NASA/TM—20205003981

In-time System-wide Safety Assurance (ISSA) Concept of Operations and Design Considerations for Urban Air Mobility (UAM)

Kyle Ellis and John Koelling
Langley Research Center, Hampton, VA

Misty Davies
Ames Research Center, Mountain View, CA

Paul Krois
Crown Consulting Inc., Aurora, CO

June 2020

NASA STI Program ... in Profile

Since its founding, NASA has been dedicated to the advancement of aeronautics and space science. The NASA scientific and technical information (STI) program plays a key part in helping NASA maintain this important role.

The NASA STI program operates under the auspices of the Agency Chief Information Officer. It collects, organizes, provides for archiving, and disseminates NASA's STI. The NASA STI program provides access to the NTRS Registered and its public interface, the NASA Technical Reports Server, thus providing one of the largest collections of aeronautical and space science STI in the world. Results are published in both non-NASA channels and by NASA in the NASA STI Report Series, which includes the following report types:

- TECHNICAL PUBLICATION. Reports of completed research or a major significant phase of research that present the results of NASA Programs and include extensive data or theoretical analysis. Includes compilations of significant scientific and technical data and information deemed to be of continuing reference value. NASA counterpart of peer-reviewed formal professional papers but has less stringent limitations on manuscript length and extent of graphic presentations.

- TECHNICAL MEMORANDUM. Scientific and technical findings that are preliminary or of specialized interest, e.g., quick release reports, working papers, and bibliographies that contain minimal annotation. Does not contain extensive analysis.

- CONTRACTOR REPORT. Scientific and technical findings by NASA-sponsored contractors and grantees.

- CONFERENCE PUBLICATION. Collected papers from scientific and technical conferences, symposia, seminars, or other meetings sponsored or co-sponsored by NASA.

- SPECIAL PUBLICATION. Scientific, technical, or historical information from NASA programs, projects, and missions, often concerned with subjects having substantial public interest.

- TECHNICAL TRANSLATION. English-language translations of foreign scientific and technical material pertinent to NASA's mission.

Specialized services also include organizing and publishing research results, distributing specialized research announcements and feeds, providing information desk and personal search support, and enabling data exchange services.

For more information about the NASA STI program, see the following:

- Access the NASA STI program home page at http://www.sti.nasa.gov

- E-mail your question to help@sti.nasa.gov

- Phone the NASA STI Information Desk at 757-864-9658

- Write to:
  NASA STI Information Desk
  Mail Stop 148
  NASA Langley Research Center
  Hampton, VA 23681-2199

NASA/TM—20205003981

In-time System-wide Safety Assurance (ISSA) Concept of Operations and Design Considerations for Urban Air Mobility (UAM)

Kyle Ellis and John Koelling
Langley Research Center, Hampton, VA

Misty Davies
Ames Research Center, Mountain View, CA

Paul Krois
Crown Consulting Inc., Aurora, CO

National Aeronautics and
Space Administration

Langley Research Center
Hampton, VA

June 2020

Acknowledgements

The authors would like to thank NASA's Aeronautics Research Mission Directorate for its leadership, support, and sponsorship regarding the subject of this report. In particular, the Associate Administrator, Robert (Bob) Pearce, and his predecessor, Jaiwon Shin. They along with their team established a strategic vision that recognized safety assurance as one of the most difficult challenges facing an aerospace community that seeks to fly using increasingly complex, autonomous, and novel designs, where hazards and risks may emerge in new and unexpected ways.

In addition, thanks to Program Managers Akbar Sultan and Cheryl Quinn, as well as System-Wide Safety (SWS) Project Managers John Koelling and Misty Davies. Their support was vital to continued and prolonged engagement with industry for obtaining input and feedback. Support is also recognized from NASA line management including George Finelli, Mary Di Josef, and Dana Gould from Langley Research Center (LaRC), and Huy Tran from Ames Research Center (ARC).

Very special thanks to Jessica Nowinski and Kai Goebel. Their work with the National Academies that resulted in its 2018 report "In-Time Aviation Safety Management: Challenges and Research for an Evolving Aviation System," they set the stage for this report on the In-Time System-Wide Safety Assurance (ISSA) Concept of Operations (ConOps) that responds to the National Academies top recommendation.

Special recognition is given to Steve Young and Wendy Okolo for the collaboration they supported between their SWS sub-project team's reports on ISSA concepts and data architecture and this ISSA ConOps. Their prototypical advancements of ISSA capabilities lay a solid foundation for future concepts to transform aviation safety.

The authors extend wide appreciation for the engagement and collaboration afforded by industry especially with leading thought leaders, technical experts, and business representatives across original equipment manufacturers (OEMs), large and small businesses, academia, and government agencies. In particular, those associated with the NASA UTM project including Parimal Kopardekar have been instrumental in providing invaluable insight into future operations and connecting the ConOps development team with the industry. Peter Shannon provided indispensable subject matter expertise regarding industry vision, priorities and concerns early in the development of the ISSA ConOps. The American Institute of Aeronautics and Astronautics (AIAA) and its SciTech Conference and Software Technical Committee hosted sessions for review and feedback on the ISSA ConOps yielding valuable inputs.

The contributions of many others are also acknowledged. Laura Bass provided important support as the Project Coordinator. NASA colleagues Joel Lachter, Mike Feary, Lisa Vanderaar, and Corneilius O'Connor developed an early version of the ISSA ConOps in 2018. The NASA Aviation Research Institute (NARI) hosted workshops and webinars, and Christine Clark and Alina Eskridge helped with coordination and execution. The National Institute of Aerospace (NIA) also assisted by hosting a workshop.

Table of Contents

Acknowledgements **Error! Bookmark not defined.**

Table of Contents 2

Introduction 5

Need for ISSA 5

In-Time Aviation Safety Management Systems 6

Vision of an In-time Aviation Safety Management System 7

Industry Engagement 8

Objectives 10

Scope of ISSA ConOps 10

Users of the ISSA Concept of Operations 13

Integration of FAA Regulatory Requirements 17

Identification of Safety Critical Risks 18

Unsafe Proximity to People on the Ground, Air Traffic, or Property 20

Flight Outside of Approved Airspace 20

Causal or Contributing Factors 20

Critical System Failures 20

Loss of Control 22

Cyber-Security Related Risks 22

Physical Security Risks (Unintentional or Malicious) 22

Environmental Risks 23

Regulatory Risks 23

Safety Culture 23

Approach to Risk Assessment and Prioritization 24

Risk Discussion 26

IASMS Services 27

Key IASMS Services 28

Monitor Function and Data Services - Categories of Service Types 29

Assess Function and Data Services 31

Mitigate and Implementation Function and Data Services 33

Resilience, Graceful Degradation and Contingency Management 33

IASMS Services Discussion 34
Data Requirements and Architecture 36
Information Classes and Data Requirements 39
Principles and Traits 39
Data Architecture 40
Integration with Existing ConOps Architectures 41
Information Requirements - Databases and Models 43
Standards and Recommendations 44
Data Quality 45
Additional Industry Considerations for Data and Architecture 45
Use Cases 46
Non-Participant UAS Operations 48
Responsibilities/Activities 49
Flow Diagram 49
Additional Assumptions and Considerations 50
Vertiport emergency and closure 50
Responsibilities/Activities 51
Data Requirements 52
Additional Assumptions and Considerations 52
Emergent Risk in Mixed Airspace 53
Responsibilities/Activities 54
Data Requirements 55
Additional Assumptions and Considerations 56
Battery Health/Performance 57
Vehicle Lost Link – NORDO 57
Bird Strike – Physical Damage 57
USS/U4-SS Service Disruption 58
IASMS Use Case Capabilities: Time-Based Flow Management 58
Summary and Plan for Updates 58
Futurum Consilia 59
Towards an IASMS ConOps 59

Path to Certification - Assurance of Autonomy 60

Model and Database Development 60

References 61

List of Acronyms 63

Introduction

Emerging operations involving Advanced Air Mobility (AAM), such as Urban Air Mobility (UAM), pose a challenge to safety assurance and to accessibility within the National Airspace System (NAS). In particular, the public has a low tolerance for risk in aviation and the current NAS tends to be labor-intensive with limited ability to scale up for UAM. In response to this landscape, NASA is collaborating with industry to define a Concept of Operations (ConOps) for In-time System-Wide Safety Assurance (ISSA) for scalable UAM involving a service-oriented architecture. This architecture focuses safety investments for technological solutions that can overcome safety related barriers for emerging operations. By working with industry, consensus can be reached on desirable system traits that are based on integration and fusion of data and leverage increasingly autonomous and automated systems. These complex systems can identify anomalies, precursors, and trends that together enable more proactive management of operational risks.

AAM and UAM elevate the need for risk management in relation to increasing density and heterogeneity of vehicles and operations. Whereas safety in today's NAS is built on a history of programs and technologies that react to incidents and accidents, AAM presents an opportunity to leverage that experience and its implications and proactively integrate safety into the earliest designs of vehicles and systems. In a perfect world AAM and UAM would not be inherently dangerous but until then ensuring the highest quality of safety requirements is the bridge to mitigating risks.

Need for ISSA

Maintaining the safety of the NAS as it evolves will require integration of a wide range of safety systems and practices, some of which are already in place and many of which need to be developed. Maintaining system safety into the future will require rapid detection and timely mitigation of safety issues as they emerge and before they become hazards.

As part of its Aeronautics program, NASA is pursuing and progressing new concepts and technologies in its strategic implementation plan under Thrust 5, In-Time System-Wide Safety Assurance [1]. A key element of this work involved a NASA request to the National Academies to review the current state, policy, and technology for aviation safety management. NASA currently has three high-level milestones for technology advancement:

1. Domain-Specific Safety Monitoring and Alerting Tools
2. Integrated Predictive Technologies with Domain-Level Application
3. Adaptive real-Time Safety Threat Management

NASA in developing the ISSA ConOps defined the scope, functionality, and technical challenges required for an integrated ISSA. The ISSA ConOps is framed by the safety services essential to system safety, exemplified via effective use cases with reference to the UAM ConOps, the FAA UTM ConOps, and the National Academies report on the IASMS as threads to ensure a full scope of necessary capabilities. For the purposes of this ISSA ConOps, IASMS capabilities are defined as operational systems with functional elements including ISSA services. ISSA services provide monitor, assess, and mitigate capabilities in order to provide safety assurance for operations in the NAS. IASMS capabilities address the need to provide risk management and safety assurance to the NAS. Timely feedback from stakeholders on this initial approach to the ConOps is an important check to ensure the right capabilities and

challenges have been identified as foundational to further development of the ConOps. This includes participation from UAS operators, commercial industry, airports, FAA, and others.

The scope of the ISSA ConOps is framed by the International Civil Aviation Organization (ICAO) definition [2] of the overall Safety Management System (SMS), as shown in Figure 1. Traditionally Risk Management and Safety Assurance are separate yet related pillars of the overall Safety Management System. The National Academies proposes an increased integration of Risk Management and Safety Assurance pillars to enable IASMS. IASMS provides safety assurance for known and unknown hazards that have been identified, uses Risk Management controls as the logical basis for evaluation to achieve a targeted level of safety performance, and achieves this by collecting and analyzing data with prioritized resources. Figure 1 shows the relationships of IASMS and traditional ISSA within the SMS as a whole.

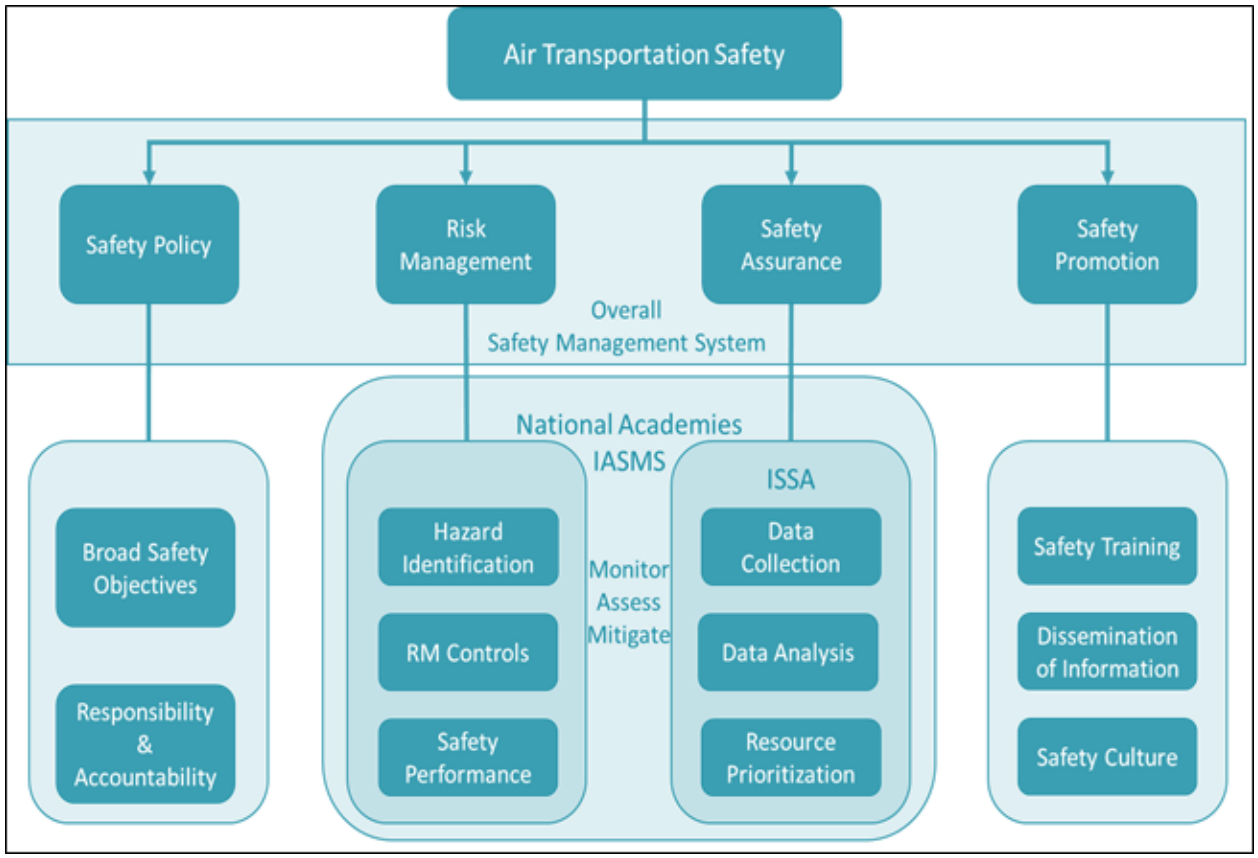

Figure 1. ICAO Safety Management System.

In-Time Aviation Safety Management Systems

The concept of real-time system-wide safety assurance should be approached in terms of an in-time aviation safety management system (IASMS) that continuously monitors the NAS, assesses the data that it has collected, and then either recommends or initiates safety assurance actions as necessary. Some elements of such a system would function in real time or close to real time, while other elements would search for risks by examining trends over a time frame of hours, days, or even longer.

Vision of an In-time Aviation Safety Management System

The National Academies report provided a vision for an IASMS [3]. This vision posits that an IASMS will continuously monitor the NAS or sub-element(s) within the NAS to collect data on the status of aircraft, air traffic management (ATM) systems, airports, weather, and other relevant elements. The IASMS would assess data on a second-by-second, minute-by-minute, or hour-by-hour basis to detect or predict elevated risk states based on rapid changes in system status. That is, different elements of a safety assurance system will operate on different time scales. Data of interest include the status and performance of vehicle systems, ground systems, operators, and weather. However, the system would not be designed to predict or respond to emergencies caused by catastrophic equipment failures, such as an uncontained engine failure or a landing gear collapse.

The vision was to detect and predict elevated risk states that arise from a confluence of factors, none of which by itself would be noteworthy. Data would be assessed to provide a thorough understanding of (1) the nominal performance of systems and operators, (2) historical data regarding both the occurrence and consequences of off-nominal situations, and (3) the fault tolerance of the NAS and its key elements.

Data could also be assessed over periods of days and weeks to detect risks based on longer-term trends. By assessing system outputs over long periods of time, emergent risks could be identified that in some cases should be added to the list of risks that the system is designed to monitor.

The vision was that an IASMS will be focused on risks that require safety assurance action in-flight or prior to flight. Preflight safety assurance action may include a decision to postpone or cancel a flight until, for example, flight conditions change or equipment is repaired. The span of IASMS services include use of data that involve multiple temporal markers that range from seconds or minutes (near real-time) to a period of days, weeks, months, or longer. Longer time frames leveraging data from IASMS services may have implications to changes such as in pilot training programs, operational procedures, equipment design, or the content of scheduled maintenance checks. The output of an IASMS while largely relevant to operational assurance is useful to those who are responsible for these longer-term areas of interest. Safety assurance actions generated by an IASMS may take the form of a recommendation that operators take action. In some cases when urgent action is required, IASMS may be designed to initiate safety assurance actions on their own.

The National Academies report was oriented toward the end state that relies on increasingly autonomous vehicles and enables scalability and accessibility for emerging operations. The requirements for data communications drive the design of the architecture to ensure resilience. Metadata must be extensible to ensure data integrity and accuracy.

The National Academies did not specify or endorse the use of any particular programmatic approach for accomplishing the work and achieving the vision. They noted the UAS traffic management (UTM) system is designed to facilitate UAS operations and it remains for the ConOps to determine what aircraft types and types of operations in different classes of airspace will become part of an IASMS.

Industry Engagement

Development of the ISSA ConOps relied heavily on integration of input and review with the UAS industry. Consensus with industry was deemed key to development of the ISSA ConOps. This was driven largely because industry has the requisite knowledge and expertise. This unique perspective involved understanding the safety barriers that are limiting UAM operations and identifying safety critical risks. It also included defining key IASMS services that demonstrate the potential to assure safety and enable UAM access to the National Aviation System (NAS). Industry was also positioned to provide its expertise to create an ISSA functional architecture that is service oriented and to define the minimum data requirements that the architecture supports. Industry could also communicate its business concerns with data ownership and sharing data in the context of the ISSA ConOps.

There were a total of eight events through which industry was engaged. These events brought together leading thought leaders, technical experts, and business representatives across original equipment manufacturers (OEMs), large and small businesses, academia, and government agencies. Their individual and collective subject matter expertise was vital to capturing industry vision, priorities, and concerns. These industry events are shown in Table 1. The events differed in terms of their purpose of engaging industry on different parts of the ISSA ConOps.

Table 1. Listing of industry engagement events.

