SHALL** send Constraint References to the managing USS of the craft whose telemetry data is faulted.	pass	TC02.1
FAA129 - Register Monitored Components	The system **SHALL** register all monitored components. This will enable functions down the processing chain to register faults and apply mitigations to these components.	pass	TC02.1
FAA033 - Register Surveillance Sensitivity Fault	The system **SHALL** register all Surveillance Sensitivity Faults when it is determined that a sensor's sensitivity is off nominal.	pass	TC02.1
FAA105 - Manual Surveillance Fault Mitigation	The system **SHALL** provide Manual Surveillance Fault Mitigation options upon detection of a sensitivity fault.	pass	TC02.1
FAA034 - Surveillance Fault Mitigation	The system **SHALL** provide TBD options for Surveillance Fault Mitigation.	pass	TC02.1
FAA106 - Determine Non-Overlapping Airspace Coverage	The system **SHALL d**etermine Non-Overlapping Airspace Coverage where a surveillance sensor has exclusive ownership of.	pass	TC02.1

PUI/Name	Body	Verdict	Allocated To
FAA013 - Detect Track and Sensitivity Faults	The system **SHALL** detect track and sensitivity faults should there be any deviations or failures in surveillance sensitivity data.	pass	TC02.1

4. Test Case Summary

TC02.1 was completed successfully, resulting in all requirements for TC02 having a verdict of *pass.* This demonstrated that FRAIHMWORK can detect failure modes for Surveillance Monitoring.

D. Monitor SDSP

1. Test Case Number

SDSP monitoring was tested in TC04 with two sub-cases, TC04.1 – SDSP Latent Data Rate Failure and TC04.2 – SDSP Loss of Liveliness Failure

2. Test Case Description

To verify slow or unresponsive SDSP scenarios, the system administrator disconnects the SDSP or configures it to send deviant heartbeats. When the SDSP is disconnected or send heartbeats not according to the SLA, a fault is displayed on the TMI Display.

3. Test Case VRTM

Table 13 SDSP Monitoring VRTM

PUI/Name	Body	Verdict	Allocated To
FAA081 - Define Fault Code Configuration	The system **SHALL** define Fault Code Configuration items to be used for fault-to-mitigation mapping.	pass	TC04
FAA022 - SDSP Data Integrity Rules	The system **SHALL** contain SDSP Data Integrity Rules and bounds to determine degraded SDSP data links.	pass	TC04
FAA019 - Monitor SDSP Status	Failure Mode: Failure arising from a connected SDSP being latent or unresponsive, occurs when the interconnected components experience delays or become non-responsive, hindering the overall ecosystem's performance The system **SHALL** monitor the status of all Supplemental Data Service Providers (SDSP).	pass	TC04
FAA039 - SDSP Fault Mitigation	The system **SHALL** provide TBD options for fault mitigation surrounding SDSP loss of connection and degradation.	pass	TC04

PUI/Name	Body	Verdict	Allocated To
FAA129 - Register Monitored Components	The system **SHALL** register all monitored components. This will enable functions down the processing chain to register faults and apply mitigations to these components.	pass	TC04
FAA128 - Update Component State to Faulted	The system **SHALL** update the component state to Faulted.	pass	TC04
FAA021 - Detect Status Degradation	The system **SHALL** Detect Status Degradation for all SDSPs.	pass	TC04
FAA040 - Register SDSP Faults	The system **SHALL** register SDSP Faults for loss of connection and degradation faults.	pass	TC04
FAA053 - Manual SDSP Fault Mitigation	The system **SHALL** provide manual SDSP fault mitigation options upon detection of degraded or loss of connection of a SDSP.	pass	TC04
FAA039 - SDSP Fault Mitigation	The system **SHALL** provide TBD options for fault mitigation surrounding SDSP loss of connection and degradation.	pass	TC04.1
FAA055 - SDSP Update Rate Violation	The system **SHALL** detect SDSP Update Rate Violations based on defined heartbeat rates.	pass	TC04.1
FAA078 - Register SDSP Latency Fault	The system **SHALL** register SDSP Latency Faults.	pass	TC04.1
FAA111 - Detect SDSP Loss of Liveliness	The system **SHALL** detect Loss of Liveliness of any SDSPs.	pass	TC04.2
FAA079 - Register SDSP Loss of Connection Fault	The system **SHALL** register SDSP Loss of Connection Faults.	pass	TC04.2

4. Test Case Summary

TC04.1 and TC04.2 were completed successfully, resulting in all requirements for TC04 having a verdict of *pass.* This demonstrated that FRAIHMWORK can detect failure modes for SDSP Monitoring.

E. Network Monitoring

1. Test Case Number

Network monitoring was tested in TC03 with two sub-cases, TC03.1 – Network Loss of Link and TC03.2 – Network Latency Degradation.

2. Test Case Description:

Network monitoring verifies two failure modes: loss of network link and degraded latent networks. For the first, hosts are physically disconnected; for the second, third-party software is configured to induce latency faults.

3. Test Case VRTM

Table 14 Network Monitoring VRTM

PUI/Name	Body	Verdict	Allocated To
FRAIHM341 - Apply Network Monitoring Configuration	The system **SHALL** apply network monitoring configurations to the system.	pass	TC03
FRAIHM339 - Monitor Network Failures	The system **SHALL** monitor components for network related failures.	pass	TC03.1
FRAIHM340 - Monitor Degraded Network Connection	The system **SHALL** monitor components for a degraded network connection.	pass	TC03.2

4. Test Case Summary

TC03.1 and TC03.2were completed successfully, resulting in all requirements for TC03 having a verdict of *pass.* This demonstrated that FRAIHMWORK can detect failure modes for Network Monitoring.

F. Monitor Cybersecurity

1. Test Case Number

Cyber Security Monitoring was tested in TC06 with three sub-cases; TC06.1 – Unknown Device, TC06.2 – Security Vulnerability, and TC06.3 – Unknown Accounts

2. Test Case Description:

Cyber Security Monitoring involves detecting unknown devices, security vulnerabilities, and unknown accounts. AIS's Artemis system targets each of these modes. Using a provided laptop, simulations of these failure modes are conducted. For any failure mode detected, corresponding faults and mitigation were presented for operator review.

3. Test Case VRTM

Table 15 Monitor Cybersecurity VRTM

PUI/Name	Body	Verdict	Allocated To
FAA097 - Target Component Map	The system **SHALL** provide Target to Component Mappings so that registered components on FRAIHMWORK can be monitored.	pass	TC06
FAA027 - Cyber Security Integrity Rules	The system **SHALL** contain Cyber Security integrity rules and bounds.	pass	TC06
FAA046 - Cyber Security Configuration	The system **SHALL** load a Cyber Security Configuration.	pass	TC06
FAA100 - Apply Cyber Security Collector	For each target/component, the system **SHALL** apply Cyber Security Collectors. Multiple collectors can be used for one target.	pass	TC06

PUI/Name	Body	Verdict	Allocated To
FAA023 - Monitor Cyber Security Service	Failure Modes: • A failure resulting from an unauthorized or malicious device occurs when an external device gains unauthorized access to the ecosystem. • A failure from a determined security vulnerability on a device occurs when a security control is not implemented, or another vulnerability is discovered on a device. • A failure from a determined security vulnerability on a device occurs when malicious actors exploit weaknesses in the device's cybersecurity defenses, gaining unauthorized access or compromising sensitive data. The system **SHALL** monitor Cyber Security data.	pass	TC06
FAA042 - Cyber Service Fault Mitigation	The system **SHALL** provide TBD options for fault mitigation surrounding malicious accounts, unauthorized devices, and security vulnerabilities.	pass	TC06
FAA098 - Collector to Target Mapping	The system **SHALL** contain a Collector to Target Mapping that allows multiple collectors to monitor cyber risks on a specific target.	pass	TC06
FAA099 - Retrieve All Registered Components	The system **SHALL** retrieve all registered components.	pass	TC06
FAA102 - Manual Cyber Mitigation	The system **SHALL** initiate a manual Cyber Mitigation operation for non-automated mitigations. This includes Suspicious Data Activity and Device Vulnerabilities conditions.	pass	TC06
FAA128 - Update Component State to Faulted	The system **SHALL** update the component state to Faulted.	pass	TC06
FAA043 - Register Cyber Security Fault	The system **SHALL** register the following as faults: • MEDIUM severity for all Unauthorized Access. • MEDIUM severity for Unknown Accounts. • MEDIUM severity for any Device Security Vulnerabilities of high criticality.	pass	TC06
FAA025 - Detect Unknown Device	The system **SHALL** detect any unknown or unauthorized devices connected to the network infrastructure.	pass	TC06.1
FAA024 - Security Vulnerability	The system **SHALL** detect security vulnerabilities.	pass	TC06.2
FAA026 - Unknown Account	The system **SHALL** detect Suspicious Data Activity conditions via account information aggregation and historical comparison.	pass	TC06.3
FAA103 - Monitor for Operator Approval of Mitigation	The system **SHALL** monitor for Operator Approval of Mitigation by polling the mitigation state of the reported fault.	pass	TC06.3
FAA101 - Removal of Unauthorized Account	Upon identified Unauthorized Access, the system **SHALL** institute Removal of Unauthorized Account.	pass	TC06.3

4. Test Case Summary

TC06.1, TC06.2, and TC06.3 were completed successfully, resulting in all requirements for TC06 having a verdict of *pass.* This demonstrated that FRAIHMWORK, when integrated with Artemis, can detect failure modes for Cybersecurity Monitoring.

IV.Data Analysis

A. UTM Arbitration

USSs manage the constraints and operations for a given airspace volume and have predetermined coverage areas when they register with the DSS. Since many USSs can operate in overlapping areas and are the central authority for managing local operations, ASTM F3548-21 [5] provides requirements and guidance for USS to maintain and communicate availability. However, since a service's ability to self-monitor for failures is sometimes limited, a 3rd party service (IASMS) can and should exist to perform arbitration and request specific state overrides of a USS's self-reported status if a failure is detected. Typical questions that come to mind with self-monitoring status are; “How will other USSs or operators know if a service is not performing as intended but reporting it’s available”, or “If a USS is intentionally offline or unavailable how is that information shared”. Additionally, the DSS does not assess the health of a USS, it only sets availability based on what the USS says its availability is. If a USS abruptly shuts down, the DSS has no way of knowing that the USS is down unless an IASMS is there to arbitrate.

