Key Challenges and Solutions for Scaling BVLOS Operations

January 15, 2025

RESILIENX

Making Future Skies Safer

Syracuse, NY
info@resilienx.com

RESILIENX

Key Challenges and Solutions for Scaling BVLOS Operations

The successful adoption and scaling of Beyond Visual Line of Sight (BVLOS) operations faces critical challenges. These issues stem from the inherent complexities of interconnected systems, especially with federated ecosystems[1], given their cybersecurity, operational scalability, and regulatory requirements. ResilienX recently completed a yearlong project for the FAA, along with a team of partners[2] to investigate how an In-Time Aviation Safety Management System (IASMS) could be used to address these challenges and progress the safe adoption of scaled BVLOS operations. Below is a breakdown of the primary challenges identified in the report and recommendations to more effectively address them.

1 Interoperability Challenges in Federated UTM Ecosystems

UTM ecosystems are inherently federated, meaning they consist of multiple independent service providers, including UAS Service Suppliers (USS) and Supplemental Data Service Providers (SDSP). The main challenges in this setup include:

- Lack of a centralized Data Exchange: Reliable data sharing between disparate entities remains challenging due to a lack of standardized interfaces. Fragmented data protocols inhibit seamless collaboration, essential for real-time situational awareness and safe operations.
- USS and SDSP Synchronization: Current standards, like the ASTM USS interoperability standard (F3548-21), provide some guidance but lack specific requirements for standardized USS and SDSP interactions, leading to inconsistencies in data availability and performance management.

2 Cybersecurity Requirements for UTM and AAM Systems

As UTM expands, the risk of cyber threats increases. There exists a variety of cybersecurity concerns, including:

- Unauthorized Device and User Access: The open architecture of UTM enables multiple entry points for devices which, if unauthorized, can compromise system integrity.
- Data Security and Malware: The high volume of sensitive data, if unsecured, is vulnerable to malware attacks and breaches, potentially impacting critical flight data and long-term trustworthiness for ecosystem data.
- Network Intrusion and Performance Degradation: Federated systems without robust network security measures may suffer from interruptions due to cyber intrusions.

3 Operational Safety and Failure Mode Management

Safety management is crucial in ensuring UTM ecosystem reliability and scalability. Current standards inadequately address real-time safety assurance, a significant gap given the complexity of UTMs. Major failure modes include:

- Telemetry and Surveillance Data Reliability: Ensuring accurate and timely telemetry data is critical for detecting and responding to out-of-bounds maneuvers or performance issues. Unreliable telemetry or sensor degradation can compromise situational awareness.

---

[1] Federated ecosystem refers to an operational environment where systems interoperate collaboratively, with governance is divided between a central authority and constituent units, balancing organizational autonomy with enterprise needs – *MITRE Systems Engineering Guide*

[2] Demonstrated UTM system included subsystems from ResilienX, Assured Information Security (AIS), and OneSky. Included flight operations conducted by NUAIR and was demonstrated both at NUAIR operations center in Canastota NY and the NY UAS Test Site in Rome, NY.

- Network Performance and Availability: Failures in network connectivity or latency issues can disrupt critical UTM functions, affecting response times in contingency situations, and the ability to recover from system degradations.

4 Regulatory Gaps and Compliance Barriers

Current regulatory frameworks are insufficient for the unique demands of UTM and AAM. Traditional aviation regulations focus on design assurance, but for UTM, operational assurance is equally vital:

- Inadequate BVLOS Standards: BVLOS operations are critical for the adoption of UAM and AAM. The current standards around these operations lack comprehensive guidelines for uncrewed operations, leaving gaps in operational and safety assurance.
- Operational Safety Assurance: Existing rules largely focus on preventing failure rather than managing in-operation risks. UTM requires a shift toward continuous risk assessment and mitigation to ensure safety.

Quantifying the impact of an IASMS

The ResilienX-led project, supported by OneSky, AIS, NUAIR, and the NY UAS Test Site focused on measuring and quantifying the efficacy of an IASMS within a UTM ecosystem. This collaborative effort aimed to address and overcome major challenges associated with interoperability, cybersecurity, operational safety, and regulatory compliance. Our Team leveraged our collective expertise to identify the architecture and execute the project. Figure 1 depicts the simplified, high-level view, of the project approach.