Date	Event	Purpose	Participant Count
August 6, 2019	Special session held during the Enabling Autonomous Flight and Operations in the National Airspace System Workshop #2 held at NASA Ames	Discussed ConOps followed by breakout groups on risks/hazards, data/architecture, and use cases	88
September 26, 2019	Webinar #1	Discussed risk identification, causal factors, and prioritization	14
October 9, 2019	Webinar #2	Addressed what information the services need to provide on critical safety risks and how often. Identify who needs this information.	38
October 18, 2019	Webinar #3	Addressed what data and associated architecture are needed on critical safety risks and how often.	49
October 23, 2019	Workshop #1 held at the National Institute of Aerospace near NASA Langley	Reviewed and discussed UAM operations including risks, services, data sources, and supporting architecture. Completed walk-through of UAM operations	27

		using New York City to JFK airport. Identified assumptions.	
December 10, 2019	Workshop #2 held at NASA Ames	Developed three use cases including associated risks, services, and data requirements. Reviewed assumptions.	42
January 6, 2020	Two activities were the program session titled "Stakeholder Engagement for an Emerging Operation's Safety Management System" followed later in the day with a presentation to the Software Technical Committee at the AIAA Sci Tech Conference in Orlando, FL	Developed an integrated set of risks and services across the use cases including data requirements and architecture. Reviewed assumptions and identified gaps and shortfalls. Identified research needs.	17
January 15, 2020	Meeting of the North Carolina UAS Implementation Pilot Program (IPP)	Reviewed and discussed the ISSA ConOps including risks to UAM operations, services, data sources and supporting architecture, and use cases. Identified gaps and shortfalls.	45

The typical process was an introductory briefing explaining the purpose of the ConOps in relation to the recommendation from the National Academies, and the approach taken during the session involving breakout groups if possible. In some instances, poster-sized sheets were used by the breakout groups to facilitate discussion and record inputs.

A mailing list was developed starting with the first event and was expanded with each subsequent event. Industry participants ranged from large to small aircraft and UAS original equipment manufacturers (OEMs), UAS business companies (such as specializing in agriculture or package delivery), FAA and NASA staff, consultants, and academics.

Some events were webinars to accommodate virtual participation and did not involve breakout groups. Webinars were typically two hours in duration. Workshops also used a web-based format for virtual participation at least for the introductory briefing part of the event as this format did not readily accommodate the process used in breakout group discussion. Workshops were typically all-day events.

Objectives

The ISSA ConOps identifies the highest priority risks and is intended to be the framework from which all other safety research projects flow and are formulated. It establishes the blueprint for system architecture and identifies interdependencies between operating subsystems. It defines the operational parameters such as system authority, time constants, scope of risk, range of operations, and technology tradeoffs. Finally, the ConOps accommodates for an evolving NAS that includes improvements to existing operations as well as new operations such as Urban Air Mobility (UAM), On-Demand Mobility (ODM), Unmanned Aerial Systems (UAS), the use of Class E airspace, and space launch.

Scope of ISSA ConOps

The ISSA ConOps exists to describe how future ISSA capabilities will operate on a functional level and describes the system-of-systems architecture that will comprise what is known as an IASMS. The ISSA ConOps will identify key issues that may impact the industry's ability to develop and integrate ISSA capabilities in the existing NAS and its operational sub-elements. Most importantly, the primary intent of the ISSA ConOps is to manage the complexity and cost of an IASMS, primarily through prioritization of risks requiring mitigation through deployment of ISSA capabilities. This requires an evaluation of the risks that are a) most likely to occur and b) have the most severe consequences in an evolving NAS that incorporates new entrants.

The scope of the ISSA ConOps includes different aircraft types including new entrants across aviation domains (e.g., traditional scheduled operations, UAS/UAM, general aviation). Across aircraft types and operational domains, the ISSA ConOps considers the data requirements necessary to enable an effective prototypical ISSA capability, its interface(s) in an IASMS network, and to identify known and emergent risks.

Other considerations include cross-references to other ConOps including the UTM ConOps originally developed by NASA [4], the UTM ConOps recently published by the FAA [5], a concept for in-time safety assurance systems [6], and the UAM ConOps [7] so as to incorporate increasingly autonomous flight in future operations across different classes of airspace. The ISSA ConOps will define the relevant time scales for each functional element of the proposed general system model (monitor, assess, and mitigate). The time scale considerations will be determined based on the critical safety risk mitigation requirements to ensure equivalent or improved safety of the overall NAS and the elements operating within it. Finally, the ISSA ConOps must consider the scalability of the proposed capabilities. This means that the ISSA ConOps must be flexible in nature so that future adaptations may be made as technology advances to solve increasingly complex system challenges that would be shown in new and evolving use cases. Scalability considerations include not only expanding the data and systems architecture to account for additional safety services but also more complex designs as highlighted with additional use cases involving those safety services. In addition, the National Academies noted that scalability is bounded by the limitations of human operators and their ability to safely manage increasingly dense operations [8]. With the human tactically in-the-loop or in a supervisory over-the-loop role, concerns include how many vehicles the human operator can safely handle and ensuring the right information is provided in a timely manner so that human intervention is operationally feasible.

A key factor for scalability is the proportional growth in complexity of the AAM infrastructure. The National Academies identified infrastructure as an AAM gap to handle the mix of smaller parcel

delivery vehicles to larger emergency, air taxi and cargo shipment vehicles. This gap spans new airways and terminal approach procedures tailored for short, low-altitude urban flights; numerous locations for vertiports on the ground and as part of buildings such as on the roof that are sized for single and multiple vehicles; and ease of access for the general public including to and from vertiports with other transportation modes [9].

The ISSA ConOps builds on the National Academies report that identified four fundamental system elements that an IASMS would have to develop. These were a concept of operations for what the system would do and how it would prioritize risks, and the system functions of system monitoring, system analytics, and mitigation and implementation. It placed the highest priority on developing a concept of operations that would define the architecture and scope of the three system functions. These functions are shown in Figure 2 [3].

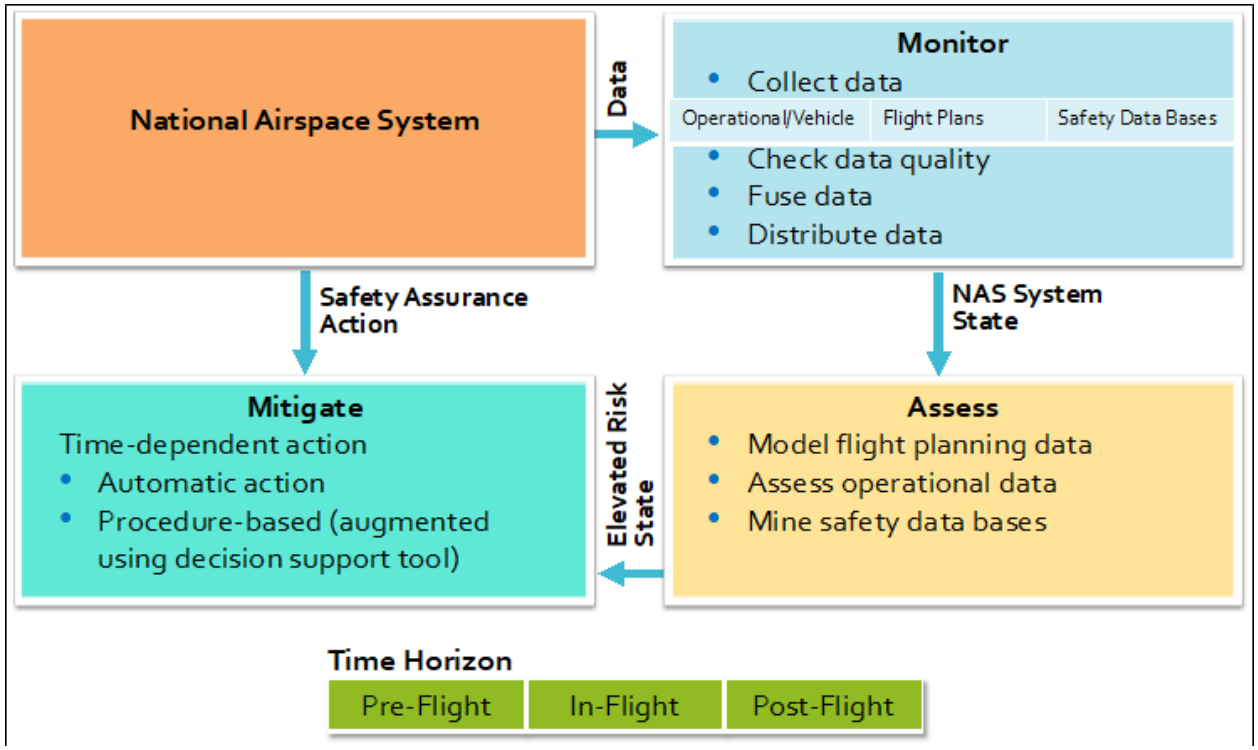

Figure 2. IASMS High-Level Architecture [3].

Additional considerations important to the development of ISSA capabilities are the effectiveness of the services comparing costs and benefits, the limitations of human performance relative to human-machine roles, system authority in the balance between humans and autonomy, and the interoperability of UAS with legacy ATM and flight deck systems and procedures. Further consideration should be given to the transition path from SMS to IASMS, uncertainties associated with each functional element of the generic ConOps, and requirements for system verification, validation, and certification. It should be noted that currently there is no accepted approach to verification and validation that leads to certification of a software system as complex as an IASMS, particularly if, as expected, the system includes adaptive, nondeterministic algorithms.

The ISSA ConOps provides a perspective on transforming safety assurance and risk management in the current safety management system used in the NAS today to the IASMS as envisioned by the National Academies report (see Figure 1). As shown in Figure 3, this transformation shows current solutions and requirements for new research to enable NAS accessibility and scalability for Advanced Air Mobility (AAM). ISSA capabilities could address different sources, types, and risk/safety impacts of various hazards. ISSA capabilities that use increasingly complex technology will likely necessitate new approaches to certification.

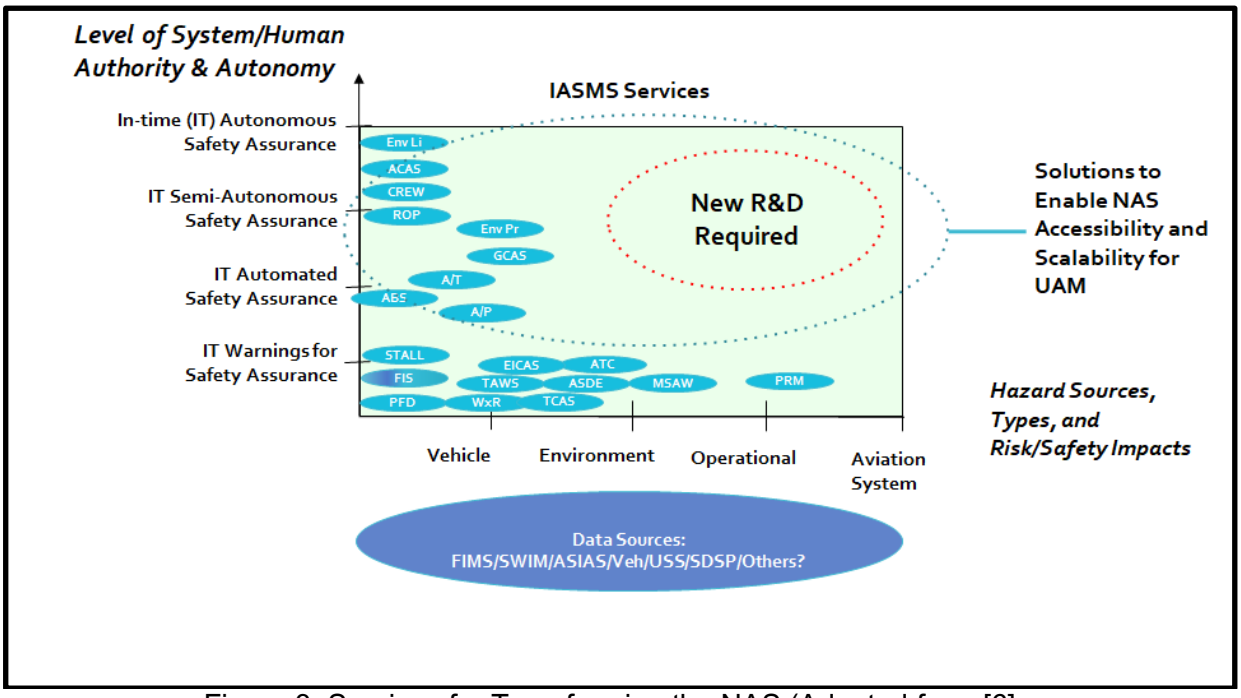

Figure 3. Services for Transforming the NAS (Adapted from [6].

ISSA capabilities become increasingly complex with higher levels of autonomy with the need to continuously monitor and assess performance and safety risk. The National Academies were concerned about the ability of vehicles to autonomously stay “well clear” of other vehicles as well as to routinely “file and fly” through the airspace shared with other vehicles, holding these abilities as essential to increasingly autonomous vehicles operating with advanced aerial mobility [3]. One barrier to increased autonomy is contingency management and handling nominal and off-nominal operations. Such operations follow a predictable and repeatable set of rules that cover possible known-unknowns. For example, a vehicle detected crossing your flight path is a known unknown. In contrast, there are by definition no rules that cover unknown unknowns. An automation surprise is when a system does something on its own authority without anticipation or understanding by the human operator. There could be classes of unknown unknowns to help distinguish between an automation surprise and an automation trap. An automation trap is some aspect of the automation the designer knows about (and thinks unlikely to occur) whereas the automation surprise occurs when the operator is not informed about the trap (i.e., not included in training or the operations manual). Contingency management is also important to resiliency of autonomous vehicles to safely continue flight when communications links are disrupted from an outage or cyberattack. In this case, operational requirements could involve landing at the nearest possible appropriate location or deploying a parachute.

Users of the ISSA ConOps

Stakeholders in the ISSA ConOps are entities that represent different business sectors, government roles, academic technology and research expertise, and aviation safety experts. Some of these entities and their definitions are taken from the UTM Concept of Operations [5, 6] and the UAM Concept of Operations [7].

1. **Public consumers of businesses using UAM.** This can include members of the public who request and receive medical, food, and other package delivery, and UAM-based public and private transportation.

2. **Operators, e.g., cargo carriers.** The Operator is the person or entity responsible for the overall management of his/her UTM operations. The Operator meets regulatory responsibilities, plans flight/operations, shares operation intent information, and safely conducts operations using all available information. Use of the term 'Operator' in this document is inclusive of airspace users electing to participate in UTM, including manned aircraft Operators, except when specifically called out as a manned or UAS Operator.

3. **Remote pilot in charge (RPIC)**. The RPIC is the person responsible for the safe conduct of each UAS flight. An individual may serve as both the Operator and the RPIC. The RPIC adheres to operational rules of the airspace in which the UAS is flying, avoids other aircraft, terrain and obstacles, assesses and respects airspace constraints and flight restrictions, and avoids incompatible weather/environments. The RPIC is capable of monitoring the flight performance and location of the UAS. If safety of flight is compromised, due to sensor degradation or environmental vulnerabilities, the RPIC is aware of these factors and intervenes appropriately. More than one RPIC may take control of the UAS at different, but sequential times during the flight, provided one person is the Pilot In Charge for the operation at any given time. The RPIC may be located at a **Ground Control Station (GCS)**.

4. **USS.** A UAS Service Supplier (USS) is an entity that provides services to support the safe and efficient use of airspace by providing services to the Operator in meeting UTM operational requirements. This general characterization of a USS is based on the FAA UTM Concept of Operations [5]. A USS (1) acts as a communications bridge between federated UTM actors to support Operators' abilities to meet the regulatory and operational requirements for UAS operations, (2) provides the Operator with demand forecasts for a volume of airspace so that the Operator can ascertain the ability to efficiently conduct their mission, and (3) archives operations data in historical databases for analytics, regulatory, and Operator accountability purposes. In general, these key functions allow for a federated network of USSs to provide cooperative management of low altitude operations without direct FAA involvement. USS services support operations planning, aircraft deconfliction, conformance monitoring, and emergency information dissemination. USSs may also work, if applicable, with local municipalities and communities to gather, incorporate, and maintain airspace restrictions and local airspace rules into airspace constraint data (e.g., preemptive airspace). USSs may also provide other value-added services to support UTM participants as market forces create opportunity to meet business needs. See Appendix D for a more detailed description of a USS.

5. **USS Network**. The term 'USS Network' refers to an amalgamation of shared UAS Operator data, or the mechanism by which Operators and their supporting USSs share data or interact with one another. For example, a USS can make intent (or other) flight information available to all of the other USSs in a specific geographic area, region, or nation-wide. In the UTM construct, multiple USSs can and will operate in the same geographical area and thus may support "overlapping" operations that require orchestration. In this environment, the USS network shares operational intent and other relevant details across the network to ensure shared situational awareness for UTM participants. Given this need for USSs to exchange a minimum set of data, the USS network must implement a shared paradigm, with methods for resolving conflict or negotiation, and standards for the efficient and effective transmission of intent and changes to intent. This reduces risk to each USS and improves the overall capacity and efficiency in the shared space. The USS network is also expected to facilitate the ready availability of data to the FAA and other entities as required to ensure safe operation of the NAS, and any other collective information sharing functions, including security and identification. Prioritization of flight planning, negotiation, and de-confliction between USSs may follow such principles as first-in/first-out or best-equipped-best-served.

6. **Supplemental Data Service Provider (SDSP)**. A USS can access one or more Supplemental Data Service Providers (SDSPs) via the USS network for essential or enhanced services (e.g., terrain and obstacle data, specialized weather data, surveillance, constraint information). SDSPs may also provide information directly to USSs or Operators through non-UTM network sources (e.g., subscription to public/private internet sites**).**

    1. **Supplementary Data Service Suppliers (SDSSs):** As described by the UML-4 Concept of Operations (Deloitte and NASA, in press) and similar to SDSPs, SDSSs provide information that is supplemental to flight operations. This information, such as weather, additional traffic awareness, etc. may be critical to safe operation, but goes beyond the basic information necessary for takeoff, separation, and landing. SDSSs will allow the opportunity for value-added services to be provided by industry to UAM operators that enhance the flight experience. SDSS services may be mandatory for flight such as a weather system (but the actual service supplier is the choice of the operator), or optional (such as systems that allow for a more comfortable or efficient flight).

7. **Flight Information Management System/FIMS.** FIMS is a gateway for data exchange between UTM participants and FAA systems through which the FAA can provide directives and make relevant NAS information available to UAS Operators via the USS Network. The FAA also uses this gateway as an access point for information on operations (as required) and is informed about any situations that could have an impact on the NAS. FIMS provides a mechanism for common situational awareness among all UTM participants and is a central component of the overall UTM ecosystem. FIMS also enables integration of additional commercial UTM products such as involving weather and population density data in different forms and formats. FIMS is the UTM component the FAA will build and manage to support UTM operations.