UTM arbitration is the ability for an IASMS to perform this arbitration function and answer the concerns above. Team ResilienX determined that UTM arbitration needs to exist to monitor at least the following failures:

- A USS being:
    - Unavailable or unresponsive: occurs when the interconnected components experience delays or become non-responsive, hindering the overall ecosystem's performance
    - Intentionally removed or taken offline for a period of time (also considered USS self-reported unavailable)

In the FAA UTM Implementation plan [2] the FAA specified in section 4 the need for UTM services to support interoperability. The discussion of this focused on FAA oversight in approving a USS for connections, SDSPs serving more than just USSs, and reliance on industry to verify sufficient interoperability. The analysis and testing for the IASMS to provide arbitration services to the UTM ecosystem supports the vision for ongoing validation checks and information sharing. FRAIHMWORK implements USS arbitration and can detect failure modes for USS Monitoring.

B. Monitor Craft Telemetry

Monitoring craft telemetry is crucial for ensuring safety in unmanned aviation systems, especially when addressing failure modes such as unreliability and out-of-performance issues. Currently, the USS interoperability ASTM F3548-

21 Section A2.5.2 [5] standard mandates telemetry sharing only when a craft exits its designated operational volume. This limitation overlooks potential critical issues occurring within the operational area, such as GPS or navigation failures, which could jeopardize safety but remain undetected under the current regulations.

If a craft experiences issues with its telemetry system, such as intermittent or inconsistent data transmission, there is no requirement to report these issues if the craft remains within its operational area. This can obscure potential safety concerns. Additionally, a craft might operate within its designated volume but experience performance issues, such as deviations in GPS accuracy or navigation errors. These issues may not be immediately apparent and could affect the craft's ability to perform safely and effectively.

The importance of comprehensive telemetry monitoring as a specific function within the UTM ecosystem is to:

- Enhanced Safety: By monitoring all telemetry data, the IASMS ensures that both reliability and performance issues are addressed proactively, reducing the risk of accidents and enhancing overall safety.
- Proactive Issue Detection: Continuous monitoring allows for the early detection of problems that might not trigger standard reporting requirements, enabling timely intervention and resolution.
- Regulatory Advancement: This approach supports the evolution of safety standards by addressing gaps in current regulations and setting a higher bar for safety in uncrewed aviation.

In summary, integrating comprehensive telemetry monitoring through the IASMS addresses the critical gaps in current standards, ensuring a higher level of safety by identifying and managing potential issues before they compromise operational integrity. FRAIHMWORK implements and can detect failure modes for unreliable telemetry faults.

C. Monitor Surveillance

Surveillance information is fundamental for maintaining airspace awareness and ensuring the safe and efficient operation of UAS. Accurate and reliable surveillance data is essential for understanding the positions, movements, and status of aircraft within a given airspace, particularly in complex and dynamic environments. Current standards only require a Surveillance SDSPs to report the health of its surveillance systems. This limited reporting does not encompass the full scope of surveillance performance, such as sensor reliability and data accuracy. As a result, critical issues such as sensor degradation or inaccuracies in detecting aircraft may go unnoticed, potentially leading to safety risks. Additionally, sensors used in surveillance systems can experience degradation in performance over time due to

various factors such as environmental conditions, wear and tear, or technical malfunctions. Current regulations do not require systematic monitoring of these performance aspects.

Without real-time performance monitoring, users may not be immediately aware of a sensor's failure to detect or track aircraft effectively. This can lead to gaps in situational awareness and increased risk of collisions or other safety incidents. Team ResilienX determined that the IASMS provides comprehensive surveillance monitoring in real-time to assess and alerts relevant users when a sensor's performance falls below acceptable thresholds. These alerts enable quick intervention to rectify issues, ensuring continuous and effective surveillance coverage. The IASMS can mitigate risks through the use of constraints or other user alerts, ensuring that current and planned flights are deconflicted with airspace that is reliant on surveillance information from a degraded sensor. This provides:

- Enhanced Airspace Awareness: By maintaining high standards for sensor performance and data accuracy, the IASMS ensures that airspace awareness is consistently reliable, supporting safer and more efficient UAS operations.
- Early Detection of Performance Issues: Continuous monitoring and proactive alerts allow for the early detection and resolution of performance problems, reducing the likelihood of undetected failures that could compromise safety.
- Improved Safety Standards: Implementing comprehensive surveillance checks and alerts advances safety standards by addressing gaps in current regulations and providing a higher level of assurance for surveillance effectiveness.

Robust surveillance monitoring and mitigation through the IASMS is essential for maintaining accurate and reliable airspace awareness. By continuously monitoring sensor performance and providing timely alerts for performance degradation, the IASMS enhances safety and operational effectiveness in the UTM ecosystem. FRAIHMWORK implements the ability to monitor surveillance devices within the UTM ecosystem for two types of failure modes assessed in this project.

D. Monitor SDSP

SDSPs play a pivotal role in the UTM ecosystem by delivering critical data and services essential for safe and efficient operations. This includes providing surveillance, weather, and other vital services. Monitoring the performance and reliability of these SDSPs is crucial for maintaining the integrity of the UTM system.

SDSPs deliver essential data and services, such as surveillance and weather information, that are integral to the UTM ecosystem's operations. While ASTM standards outline service level agreements (SLAs) and performance metrics for these services, there is currently no mandated mechanism for confirming that these standards are being met unless specifically implemented by the subscriber. To ensure that SDSPs are performing as required, it is critical to have a monitoring system in place that verifies compliance with SLAs and assesses the quality of the services provided. This monitoring helps ensure that the data and services delivered meet the required standards for safety and operational effectiveness.

ASTM standards provide a framework for SDSP performance but do not mandate continuous, automated verification of these standards. This limitation can lead to gaps in service quality assurance and operational oversight. Without a dedicated monitoring service, there is no assurance that SDSPs are consistently meeting performance requirements, which could lead to unrecognized service failures or degradation.

The IASMS should incorporate capabilities to continuously monitor the performance of SDSPs. This includes verifying that surveillance, weather, and other critical data services adhere to the prescribed SLAs and performance criteria. The IASMS should assess the quality and reliability of the services provided by SDSPs. This involves monitoring service delivery metrics, detecting deviations from expected performance, and ensuring that data accuracy and timeliness meet the operational needs of the UTM ecosystem.

By incorporating an IASMS, the UTM ecosystem gains an automated, independent verification mechanism that confirms SDSP compliance with SLAs and performance standards. This ensures that critical services are consistently reliable and meet the required safety and operational criteria. Additionally, the IASMS provides:

- Enhanced Service Reliability: Continuous monitoring of SDSPs by IASMS helps identify and address potential issues before they impact UTM operations, thereby enhancing the overall reliability of the services provided.
- Improved Operational Oversight: IASMS provides comprehensive oversight of SDSP performance, offering real-time insights and alerts on service quality. This facilitates timely intervention and corrective actions to maintain optimal service levels.

Overall, monitoring SDSPs within the UTM ecosystem is essential for ensuring the quality and reliability of critical data and services. While ASTM standards provide performance guidelines, the IASMS plays a crucial role in automating and verifying compliance with these standards. By incorporating robust SDSP monitoring capabilities, the

IASMS enhances service reliability, operational safety, and overall performance of the UTM ecosystem. During this project, FRAIHMWORK was configured to monitor SDSPs within the target ecosystem and it's functionality was validated.

E. Network Monitoring

In the UTM ecosystem, various physical components and devices are interconnected through a network infrastructure. These components are crucial for the overall success and safety of the UTM ecosystem, supporting vital functions such as communication links, processing, detect-and-avoid services, and surveillance. Ensuring that the network between these interconnected components performs as designed is critical for maintaining the integrity and effectiveness of the UTM system.

The UTM ecosystem relies heavily on a complex network infrastructure to enable effective communication and data exchange between its various components. Any degradation in network performance or loss of connectivity can severely impact the functionality and safety of the entire system. In a federated UTM ecosystem, where multiple independent systems and services interact, there is an inherent need for situational awareness regarding the performance of the network. The FAA UTM ConOps [1] highlights the necessity of monitoring network performance to ensure seamless integration and operation across different services.

Team ResilienX determined that comprehensive network monitoring is essential to ensure that the network infrastructure performs as expected. This includes monitoring for network degradation, loss of link, and other issues that could compromise the operation of the UTM ecosystem. The IASMS is well-suited to provide this situational awareness. It should include capabilities for monitoring network performance, identifying degradation, and detecting loss of link. The IASMS ensures that any issues affecting network connectivity and performance are promptly addressed. All of this provides:

- Enhanced Reliability: Continuous network monitoring helps maintain the reliability of communication links and data exchanges, supporting the overall stability and effectiveness of the UTM ecosystem.
- Early Issue Detection: Proactive monitoring enables early detection of network issues, allowing for timely intervention and resolution before they escalate into more significant problems.
- Improved Situational Awareness: By providing real-time insights into network performance, the IASMS enhances situational awareness for operators and stakeholders, contributing to better decision-making and operational safety.

Effective network monitoring is essential for ensuring the reliable performance of interconnected components within the UTM ecosystem. The IASMS provides a robust framework for monitoring network performance, detecting degradation, and managing loss of link. By incorporating these capabilities, the IASMS supports the overall safety and operational success of the UTM system. FRAIHMWORK implements and can detect key failures related to network monitoring, this was validated during this project.

F. Monitor Cyber Security

In UTM ecosystems, cybersecurity is critical to ensuring the safety and integrity of operations. This was a prime focus of the GUTMA Secure and Resilient UTM Task Force Report [6] and previous BAAs. Monitoring for unknown devices, malicious malware, unauthorized users, and other potential threats is essential for maintaining the security and reliability of the system. Given the complexity and federated nature of UTM systems, robust cybersecurity measures must be implemented to address these challenges effectively. This project focused on three main needs"

- **Monitoring for Unknown Devices:**
    - **Problem:** The UTM ecosystem consists of various interconnected devices and systems. The introduction of unknown or unauthorized devices can pose significant risks, including potential breaches of sensitive information or disruptions to system operations.
    - **Solution:** Implementing continuous monitoring to detect and identify unknown devices is crucial. This includes establishing a baseline of authorized devices and using intrusion detection systems to flag any unauthorized or unfamiliar devices attempting to connect to the network.
- **Detection of vulnerabilities or malware:**
    - **Problem:** Security vulnerabilities can compromise the integrity and functionality of UTM systems by disrupting operations, stealing data, or introducing vulnerabilities. Traditional antivirus and anti-malware solutions may not be sufficient for the dynamic and complex environment of UTM ecosystems.
    - **Solution:** Advanced detection mechanisms, including real-time scanning, behavioral analysis, and anomaly detection, should be employed. This involves monitoring network traffic, system logs, and application behaviors to identify and respond to potential malware threats swiftly.
- **Unauthorized User Access:**

- **Problem:** Unauthorized access by individuals with malicious intent or insufficient clearance can lead to data breaches, system manipulations, or operational disruptions. Ensuring that only authorized personnel have access to critical systems and data is a fundamental security requirement.
- **Solution:** Implementing robust authentication and access control mechanisms is essential. This includes monitoring user access logs, enforcing multi-factor authentication, and conducting regular audits of user permissions to prevent unauthorized access.