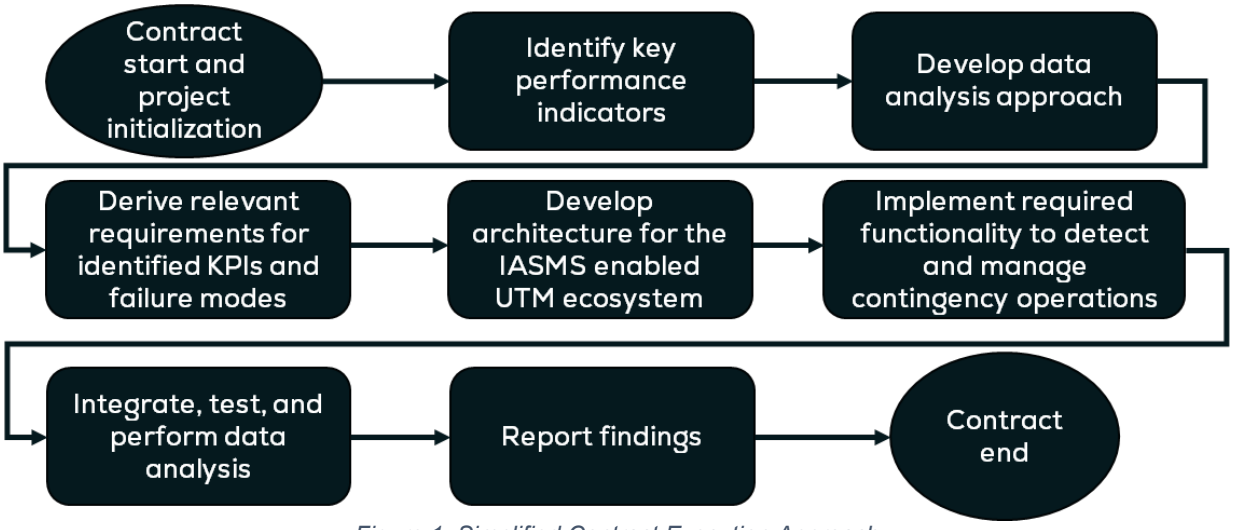

Figure 1: Simplified Contract Execution Approach

Initially, ResilienX and FAA selected a set of UTM failure modes that were high priority for an IASMS to monitor, assess, and mitigate. To quantify these failure modes, and the mitigations that would be eventually tested as part of the FAA BAA 004 effort, ResilienX identified key performance indicators (KPIs) for the IASMS-enabled ecosystem. In most, if not all cases, the level of ecosystem health and resilience reflected by these KPIs would be only possible with an IASMS, which is included in the findings that are documented in the final report to the FAA.

The KPIs and test outcomes are further discussed in the sections that follow.

RESILIENX

Key Performance Indicators

As part of this effort, ResilienX identified a set of 20 key performance indicators (KPIs) relating to the failure modes, which link to the project test cases, ultimately addressed by the team's systems. The KPIs are associated using a verification requirements traceability matrix to the FAA failure modes and requirements within the FAA project verification deliverables. Those KPIs are shown below.

Data Integrity			
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
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
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
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
5	Data Validation Failures	Number of data validation failures or anomalies detected	**<1 / 10,000 records** Provides reliable and accurate information for operational decisions

Information Assurance / Cybersecurity			
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.
7	Security Policy Compliance	Percentage of system components and	**95%** Essential to ensure that the majority of system components and users adhere to established

		users in compliance with security policies.	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.
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.
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.

Surveillance Tracking			
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.
14	(a) False Positive and (b) False	Percentage of false alarms or erroneous tracking reports.	**<5%** Ensures reliable system performance, effective decision-making, and increased confidence from users and stakeholder

	Negative Rate		
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

Health and Status			
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.
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.
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

Test Outcomes

The test was structured in ten individual test cases that aligned one to one with the IASMS-enabled UTM ecosystem failure modes and their associated mitigations. Four of the ten cases were identified for live flight testing. Additional flights were repeated for the test cases as regression executions for additional analysis. All test cases passed, showcasing the efficacy of an IASMS in a UTM ecosystem. IASMS has a place within BVLOS operations as an active, practical means for monitoring, assessing and mitigating off-nominal conditions, using technology that is currently commercially available.

RESILIENX

About the project team

RESILIENX

ResilienX, a software company founded in 2019, is commercializing In-Time Aviation Safety Management Systems (IASMS) and safety assurance for autonomous operations, with a particular emphasis on UAS and Advanced Air Mobility (AAM). ResilienX's flagship product, FRAIHMWORK®, is the only commercially available IASMS and provides continuous monitoring, fault detection, and real-time mitigation to ensure safe and efficient BVLOS operations.

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.

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.

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).