8. **FAA.** The FAA is the federal authority over air traffic operations in all airspace, and the regulator and oversight authority for civil aircraft operations in the NAS. The FAA maintains an operating environment that ensures airspace users have access to the resources needed to meet their specific operational objectives and that shared use of airspace can be achieved safely and equitably. The FAA develops rules, regulations, policy and

procedures as required to support these objectives. With UTM, the FAA's primary role is to provide a regulatory and operational framework for operations and to provide FAA originated airspace constraint data to airspace users, e.g., airspace restrictions, facility maps, Special Use Airspace (SUA), or Special Activity Airspace (SAA) activity. The FAA interacts with UTM for information/data exchange purposes as required, and has access to data at any time (via FIMS) to fulfill its obligations to provide regulatory and operational oversight.

9. **Ancillary Stakeholders.** Other stakeholders, such as public safety and the public, can also access and/or provide UTM services as an SDSP or via USSs/USS network. As a means to ensure safety of the airspace and persons and property on the ground, and ensure security and privacy of the public, public entities can access UTM operations data. This data can be routed directly to public entities such as the FAA, law enforcement, Department of Homeland Security, or other relevant government agencies on an as-needed basis. To accomplish this, a USS must be (1) discoverable to the requesting agency, (2) available and capable to comply with an issued request, and (3) a trusted source as mitigation actions may be taken as a result of the information provided.

10. **Vertiport operators.** Vertiports and vertistops are private and public infrastructure platforms for loading and unloading passengers and cargo for UAM operations. Vertiports may have space for one or more UASs at a time, provide battery charging stations, and work as service stations for UAS maintenance. Vertiports may be located based on specified UTM routes.

11. **Pilots, e.g., commercial, GA, rotorcraft.** Individuals trained and certified for operation of manned aircraft.

12. **Maintenance personnel.** Individuals trained and certified for maintenance of aircraft.

13. **Weather forecasters.** Meteorologists use sensors, algorithms, and expertise to develop weather forecasts. Forecasts are for different time scales and include ceiling and visibility, winds, and precipitation.

14. **Vehicle and system design engineers, and test engineers.** Engineers and others having specific knowledge and skills necessary for the design, development, test and implementation of aviation vehicles and systems.

15. **Members of Standards Committees.** Industry, government and academic participants on committees responsible for developing standards and guidance to ensure design and operational suitability of aviation vehicles.

16. **IASMS safety experts (e.g., ASIAS-like analysts for post-flight data fusion and analysis).** Safety experts who develop expansive safety databases and use complex data mining algorithms to identify anomalies, precursors, and trends,

17. **FAA Air Traffic Organization personnel (e.g., air traffic controllers, airspace and procedures specialists).** Individuals having the training and operational expertise to be Certified Professional Controllers (CPCs). CPCs can be assigned responsibilities as airspace and procedures specialists who design airspace volumes and their associated procedures and letters of agreement between air traffic control (ATC) facilities.

18. **State and local officials.** Elected officials, law enforcement, fire safety, medical evacuation, emergency management, and other civil servants responsible for policies, procedures, and processes associated with UAM, UAS operations, and On-Demand Mobility (ODM) as these concepts and capabilities relate to state and local requirements and constraints.

19. **U4-AOM Network.** The U4-Airspace Operations Management (AOM) network represents a fully integrated system of multiple U4-SSs servicing the same geographic area/airspace volume. This network delivers UAM traffic management services to enable safe and efficient UAM operations with minimal FAA involvement. Combined, the U4-SSs make up the U4-AOM network. The U4-AOM network provides secure information exchange between users of the U4-AOM system, operators, the FAA, UAM port operators, infrastructure, the general public, and others. Cooperative data exchange between the various suppliers and users provide a fully integrated operating picture to support planning, aircraft deconfliction, conformance monitoring, and emergency information dissemination and response. The U4-SSs will communicate airspace restrictions or dynamic route changes to its users. U4-SS's also exchange data and record data as required for regulatory and operator accountability purposes.

20. **U4-Service Suppliers.** The UTM Maturity Level 4 – Service Supplier (U4-SS) is an industry-supplied federated service delivered under FAA's regulatory authority that supplements and seamlessly integrates UAM with ATM. As U4-SSs provide seamless and cooperative data exchange, U4-AOM users share a common operating picture and shared situational awareness of the airspace. U4-SSs would be required to share data to support operational planning, aircraft de- confliction, conformance monitoring, and emergency information dissemination, and facilitate operator response. Defined standards and requirements for U4-SS data exchange would be well established by UML-4 and are expected to be required by FAA for U4-SS authorization. There may be a provision posing that operators will be able to switch to a different U4-SS in the event of an emergency or system failure considering that multiple U4-SSs in the AOM reduces risk to the overall system. The U4-SS is a USS at the specific maturity level.

21. **UAM Vehicle Monitor.** The concept of a Vehicle Monitor, as part of UML-4, is an individual onboard the UAM vehicle who communicates with and ensures the comfort of passengers and also provides some limited over the loop monitoring of flight systems. The Vehicle Monitor does not assume operational control of the vehicle even under off nominal scenarios but may take operational actions under restricted circumstances. For example, they may cancel a takeoff, activate an emergency landing, or interact with an air traffic controller via voice communications. The Vehicle Monitor receives training and certification at a level deemed appropriate by the FAA. These limited responsibilities of the Vehicle Monitor could lower the barriers of entry to becoming an aircraft operator (e.g., qualifications and the time and costs associated with pilot training). Lower entry requirements for becoming a simplified pilot could help ensure a sufficient supply of qualified persons to serve in the role and lower operating cost of UAM aircraft. This is necessary to overcome pilot supply limitations and training costs needed for UAM to operate at a price point that is acceptable to travelers. In addition to Vehicle Monitor, UML-4 will include traditional pilots operating VTOL/eVTOL aircraft and other aircraft within the U4-AOM system.

In the above listing, FIMS could be partitioned into multiple services. One characterization could be extrapolated from the UAM ConOps [7]. These services could involve the following capabilities:

22. **Vehicle Communications, Navigation, Surveillance, Information (CNSI) and Control Facility Infrastructure**: Highly autonomous vehicles and systems that use improved processing power and onboard sensors including advanced computer vision and microweather reports are expected to deliver significantly increased CNSI capabilities on the vehicle. These capabilities can overcome lost link and improve detect and avoid operations. This enables safe operations at reduced separation minima, long-range obstacle avoidance, and autonomous exception of planned operations or emergency landing. As UAM vehicles at UML-4 continue to have pilots, voice communication could enable interaction with other pilots, USS dispatchers, and individuals operating vertiports, as well as air traffic controllers when required.

23. **U4-SS CNSI**: Operators would maintain communication with U4-SS in compliance with performance authorization criteria and regulatory requirements for data exchange required for the operation such as for transmitting the flight plan or supporting inflight tactical coordination with other operators to comply with airspace restrictions. The combination of dense UAM operations and the large amount of data and information to be exchanged may exceed current aviation-protected spectrum that would require transition to digital Internet Protocol (IP)-based communications. Emerging technologies such as 5G that provide high-bandwidth and low-latency could support scalable networks across ground-to-air systems.

24. **Ground Infrastructure CNSI**: Reliance on and integration of ground and satellite-based infrastructure could increasingly support UAM operations by augmenting CNSI with additional information such as more precise 4-D trajectory information. Data exchange may occur directly between the equipped vehicle and ground/satellite infrastructure to support operations under IFR conditions and increasingly autonomous arrival, departure, and emergency operations.

Integration of FAA Regulatory Requirements

The FAA UTM Concept of Operations version 2 (UTM ConOps) identifies Remote Identification (RID) as a capability important to safety, security, and privacy [6]. RID is an electronic identification of a UAS vehicle that ties it to a specific RPIC/operator by a unique code. The FAA is currently in the process called Notice of Proposed Rulemaking (NPRM) for remote identification. Consequently, the ISSA ConOps addresses RID on a preliminary high level.

The RID capability consists of a set of information that enables a recipient to determine location and establish traceability back to a UAS Operator/RPIC responsible for a specific aircraft. There would be a minimum set of informational message elements that the vehicle transmits that could include, pending final a final FAA rule, the following: (1) a unique identification number - or UAS ID, (2) UAS location, and (3) a timestamp. RID data provides 4-dimension position track

information that can be correlated with intended/filed route of flight, reroute changes, and off-nominal events.

These data could be transmitted by direct broadcast (e.g., open radio broadcast) or network publishing (e.g., cell line internet service or federation of services).

The UTM ConOps described two types of USSs. A RID USS is qualified by the FAA to provide RID services that exchange all RID messages to all RID USSs for a complete distributed database. A public safety USS is qualified by the FAA to provide public safety services and may have increased access-to-information privileges within the USS Network, e.g., the public safety USS would respond to queries from an authorized subscribing law enforcement officer.

The FAA and USSs can use RID data along with intent and other information to ensure accountability and traceability for Operator compliance and conformance with regulatory and federated standards, and to identify and hold accountable the RPICs/operators who are responsible for accidents and incidents. They can also use RID data to inform other NAS users operating in that airspace of the UAS activity. RID enables accountability and traceability, particularly for BVLOS operations, where an Operator and vehicle are not co-located. USSs that provide RID services process and distribute RID data to the general public, law enforcement, the FAA, and other public officials according to FAA-established protocols. Depending on mission requirements, the RID may be cryptographically protected by an authentication message to ensure its authentication, non-repudiation, and integrity.

RID is used for traceability and accountability, and it can also be used by the IASMS to characterize flight information of vehicles participating in the NAS. Characterizing data is essential to enabling assessment functions that may evaluate specific operational risks in the NAS, and RID is a potential solution.

The National Academies noted that regulations will need many changes for AAM. To accommodate and enable the rapid pace of AAM innovations, regulators can use risk-based approval for certain unmanned operations. The challenge is that risk cannot be determined for those non-stochastic designs and operations that are new and consequently have no historical track record [9]. New standards and advisory guidance to show alternate means of compliance for achieving certification would be useful to help industry prioritize its investments.

Identification of Safety Critical Risks

The ISSA Concept of Operations addresses safety critical risks by examining the sources of hazards that can challenge the viability of design and operations for UAM. These sources are the vehicle itself, the environment, the operational context, and the aviation system. These sources reflect the different types of hazards and their associated risk/safety impacts.

The ConOps looks to define a set of safety risk categories that IASMS services would work to resolve and/or mitigate. The risks stated must indicate an overall risk category and the relevant

agents of the system. Later a discussion can be made under the architecture that identifies the interfaces between the operators that are necessary in order to provide the monitoring and the assessment of data and also identifies the agent(s) responsible for implementing the mitigating action.

In addition to these AAM system-wide safety risks there are also implications to societal safety risk outcomes. Accidents and incidents can lead to a lack of public trust that can reduce access to airspace, limit market growth, and increase operational cost, regulations, and litigation. The National Academies noted that societal concerns most commonly occur after a high profile accident [3]. The National Academies posited that AAM safety needs to be better than the safety rates for General Aviation (GA). They noted that GA has a fatality rate worse than automobile travel albeit on the basis of passenger miles traveled, and that AAM safety rates that are the same as GA safety rates would not be viable [9]. The National Transportation Safety Board (NTSB) reported preliminary statistics for 2018 that showed there were 1,275 GA accidents (or 3.49 accidents per day on average) and 225 of these involved fatalities [10]. With 21,663,367 GA flight hours, the GA accident rate was 5.876 per 100,000 flight hours, and 1.029 fatal accidents per 100,000 flight hours. There is a need to develop new safety metrics for AAM that account for both distances traveled, hours of operation and number of operations completed to properly evaluate acceptable safety rates. That is, shorter distances and shorter flight times for envisioned UAM operations will likely have high numbers of flights per day yet short overall flight times.

Trust in the AAM automated system is a multi-dimensional human response. The scale of the challenge is commensurate with the increased pace and uncertainty of new entrants (e.g., increasingly autonomous UAS and sUAS, larger on-demand mobility aircraft, unauthorized UAS operations, autonomous freighters, federated traffic management systems, and commercial space launch and reentry operations) and any related emergent risks. Factors that increase trust are both soft and data-driven and can include the physical appearance of the system, experience interacting with the system, reputation of the system designer, predictability of being able to depend on it for all nominal and off-nominal operational conditions, actual or perceived susceptibility of tampering, reliability, and transparency [11]. At the same time, trust depends on the propensity of the individual to trust automation such as based on past experience and being able to form a mental picture of how the automation works. Trust also depends on contextual factors like training and under what circumstances the human operator can intervene.

The National Academies indicated that AAM should build margins around vulnerabilities such as by placing humans in the loop, designing procedural safeguards for traffic spacing requirements and other operations, and anticipating that new hazards can emerge as airspace complexity increases. These buffers would be especially important to ensuring safety when the operational envelope is not fully understood.

Our delineation of ISSA safety critical risks was informed by an integration of multiple sources of expert reference. These sources represent different perspectives on UAM and IASMS. Some identified risks were common across multiple sources, while in other instances a single source because of its unique perspective identified particular risks. These risks have been classified as safety risk outcomes and causal/contributing factors to those outcomes [6]. Other sources

included the FAA Helicopter Flying Handbook that identifies common errors with flight maneuvers and helicopter emergencies and hazards [12].

Unsafe Proximity to People on the Ground, Air Traffic, or Property

The first safety risk is Unsafe Proximity to People on the Ground, Air Traffic, or Property. The National Academies identified this as a known risk. Industry engagement noted this may result from loss of detect and avoid systems, and can lead to midair and ground collisions with people, obstructions, and other UASs. The FAA UTM Concept of Operations indicated that in the UTM environment, BVLOS UAS share responsibility with other BVLOS UAS and manned aircraft for collision avoidance [5]. Risk metrics should include the number of people on the ground such as in terms of the density of people on sidewalks, in open spaces, and other locations where vehicles might operate, as well as the risk of harming people as casualties in a UAS accident. Other risk metrics could include the amount and value of property on the ground, the number of manned aircraft in close proximity to the UAS operations, and the density of UAS operations.

Associated with the above safety risks are causal or contributing factors. Three factors were identified by Young et.al. [6], and another three factors were identified through a combination of the National Academies report [3] and stakeholder engagement [7].

Flight Outside of Approved Airspace

Another safety risk is Flight Outside of Approved Airspace. The National Academies also identified this as a known risk. Industry engagement noted there may be differences in how permanent obstructions (e.g., radio towers, tall buildings and advertising signs) may be displayed, for example, these hazards may not show up on map products until the next update cycle time.

Causal or Contributing Factors

Critical System Failures

Failures of critical systems include loss of the command and control (C2) communication link, loss or degraded GPS positioning system performance, RFI, loss of power, and engine failure. The National Academies identified this as a known safety factor [3]. Failure could be limited to the sensor hardware or impact the system itself.

The goals and metrics for critical system performance need to be collaboratively defined including whether there are required performance thresholds and tolerances.

The severity of the failure depends on different considerations. These include the following:

- Environmental factors influence the risk to people. Population density under the flight path could be modeled such as based on type of housing and roadway and traffic

patterns. Modeling could also follow the movement of people on the ground derived from cell phone data collected by cell towers and aggregated by mobile phone providers.

- Human-automation teaming concerns the balance between operational authority allocated to automation versus the human operator relative to who is responsible for handling nominal operations and system failures. Automation can evolve through machine learning and certification that increases requirements for safety assurance. This could include certification requirements for a non-deterministic system, which is being addressed through a SAE G34 committee on artificial intelligence in aviation.

- Vehicle performance and system failures under different weather conditions. This can include general weather conditions as well as micro weather in an urban environment such as city winds. Further work is needed for collecting data to examine impacts of wind and cold temperature on battery performance, and effects from icing/precipitation on vehicle performance.

These considerations point to key questions concerning to what extent would specific in-time (raw) data be needed on vehicle performance or could manufacturer vehicle performance capability information be sufficient to determine the safety of the system, and to what extent would an IASMS be owned by the operator as a proprietary system such that only selective information and data might be shared as part of a federated air traffic management system? That is, standards would be needed on what performance data would need to be collected and what data would need to be shared. While the Operator and/or the USS would be responsible for hosting the appropriate IASMS capability, it could share a safety dashboard of status information. In addition, a common model could be shared across all agents through a partitioned IASMS. The operator-USS-SDSP network that shares information can be used to create a model to provide the necessary functionality of the IASMS.

There is an analogy to commercial transportation and other operations. Aircraft performance data are collected today such as by airlines in their Flight Operations Quality Assurance (FOQA) programs. Airlines together participate in the Aviation Safety Information Analysis and Sharing (ASIAS) program for trend analysis of historic data. An IASMS system could monitor and assess trends and identify failures that would compel the operator or USS to prioritize and execute contingencies.

Models are needed for system performance including the battery, aerodynamic, and weather interactions/effects on vehicle performance. Determinations would be needed specifying the thresholds for information classes and data requirements to have a risk status.

There is an expectation that an airspace service will be available to handle flow management in the vertiport and airport terminal areas.

Loss of Control

Loss of control failures can Include unintentional envelope excursions and flight control system failures. Loss of control can result from failure of the Ground Control Station (GCS). It can result in flight outside of approved airspace or unsafe proximity to people or property or other vehicles.

Cyber-Security Related Risks

Cybersecurity risks involve a complex array of UAS and UAM operational considerations. The National Academies included emerging risks such as cyber-attacks as well as a breach of the firewall protecting data management and exposing personal protected information (PII).

Industry concerns with security include digital hijacking, cyber-attacks, crypto key management, and phishing attacks directed at operators, which could be the easiest thing a hacker could attempt.

The FAA UTM Concept of Operations defined security as the protection against threats that stem from intentional acts such as terrorism, or unintentional acts such as human error or natural disasters, that affect aircraft, people, and/or property in the air or on the ground.

The information collected through the architecture and the portals that would conceivably exist in the architecture pose a challenge to ensuring cyber security. Industry would need to determine how cyber security risks would be handled and mitigated. The threat includes the case where the operator does not share full data and some other operator possibly misinterprets what data it does have and further generates actions from it such as for a flight plan or conflict avoidance, depending on the analytic approach. Another threat identified by the National Academies concerned gaps in technology to address fallback navigation methods for autonomous systems in response to outages or spoofing of the global navigation satellite system [9].

Physical Security Risks (Unintentional or Malicious)

The National Academies addressed physical security risks as an emerging risk associated with the instability of human operators, an emergent risk that could mimic one or more known risks, and new entrants such as on-demand mobility or commercial space operations.

Industry concerns with physical security risks include the heterogeneous mix of vehicles and their algorithms resulting in vehicles having different hardware and software working in different ways. Vehicles may operate differently based on cargo weight, size, and shape. This can be compounded by inexperienced pilots having poor training.