Additional IASMS functionality for cybersecurity should include network intrusion detection and prevention, data integrity and confidentiality. These were not the focus items of this project but are clear capabilities that should have focus. The IASMS should integrate comprehensive cybersecurity monitoring capabilities to address the above challenges. This includes real-time monitoring, threat detection, and response mechanisms to safeguard the UTM ecosystem.

The IASMS should adopt a holistic approach to cybersecurity, encompassing network monitoring, device management, user authentication, and data protection. By providing end-to-end visibility and control, IASMS helps ensure the overall security and resilience of the UTM ecosystem. As cybersecurity threats evolve, the IASMS must adapt its monitoring and response strategies accordingly. This involves updating security protocols, enhancing detection algorithms, and staying informed about emerging threats and vulnerabilities.

In the UTM ecosystem, effective cybersecurity monitoring is essential for protecting against potential threats and ensuring the safety and reliability of operations. By addressing the challenges of unknown devices, malicious malware, and unauthorized access, and integrating these monitoring capabilities within the IASMS framework, the UTM ecosystem can achieve a higher level of security and resilience. FRAIHMWORK, integrated with Artemis, provides a robust IASMS with proven cybersecurity functionality. This project focused on the three cyber related failure modes validating baseline functionality and the solution is flexible to growing concerns and needs in this space.

V.Challenges

UTM ecosystems face significant challenges due to the fundamental differences between traditional aviation systems and the current state of the uncrewed aviation industry. While traditional systems benefit from established design assurance standards and safety requirements built over years of experience, these standards are not easily applicable to uncrewed aviation due to industry immaturity, scale complexities, and innovative technology implementations within federated, service-based architectures.

The federated nature of UTM systems introduces additional risks and complexities, including the need for standardized interfaces and data exchange protocols to ensure interoperability between disparate components. Cybersecurity concerns are amplified in federated systems, where the distributed nature of components requires robust mechanisms for authentication, secure data distribution, and protection against various cyber threats. These systems must also address challenges related to verifying the security and reliability of individual components and their interactions within the ecosystem.

Specifically, the application of safety-critical engineering principles, such as increasing robustness, resiliency, and fault tolerance, encounters hurdles in federated system-of-systems environments. Rapid technology evolution and the comparative immaturity of involved systems exacerbate gaps in addressing safety, performance monitoring, fault management, and cybersecurity. The lack of comprehensive guidance and regulations tailored specifically to UTM ecosystems and specifically the IASMS construct further complicates the situation.

The project faced notable challenges in defining a coherent and actionable safety and security framework for the federated UTM ecosystem. Team ResilienX navigated these challenges by leveraging our substantial expertise in ATM and UTM domains, combined with extensive experience in systems engineering and cybersecurity. We examined established frameworks and regulations applicable to similar safety-critical systems and adapted relevant principles and best practices to address the unique complexities of UTM ecosystems and IASMS.

Our approach involved:

- Standardized Interfaces and Data Exchange: Developing and implementing standardized interfaces and protocols for data exchange to ensure consistent and secure communication between federated components.
- Robust Cybersecurity Measures: Addressing cybersecurity concerns with comprehensive strategies for authentication, secure data distribution, and protection against cyber threats, adapting to the rapidly evolving technology landscape.

- System Verification and Validation: Ensuring that all components and their interactions within the federated system are secure and reliable, incorporating rigorous testing and validation processes.
- Regulatory Adaptation: Creating a security baseline that considers emerging threats and evolving regulations, ensuring that future UTM systems can meet robust security and assurance requirements.

By synthesizing domain knowledge and systems engineering proficiency, we developed a pragmatic strategy to address regulatory gaps, enhance security, and guide the implementation of effective safety measures. This approach is crucial for validating the IASMS concept and establishing a standardized framework to support the integration of UAS into the national airspace system.

VI.Lessons Learned

This section delves into the lessons learned during contract execution, viewed from the contractor's perspective. Section VII outlines recommendations pertaining to project goals, distinct from the lessons discussed in this section, with an emphasis on contract setup, execution, and related processes. Aligned with program management reviews, this section is further divided into two subsections: vendor process improvements and lessons learned, and process improvements and lessons learned for the FAA.

A. Vendor Process Improvements and Lessons Learned

In this section, we detail the process improvements implemented by Team ResilienX, driven by the ethos of continuous improvement and a commitment to enhancing execution methods. Through a dedicated focus on refining operational strategies, we have embraced a culture of continual enhancement aimed at optimizing our performance and service delivery. We've broken lessons learned into three major categories: coordination, project structure, and team collaboration.

1. *Coordination:*
    - Seek out and schedule dedicated deliverable review meetings are beneficial for feedback and understanding of all parties.
    - Maintain open communication with FAA personnel regarding schedule revisions.
2. *Project Structure:*
    - Have a robust integration plan and begin data collection on existing functionality early vice all at once.
3. *Team Coordination:*
    - Model based artifacts are difficult to digest for audiences not accustomed to reviewing the material or viewing it in a medium that is not a model-based engineering tool
    - With a distributed team and the design being MBSE based, setup external model collaboration environment as part of the project initiation phase to streamline design efforts.
    - Maintain engaging representative users of the system early to inform the design. Specific to this period, having representative system operators participate in the contingency management requirement derivation was critical to ensure efficient SOP development.

B. Process Improvements and Lessons Learned for the FAA

In this section, we highlight the process improvements and lessons learned for the FAA, stemming from our collaborative program. Through our engagement, we've identified opportunities for the FAA to enhance their contract execution processes, promoting efficiency and effectiveness in their operations.

- Dedicated deliverable review meetings are beneficial for feedback and understanding of all parties.
- If resources allow, it might be beneficial for regularly scheduled Technical Interchange Meetings (TIMs) to discuss technical deliverables, gain valuable insight and vision for the path forward, etc.
- For iterative design processes, the ability to submit revised, previously provided deliverables would be beneficial.

VII. Recommendations

This section details recommendations stemming from our contract execution, data analysis, testing, and demonstration phases. Through examination and evaluation of project outcomes, we have identified key areas where strategic improvements and enhancements can be implemented to further UTM adaptation, reliability, and operational effectiveness. We've categorized the recommendations into three groups: enhancements to existing standards, rulemaking, and additional considerations.

A. Enhancements to Existing Standards:

- ASTM F3548-21, USS Interoperability:
    - This standard specification lacks a function in the A2.3 USS-DSS Interfaces, A2.4 Other DSS Interfaces sections, and A2.7 DSS Testing for corresponding testing requirements for querying all registered USSs and retrieving their availability.
        - Currently, USSs can only be discovered if they have recently posted an Operational Intent or Constraint Reference
    - The standard might consider SDSPs, specifically an IASMS, to have roles in the Discovery and Synchronization Service (DSS) that enable USS monitoring and contingency management. The final report revision will include suggested edits to ASTM and other standards that include the construct of a UTM system utilizing an IASMS to enhance security.
        - DSS role for IASMS that allows for global subscriptions and constraint management.
    - USS standard interface allowing for alerting.
- ASTM F3673-23, Standard Specification for Performance for Weather Information Reports, Data Interfaces, and Weather Information Providers (WIPs):
    - The specification provides specificity for the types of Weather Information present in the WIP interface but lacks guidance on message structure. It is recommended for harmonization that exemplar schemas for the types highlighted in the standard are included in an appendix.
    - Requirement 5.2.2 points to ISO/IEC 27001, which is an open framework for compliance, which can vary based on specific needs of a cybersecurity program. The requirement does not provide guidance on minimum levels of compliance.

- Requirement 5.2.3 is overly constraining to the data exchange implementation of a Weather Information Provider.
- The term, “Weather Information” is used throughout the standard, as is “Weather Data”, but neither is defined. Subtypes of weather data are however defined, but the distinction between Weather Information and Weather Data are essential.

- ASTM F38 General Topics:
  - IASMS Standard: develop an ASTM standard that defines minimum required functions and performance for an IASMS within the context of UTM. This would relate IASMS functions to the safety constituents of flight operations (operators, aircraft, the environment, and associated elements).
    - FAA UAS BVLOS Aviation Rulemaking Committee, Final Report, dated March 10, 2022 provided recommendations for BVLOS. With Part 108 on the horizon, it is critical that a standard that identifies what is needed within the UTM ecosystem to support BVLOS operations, not just specific to aircraft operations, but across the full gamut of enabling capabilities on the ground and in the air, aircraft, operator and environment from a safety management standpoint.
    - There is a need for safety assurance and fault recovery functions throughout the UTM ecosystem for BVLOS at scale. A specification for an IASMS would provide consistency and standardization and interoperability to these systems.
    - This work would be most beneficial to industry if it included an API specification (such as what was done with the USS interoperability standard) that could be used by UTM integrators to connect their systems to an IASMS, and to make use of validated or trusted data flowing through the ecosystem.
    - Additionally, beyond an API specification, the standard should include a template means-of-compliance as an appendix for UTM systems implementing the standard, including workflows or sequences in which the UTM elements interact with the IASMS to meet IASMS requirements.

B. Proposed BVLOS Ruling

When considering the arduous process of rulemaking for operations such as BVLOS flights, Team ResilienX concludes that data and concepts relating to this project are paramount to the FAA. Below are a number of recommendations for the FAA's consideration:

- Operational safety assurance vs design assurance: Current aviation software design assurance standards are not viable for the emerging aviation industry. Team ResilienX recommends a focus on operational safety assurance. Whereas design assurance is in place to reduce the failure rate of a system, operational safety assurance assumes things will fail and that the ecosystem can maintain safe operations in the face of failure through monitoring, assessing, and mitigating those failures in-time to prevent an incident. We recommend that the FAA lean into operational safety assurance in Part 108, supported by IASMS concepts, to maintain safety in these emerging uncrewed operations.
- Establish IASMS Guidelines: Develop clear guidelines and standards for utilizing an IASMS for BVLOS operations. The guidelines should outline the essential components, requirements, and implementation steps for adopting and maintaining an effective IASMS to support scaled BVLOS operations especially when ancillary technologies (service providers such as USS/DSS/SDSPs, sensors, proprietary technology, etc.) are key to enable safe operations. An IASMS is necessary to ensure safety assurance and contribute to contingency management and operational safety assurance.
- Inclusion of applicable risk assessment methodology of BVLOS operations that includes quantified measures of acceptability which sufficiently account for the total air and ground risks associated operations and mitigating risks.
- Ensure Scalability and Flexibility: Design IASMS guidelines and requirements to be scalable and adaptable to varying sizes, complexities, and types of BVLOS operations. Allow for flexibility in implementation while maintaining core safety and risk management principles.
- Establish Compliance and Monitoring Mechanisms: Define compliance criteria, performance metrics, and monitoring mechanisms to assess the effectiveness and performance of IASMS in BVLOS operations.
- Standardize UTM system interfaces: The data within UTM ecosystems today is messy. For the most part, the formats are not standardized, the protocols are not standardized, and the interactions and data flows are not standardized. This is a limiting factor for scalability as every new location requires a massive integration effort just to get the subsystems talking to each other. Many standards describe the functional and/or performance

requirements, but leave the interoperability of the data up to the implementation. We have come to a point in the industry where we need to standardize this interoperability to scale.

C. Additional Considerations

1. Standardized UTM Ecosystem Interfaces

In addition to the recommendations above, Team ResilienX observes that for each entity in the UTM ecosystem (SDSP, USS, GCS, etc.), a required standard and secured interface for ecosystem health status, including functionality for alerting is vital for information sharing. These interfaces facilitate information sharing, collaboration, and communication among BVLOS operators, regulatory authorities, and industry stakeholders. Having the ability to communicate and share ecosystem health information drives knowledge exchange, continuous improvement, and enhances safety of the airspace.

2. Follow-on Activities

A follow-on R&D effort is envisioned to advance the understanding and application of KPIs across the UTM ecosystem. This initiative will focus on identifying additional KPIs critical to the comprehensive assessment of UTM performance and safety, particularly in the context of BVLOS operations. The effort will involve researching and establishing robust mechanisms for measuring these KPIs, addressing gaps and challenges, and ensuring accurate data collection and analysis. By advancing the understanding of KPIs and their measurement, this effort aims to support the development of proposed BVLOS regulations, enhance performance metrics, and refine complex cybersecurity KPI values. This approach will contribute to a more detailed and reliable framework for UTM operations, ultimately strengthening safety protocols and regulatory compliance.

VIII.Conclusion

In conclusion, this project successfully achieved its primary objectives of identifying failure modes, testing these against an IASMS, and validating the effectiveness of the IASMS within the UTM ecosystem. Our comprehensive approach involved measuring ten critical failure modes and rigorously testing them to assess the IASMS's performance and reliability.

Through extensive testing and analysis, Team ResilienX demonstrated that the interfaces between system components are robust and meet the required standards. The IASMS proved to be an effective solution for managing and mitigating failure modes, addressing the challenges inherent in federated, service-based architectures. Our efforts showed that the IASMS framework is capable of handling the complex safety and cybersecurity demands of the UTM ecosystem.

The project also confronted and overcame significant challenges related to cybersecurity, federated system complexities, standardized interfaces, and data exchange protocols. By developing and implementing a structured framework for the IASMS, we provided a foundational security baseline and addressed critical issues such as authentication, secure data distribution, and system verification.

Overall, the IASMS framework not only met but exceeded expectations, proving to be a viable solution for ensuring safety and reliability within the UTM ecosystem. The insights gained and the solutions developed during this project pave the way for future advancements and provide a robust foundation for integrating uncrewed systems into the NAS.

Appendix A: Operational Scenarios

Incorporated within this appendix are the operational scenarios associated with the failure modes outlined in the Data Analysis Plan submitted in Task 2.1 of this project. The operational scenarios presented herein offer crucial contextual insights for stakeholders, enhancing their comprehension of the project's requirements and facilitating informed decision-making.

Operational Scenarios in this appendix are depicted on a parallel timeline to demonstrate how Users and the system itself interact through the usage of its functions and capabilities. Specific instances of details in the Operational Scenarios are not meant to be exhaustively specified. For example, it isn't worth specifying every type of car that a camera system can track, there would be a single Operational Scenario where the camera system tracks a sports car, which would cover types of other cars that would be more exhaustively described by functional and performance requirements.