Physical security risks can include physical hijacking and counter drone systems used by malicious operators. A hostile property owner may threaten a vehicle to get out of the airspace around a residence that in turn affects people on the ground. A vandal could intentionally damage a vehicle or operating system. A laser could be used to effect vehicle operation. A rogue operator could deliberately fly into controlled airspace whereas an amateur or non-communicating operator could unintentionally fly into controlled airspace.

Environmental Risks

Weather encounters pose a serious safety risk to UAS and sUAS vehicles. This can include wind gusts especially in urban environments where buildings of different heights can change wind speed and create eddies and other wind phenomena. Cold weather can change battery performance, and rain and snow can affect vehicle performance. Wind forecast models can be used to check flight plans for loss of safe separation from people on the ground, air traffic, and property as well as for flight outside of approved airspace. Precipitation forecast models can be used in a similar manner to check flight plans.

Regulatory Risks

The National Academies referenced regulatory risks but only at a higher level. Industry concerns with regulatory risks include operator certification requirements, new entrants without appropriate aircraft type designations, use of drone umbrellas by individuals to protect privacy, intentionally ignoring or violating regulations, and lack of enforcement capability. Regulatory risk pivots on determining the appropriate safety margin for UAS/UAM operations for the vehicle, the USS, and for people on the ground. This points to the need to determine safety margins for operational ISSA capabilities such as involving minimum aviation safety performance standards (MASPS).

Safety Culture

Industry concerns with safety culture include the trade-off between safety and profitability, use of an aggressive business model, and the shift or clash with the public's expectations for safety.

Taken together these safety risk outcomes and causal and contributory factors provide a broad perspective to the operational and technical challenges addressed by ISSA. This is portrayed in Figure 4 as a 360-degree view that ties the IASMS functions of monitor, assess, and mitigate with the safety risk outcomes and causal and contributory factors, hazards, vehicle state, NAS transition paths for USSs, vehicles and BVLOS operations, levels of autonomy, and phases of flight.

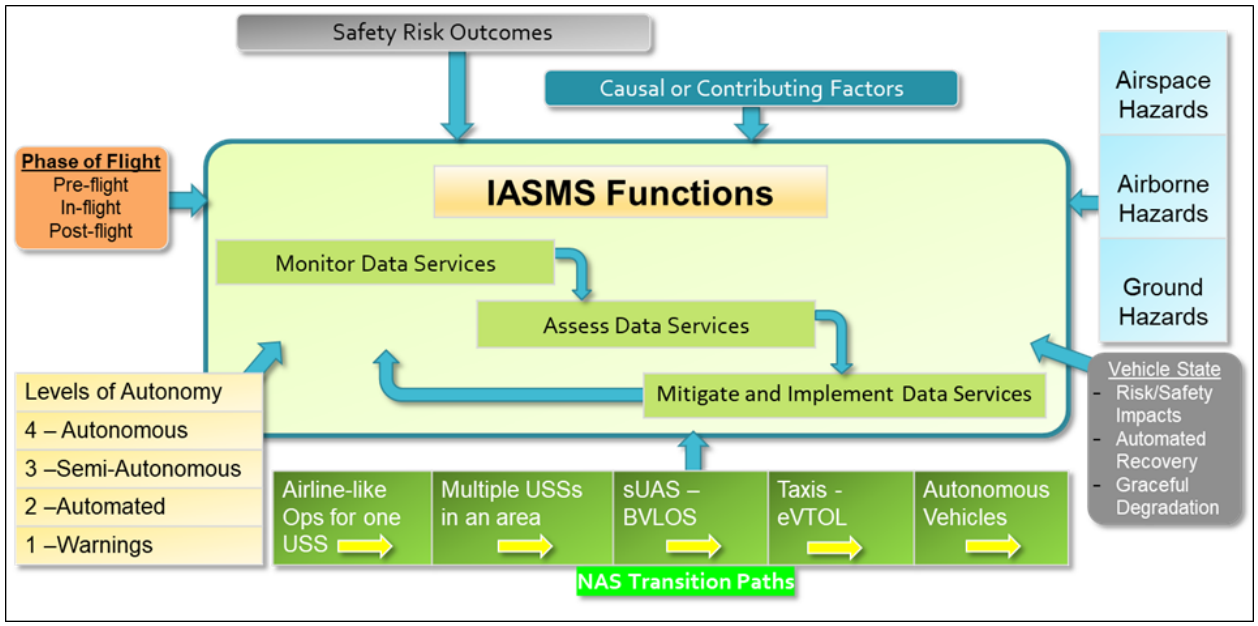

Figure 4. IASMS 360-Degree View

Approach to Risk Assessment and Prioritization

The National Academies IASMS report underscored the importance of prioritizing risks commensurate with those risks having the most impact on system safety. The intent is to address higher priority risks first in order to balance the resulting safety benefits relative to the costs of cumulative risk mitigation based on the complexity of the system.

There are at least four approaches to risk assessment and prioritization relevant to UAM:

- Traditional SMS approach involving probability of occurrence and consequence of an event [14].
- Unmanned Aircraft Safety Team (UAST) is an industry-government partnership that mirrors the collaborative model used by the Commercial Aviation Safety Team (CAST) and General Aviation Joint Steering Committee (GAJSC).
- Specific Operations Risk Assessment (SORA) developed by the Joint Authorities for Rulemaking of Unmanned Systems (JARUS).
- National Academies report that provided a set of IASMS criteria.
- National Academies report that recommended a research program in probabilistic risk analysis (PRA) addressing comparative risk for proposed technology innovations [8].

Safety management systems use a traditional approach to risk assessment, based on the probability of occurrence and the consequence of an event. This approach is viable for known risks in which it is possible to leverage the historic data obtained from design and operation of conventional aircraft. This approach does not work as effectively for the case of emerging risks with new entrants. In particular, the National Academies report noted that new entrants can increase the level of uncertainty for both the safety and efficiency of the NAS. This uncertainty builds from a paucity of data on the effect of new entrants on NAS operations, the performance of human operators and their trust in increasingly autonomous systems, and the prevalence of unauthorized UAS operations.

The National Academies underscored that traditional testing and simulation by themselves are not sufficient for the safety assurance of software systems that comprise complex AAM autonomous systems [9]. Safety is more effectively built into the design through the up-front analysis and definition of system requirements before a design is completed. That is, incomplete, incorrect, or missing requirements can result in a design that could be unsafe. Retrofitting the design to accommodate unanticipated requirements can be costly especially when the design is brittle. The challenge of safety assurance is compounded by interdependencies among system requirements across collision avoidance, contingency management, traffic management, and cybersecurity.

One promising method is Specific Operations Risk Assessment (SORA) developed by the Joint Authorities for Rulemaking of Unmanned Systems or JARUS [15]. At a higher level, the SORA process starts with risk modeling such as with bow tie diagrams to model the risks. This model is used in risk assessment and the identification of risk mitigation measures. The SORA approach involves guidance developed through consensus of various national aviation authorities on a common process to identify, qualitatively assess, and manage the safety risk posed by unmanned aircraft systems (UAS), when preparing the safety case required for regulatory approval to conduct certain types of operations [15]. SORA is described as a barrier model of safety that can use bow tie diagrams in a graphical representation of safety-relevant scenarios and the suite of related SRM measures (termed as barriers). SORA is a flexible and risk-based approach to trade off safety-relevant considerations such as technical airworthiness, equipment and operator performance and capabilities, and operating rules, restrictions, and procedures. This information and data can be used to build the operational safety case from which safety measures can be selected that are proportional to the risk posed by the particular operational concept.

Denney et. al. evaluated and extended the SORA approach focusing on providing a formal basis for determining barrier integrity and a simple probabilistic formalization of the underpinning barrier-based safety model. This included Escalation factors (EFs) that are weaknesses, vulnerabilities, threats, or other operational conditions that can compromise, defeat, or otherwise degrade control effectiveness (e.g., electromagnetic interference). They also incorporated Escalation Factor Barriers (EFBs) that are analogous to barriers but are a secondary system of controls used to manage, reduce, or modify the impact of EFs [16].

SORA applicability was demonstrated as a formal quantitative method using a NASA UTM project [16]. The purpose was to show how implementation of a simple formal risk model can work with SORA. Part of the formalization included foundations for barrier properties such as reliability and integrity and for risk assessment including use of bow tie diagrams and a safety architecture. The concept involved conducting BVLOS flight on defined paths, with small UAS within an operating range (OR), a predefined volume of airspace that encloses, for the most part, sparsely populated and minimally built-up areas on the surface. The air traffic within and outside the OR includes conventionally piloted aircraft. Findings included that their Bayesian Network-based enhancement enhanced risk assessment by starting from a safety target from which risk and its probability component could be allocated across the various barriers known to be independent. Research concluded that SORA can overcome challenges in data collection and handling uncertainties that are used to justify the use of qualitative methods although such methods have difficulty for use in more complex, higher-risk operations. NASA research suggests the use of SORA is a sound approach to measure qualitative assumptions by which risk under uncertainty can be more carefully examined [16].

The National Academies report identified a set of criteria for prioritizing risks. For the purpose of this ISSA ConOps, uncertainty is used as a preliminary indication of risk. That is, uncertainty represents the level of confidence that a risk is well understood and warrants only limited future research that focuses on particular aspects of the risk. A risk could have low uncertainty, for example, if understanding of the hazard is based on commercial or GA safety information that is extensible to UAM, or if the risk has a minimal impact for safety assurance or risk management. A risk could have high uncertainty, for example, if there is limited understanding of the hazard and no history of its mitigation with commercial or GA. An actual rating of risk priority would depend on the relationship of the underlying hazard with design, operational, and maintenance aspects.

Risk prioritization is influenced by several factors such as: a.) how well the hazards that underlie risks are understood and can be monitored and detected, b.) the types of data that can be used to identify elevated risk states, and c.) societal risks. Conversely, it is unknown which risks do not warrant monitoring due to high cost, low uncertainty, and minimal safety impact.

Prioritization of risks changes dynamically over time. Significant changes in airspace operations, the emergence of new risks, the transition of new technologies and advanced automated capabilities, and aggregation of new data on risks all contribute to this dynamic risk prioritization.

The National Academies report provided a set of eight IASMS criteria for risk prioritization: consequence, probability, experience with hazard, detectability by monitoring data that can identify an elevated risk state, viability of risk mitigation, cost of mitigation, undesirable secondary effects, and societal risk.

The National Academies reported that safety and societal acceptance are among the most important barriers to adoption of AAM technology [9]. For AAM, absolutes about safety and social acceptance are closely intertwined in gauging its relative tradeoffs between risks and benefits. An important challenge to societal acceptance is controlling the noise generated by AAM vehicles flying overhead and at vertiports. The National Academies considered noise a complex challenge involving psychoacoustics, which are the physiological response of humans to noise and the psychological perceptions people have about vehicles and the annoying noise they can produce.

Risk Discussion

Overall, the above discussion responds to the recommendation from the National Academies report that risks be identified and prioritized for assessment and mitigation by the envisioned IASMS. This information is important in developing the ISSA concept of operations including the data and architecture necessary for the functions comprising IASMS. With this information collaboration with industry can progress to complete the definition of the ConOps for a scalable UAM IASMS. This provides a foundation for a service-oriented architecture that can better focus safety investments in technological solutions with emerging operations.

Further industry discussion regarding safety risks included the following considerations. It was noted the National Academies' priorities are key to the development of the IASMS ConOps. Part of the strategy is determining whether NASA, FAA, or some part of industry takes

leadership. Identification of risks is separate from and a first step toward prioritization of safety enhancements or mitigation steps, which are the responsibility of the UAST. It was recognized that risks depend on taking different points of view in terms of strategy. While Young and others presented a set of risks, the use cases could add to the risks identified. Reference was made to the FAA rotorcraft handbook that identifies some 100 failure conditions [13].

Regulatory aspects need to consider the margin of safety and the part that is allocated responsibility of the USS, operator, or vehicle. Reference was made to a report on levels of autonomy from the National Institute for Standards and Technology (NIST) [12]. With machine learning and systems developed to control the vehicle, algorithms need to be certified including under different operational and weather conditions. These might be non-deterministic systems. SAE has a standards committee working towards the assurance of autonomous systems (G-34). This panel may be examining human-automation interaction and trust in automation such as associated with automation errors.

There was extensive discussion about the development and use of UAS safety databases. Data are needed from operators although UAST has not made much progress due to organizational considerations. There are no best practices for the human operator from government, academia or industry such as in relation to voluntary reporting by UAS operators or remote pilots. The FAA ISAM model includes fault trees and probabilities from a study on commercial rotorcraft that might be useful for UAS. Eurocontrol worked with NLR on developing quantitative fault trees. For example, nodes in the fault trees could be reviewed to see if they are relevant to automated systems or to the human-computer interface. The FAA needs data to set performance standards and NASA can provide modeling of the safety margin.

Risks are analogous to current flight operations. Battery and vehicle problems can be a risk and not just a contributing factor. Flight outside of approved airspace can be a risk if the UAS is not following a PBN-based flight plan. Consideration should be made to address vehicle performance with interactions with weather for their impact on low altitude operations. Weather could include icing and precipitation as part of the performance model. Landings and takeoffs continue as the parts of flight having the most risks. Shorter trips expected in UAM operations mean more landings and takeoffs posing risk. Use of a corridor approach in UAM can change the risk of bird collision since birds typically fly at the same altitude. Vehicles have to be able to sustain an approximate 7 lb. bird strike.

IASMS Services

The suite of IASMS services important to ISSA safety assurance is framed according to the functions comprising in-time safety management. For the purpose of this ConOps, the UAM domain has been chosen to derive the necessary services to enable operations in the most challenging cases at the highest level of autonomy. Therefore, the scope of possible IASMS services pertains to the domain of future low-altitude urban flight operations. The ConOps seeks to leverage existing systems and standards where available and will look to demonstrate solutions for gaps in necessary safety assurance capabilities.

The assumptions for the low-altitude urban flight domain are:

1. Highly Autonomous (no pilot).
2. ATM/Airspace functions are separate, but interoperable.
3. Reliance on connectivity can be included as a service capability.
4. Identified hazards that span airspace, airborne, and ground categories provide good coverage of the potential harms to the envisioned operations.

IASMS services provide real-time information and data on vehicle state, known hazards, safety risks, and causal and contributing factors to safety risks. These services provide information and data corresponding to the phase of flight. The services operate on a differential time scale of seconds (near-real time), minutes, hours, days, or months depending on the risks assessed, data monitored, and actions required for mitigation.

These services are envisioned to be used in their entirety or in part by any of the entities shown in the section above called *Users of the ISSA Concept of Operations*. Some of these entities and their definitions are taken from the UTM Concept of Operations [5].

Key IASMS Services

Three service categories were identified as key to an effective IASMS consisting of monitor, assess and mitigate [6]. These categories span the three functions comprising the IASMS concept described by the National Academies [3] and as first described by Nowinski [17].

Several key IASMS capabilities will need to exist to assure the safety of the vehicle, the airspace, and the overall NAS. Each IASMS capability is envisioned to perform a safety service that at a minimum, affords each operation a reduction in risk by providing in-time feedback of current state contrasted with expected and/or nominal state. To achieve this, the monitoring of multiple sets of data is required and the analysis of that data will generate key assessments of hazards that threaten operational safety. The ConOps provides a list of key service categories, generated from multiple publications that are necessary to assure safe and scalable transformation of the NAS. These services are divided into Monitor services, Assessment services, and Mitigation services, all of which when combined form an IASMS capability.

The timeliness requirement of each service and corresponding IASMS capability depends on the risk criticality and corresponding safety assurance action necessary to mitigate it. The IASMS capability limitations vary depending on the source of information available and its key factor characteristics. When considering the time frames for IASMS capabilities, three categories have been defined for service types that address the critical needs for safety assurance, referred to as SDS-R, SDS-eXclusions (SDS-X), and SDS-Safety (SDS-S) [6]. Both SDS-R and SDS-X services address near real-time capability requirements in the seconds to minutes time frame, while SDS-S services address system-wide capability requirements on the hours to months. All three service categories are capable of interacting independently but function more effectively through interconnectivity of shared information. SDS-R services pertain to the health and safety of the vehicle. SDS-X services involve the surrounding air traffic operations and airspace constraints. SDS-S services include post-flight data analytics capabilities.

The fusion of data across multiple information classes offers an opportunity for innovative developments in enhanced scalability and efficiency when dealing with safety related issues. For example, a service capability that integrates power health information, aircraft model data and population density can leverage all three sets of information to generate a time- or distance-remaining metric and generate a list of options to safely land the aircraft with minimal harm to the vehicle and the surrounding environment in the event of an off-nominal event. To account for safety assurance amidst the growing scale and complexity of operations, IASMS service capabilities may communicate between other IASMS service capabilities or include multiple information classes to make informed risk mitigation responses.

Monitor Function and Data Services - Categories of Service Types

The Monitor Function and Data Services can be used by predictive models addressing each safety critical risk. These models can operate at different update rates and data resolutions, and use look-ahead horizons corresponding to user/operator requirements. These models may be executed in real-time or near real-time on the vehicle, at the Ground Control Station, the USS, or SDSP. These services include but are not limited to the following:

- Aircraft state information and aerodynamic model including aircraft trajectory data. This goes in the direction of addressing the question of what is the UAS doing in terms of flight performance [18].
- Positioning system state information and performance model. This goes in the direction of addressing the question of where is the UAS going?
- Communications system state information and radio frequency interference (RFI) model as well as voice communication and human performance data. This goes in the direction of addressing the question about how the vehicle, systems and people are communicating. This can involve uplink/downlink connectivity monitoring.
- Population density information and dynamics model. This goes in the direction of addressing the question of how close the UAS' flight plan and trajectory come to flying near people.
- Vehicle system health state information and model (i.e., engine and battery health as well as communication and navigation monitors). This goes in the direction of addressing the question of whether the vehicle continues to be airworthy and is it able to make flight safety decisions remotely.
- Aeronautical Information Services (AIS), e.g., special use airspace, temporary flight restrictions, weather, and geographic data representing terrain, obstacles, and airport mapping features. This type of service already exists and is transitioning to a more timely update rate such as would be needed here; however, it is not yet tailored to low altitude sUAS urban operations. This goes in the direction of addressing the question of whether there is an adequate route structure.

Young et. al. identified several models that are beneficial to the envisioned IASMS capabilities described in the ISSA ConOps. For example, these models included a weather forecast model and a battery performance model [19].

The specification of predictive models and data including synchronization and interaction between services may vary based on operational state, i.e., pre-flight, in-flight, or post-flight. Surveillance data may be used and provided by the SDSP or USS depending on operational requirements.