A. USS Arbitration Failure Mode

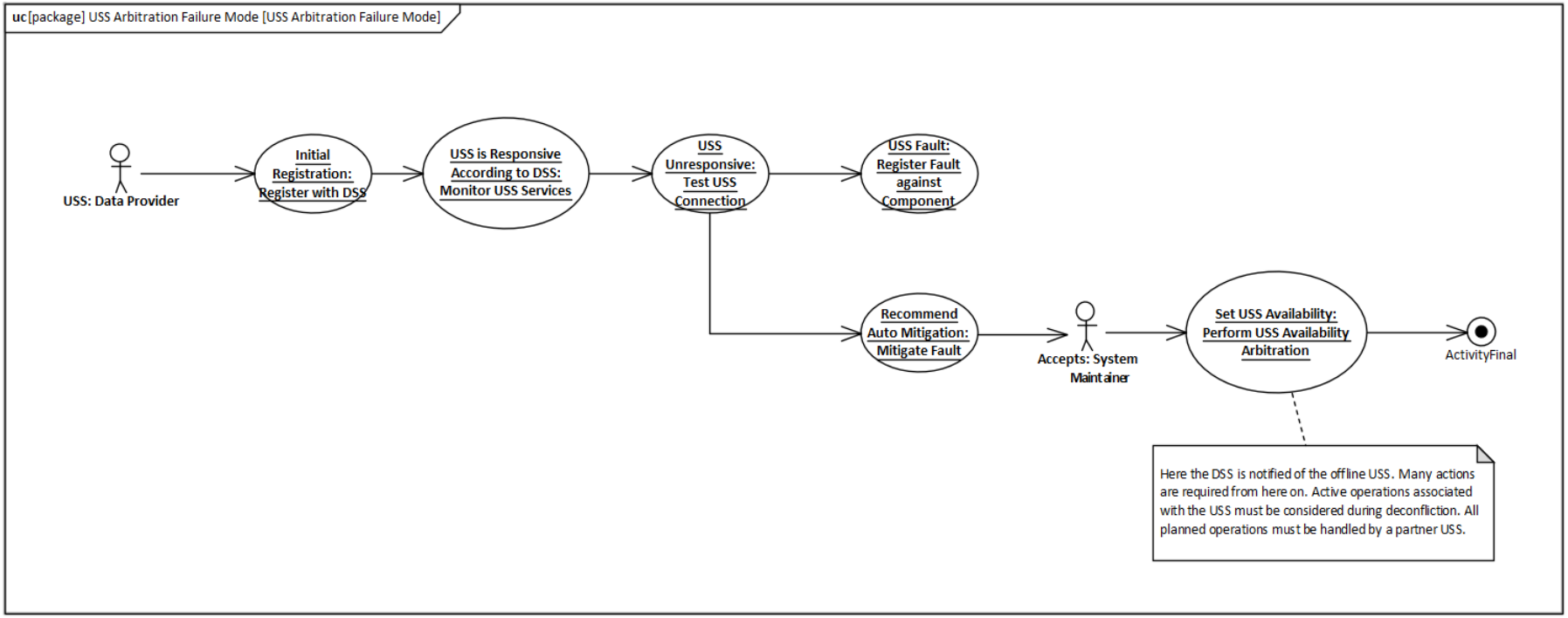

Fig: 9 USS Arbitration Failure Mode

B. Performance Envelope Failure Mode

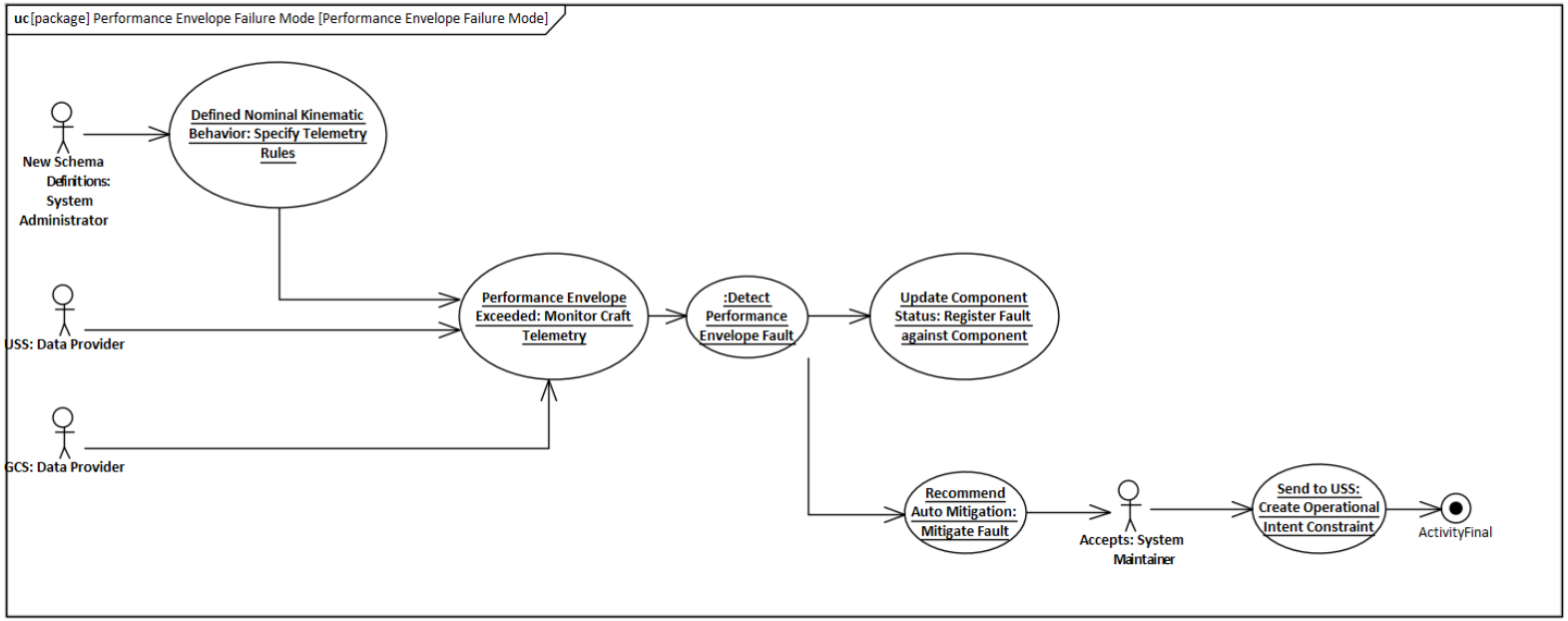

Fig. 10 Performance Envelope Failure Mode

C. Surveillance Failure Mode

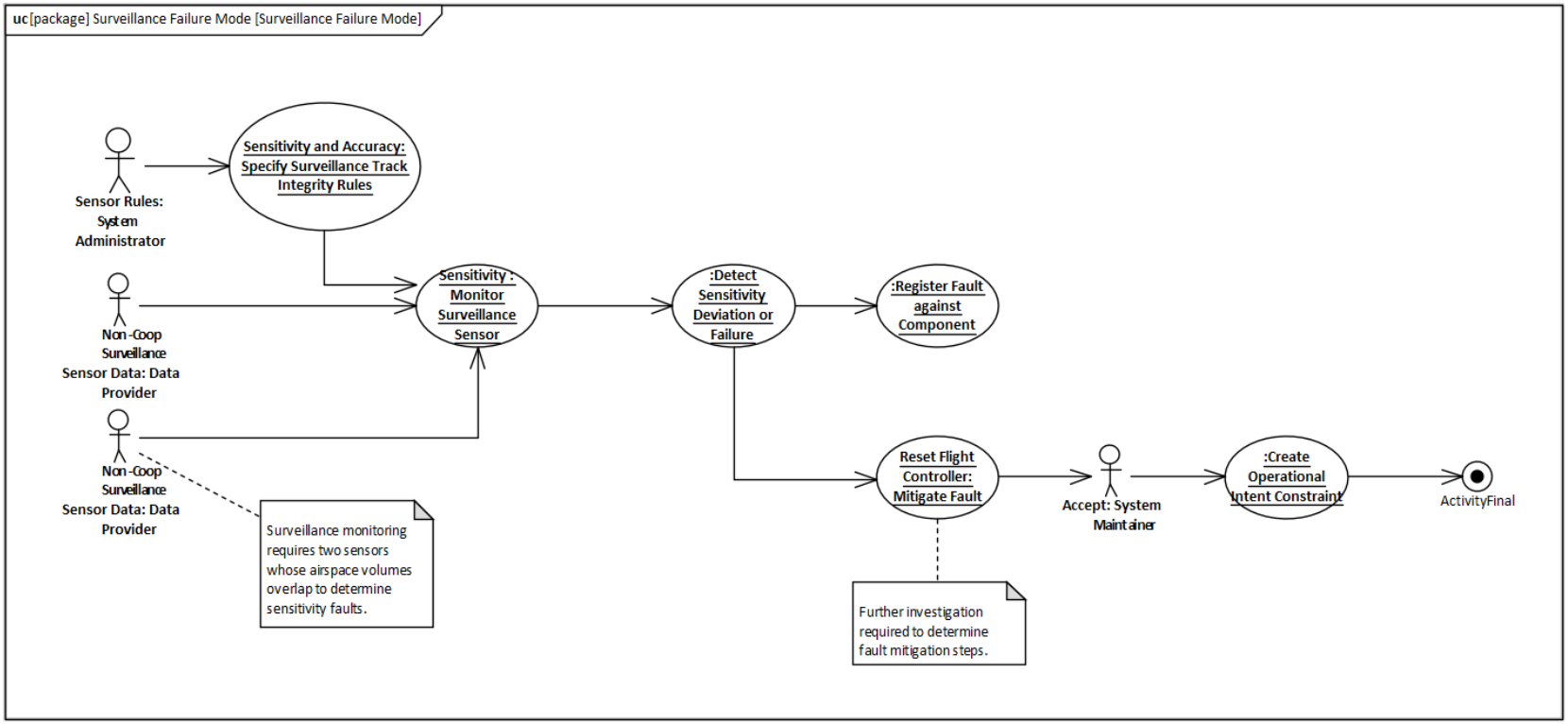

Fig. 11 Surveillance Failure Mode

D. Network Loss of Connection Failure Mode

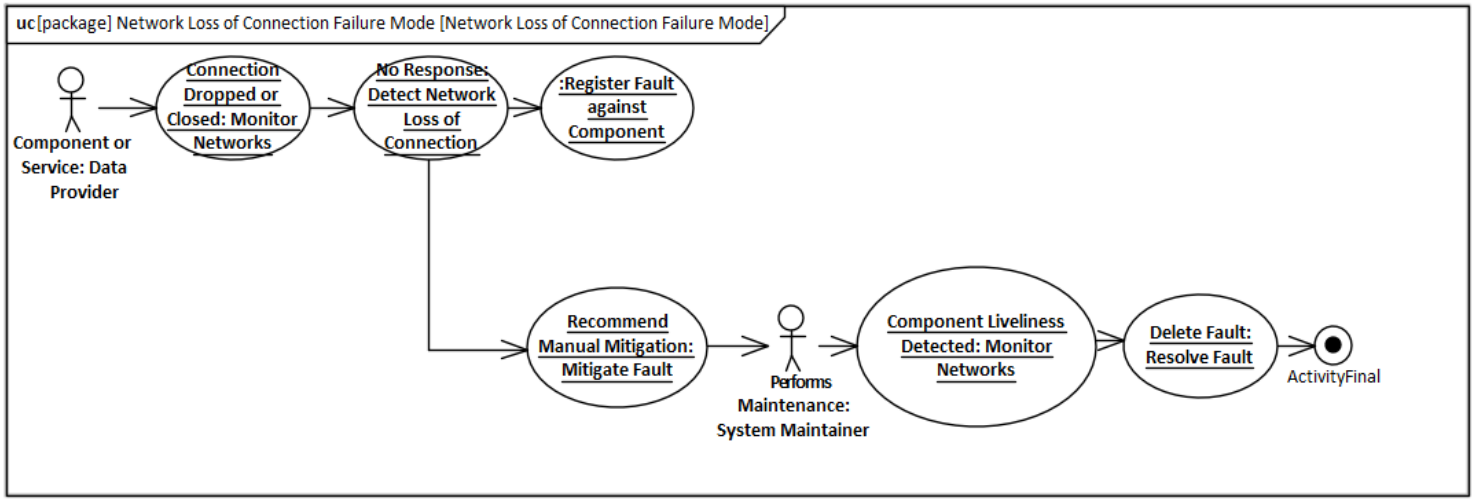

Fig. 12 Network Loss of Connection Failure Mode

E. Network Degradation Failure Mode

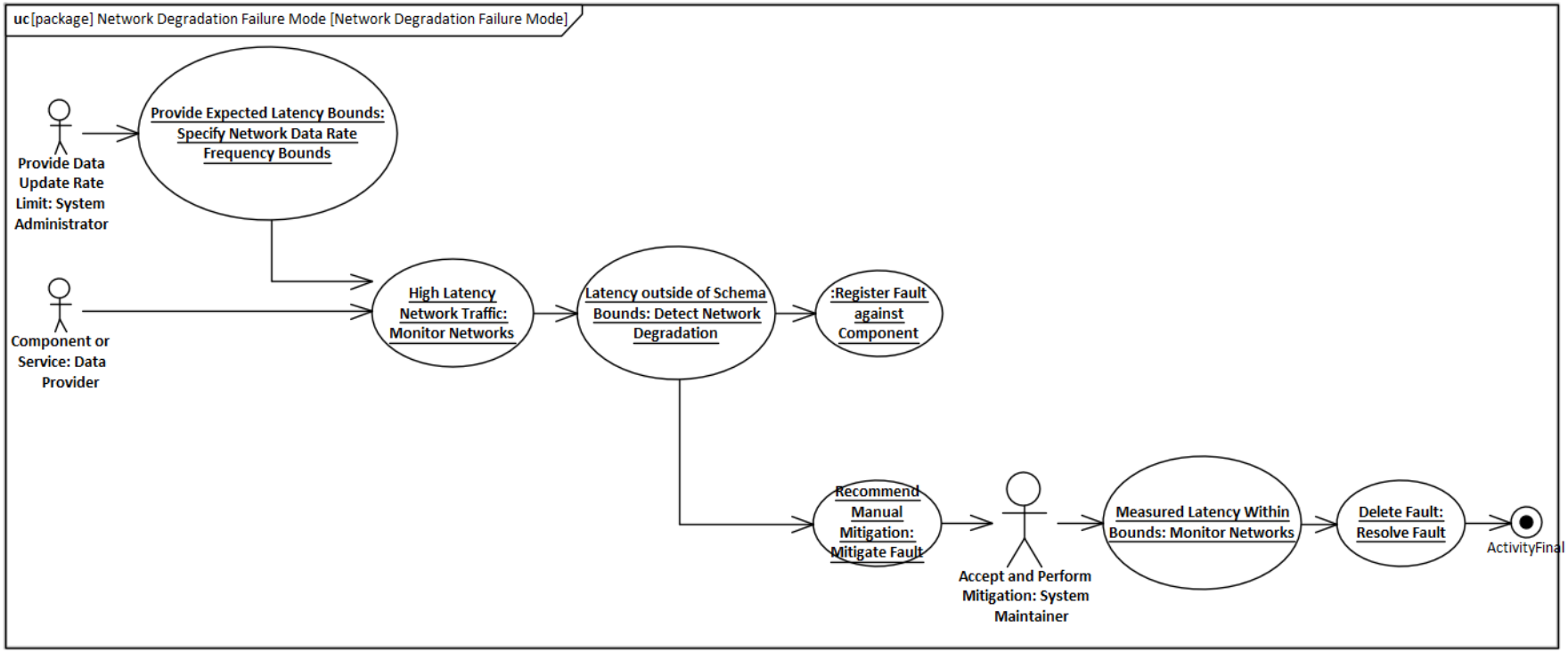

Fig. 13 Network Degradation Failure Mode

F. SDSP Degradation Failure Mode

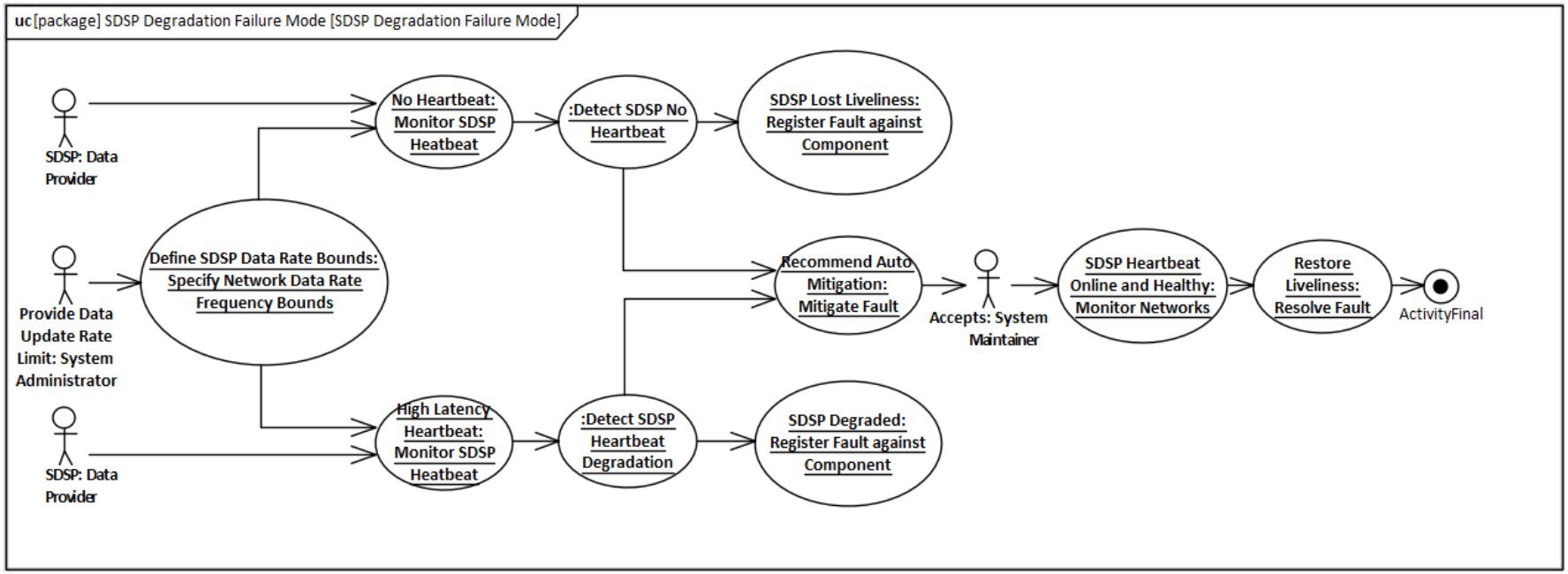

Fig. 14 SDSP Degradation Failure Mode

G. Unreliable Drone Tracking Failure Mode

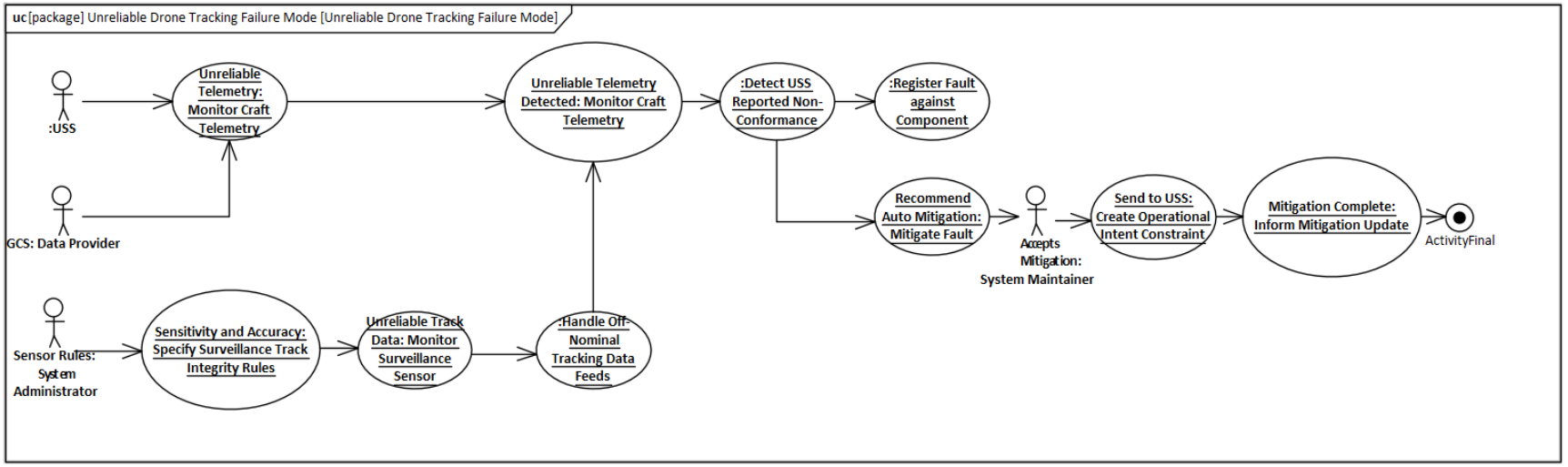

Fig. 15 Unreliable Drone Tracking Failure Mode

H. Unauthorized Device Failure Mode

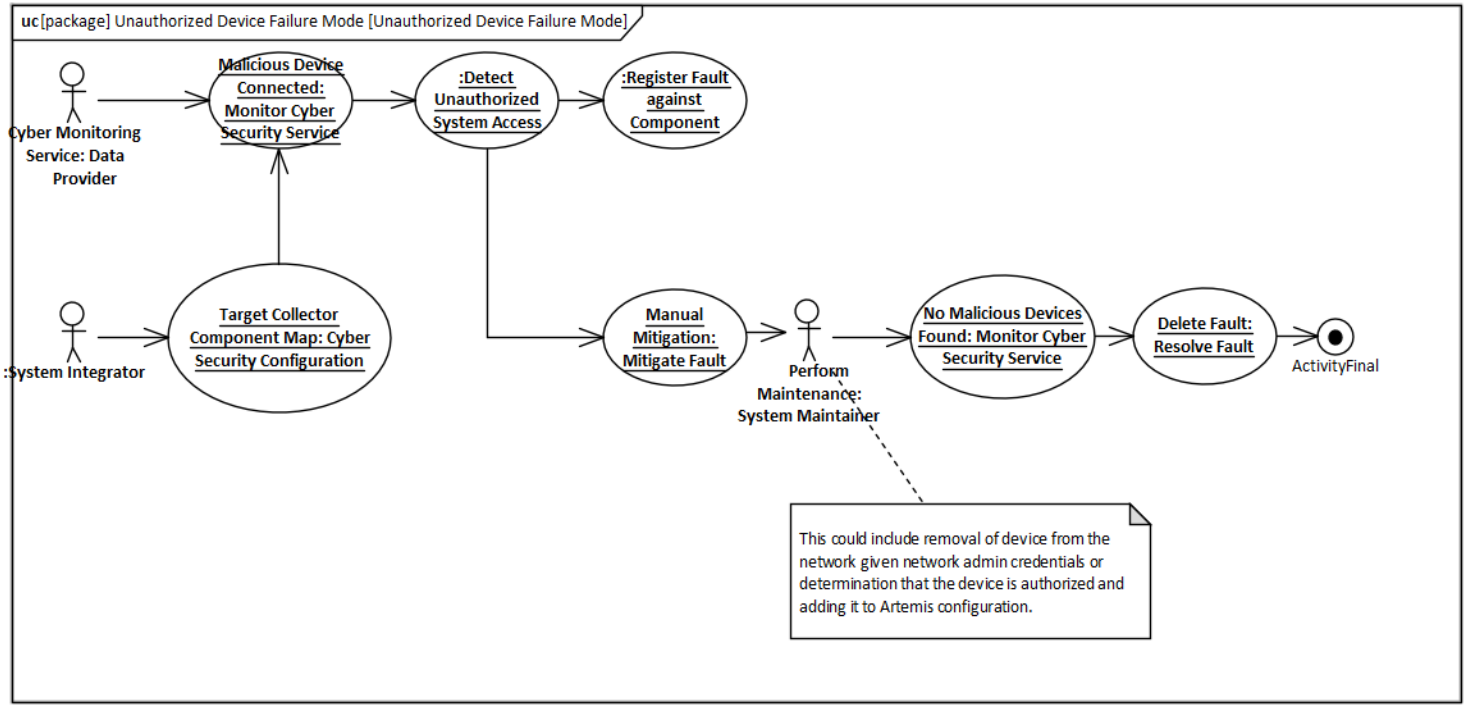

Fig. 16 Unauthorized Device Failure Mode

I. Security Vulnerability Failure Mode

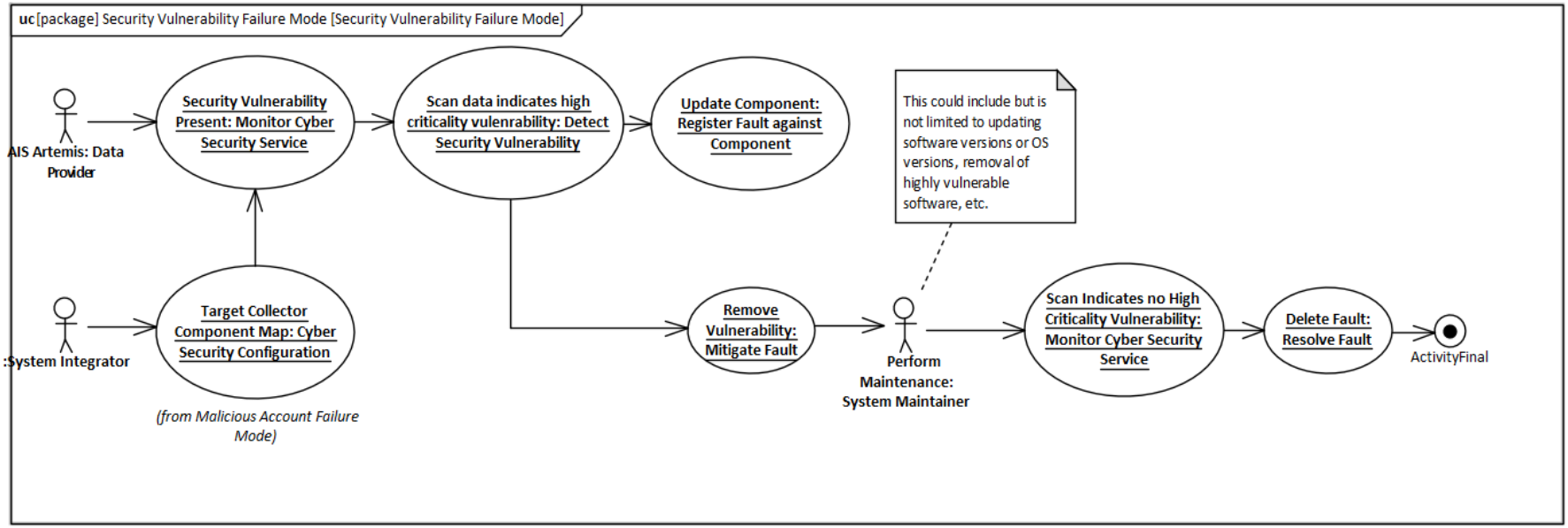

Fig. 17 Security Vulnerability Failure Mode

J. Malicious Account Failure Mode

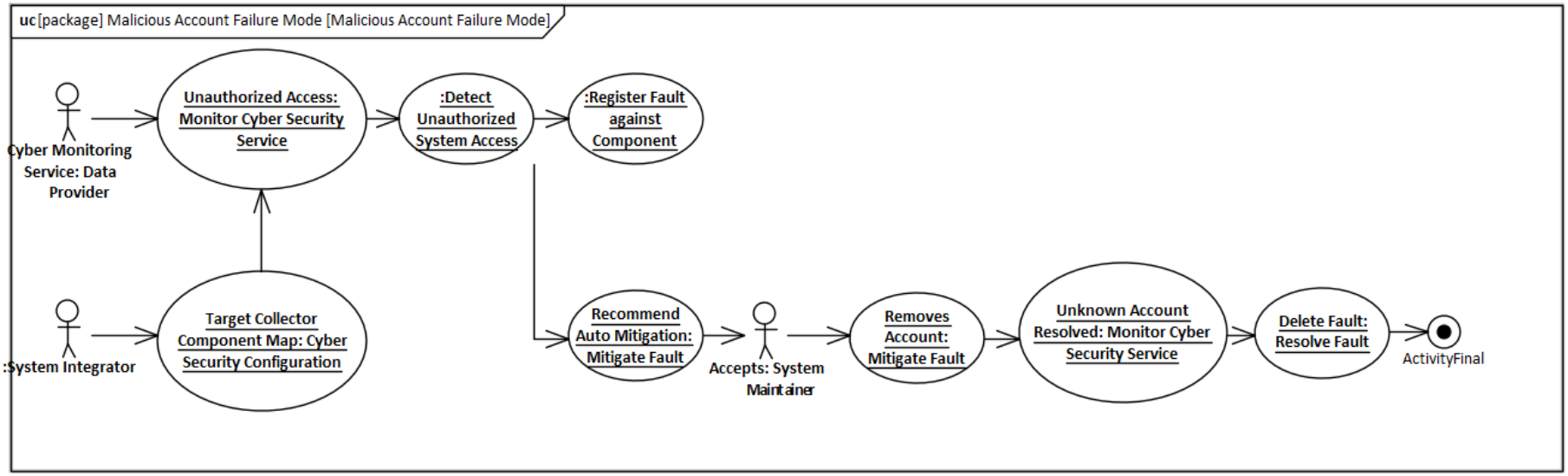

Fig. 18 Malicious Account Failure Mode

Appendix B: IASMS System Level Requirements Specific to Project Failure Modes

A. IASMS USS Monitoring Requirements

Table 16 IASMS USS Monitoring Requirements

Name	Notes
FRAIHM430 - Perform USS Arbitration	The system **SHALL** perform USS arbitration to indicate any offline or unavailable USSs within the UTM ecosystem.
FRAIHM431 - Monitor Non-Conformance	The system **SHALL** monitor non-conformance as reported by a craft's managing USS.
FRAIHM432 - Register as USS	The system **SHALL** register itself as a USS to one or more DSSs in the target UTM ecosystem.
FRAIHM438 - Monitor USS Telemetry Updates	The system **SHALL** monitor telemetry updates associated with a USS's operational intents.
FRAIHM439 - Monitor UTM Ecosystem for Failures	The system **SHALL** monitor all DSSs and USSs in a UTM ecosystem for failures, and report on them accordingly.
FRAIHM440 - Model UTM Ecosystem Entities	The system **SHALL** create components and faults within FRAIHMWORK to model the USSs and DSSs within the UTM ecosystem.

B. IASMS Telemetry Monitoring Requirements

Table 17 IASMS Telemetry Monitoring Requirements

Name	Notes
FAA028 - Failure Mode Resolution	The system **SHALL** update status for all components and services whose failure mode has been resolved.
FAA060 - Monitor Craft Telemetry	The system **SHALL** monitor Craft Telemetry. **Failure Modes:** • Performance Envelope Fault: Fault initiated following the failed validation of the integrity or reliability of a craft by assessing its performance within predefined operational limits or boundaries, performance envelope (range of conditions under which a system is expected to operate safely and effectively). • A failure arising from unreliable telemetry from a craft occurs when the transmitted data, crucial for monitoring the aircraft's status and performance, becomes inconsistent or inaccurate.
FAA061 - Detect Performance Envelope Breach	The system **SHALL** detect Performance Envelope Breaches from craft telemetry data feeds.
FAA062 - Detect Unreliable Telemetry	The system **SHALL** detect Unreliable Telemetry.
FAA063 - Telemetry Fault Mitigation	The system **SHALL** provide Telemetry Fault Mitigation steps.