The National Academies report posed use of IASMS data and large-scale data analytics to monitor for systemic or anomalous changes to the NAS [3]. Data resources include system services such as ADS-B, SWIM, FIMS, wireless links from aircraft to terrestrial or satellite-based systems, ground system-to-ground system networks, and aircraft-to-aircraft communications systems. Key factors regarding the collection of data from each information source and its corresponding information class include the following [3, 18]:

- **Availability of data** originating from the vehicle and its systems as well as data from performance models,
- **Latency and accuracy of data** collected from different sources where lags, different resolutions of data, and other variations in key parameters can limit correlation and fusion,
- **Update rates** using synchronous and asynchronous timing between information classes,
- **Integrity of data** from NAS communications, navigation, and surveillance networks,
- **Security of data** involves issues that are unique to the operation of an IASMS such as detection and mitigation techniques for cyber threats that could fail or compromise the integrity of NAS communications, navigation, and surveillance networks but without having to develop more secure communications protocols or firewalls that are addressed elsewhere,
- **Formats of data** from heterogeneous sources consistent with data exchange standards and for which differences can constrain the correlation and synthesis of data along with timing, accuracy, and other characteristics,
- **Avionics standards** are important to the collection of data in real time through wireless links from aircraft to terrestrial or satellite-based systems, ground system-to-ground system networks, and future aircraft-to-aircraft communications systems,
- **Implementation** and service costs are important to the business case for the IASMS by evaluating the proprietary nature of computational architectures of on-board systems and their potential high cost of modification relative to the cost and value of providing the IASMS with additional and/or higher quality data deemed necessary and worthwhile to collect, and
- **Spectrum regulation and bandwidth utilization** to provide sufficient bandwidth for data services considering update rates, latencies, and resolutions of data from multiple sources.

Sources and quality of data collected by an IASMS must be understood and tracked over time to determine the reliability of IASMS outputs. As such, Minimum Aviation System Performance Standards (MASPS) must be developed to establish design criteria for safety critical IASMS services. Some standards may already exist and be referenced, such as DO-364, Minimum Aviation System Performance Standards for Aeronautical Information/Meteorological Data Link Services [20], and DO-200B, Standards for Processing Aeronautical Data [21]. However, there is a strong need for additional MASPS and data standards to allow for the growth and expansion of these complex systems. It is also important to note that the MASPS for safety critical systems and the location for which each IASMS service resides may and likely will vary by domain, i.e., sUAS package delivery versus UAM passenger carrying vehicles. Therefore

domain-specific MASPS may be necessary to provide the necessary design criteria and guidance. As the complexity of operations in the NAS evolves, multiple approaches should be examined ranging from relatively simple methods based on exceedance criteria to more complex model-based, conformance-based, and statistical-based methods. At the same time, it is important to consider the value proposition of safety data. This is understanding the value added by the particular data based on its importance and relative to the cost to collect it that depends on its availability (i.e., how complex it is to collect it). This cost-to-benefit ratio in developing an IASMS may be so high that it will delay or otherwise impact its implementation. A phased implementation with the AAM community would be one way to overcome any perceived cost-to-benefit barrier.

To achieve IASMS goals, data fusion may become necessary using existing and new additional sources. This includes data from ADS-B reports, voice recognition of controller-pilot voice communications and among the members of a single flight crew, flight data (e.g., aircraft state and trajectory data), as well as non-flight data (e.g., human performance measurements).

The transition paths for UAM involve integration of multiple technologies and operational capabilities. A single USS could appear like an airline operations center (AOC) simultaneously planning multiple flights and coordinating flights already en route such as for weather re-routing and traffic congestion. A large geographic area could involve more than one USS, or a given urban area could have multiple larger USSs for different business entities. Considering the size of the geographic urban area, sUAS may fly BVLOS and air taxis may use eVTOL vehicles. Eventually autonomous vehicles may become commonplace at least initially as part of a mixed equipage operational environment.

Assess Function and Data Services

The Assess Function and Data Services comprise the processing of information and data provided by the Monitor Function. The Assess Function serves to detect, diagnose, and predict risk and hazard states. The Assess sub-functions may operate concurrently on the vehicle, at the GCS, the SDSP, and/or the USS. Outputs from the Assess function may focus on an individual risk or hazard, or may be bundled into an overall risk assessment.

The Assess sub-functions and their models can evolve leveraging all the many operators, reporting systems, and operations that feed into the IASMS. Over time, data-driven operational validation can continue to improve the models, especially by reducing statistical uncertainty. These models can also evolve tailored to various equipment types (e.g., vehicle, engine, battery), operating environments (e.g., adverse weather, 3D structures), and mission profiles (e.g., flights having multiple legs).

Models can also start to look at unusual circumstances beyond those anticipated by designers or viewed as extremely improbable. Models can consider monitoring for overarching risk and safety margin such as a parallel to the FAA's Integrated Safety Assessment Model (ISAM) [22].

Three categories of safety-relevant data services (SDSs) are important to the Assess function [6]. First, the SDS-Realtime (SDS-R) service category provides a continuous risk assessment that is repeated on the scale of seconds to minutes. It uses data from the vehicle, USS, and other sources on aircraft state, vehicle system states, weather factors, and population density in the region of flight. For example, a battery health monitoring service and its commensurate IASMS service capability should function in near-real time to provide timely response to a failing battery to ensure the safety of the vehicle and the surrounding operational environment. This capability requires power health data at a minimum to perform its function.

SDS-R involves UTM Services identified in the FAA UTM ConOps version 2 such as the Operator Registration Service and USS Network Discovery Service along with separation-related capabilities involving the Strategic De-Confliction, Conformance Monitoring, Conflict Advisory and Alert, and Dynamic Reroute Services [4, 7]. Additional services for Strategic Separation could include Airspace Organization and Management Service and Strategic Deconfliction Service; for Tactical Separation Provision could include Geographic Flight Containment, Dynamic Rerouting, Conformance Monitoring, and Conflict Advisory and Alerting Services; for Collision Avoidance include Collision and Obstacle Avoidance; as well as Flight Awareness Service [23].

Second, the SDS-eXclusions (SDS-X) category involves air traffic and airspace constraints coming from the FAA or USS. With risk assessment occuring on a time scale of seconds to minutes to hours, it uses data that may include position reports, temporary flight restrictions, warnings, and/or advisories. Services identified in the FAA UTM ConOps version 2 could include Airspace Authorization, Constraint Management, and Dynamic Reroute [4, 7]. An additional service for Tactical Separation Provision could include Ground Surveillance [23].

Third, the SDS-Safety-margin (SDS-S) category assesses the evolution of safety risk compared to the desired safety margin. SDS-S would work on a post-operations basis using a time scale of hours to days to months reflecting system-wide assessments. This capability would use outputs from multiple services for post-flight data analytics to estimate, track, and predict over-arching safety risk. Connections to multiple services support identifying which data elements are most contributing to reported risk. SDS-S would include today's existing systems including Flight Operations Quality Assurance (FOQA), the Aviation Safety Reporting System (ASRS), and Mandatory Occurrence Reports (MORs) to future prognostic capabilities. Future capabilities may evolve to evaluate system-wide operational trends in increasingly near-real time, as well as validate performance models that leverage increased levels of autonomy. There would also be the provision for a new ASRS system for drone activity reporting.

The National Academies report on IASMS noted that changes in design and operation should be identified and assessed for risk potential. In addition, data fusion algorithms for non-causal post-processing may be used to produce more accurate flight state data.

In-time safety assessment for a large number of risk factors will require sophisticated system analytics. Existing computational architectures lack the ability to handle large volumes of heterogeneous data and dynamic analytics workflows, both of which are necessary to detect elevated risk states, to detect and characterize emergent risks, and to update the IASMS risk

assessment algorithms. Computational architectures will need to be able to work with high-volume and high-speed streaming of data from different locations. This includes real-time data from multiple sources (e.g., vehicle, ground station) and data from stored archives (e.g., private proprietary cloud, leased cloud, public cloud). Informational requirements of the consumers of various components of the data will also have to be accommodated.

In addition, in-time algorithms will require large volumes of heterogeneous, multimodal data, and the ability to process them in a timely fashion. Timing is important so that an IASMS can monitor ground and air operations and identify and characterize the current state of operations. Data quality and completeness as well as data fusion will impose requirements on data-driven state identification methods. These methods will have to be able to process data from multiple sources that have varying levels of uncertainty. In turn, these methods will have to determine the reliability of the assessment function as it detects elevated risk states. Algorithms will take advantage of advanced machine learning methods to analyze large volumes of heterogeneous data and find anomalous patterns and precursors to hazards.

Mitigate and Implementation Function and Data Services

The mitigate and implementation function and data services resolve either current or impending operational situations that exceed a defined safety threshold. Young and others (2018) noted that the monitoring and assessment functions ultimately determine how well mitigation can occur for any safety-adverse situation that develops and much of the R&D for this function is planned for future years [6].

Decision-making is the task of choosing a course of action among multiple alternatives, and therefore the tools that will be employed will likely utilize a suite of optimization techniques. For in-time decision-making, speed of execution is key and needs to be considered in the presence of possibly limited on-board computational resources.

Another key challenge will be defining roles and responsibilities between human(s) and machine, in particular the distribution of authority and autonomy between human(s) and machines. There is a significant amount of prior work in this area that can be leveraged and applied. However, the degree to which this can be done, versus discovering completely new approaches, will depend on the specific use-case, associated hazards, and target level of safety.

The National Academies report on IASMS supported the development of viable and effective methods for the timely detection and mitigation of elevated risk states for particular risk areas.

Resilience, Graceful Degradation and Contingency Management

The system-of-systems nature of IASMS presents a unique challenge to considerations regarding service resilience and graceful degradation of the systems providing the service and

how they relate to contingency management. Cross-cutting interdependencies of services lead to an increased complexity.

These interdependencies add complexity when one or more systems start to degrade or experience an outage. AAM systems would be designed to provide resiliency under many operational conditions based on requirements established for minimal capability. In managing contingencies there can be known and unanticipated ripple effects depending on the adaptability of systems and as they fall back to planned degraded service levels.

Resilience and contingency management would be scaled according to the complexity of automation and automated systems, and the role defined for humans in monitoring, quickly assessing, and possibly stepping in to mitigate risk in a way that automation was not designed to handle. This could be a particularly cogent requirement for a cyber risk that propagates to a safety risk.

Resilience, fault discovery and isolation, fault tolerance, graceful degradation, and contingency management necessitate strong design requirements and collection and analysis of safety data. Operational experience with vehicles and airspace will support reactive and proactive analysis of safety risks, sometimes referred to as Safety I and Safety II. Reactive analysis can include such harms as accidents, losses of separation, procedure deviations, runway or vertiport incursions, controlled flight into terrain, flying in adverse weather conditions, and pilot voluntary safety reports. Proactive analysis involves situations in which the pilot or other person “saves” an operational situation from evolving into an accident or incident.

IASMS Services Discussion

The IASMS Services provide information and data associated with airspace, airborne, and ground hazards. These Services are key to monitoring for known risks states as well as emerging unknown risks. Services become increasingly sophisticated with higher levels of automation and as vehicles, USSs, and SDSPs transition toward increased autonomy. Key factors regarding the collection of data from each of these sources include availability, latency, update rates, integrity, security, formats, avionics standards, implementation and service costs, spectrum regulation, and bandwidth utilization.

The IASMS 360-degree view (Figure 4) shows how services relate to risks, phases of flight, levels of autonomy, hazards, vehicle state, and transition paths. Feedback and input from industry included the concern for how compliance could be measured in terms of safety thresholds to trigger risks. Another concern was what separation standard would be used for mixed UAS operations. For this airspace no radio communication is required. Separation could be based on pre-declared trajectories such as with the adaptation and use of terminal STARS airspace to UTM airspace. This could lead to an RNP-like requirement such as for use of airspace corridors. Mixed aircraft operations could include the use of a best equipped, best served approach. However, legacy operators such as tour helicopters would want equitable treatment, which could be another transition path. A UAS conference held in Berkeley addressed closer separation as a way to manage traffic to vertiports.

Industry input included that the concept of operations should consider the ecosystem of the vehicle with the increased aggregation of services. The Mitigate Services to implement solutions

are important to safety assurance and could include contingency planning to de-conflict localized conflicts. This would be part of mission planning including mitigating possible risk arising from off-nominal operations. Mitigate Services need to account for weather effects. The ConOps needs an ATM point of view as much as a UTM point of view to account for legacy operations. Access would be different for air taxis compared to cargo delivery. This could be founded on airspace separation or some other priority, or involve a waiver for separation. For example, an eVTOL could be cleared into Class B restricted airspace as opposed to being considered a threat. Industry noted that public-private partnerships could be used to address many of these issues. These issues do not fall exclusively under the responsibility of the government.

Regarding safety risks addressed by IASMS functions, industry concerns included that the ConOps may need to include emergency conditions such as failed motor or uncontained engine failure. The ConOps may also need to identify additional concerns such as from mitigation of risk from use of RNP. The recent UAS conference in Berkeley addressed vehicle sovereignty versus ground systems in terms of where software capability is located. Vehicles should as an end state have resident software and models to operate independent of ground systems as a fully autonomous mode. If the vehicle could lose the communication link then each vehicle needs to be fully autonomous. A higher level of integrity is required to ensure the safety of the affected vehicle and other vehicles near it. Otherwise the airspace around the vehicle having the failed communication system would need to change. Further, other nearby vehicles may also lose their communication links as a localized degradation issue. A remote or bunker pilot could be used as a backup approach to maintain some level of control over the vehicle. A question is how to manage the V&V process over time as a certification risk? Another question is how to develop trust in autonomy and automation through the V&V process.

Regarding data services required by IASMS functional category (Monitor, Assess, Mitigate), industry considerations included that monitor services involving independent surveillance could be part of the ConOps. Services similar to UTM concepts could use more consistent language, e.g., vehicle system health or vehicle real time health. UTM may not meet all IASMS needs. Data services need to distinguish what is critical or not, e.g., what data are needed for a common situation awareness among operators. The ConOps may use a service-oriented ATM architecture that can be referred to as “UTM-inspired ATM” as an ATM retooled for UAM. ATM is a layer above services such as warnings from big data analysis. This would be an open system that could add new models and data. For Mitigate services this could include the use of a parachute deployed when the UAS was carrying an elderly person needing emergency attention. It was noted that a standard is needed for certification of each service. Business models involve different objectives that can reduce or change certification requirements. The concept should account for traffic load, route loading, and capacity changes to improve safety for vertiports. This includes the need for a measure of risk for vertiports to show how quickly it can change and the effects from mitigations.

Regarding information requirements between people, systems, and monitors, industry considerations included that minimum capabilities for systems and equipment need to be identified. This could include the interconnectivity between services. Detect and Avoid would be added to the information requirements.

Data Requirements and Architecture

The National Academies identified and discussed a number of considerations pertaining to data requirements and their associated architecture. These considerations can be organized separately according to the Monitor, Assess, and Mitigate services.

Regarding the Monitor services, the National Academies noted that an IASMS would use large-scale data collection and analysis as necessary to monitor for systemic or anomalous changes to the NAS. Different potential approaches should be examined for effects on data quality, which can range from relatively simple methods based on exceedance criteria to more complex methods involving use of model-based methods, conformance methods, and statistical methods. In addition, new data sources should be investigated for effects on data quality including ADS-B, SWIM, wireless links from aircraft to terrestrial or satellite-based systems, ground system-to-ground system networks, and aircraft-to-aircraft communications systems.

In addition to data quality considerations, the IASMS will need to use data fusion techniques with flight and non-flight data. The fusion of data would correspond to the time scales of interest and be stored for further processing or augmentation using additional or higher quality data. Flight data could include aircraft state and trajectory data. Non-flight data could involve human performance measurements and voice communications between controllers and pilots as well as between pilots on the flight deck and among the members of a single flight crew. For more complex IASMS goals, data fusion may be extended to fuse data from additional sources such as from ADS-B reports or voice recognition of controller-pilot voice communications.

Measurement of human performance is important to achieving the full potential of the envisioned IASMS. Barriers for collecting this type of data will need to be addressed including privacy concerns and potential punitive outcomes for the operator. Resolutions of barriers could involve ensuring confidentiality of submitted data and de-identifying data sources. Human performance considerations with increasing automation and traffic complexity involve automation state awareness and information requirements, workload, automation surprise, skill degradation, training, use of digital data communications and voice communications, and staffing.

Key factors regarding the collection of data from each source include availability, latency, update rates, integrity, security, formats, avionics standards, implementation and service costs, spectrum regulation, and bandwidth utilization. These sources and the quality of data collected by an IASMS need to be understood and tracked over time to determine the quality of IASMS outputs. At the same time, it is important to identify which data are necessary and worthwhile to collect relative to the cost and availability of data as a value proposition.

Regarding the Assess services, the National Academies report noted that data fusion can involve non-causal post-processing algorithms to produce more accurate flight state data. These data would better enable the identification of changes for risk potential [3]. For system analytics, the in-time safety assessment for a large number of risk factors will require the development of computational architectures for data input and output devices, processing

capabilities, and storage that can work with high-volume and high-speed streaming of data from multiple sources.

New in-time algorithms will require large volumes of heterogeneous, multimodal data, and the ability to process them in a timely fashion so that an IASMS can monitor ground and air operations and identify and characterize the current state of NAS. Existing algorithms for identifying and predicting elevated risk states have limited ability to integrate these diverse data sources. As part of IASMS algorithms, data quality and completeness as well as data fusion will impose requirements on the data-driven state identification methods regarding the ability to process data from multiple sources of varying levels of uncertainty to determine their impact on the reliability of the assessment function as it detects elevated risk states. Alternatively, it will be difficult to develop algorithms that analyze and predict the effects of emergent risks before incidents or accidents occur because the increasingly complex NAS will lead to new anomalies with unknown root causes. Further, an IASMS could inject new risks into the NAS due to unintended and unforeseen consequences of actions that it recommends or initiates as in the vein of an automation surprise.

A range of simple to complex IASMS computational architectures will be needed to support both multiple data sources and consumers of various components of the data. These architectures should be specified to take advantage of the development of advanced machine learning methods and algorithms to analyze large volumes of heterogeneous data and find anomalous patterns and precursors to hazards.

Regarding the Mitigate services, the National Academies report noted that viable and effective methods should be developed for the timely detection and mitigation of elevated risk states for particular risk areas [3].

The National Academies underscored the importance of addressing policy and technological gaps with communications [9]. They noted that further consideration is required to determine under what circumstances vehicles would communicate with each other directly and when all communication would flow through a centralized traffic management system. These circumstances would drive whether communication methods and standards would be considered safety-critical relative to either nominal or off-nominal conditions. This trade space would frame the concept architecture and technology infrastructure needed for air-air and air-ground communication. From this perspective one might hypothesize that vehicles would communicate immediately with each other for Detect-and-Avoid due to the abbreviated time scale in contrast with a centralized traffic management system to receive efficient route changes that have been probed for future conflicts.