FAA064 - Craft Telemetry Configuration Rules	The system **SHALL** ingest Craft Telemetry Integrity Rules to detect off-nominal craft telemetry. These rules should include: • Off-Nominal Velocity. • Off-Nominal Acceleration
FAA065 - Register Craft Telemetry Fault	The system **SHALL** register Craft Telemetry Faults.

Name	Notes
FAA074 - Register Performance Envelope Fault	The system **SHALL** register Performance Envelope faults.
FAA075 - Register Unreliable Telemetry Fault	The system **SHALL** register Unreliable Telemetry Faults.
FAA076 - Mitigate Performance Envelope Fault	The system **SHALL** Mitigate Performance Envelope Faults.
FAA077 - Mitigate Unreliable Telemetry Fault	The system **SHALL** mitigate Unreliable Telemetry Faults.
FAA088 Manage Constraint Reference	The system **SHALL** create Constraint References given the Operational Intent of the Craft who's telemetry data is faulted.
FAA089 - Send Constraint Reference	The system **SHALL** send Constraint References to the managing USS of the craft whose telemetry data is faulted.
FAA090 - Receive GCS Telemetry Data	The system **SHALL** receive GCS Telemetry Data when requested.
FAA091 - Retrieve USS Telemetry Data	The system **SHALL** Retrieve USS Telemetry Data when requested.
FAA092 - USS Telemetry Permissions	The system **SHALL** utilize USS Telemetry Permissions that allow request of telemetry details in the Activated mode. Please see ASTM F3548-21 for more information surrounding UTM - USS Interoperability.
FAA093 - Specify Preferred Data Source	The system **SHALL** be capable of determining which telemetry data source is used for monitoring by default.
FAA094 - Receive Craft Telemetry Data	The system **SHALL r**eceive Craft Telemetry Data.
FAA096 - Operator Accept or Reject Recommended Mitigation	The system **SHALL** allow an operator to accept or reject recommended mitigations.
FAA112 - Determine Craft Kinematics	The system **SHALL** utilize telemetry data to determine Craft Kinematics such as velocity and acceleration. Velocity of the craft can be determined from either the AMS API v1.10.0 or, if done from a raw telemetry feed a second degree time derivative of position.
FAA113 - Detect Off-Nominal Acceleration	The system **SHALL** detect Off-Nominal Acceleration by monitoring changes in velocity and comparing against Craft Telemetry Integrity Rules.
FAA114 - Detect Off-Nominal Velocity	The system **SHALL** detect Off-Nominal Velocity of the craft by measuring changes in position over time and comparing to Craft Telemetry Integrity Rules.
FAA115 - Detect Latent Telemetry Data	The system **SHALL** detect Latent Telemetry Data when a telemetry feed or AMS is providing a lack of track updates.
FAA116 - Determine Constraint Size	The system **SHALL** determine the Constraint Size via TBD methods. Some methods could include: • Bollinger Bands based on SMA and STD of position updates. • Scaling the operational intent volume
FAA117 - Determine Constraint Shape	The system **SHALL** determine the Constraint Shape. The shape will be dependent on the behavior of the craft velocity based on TBD methods.
FAA118 - Update Constraint Reference	The system **SHALL** update Constraint References based on TBD methods. Look through the ASTM 3548-21 for more information.
FAA119 - Remove Constraint Reference	The system **SHALL** remove Constraint References based on TBD methods.

Name	Notes
FAA120 - Determine Constraint Location	The system **SHALL** determine Constraint Locations based on TBD.
FAA128 - Update Component State to Faulted	The system **SHALL** update the component state to Faulted.
FAA129 - Register Monitored Components	The system **SHALL** register all monitored components. This will enable functions down the processing chain to register faults and apply mitigations to these components.
IASMS110 View Faults	The IASMS shall provide a means to view conditions that impact the state of components. Note: These conditions are denoted by the term "fault".
IASMS307- Fault Informing	The IASMS shall provide fault information to an external client.
IASMS400 - User Mitigation of Faults	The IASMS **SHALL** enable a user to take action for a given fault. Note: This function is analogous to "fault mitigation".

C. IASMS Surveillance Monitoring Requirements

Table 18 IASMS Surveillance Monitoring Requirements

Name	Notes
FAA012 - Monitor Surveillance Service	**Failure Mode:** • A deviation or failure in the system's ability to accurately and reliably detect and track intended targets. The system **SHALL** monitor surveillance sensitivity data from available surveillance sources.
FAA013 - Detect Track and Sensitivity Faults	The system **SHALL** be detect track and sensitivity faults should there be any deviations or failures in surveillance sensitivity data.
FAA028 - Failure Mode Resolution	The system **SHALL** update status for all components and services whose failure mode has been resolved.
FAA033 - Register Surveillance Sensitivity Fault	The system **SHALL** register all Surveillance Sensitivity Faults when it is determined that a sensor's sensitivity is off-nominal.
FAA034 - Surveillance Fault Mitigation	The system **SHALL** provide TBD options for Surveillance Fault Mitigation.
FAA089 - Send Constraint Reference	The system **SHALL** send Constraint References to the managing USS of the craft whose telemetry data is faulted.
FAA096 - Operator Accept or Reject Recommended Mitigation	The system **SHALL** allow an operator to accept or reject recommended mitigations.
FAA105 - Manual Surveillance Fault Mitigation	The system **SHALL** provide Manual Surveillance Fault Mitigation options upon detection of a sensitivity fault.
FAA106 - Determine Non-Overlapping Airspace Coverage	The system **SHALL d**etermine Non-Overlapping Airspace Coverage where a surveillance sensor has exclusive ownership of.
FAA128 - Update Component State to Faulted	The system **SHALL** update the component state to Faulted.

Name	Notes
FAA129 - Register Monitored Components	The system **SHALL** register all monitored components. This will enable functions down the processing chain to register faults and apply mitigations to these components.
FAA132 - Calculate MTTR	The system **SHALL** calculate MTTR if a fault is considered repairable.
FAA133 - Calculate MTBF	The system **SHALL** calculate MTBF for repairable faults and if the component has been repaired once in the past.
FRAIHM129 - Calculate Reliability/Availability Metrics	The system shall calculate reliability/availability metrics for each monitored component.
IASMS110 View Faults	The IASMS shall provide a means to view conditions that impact the state of components. Note: These conditions are denoted by the term "fault".
IASMS307- Fault Informing	The IASMS shall provide fault information to an external client.
IASMS400 - User Mitigation of Faults	The IASMS **SHALL** enable a user to take action for a given fault. Note: This function is analogous to "fault mitigation".