In sum, the National Academies report identified a complex landscape of data requirements and architecture necessary to in-time identification of critical risks safety and proportional to operational complexity and cost effectiveness [3]. The need to narrow down to requisite communication methods and standards exemplifies this complex landscape and the gap to be overcome.

Data sources involve different systems and equipment having different physical and virtual locations in the architecture. The current FAA UTM architecture is shown in Figure 6 and has been annotated to show that the ISSA monitor, assess, and mitigate functions can reside with the SDS Providers, GCS functions, and vehicle system functions [6]. It is noted that the monitor, assess, and mitigate functions could also be part of the USS systems directly without being tied to the GCS functions as shown in Figure 6.

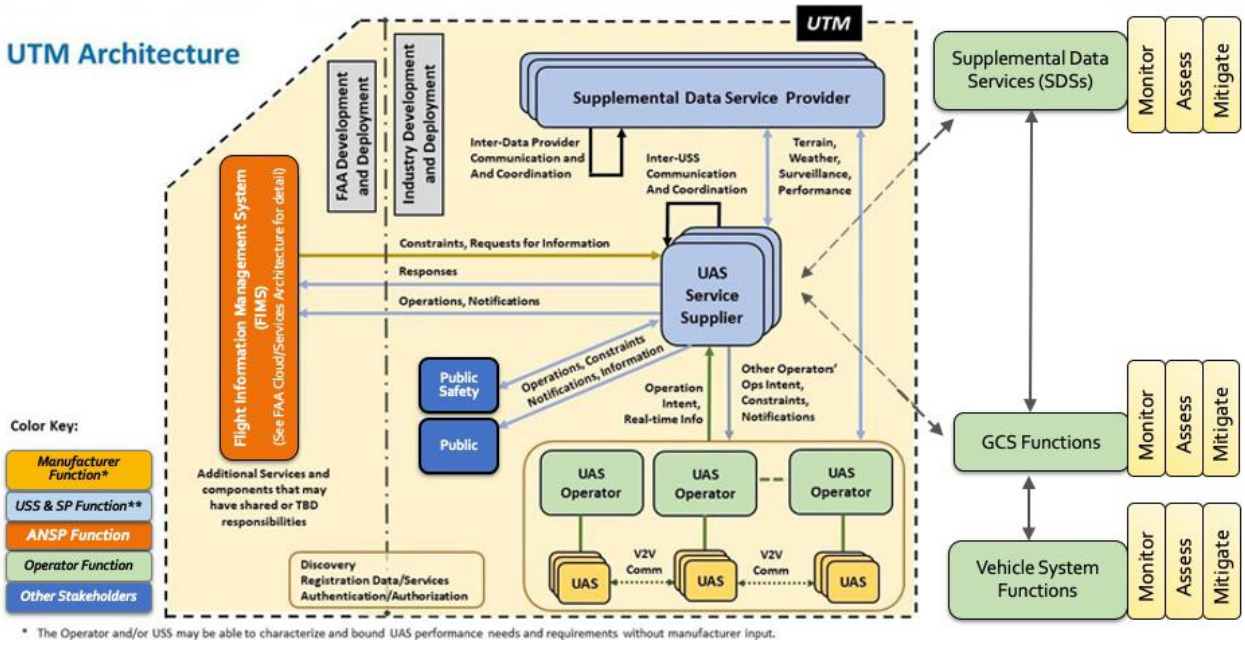

Figure 6. UTM Architecture (adapted from [5]).

This depiction of the architecture illustrates where IASMS capabilities could reside within the UTM architecture. The decisions of when and where to place specific IASMS capabilities are driven by several factors. A partial list of the factors that inform the logical deployment of an IASMS capability includes the following considerations:

- The ability to source the necessary data with the necessary quality to drive the Monitor and Assess functions of the IASMS capability.
- The time criticality of the risks the IASMS capability is addressing.
- The origin of the risk the IASMS capability is addressing.
- The responsibility of the agent in the system.
- The mitigation action of the IASMS capability.
- The resilience required of the agent in the system.
- The acceptable level of risk of the given operation.

Design requirements for a distributed service-oriented architecture should consider what information is shared, how detailed that information should be, when the information is exchanged, and who has access to the information. For example, without detailed data, it is not clear how a vehicle operator could estimate the power remaining for another vehicle that is using a different USS. This might also interact with the vehicle's battery warranty provisions. In

a similar manner, the design should consider whether a USS has a monopoly over its airspace and the information for vehicles in it.

Information Classes and Data Requirements

The classes of data underlying the architecture provide status on quantitative parameters important to vehicle and system control and ensuring the safety of flight. A taxonomy of information classes that represent the different types of vehicle, airspace, and other categories of information has been proposed as shown in Figure 5 [19]. Each of these information classes consists of one or more data parameters that provide quantitative information. These information classes either singularly or in combination can be used to generate an IASMS service capability.

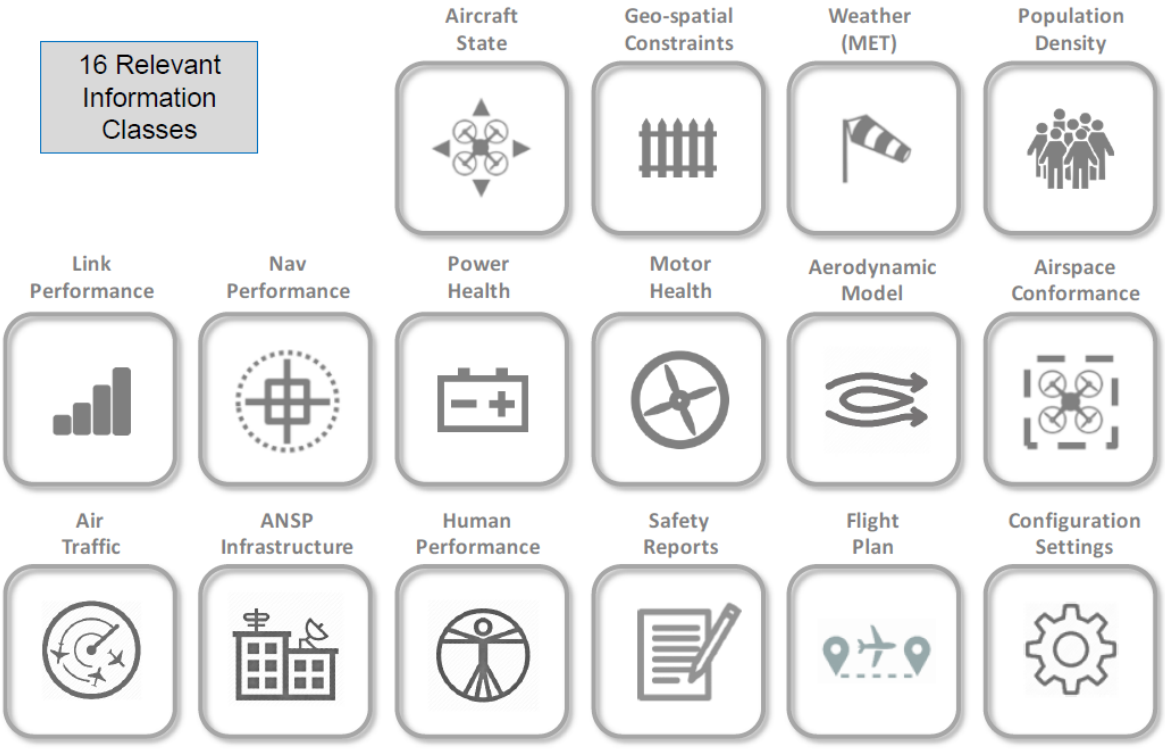

Figure 5. Information classes to generate IASMS service capabilities [from 19].

Principles and Traits

Several guiding principles and overarching traits are pertinent to the development of the data architecture required to support IASMS capabilities [19]. These principles and traits reflect best practices from software engineering as applied to aviation and include the following:

1. Use of an incremental approach that adds scalable functionality for increased IASMS service capability.

2. An open and extendible architecture that can address new risks or hazards as they appear.

3. Sustains interoperability with existing relevant systems such as SWIM and ATM/ANSP services and leverages interdependencies to avoid unnecessary duplication of functions.

4. Continuously transformative from the existing NAS to ensure seamless transitions and avoid brittle design.

5. Design approach uses techniques that assure required levels of data/information quality.

6. Applies run-time assurance techniques so that system failures are reported back to designers.

7. Flight-critical failures are trapped and isolated to meet higher fail-safe assurance levels.

8. Requirements for autonomous functions are robust to bound the behavior of autonomous systems for nominal and off-nominal operations.

9. Regulations establish how service providers become certified as “trusted sources.”

10. Design capability minimizes exposure to cyber threats such as by exchanging only the necessary data during each phase of flight.

11. Data exchanges protect the integrity of information based on data quality requirements.

12. Data flows through AAM services using SWIM-like connectivity to ASIAS-like data stores, analytics, and processes.

13. AAM design and operations are supported by a safety case for flight-critical elements, e.g. auto-mitigate functions.

14. IASMS integrates existing industry SMS processes, standards, and best practices for risk analysis and safety assurance.

The ISSA Concept of Operations leverages these principles and traits in order to ensure an effective and common approach for use by designers and operators. This approach also helps to avoid costly redesign necessary to compensate for unique designs that do not efficiently interface with other NAS capabilities.

Data Architecture

The data architecture can be conceptualized in a manner that data and event “logs” are linked from the vehicle to the UAS ground control station, USS, SDSPs, or other elements in the UTM architecture. In a similar manner, the aggregation and dissemination of multiple sources of data and analyzed information enables IASMS capabilities that assure resilient and robust operations on a scalable level. The associated vehicle system monitors and their interactions are adapted from [6] and shown in Figure 7. These monitors collect data from vehicle systems and send it by downlink to the UAS Ground Station, USS, or SDSP. Weather and other data can be uplinked to the vehicle directly depending on the service used by the operator.

The architecture model highlights the vehicle systems and equipment monitors that connect with the vehicle flight system. The flight system connects with a GCS and UTM gateway that connects to USS or SDSP services. The UTM ecosystem components such as the USS and SDSPs provide services such as weather, traffic, and/or other relevant flight information that is useful on a varying scale from simple situation awareness to information that enables actionable autonomous decisions. It is also assumed that for operations in mixed airspace that demand a more structured approach to scheduled operations, a connection to a more traditional ATM will be required.

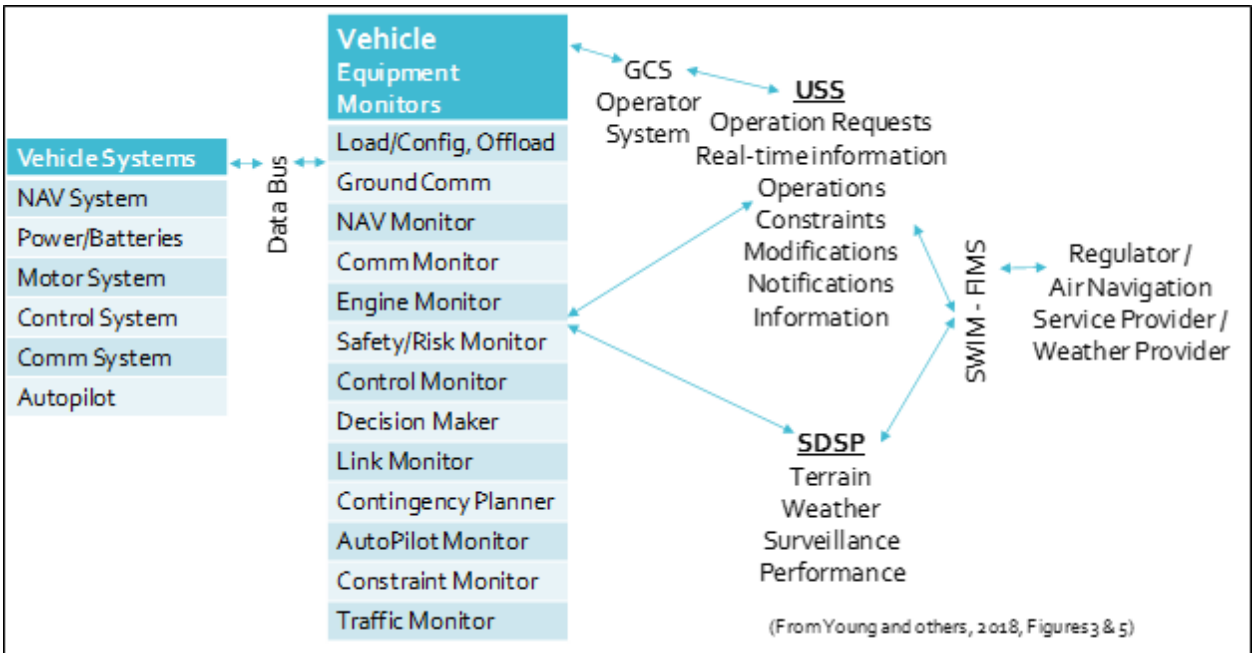

Figure 7. Vehicle equipment monitors and their interactions as adapted from [6].

Integration with Existing ConOps Architectures

Existing ATM architectures that are already in use today as well as the safety management systems that operate within that architecture provide a substantial foundation to build upon to gather valuable information and connect with emerging UTM architectures. It is envisioned that the ATM architecture currently in operation will connect with the proposed UTM architecture as proposed in the UTM Concept of Operations [5]. This leads to a UTM inspired ATM concept that IASMS capabilities and the monitor, assess, and mitigate services that drive them can operate with system-wide network services such as SWIM and FIMS.

IASMS capabilities should be tailored to address a specific risk or set of risks and therefore function within individual elements of the architecture, such as the vehicle itself, the ground control station, a USS, or other operations center. Additionally, an IASMS capability should share updated operational risk assessment information and any mitigation actions taken with pre-assigned stakeholders in the system it is operating with. These necessary stakeholders may be defined in a ConOps for a particular operation, such as UTM [5] or UAM [7] where stakeholders are identified as “responsible,” “accountable,” “consulted” or “informed.”

Depending on the operation, the vehicles and the managing USS or other operations center are expected to deploy IASMS capabilities that leverage the appropriate system elements of a given architecture, be it the existing ATM system elements, the UTM system elements, or a combination of both. This defines the notion of the UTM inspired ATM. UTM capabilities would not necessarily duplicate ATM system elements unless determined to be operationally required.

It is possible that there will be different approaches and technical models for deployment of safety assurance services. That is, it is not expected that an operator be constrained to subscribe to one predefined model for how safety assurance services are deployed. The nature of the operation would establish the requisite level of safety assurance such as in relation to the purpose or goal of the operation (e.g., transport a human passenger, medical specimen, or other cargo), operational complexity, geographic factors, or environmental constraints.

Additionally, the level of acceptable risk as defined by the governing regulatory body will prescribe the necessary responsibilities that would be addressed by an IASMS capability to reduce the operational risk for a given operation. For example, an urban operation that delivers lightweight packages has a different level of acceptable risk as opposed to an operation that is delivering a medical organ transplant. The level of operational and safety assurance of the latter operation is stricter and therefore the IASMS capabilities to achieve that level of assurance are greater. With the service-oriented architecture and variable levels of assurance afforded through variations in IASMS capability deployment, it is possible to vary the level of assurance to meet the operational objectives (including cost) and regulatory safety requirements.

Figure 8 below depicts the high-level view of interactive connections across the NAS and today's air traffic management (ATM) and its systems that support the broad spectrum of operations. The inclusion of UTM architecture elements such as USSs and SDSPs provides the data monitoring and assessment services that are required to enable the IASMS capabilities. Note that some of the services offered support both scheduled and unscheduled operations that leverage both UTM and traditional ATM architectures. This depiction of the NAS as a whole demonstrates the need for a UTM inspired ATM for growth and scalability to accommodate all traditional and emerging operations.

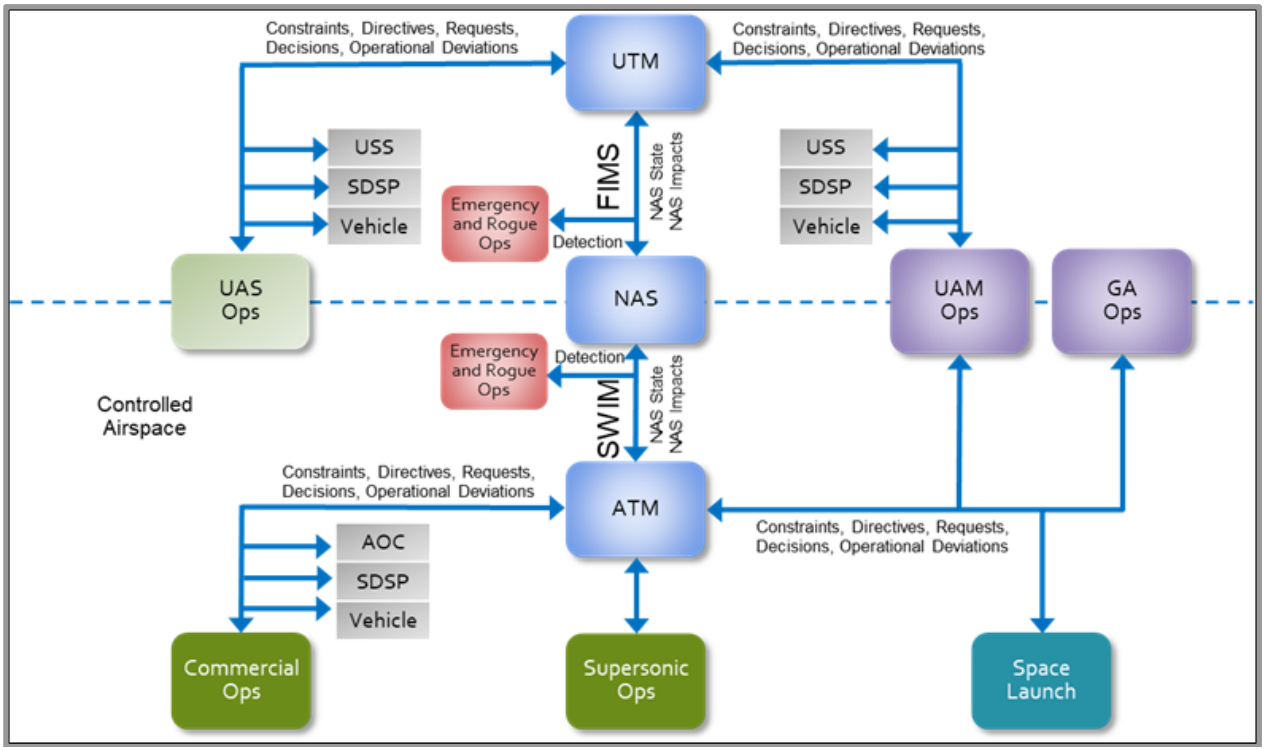

Figure 8. UTM inspired ATM for the National Airspace System

Information Requirements - Databases and Models

For the monitor and assess functions of an IASMS capability to perform properly, several databases and models are required. The design and use of databases and models represents a significant body of research and development that must be continually pursued to improve the IASMS capabilities and improve safety assurance of existing and emerging operations. The databases and models can be maintained by the USS or SDSP, and be provided as a monitor and assessment service, or it can simply be integrated into a system agent itself depending on the operation or application.

To achieve scalability in a transformed NAS, increasing levels of automation and autonomy will be required. To assure the safety of these increasingly complex operations with increasingly concentrated traffic and geo-fencing around dense populated areas, the connected databases and models that drive the IASMS capabilities that assure the functional elements of the operation must continue to improve and provide shared awareness to the relevant agents in the system.

The information requirements are defined by the services that make up a specific IASMS capability. The database or system level source provides the raw data necessary to evaluate a particular aspect of the operation. This element of the IASMS capability is performed by the Monitor function. The data can then be processed using a system monitor in a traditional sense using simple threshold monitors or could be processed using a more advanced model driven approach that evaluates the system data with a model that can identify anomalous behavior through trend analysis, a nominal behavior functional assessment, or other means that can

include advanced machine learning techniques. It is also envisioned that advanced IASMS capabilities will leverage increased levels of integrated datasets.

Monitor and assessment models provide risk probes that check on parameter values against established thresholds and provide risk warnings when thresholds are approached, alerts when affordances are exceeded, and an overall assessment of flight risk. One example would be a battery health performance model, which would provide data on its status such as power remaining, and its estimate for the amount of time remaining until power is depleted. The model could also monitor data on current, voltage, and temperature for risk assessment.

Another example would be a population density model that would support planning and operations to avoid or minimize flight over people. The model would monitor and use data from several sources including cell phone service providers on population densities across an urban landscape as well as observations of people movements via remotely controlled cameras. The model might also use geographic information system maps showing locations of public transportation stations such as bus and light rail stops where people might be expected to congregate.

Standards and Recommendations

In order to successfully develop an effective IASMS capability there is a critical need for standards and consensus recommendations from the aviation community and regulatory bodies. The standards and recommendations provide the basis for the minimum performance that should be expected for the various functional elements of an IASMS capability and provide design-to criteria. Minimum Aviation System Performance Standards (MASPS) and other recommendations and advisories (DO documents and Advisory Circulars) should be developed for safety critical IASMS capabilities and should address data quality requirements, redundancy requirements, and test and validation requirements.

Key questions are what the minimum data should be to ensure safety and how these data requirements should be determined? The Minimum Operational Performance Standards (MOPS) need to be determined for vehicles. Today the vehicle is trusted to be self-certified by the manufacturer and operator.

There are committees and organizations that are collaboratively working and developing standards and recommendations for possible use by civil aviation authorities. The ASTM International, formerly known as the American Society for Testing and Materials, is a multinational organization that develops and publishes technical standards related to materials, products, systems, and services. ASTM Committee F38 is on Unmanned Aircraft Systems and is concerned with their design, performance, quality acceptance tests, and safety monitoring. F38 works via consensus with over 130 stakeholders who include UAS manufacturers, federal agencies, design professionals, professional societies, maintenance professionals, trade associations, financial organizations, and academia. Subcommittees are responsible for active and proposed standards such as in the areas of Airworthiness, Flight Operations, and Personnel Training, Qualification and Certification.

SAE International, formerly known as the Society of Automotive Engineers, is another standards development organization. The SAE AS-4 Steering Committee on Unmanned Systems focuses on UAS design, maintenance, and in-service experience, and had 35 members in 2018. AS-4 focuses on open systems standards and architecture development with three subcommittees

addressing Architecture Framework, Network Environment, and Information Modeling and Definition.

Data Quality

Several existing special committees and groups have developed aviation standards and other guidance. These include participation by FAA, ASTM, EASA, OGC, and ARINC [19]. These entities work together collaboratively to develop these standards and recommendations to inform regulatory bodies. Besides the standards and guidance identified in [19] are the following:

- ASTM, F3178-16, Standard Practice for Operational Risk Assessment of Small Unmanned Aircraft Systems (sUAS) [24].
- ASTM, Standard Practice for Methods to Safely Bound Flight Behavior of Unmanned Aircraft Systems Containing Complex Functions [25].
- Relevant European standards and guidance

Additional Industry Considerations for Data and Architecture

In the third webinar conducted by NASA with industry on the data and architecture comprising the ISSA ConOps, discussion about these principles and traits included questions about how operators will choose and access data from different sources or services? Would there be a central service repository or service marketplace? Would the sources have to be certified? Would these services be reviewed and rated in terms of user satisfaction? Who would be responsible for the initial definition of the architecture for a minimum set of services for UAM? Is there a current assessment of services or capabilities? The operator could select which services to use and submit these as a package to the FAA.

Autonomous functions could have several traits including that these could be emergent behaviors, could be distributed across vehicles, could be non-deterministic operating with a high degree of confidence, and could be composed of human-machine teams.

Considerations regarding UTM-inspired ATM included that there is not a fixed separation between controlled and uncontrolled airspace. For example, the NAS 2045 concept has a more integrated view between ATM and UTM. It was noted that NASA's UTM-X program moves ATM into UTM as a singular concept. The diagram of UTM-inspired ATM could show services provided by USSs and SDSPs.

A comment on the notional architecture concerned the inter-connectivity between services. The UAS Ground Station could be an autonomous fleet center or constitute its own service, for example.

Regarding vehicle equipment monitors and their interactions it was noted that the UAS Ground Station could be positioned between the USS and the vehicle. It was also noted that the Ground Control Station could be a service itself. There was a comment that as more UAS operate they can themselves become a source of data such as for urban winds considering their high data rate although data accuracy may be an issue.

The USSs and SDSPs could provide data on constraints that should be monitored. This includes population density maps as well as noise maps that could show freeway routes and rivers that UASs could fly over to minimize noise.

Another SDSP service could be network availability for communications. For example, the route planning service provided by the SDSP could be done in real-time based on availability and quality of communications services. It was noted that NASA has prototyped communication service with RFI interference in UTM.

Monitoring of risk would be centrally reported but detection would be distributed to the vehicle or Ground Control Station, e.g., for monitoring an overheated engine. A question was raised about how risk information would be distributed across multiple USSs. The ISSA ConOps should address permeability of safety critical data as it is shared across different affected operators. Another question was whether backup systems are needed for redundancy to ensure safety critical data. Identifying information should be removed such as for proprietary reasons.

Modeling and databases would be used to model the number of current and projected operations such as in relation to possible saturation of the airspace and operations not being approved due to reaching a traffic density threshold. This could help to identify the best time to fly. Additional models could be added such as for noise, traffic flow, and forecast weather (e.g., local winds, Venturi effect of buildings on winds). Safety critical functions could lead to defining airspace requirements.

ISSA services can be separated into the functional categories for Monitor, Assess, and Mitigate such that each service has only one piece of a broader picture. The National Academies report took a broad integrated risk perspective to tie the services together. The challenge for NASA and the IASMS community is to ascertain which parts industry should address and the parts that NASA can do best. Industry tends to be focused on nearer term safety issues that can be addressed without releasing proprietary information. NASA may serve the industry best by developing prototypical IASMS solutions and architectures that overcome technical challenges in cutting edge operational contexts and use the information generated to develop data driven MASPS with industry bodies such as RTCA, ASTM, ICAO and others. This approach intends to provide tangible guidance to industry while providing opportunity for innovative solutions in an accessible and equitable airspace. Some services and risk monitoring could be centralized to the FAA while some could be distributed to the USSs depending on the nature of the risk.

Use Cases

Use cases are designed to illustrate the functionality of envisioned ISSA services that exemplify the Monitor, Assess, Mitigate function to reduce the risk inherent to flight operations. The use cases identified in this section are designed to be representative of real-world scenarios that will be dependent on ISSA services to provide safety assurance to the operation. Each use case highlights at least one related safety critical risk that must be addressed by a distributed network of ISSA services. Scenarios were selected to reflect traditional part 121, UAS, and UAM flight operations concepts that are envisioned to be part of the transformed and increasingly complex airspace of tomorrow. Passenger carrying UAM flight is a highly challenging environment to

operate and therefore represents the risk of a solution space we are focusing on. Other operations (such as sUAS) will necessitate a subset of ISSA required for UAM.

Use cases are designed to help illustrate the concept of operations and how its associated constructs are used. Previous research noted that UAM and urban sUAS-based use-cases can vary with complexity and boundary conditions [6]. Examples include the transport of goods/supplies, infrastructure inspection, fire department and law enforcement support, and air taxi. The transport of medical specimens from a suburban medical office to a large downtown laboratory for testing at a hospital represents a simple example to illustrate the concept of operations [6].

Use cases were also part of the FAA UTM Concept of Operations [5]. Four use cases were shown that illustrate operations in predominantly uncontrolled airspace and interactions within the UTM environment. Nine additional use cases were developed and reported by the UTM RTT [26, 27, 28]. These use cases focused on different aspects of unmanned operations showing multiple actors working together to foster shared situational awareness between Operators/RPICs, the creation and dissemination of airspace constraints that affect UAS Operators, and the types of interactions with manned aircraft.

Industry engagement events provided an important forum to test assumptions about the application of ISSA concept to low altitude urban flight. Part of the approach was to leverage existing systems and standards as feasible, and demonstrate solutions for gaps. The assumptions framing the use cases included highly autonomous flight (no pilot), ATM/Airspace functions are separate and interoperable, reliance on “connectivity” as needed, and identified hazards provide good coverage of the “waterfront” of possible issues. These assumptions mirrored past NASA research for continuity of concept development.

In addition to the above assumptions, there were additional contextual assumptions [29]. These assumptions were that a federated traffic management system (cooperative, community based) is used as an operational environment in which the operators are responsible for the coordination, execution, and management of operations within the rules of the road established by the FAA. The FAA has a small footprint because it is not providing direct services; it exchanges information on the status of airspace and can ask for information when required. IP used to share information and data, that is, there is no voice communication. Security and authentication guard against malicious activities, and law enforcement can get all necessary information about a vehicle from the USS. A certificate of trust framework means the UAS trusts that the person/entity requesting information about them from the USS is authorized to get that information.

For the purpose of the ISSA ConOps, eight use cases were identified and three were selected during the industry engagement events for in-depth review and discussion. The three selected use cases were Non-Participant UAS Operations, Vertiport emergency and closure, and Emergent Risk in Mixed Airspace. The other five use cases were Battery Health/Performance, Vehicle Lost Link—NORDO, Bird Strike—Physical Damage, USS/U4-SS Service Disruption, and IASMS Use Case Capabilities Involving Time-Based Flow Management (PBN, TBO, Sequencing & Spacing, Congestion Management).

Each Use Case that was reviewed and discussed in-depth with industry included identifying the different actors or agents who would be involved and the nature of their responsibilities or activities. In addition, the discussions identified the data elements important to the use case. These discussions noted that some considerations were not unique to a particular Use Case but rather could be generalized as relevant to the other Use Cases.

Non-Participant UAS Operations

Narrative:
A passenger-carrying UAM vehicle is transporting passengers as scheduled and approved across an urban city airspace from downtown to the local international airport. The operation occurs in urban city airspace with densely populated streets. After departure from the vertiport a passenger becomes sick and an in-flight emergency is declared for the ill passenger aboard the UAM vehicle. In response to the on-board passenger emergency, the system automatically re-routes the vehicle to deliver the passenger to the closest hospital. During the flight a military restricted airspace appears causing the system to re-route the vehicle a second time. Through an IASMS service, a Non-Participant/Rogue drone operation has been reported in the area by local authorities and civilian observation. The UAM vehicle detects the rogue drone and sends out an IASMS message confirming its presence, and the system re-routes the vehicle a third time. The UAM vehicle detects a VFR helicopter and determines it is at a higher altitude so does not need to be avoided. The UAM vehicle has information about an UAS VLOS operation present in the area with approved waivers via LAANC. The UAM vehicle approaches the hospital and is assigned a vacant landing pad on the roof, whereas if both landing pads were occupied it could land at an alternate landing zone with an ambulance transporting the passenger to the airport. This is notionally depicted in Figure 10.

Questions:

What IASMS services are needed to safely execute this scenario and return subsequent operations to normal? Where will the identified IASMS services reside?

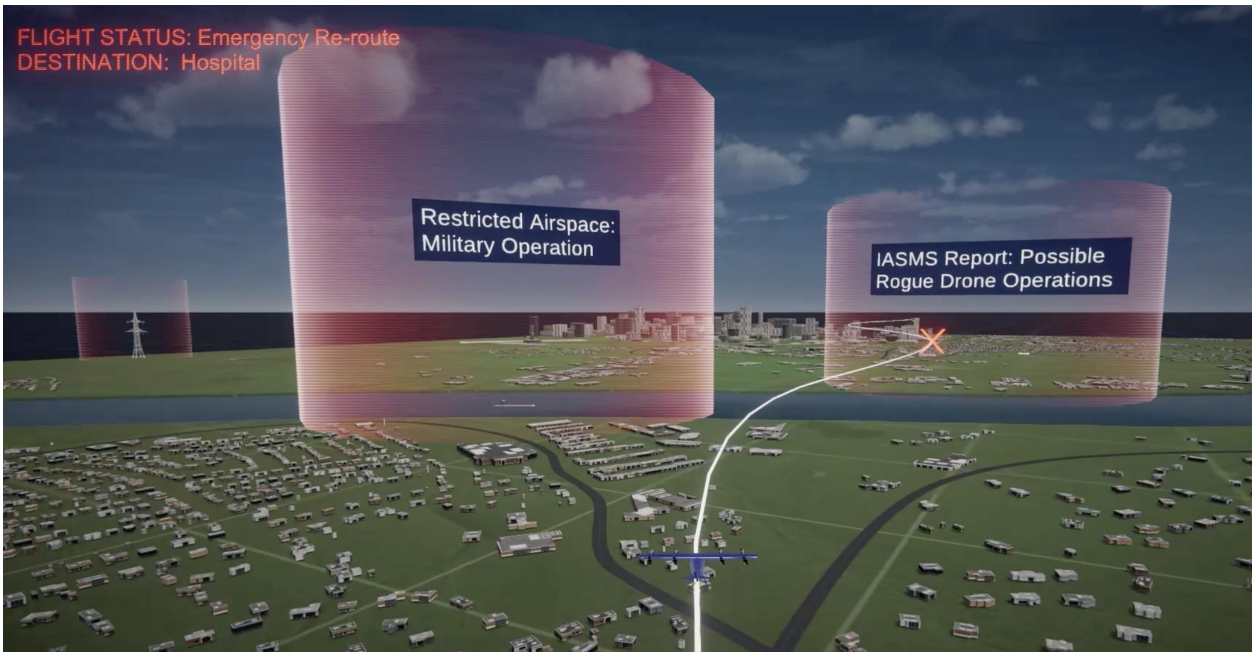

Figure 10. Non-participant UAS operation.

Responsibilities/Activities

FIMS/SWIM would provide information on the rogue drone and possible associated penalties. The USS/U4-SS would be responsible for Monitoring weather in the environment to ensure a common air picture; Assess the best reroute plan; and Mitigate risk by giving priority assignment to the vehicle carrying the distressed passenger with an update to the flight plan coordinated with other participants.

The GCS Operator would decide whether to reroute the flight such as to update flight intent or fly to the emergency landing site using detect-and-avoid for VLOS and Rogue operations.

The Vehicle Autonomous Systems would provide video and voice to the GCS. The systems would be responsible for Monitoring intention sharing, and Mitigate risk by rerouting to the best of its ability relative to energy and use of detect-and-avoid including with use of on-board camera vision.

Other Vehicles such as Rogues would face penalties or be subject to remote control of its chute deployment as feasible. The non-participant vehicle could be replaced such as a VFR low flying helicopter.

The Vertiport would be responsible for removing the vehicle from the hospital helipad (no battery charging).

Ancillary Stakeholders have responsibility for regulation such as to minimize non-participants by using a geofence around the helipad and dynamic geo-monitoring for all drones. Drones would give the right of way to the vehicle carrying the distressed passenger. In addition, there could be a passenger on board who could be designated to assist the distressed passenger. There may be an energy procedure needed to ensure flight to the landing site. The report of drone operations in the area could be friendly or not. Law enforcement would be notified of the emergency and the rogue operations.

Flow Diagram

Discussion with industry generated a flow diagram depicting the different actors/agents and the data that would be passed as part of the use case. This flow diagram is shown in Figure 11.

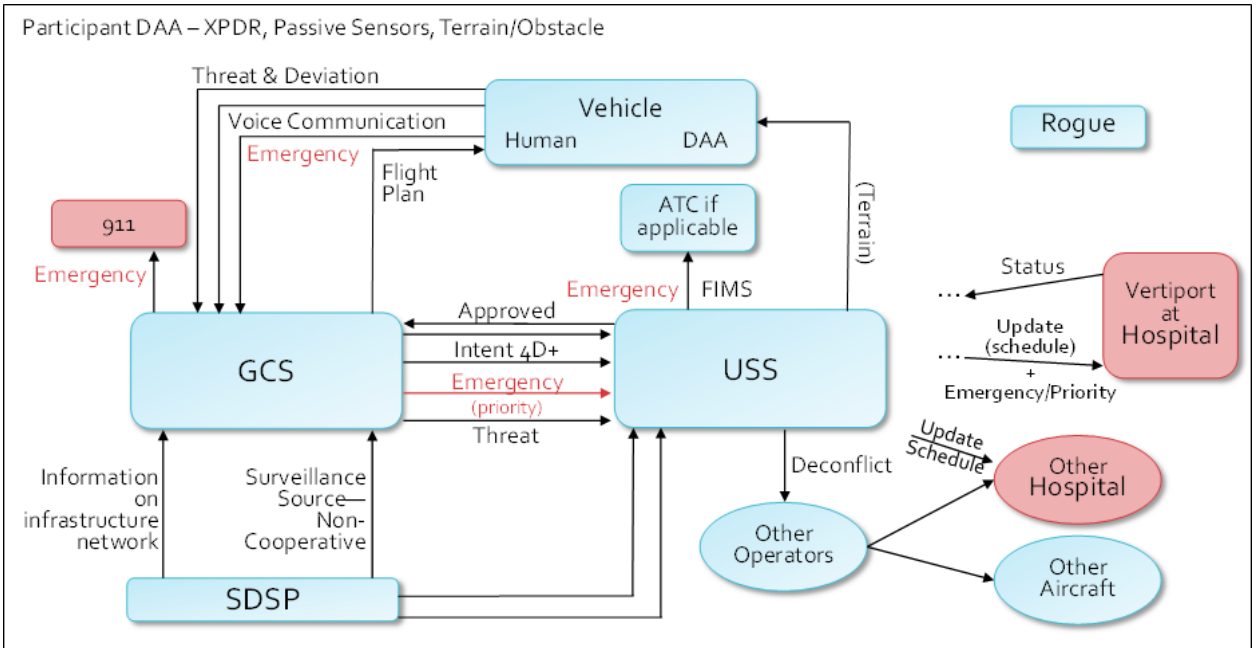

Figure 11. Non-Participant UAS Operations – Flow Diagram.