D. IASMS SDSP Monitoring Requirements

Table 19 IASMS SDSP Monitoring Requirements

Name	Notes
ASTMSURVSDSP7.11 Latency	Latency is the measure of time delay. Several latencies are relevant to the use of surveillance data. Latency is expressed in the time delay from the time of applicability to the sensor; from the sensor to the Surveillance SDSP; in the internal processing time of the Surveillance SDSP itself; and from the Surveillance SDSP to the user (including network latencies). See Appendix B for Surveillance SDSP system latency design considerations.
ASTMSURVSDSP7.12 Nominal and Maximum Latency	The Surveillance SDSP shall define its nominal and maximum latencies in milliseconds from the time of applicability to the Surveillance SDSP's dissemination endpoint. The Surveillance SDSP shall indicate nominal latency in its heartbeat messages, including alerts if latencies exceed those specified by SLA.
ASTMSURVSDSP7.14 User Latency Response	The User shall monitor the network and latency between the Surveillance SDSP and the user and shall respond to diminished network and latency performance in a manner consistent with their safety management system and standard operating procedures, if defined. This can be achieved by measuring the delay between timestamped messages and their reception time at the user's. Note: This requirement trails off before the trailing period. It's assumed the requirement intends to compare the timestamped message from an upstream system component, and the time synchronized timestamp at the latency monitoring function.
ASTMSURVSDSP7.3 Heartbeat Messages and Rates	The Surveillance SDSP shall send heartbeat messages to all users at the rate specified in the SLA. This rate shall not be less frequent than twice the update rate (e.g., for an update rate of 4 seconds, the heartbeat rate shall not be less frequent than 8 seconds).
FAA019 - Monitor SDSP Status	**Failure Mode:** Failure arising from a connected SDSP being latent or unresponsive, occurs when the interconnected components experience delays or become non-responsive, hindering the overall ecosystem's performance The system **SHALL** monitor the status of all Supplemental Data Service Providers (SDSP).
FAA021 - Detect Status Degradation	The system **SHALL** Detect Status Degradation for all SDSPs.

Name	Notes
FAA022 - SDSP Data Integrity Rules	The system **SHALL** contain SDSP Data Integrity Rules and bounds to determine degraded SDSP data links.
FAA028 - Failure Mode Resolution	The system **SHALL** update status for all components and services whose failure mode has been resolved.
FAA039 - SDSP Fault Mitigation	The system **SHALL** provide TBD options for fault mitigation surrounding SDSP loss of connection and degradation.
FAA040 - Register SDSP Faults	The system **SHALL** register SDSP Faults for loss of connection and degradation faults.
FAA053 - Manual SDSP Fault Mitigation	The system **SHALL** provide manual SDSP fault mitigation options upon detection of degraded or loss of connection of a SDSP.
FAA054 - Reconnect to SDSP	The system **SHALL** provide an automated mitigation to Reconnect to the SDSP upon loss of connection.
FAA055 - SDSP Update Rate Violation	The system **SHALL** detect SDSP Update Rate Violations based on defined heartbeat rates.
FAA078 - Register SDSP Latency Fault	The system **SHALL** register SDSP Latency Faults.
FAA079 - Register SDSP Loss of Connection Fault	The system **SHALL** register SDSP Loss of Connection Faults.
FAA081 - Define Fault Code Configuration	The system **SHALL** define Fault Code Configuration items to be used for fault-to-mitigation mapping.
FAA096 - Operator Accept or Reject Recommended Mitigation	The system **SHALL** allow an operator to accept or reject recommended mitigations.
FAA111 - Detect SDSP Loss of Liveliness	The system **SHALL** detect Loss of Liveliness of any SDSPs.
FAA128 - Update Component State to Faulted	The system **SHALL** update the component state to Faulted.
FAA129 - Register Monitored Components	The system **SHALL** register all monitored components. This will enable functions down the processing chain to register faults and apply mitigations to these components.
FAA132 - Calculate MTTR	The system **SHALL** calculate MTTR if a fault is considered repairable.
FAA133 - Calculate MTBF	The system **SHALL** calculate MTBF for repairable faults and if the component has been repaired once in the past.
FRAIHM129 - Calculate Reliability/Availability Metrics	The system shall calculate reliability/availability metrics for each monitored component.
IASMS110 View Faults	The IASMS shall provide a means to view conditions that impact the state of components. Note: These conditions are denoted by the term "fault".
IASMS307- Fault Informing	The IASMS shall provide fault information to an external client.
IASMS400 - User Mitigation of Faults	The IASMS **SHALL** enable a user to take action for a given fault. Note: This function is analogous to "fault mitigation".

E. IASMS Network Monitoring Requirements

Table 20 IASMS Network Monitoring Requirements

Name	Notes
FRAIHM304-Component Liveliness Monitoring	The system shall monitor the liveliness of components. Note: Liveliness is a thresholding function for age of most recent update on component.
FRAIHM305-Component Health Monitoring	The system shall monitor components for off-nominal conditions. Note: Off-nominal conditions are denoted by the term "fault".
FRAIHM318 - Apply Configuration to System	The system shall allow an authorized User to apply a configuration at runtime.
FRAIHM339 - Monitor Network Failures	The system **SHALL** monitor components for network related failures.
FRAIHM340 - Monitor Degraded Network Connection	The system **SHALL** monitor components for a degraded network connection.
FRAIHM341 - Apply Network Monitoring Configuration	The system **SHALL** apply network monitoring configurations to the system.

F. IASMS Cybersecurity Monitoring Requirements

Table 21 IASMS Cybersecurity Monitoring Requirements

Name	Notes
FAA023 - Monitor Cyber Security Service	**Failure Modes:** • A failure resulting from an unauthorized or malicious device occurs when an external device gains unauthorized access to the ecosystem. • A failure from a determined security vulnerability on a device occurs when a security control is not implemented, or another vulnerability is discovered on a device. • A failure from a determined security vulnerability on a device occurs when malicious actors exploit weaknesses in the device's cybersecurity defenses, gaining unauthorized access or compromising sensitive data. The system **SHALL** monitor Cyber Security data.
FAA024 - Security Vulnerability	The system **SHALL** detect security vulnerabilities.
FAA025 - Detect Unknown Device	The system **SHALL** detect any unknown or unauthorized devices connected to the network infrastructure.
FAA026 - Unknown Account	The system **SHALL** detect Suspicious Data Activity conditions via account information aggregation and historical comparison.
FAA027 - Cyber Security Integrity Rules	The system **SHALL** contain Cyber Security integrity rules and bounds.
FAA028 - Failure Mode Resolution	The system **SHALL** update status for all components and services whose failure mode has been resolved.
FAA042 - Cyber Service Fault Mitigation	The system **SHALL** provide TBD options for fault mitigation surrounding malicious accounts, unauthorized devices, and security vulnerabilities.
FAA043 - Register Cyber Security Fault	The system **SHALL** register the following as faults: • MEDIUM severity for all Unauthorized Access. • MEDIUM severity for Unknown Accounts. • MEDIUM severity for any Device Security Vulnerabilities of high criticality.

Name	Notes
FAA046 - Cyber Security Configuration	The system **SHALL** load a Cyber Security Configuration.
FAA096 - Operator Accept or Reject Recommended Mitigation	The system **SHALL** allow an operator to accept or reject recommended mitigations.
FAA097 - Target Component Map	The system **SHALL** provide Target to Component Mappings so that registered components on FRAIHMWORK can be monitored.
FAA098 - Collector to Target Mapping	The system **SHALL** contain a Collector to Target Mapping that allows multiple collectors to monitor cyber risks on a specific target.
FAA099 - Retrieve All Registered Components	The system **SHALL** retrieve all registered components.
FAA100 - Apply Cyber Security Collector	For each target/component, the system **SHALL** apply Cyber Security Collectors. Multiple collectors can be used for one target.
FAA101 - Removal of Unauthorized Account	Upon identified Unauthorized Access, the system **SHALL** institute Removal of Unauthorized Account.
FAA102 - Manual Cyber Mitigation	The system **SHALL** initiate a manual Cyber Mitigation operation for non-automated mitigations. This includes Suspicious Data Activity and Device Vulnerabilities conditions.
FAA103 - Monitor for Operator Approval of Mitigation	The system **SHALL** monitor for Operator Approval of Mitigation by polling the mitigation state of the reported fault.
FAA128 - Update Component State to Faulted	The system **SHALL** update the component state to Faulted.
FAA146 - Detect Cyber Security Vulnerabilities	The system **SHALL** detect cyber security vulnerabilities of a networked infrastructure.
FRAIHM129 - Calculate Reliability/Availability Metrics	The system shall calculate reliability/availability metrics for each monitored component.
IASMS110 View Faults	The IASMS shall provide a means to view conditions that impact the state of components. Note: These conditions are denoted by the term "fault".
IASMS307- Fault Informing	The IASMS shall provide fault information to an external client.
IASMS400 - User Mitigation of Faults	The IASMS **SHALL** enable a user to take action for a given fault. Note: This function is analogous to "fault mitigation".

References

[1] United States. Federal Aviation Administration. FAA UTM Concept of Operations V2.0. Washington D.C, DOI 2 March 2020, URL: Unmanned Aircraft System (UAS) Traffic Management (UTM) (faa.gov)

[2] United States. Federal Aviation Administration. FAA UTM Implementation Plan. Washington D.C. 2023. P.L. 115-254, Sec. 376, DOI 31 July 2023, URL: P.L. 115-254 Sec. 376 UAS Traffic Management (faa.gov)

[3] INCOSE (2023) Systems Engineering Handbook: A Guide for System Life Cycle Processes and Activities. 5th Edition, John Wiley & Sons, I., Hoboken. DOI July 2023

[4] United States of America Aeronautical Information Publication (AIP) EN ROUTE procedures, URL: https://www.faa.gov/air_traffic/publications/atpubs/aip_html/part1_gen_section_0.1.html [retrieved 14 February 2024]

[5] ASTM Standard ASTM F3548-21, 2021, " Standard Specification for UAS Traffic Management (UTM) UAS Service Supplier (USS) Interoperability," ASTM International, West Conshohocken, PA, 2021, DOI: 10.1520/F3548-21, URL: www.astm.org.

[6] Global UTM Association (GUTMA) Secure and Resilient UTM Task Force Report, DOI May 2024, URL https://drive.google.com/file/d/1FUXoBiFhjnFmCS00PQC_XtzEDfmUHVdf/view