Additional Assumptions and Considerations

The use case assumes fully autonomous operations with the operator as the certificate holder for a fleet of vehicles. In addition, a bigger challenge concerns the speed for getting a patient in this Use Case to a hospital by either a ground ambulance, helicopter, or UAS. An air ambulance has to get airspace cleared before departing the pickup location. The USS would need to deconflict the airspace and do this as a planning function in advance. On the other hand, sUAS can enable more remote hospitals such as for carrying medical specimens

Vertiport emergency and closure

Narrative:

A frequently busy vertiport located centrally in an urban city surrounded by high-rise buildings and densely populated streets is experiencing a large fire due to a battery maintenance cart malfunction in the middle of the landing pad. The vertiport is a primary node in the overall urban flight operations system. The vertiport serves not only passenger carrying UAM vehicles but also as a distribution hub for package delivery service flight operations including sUAS and UAM type vehicles. In response to the fire, the vertiport is forced to cease all operations until the situation is resolved. This is notionally represented in Figure 12.

Questions:

What IASMS services are needed to safely execute this scenario and return subsequent operations to normal? Where will the identified IASMS services reside? Consider ancillary stakeholders that must also respond to this situation (i.e., local emergency services, municipality, etc).

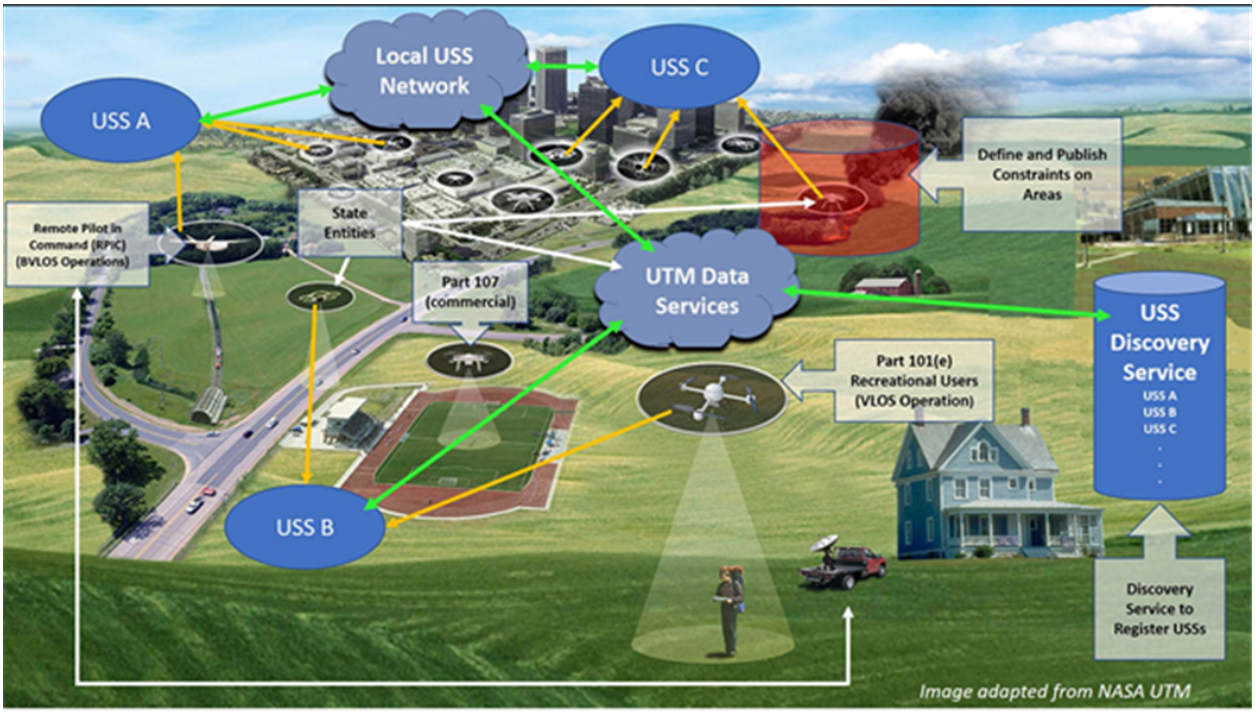

Figure 12. Vertiport emergency and closure.

Responsibilities/Activities

USS/U4-SS would provide a service to update the flight plan by determining where to land such as using a pre-planned alternate landing location. Automation could fuse data to ascertain which alternate vertiports to use depending on the types of vehicles. Reliever ports could be assessed as well as use of overnight platforms and open spaces to quickly land vehicles. Risk could be mitigated by establishing a TFR around the vertiport, managing any overload at alternate landing locations, managing airspace capacity, and prioritizing vehicle movement for energy use and availability.

The GCS Operator would assess priorities with use of alternate or emergency landing locations first for vehicles carrying people. The Operator would account for contingencies prior to the flight based on the ratio between the fleet mix and the infrastructure capable of supporting the fleet. Emergency landing sites would be assessed and prioritized. The Operator would also consider low reserves that could prevent departure if the vehicle would be unable to reach another designated vertiport.

The Vehicle Autonomous Systems will Monitor the remaining battery life/range; use its detect-and-avoid capability going to the other vertiport, and assess and mitigate risk in prioritizing emergency landing sites.

The Vertiport would be responsible for the service on communicating its availability/health to SDSPs or via FIMS/SWIM. It would assess fire severity and determine the expected reopening time. The vertiport would support assessment of the capacity of other vertiports to handle added vehicles for landing. The vertiport would know how to implement its emergency plan including fire/contingency management and the estimated return to full or partial service.

The SDSP would be responsible for fire notifications to other actors/agents and ensure the integrity of status notifications. Prognostics would be used to monitor battery health and assess wind effects on battery life.

Ancillary Stakeholders would be responsible for developing requirements for a new definition regarding fuel reserves.

Data Requirements

Discussion with industry identified candidate important data requirements for different information classes that would be passed as part of the use case. These consisted of the following:

- Vertiport Health – Battery Charging Status
    - Fire Safety Monitoring – Staff, Pad Sensors
- Contingency Management – Alternate Landing Sites: pad sensors, capacities, obstacles
- Battery Assessment Services – Life and Range/Duration – Vehicle Health Report
- Vehicle Flight Plan Contingency Planning – alternate capacities, obstacles, traffic
- Regional System Contingency Plan – alternate nodes, reduce operations – upcoming operations, alternates in range
    - Airworthiness Information – Level of Safety – vehicle sensors, LIDAR, ground obstacle detection, emergency broadcast
- New definition of fuel reserves – Battery Life Model, size of urban environment, wind conditions
- Vehicle Integrity – systems health
- Weather Modeling
- Vertiport/USS Relationship
    - Capacity Monitoring – Surveillance – flux, current, pad status, vertiport capacity, requested operations
    - Efficiency Monitoring/Assessment
    - Prioritization Services – standard, emergency, priority, intent, battery status, emergency broadcast. When a vehicle declares an emergency, its priority could depend on what priority the Operator assigns it, the vehicle equipage (e.g., how far it can still fly), and what is being carried (e.g., passenger, general delivery cargo, or a medical specimen). In addition, modeling would use different thresholds for risk identification for different services. Risk tolerance would vary for different services whether the vehicle is carrying passengers, medical specimens, or a package for delivery.

Additional Assumptions and Considerations

There could be different classes of vertiports corresponding to the different services provided. For example, one class could be for hospitals or nearby landing locations, and another class for sUAS for pizza delivery such as a designated piece of concrete along a street or driveway.

A capability would be needed to ground all UASs quickly for a system-wide emergency such as in the context of 9/11.

One important challenge is to determine risk metrics. For UAM, it has to be a community decision to determine the acceptable level of risk. A level of safety of 10-9 could be a risk level relevant to air taxis. Some in the industry say this level can be relaxed to a higher threshold due

for vehicles carrying cargo and avoiding flying over people. Research is needed to determine the appropriate level of safety for different operations.

NASA could be considered to be a SDSP providing services for a vehicle.

Another important challenge involves proprietary data and what information gets shared. Vertiports could exchange data with operators and USSs. For example, wind and vehicle performance data could be collected to establish and communicate operational safety trends. There would be industry concern with data confidentiality and the large collection of operational data such as accomplished in the ASIAS program.

It remains to be determined whether vertiports are owned and operated by municipalities. Determination is also needed for whether a vertiport controls the airspace for arrivals and departures.

There could be a difference between higher end and lower cost USSs in the services and quality provided to operators.

Emergent Risk in Mixed Airspace

Narrative:

It is the weekend following Black Friday and package delivery is at an all-time high, which has resulted in an increase in drone package delivery services as well as a substantial increase in passenger carrying operations (Both Part 121, 135 and 91 ops). The ILS at a major airport approach has gone out and is forcing operations to transition to visual or divert to a different approach. In the terminal area are also several vertiports for both package delivery and passengers traveling to/from the airport. As traffic continues to build, the burden on the airspace management system becomes strained and the risk of incident is increasingly probable. This is notionally shown in Figure 13.

Questions:

What IASMS services should be in place to detect emergent risks to all operations in the terminal area?

Figure 13. Emergent risk in mixed airspace.

Responsibilities/Activities

USS/U4-SS would provide a service to update 4D flight plans within some margin, as required. It would be responsible for Monitoring the no-fly space for drones, vehicle health status, and ILS availability. The availability of landing sites and airspace would also be monitored. Mitigation of risk could involve rerouting, metering, and flow management while providing for separation assurance. ATC could issue constraints on where the vehicle cannot fly. ATC would not provide clearance on where to land. A vehicle could be held in an area prior to arrival at the vertiport. A designated 'loiter area' could support a reservoir of pending arrivals. Air taxi demand may necessitate the use of additional vertiports that could drive change in ATC constraints. Constraints could change but have no effect on the vehicle itself. These changes could cause confusion. This could be mitigated by conformance monitoring. For example, a change in a NOTAM would have to be followed by conformance monitoring. This would be a check on all flight plans for possible non-conformance followed by determinations about what to do about vehicles that are affected. Conformance monitoring could be done as a USS or SDSP service after the NOTAM is broadcast. More air taxis would drive change in conformance monitoring. ATC could issue a NOTAM across FIMS reacting to the new airspace constraint. Alternatively, the NOTAM could be proactive if it could be anticipated that the airspace would close such as in 5 minutes. The NOTAM could be sent to all vehicles and USSs or just those affected, as appropriate. Any update to the airspace constraint could be communicated (filtered) to only the affected vehicles and USSs.

The GCS Operator would be responsible for services for different mission types and priorities, e.g., carrying passengers or goods or involvement in an emergency. The Assess responsibility could include correlation of data from different services.

The Vehicle Autonomous Systems would be responsible for Monitoring vehicle health and battery service (e.g., determining recharge or replace); for Assessing input from different sources involving data fusion; and Mitigating risk through collision avoidance.

The Vehicle Human Pilot would be responsible for coordination with ATC.

The Vertiport would be responsible for adhering to standards for equipage. It would Monitor inbound traffic, and Mitigate risk using flow management and sequencing.

The SDSP would be responsible for using the performance of vehicles to adjust the separation volume around each vehicle and account for performance of the human pilot if applicable. It would provide notification of the ILS outage to other providers and vehicles.

Ancillary Stakeholders would be responsible for determining the number of vertiports and their siting to be able to handle traffic levels. In addition, ancillary stakeholders would be responsible for safety in case a vehicle landed on a freeway. It would be involved in airspace redesign to accommodate package delivery from the ground up to 200 feet, and a transition and transit shelf between 200 to 400 feet.

There could be additional risks regarding control and communications. These include the following considerations.

- Need a procedure establishing who is in control at any one time. This includes determining how to proceed if two USSs issue contradictory information or instructions, such as involving TBFM instructions.
- The procedure for how degradation should be handled?
- The extent to which communications are ubiquitous throughout the operational area to all actors/agents and their systems. That is, the vehicle has all information all the time or at least on-demand. While all information may be available, the USS may not use or share all the information all the time.
- Information on alternate vertiports for landing could be assessed and decided upon by the USS or vehicle in response to a new NOTAM.
- NOTAMs should be part of Information Classes and Data Requirements.
- Assume sufficient quality of communications.

Data Requirements

Discussion with industry participants at workshops identified candidate important data requirements for different information classes that would be passed as part of the use case. These consisted of the following:

- Vertiport Airspace Monitoring and Assessment
    - UAS Vehicle Performance (range, resilience) – Flow Control Services (position uncertainty) – shared information – position information – cooperative, non-cooperative, additional surveillance, schedule of flights
- Not Just Airspace Separation but Landing Capacity – vertiport approach/departures contingency plan
    - Static (Flow Control Plan, vertiport structure), dynamic

    - Contingency management of all factors – landing, separation, flow, divert
- Airport Infrastructure Monitoring – ILS status, airport configuration, airspace configuration, visual approach procedures/approach plates, vertiport configuration settings
- UTM/ATC Relationships – today, tomorrow, future – ATC Information: flight delays
- What equipment/services should exist in both UTM and traditional aviation – shared information – intent information, State Status Information (UAS)
- Collision Avoidance – monitor collision avoidance for trends
- Prioritization Services – who gets landing priority, reroute priority, do operations game their prioritization?
    - Common ATC picture – Radar, ADS-B, etc.
- Conformance Monitoring
- Inbound Traffic Monitoring – schedule, ADS-B, UTM, surveillance, SWIM
- Health and Battery Services
- Performance of Aircraft to Adjust Separation – vehicle size – accounts for human factor
- Flight Plan Update with 4D Trajectory – error margin, weather information, wind direction and speed

Additional Assumptions and Considerations

A small block of airspace could possibly be assigned for UTM and converted to ATC digital instructions. These instructions could be communicated to just the one vehicle or to all vehicles, as appropriate.

A UAM corridor could be designed into Type B airspace. This could support separation between sUAS and UAM as well as with Part 91 aircraft. However, the ISSA ConOps remains generic about airspace design until there is sufficient clarity about the right balance to interactions. This depends on who will govern the airspace which depends on numerous factors. This points to the need for trade studies comparing USS operations in contrast to a centralized authority. The Use Case does not reflect sUAS operations and its constraints. For example, sUAS would have constraints over its flight path and it could fly over railroad tracks and avoid a populated stadium or school in session. sUAS can intrude from anywhere and the 400 ft altitude limits possible effective use of a parachute. This mix of constraints and operational parameters would depend on what a USS determines it can do and not do.

A rogue operation could be intentional or not intentional. The system would need to be able to detect a rogue drone and mitigate its operation. For example, the University of Michigan is looking to detect a drone upon startup but prior to its launch so that the police could intervene as appropriate. Remote ID should help with handling an unintentional rogue. A rogue operation poses a requirement for a communication link between the airport and police. Police and the regulator need to work together to provide an ATC solution to engage police with rogue operations. That is, the system needs to be able to anticipate informing the police about a rogue vehicle once the system detects and determines that a vehicle is rogue.

The approach to authorization today is only done for airspace. Additional certification requirements may be needed to handle new cases such as a vehicle used as a banner tow.

A classification system is needed to categorize different types of vehicles and types of payloads. It is understood that at least one UAS manufacturer provides the capability to optionally turn off geo-fencing. Other manufacturers have not provided this optional feature. This underscores the liability issues that are likely to grow.

For UAM the use of NOTAMs could include airspace constraints related to barriers in lower altitudes such as new construction cranes and signs. The USS could ask the vehicle/operator to report any such new barriers. A construction zone could pose a new characterization of operations besides urban/rural and nominal/off-nominal because of its dynamic nature.

Battery Health/Performance

Narrative:
A passenger carrying UAM vehicle has departed a vertiport in a densely-populated urban city with a flight plan approved to travel from the city to the airport. The flight duration from point to point is filed as a 15-minute flight. Between the vertiport and the airport is a mix of high-rise buildings, suburban housing, industrial facilities and a large river (>0.5M wide) with bridges crossing it. During cruise at the midpoint of the flight an IASMS battery health service reports the battery pack on the vehicle is overheating and is estimated to provide no greater than 5 minutes of flight time.

Questions:
What IASMS services will be required to land the vehicle as safely as possible? Who is affected and where will the envisioned IASMS services reside? What does graceful degradation look like for a vehicle affected in this way?

Vehicle Lost Link – NORDO

Narrative:
A package delivery UAS is autonomously delivering a package with a total vehicle gross weight of approximately 40 pounds. The UAS is traveling across an urban city that is densely populated with several high-rise buildings nearby and people and vehicles on the streets below. The vehicle flight plan is approved and departs the distribution center without issue. En route to the destination the vehicle loses all primary data-link connections with all remote parties, including the operator control center, USS, and SDSPs.

Questions:
What IASMS services will be required to execute a contingency plan for lost link as safely as possible? Who is affected and where will the envisioned IASMS services reside? What does graceful degradation look like for a vehicle affected in this way?

Bird Strike – Physical Damage

Narrative:
A passenger carrying UAM is taking off from a densely populated urban vertiport with several other vehicles and pedestrians traveling in both the airspace and on the ground. The vehicle is cleared to depart as scheduled within the UAM inspired ATM system. After initial ascent the vehicle encounters a critical system failure caused by bird strike. The impact results in one of the rotor/motor assemblies to become damaged affecting the nominal flight performance and control of the vehicle requiring an immediate landing of the vehicle.

Questions:

What IASMS services are needed to provide as much safety assurance as possible in this scenario? What other operations will be affected by this incident? Where will the identified IASMS services reside? What IASMS services could have been present to prevent the bird strike in the first place? What data is required to effectively monitor, assess, and mitigate the risks of bird strike (to prevent bird strike *and* if a bird strike were to occur the impact on nominal operation).

USS/U4-SS Service Disruption

Narrative:
An unplanned disruption in the services provided by one USS results in loss of data communications (e.g., loss of SWIM/FIMS data feeds, loss of power, or loss of air/ground link) with some of the U4-SS vehicles operating in an urban airspace. Another USS providing service in a partially overlapping geographic area is not affected by this disruption.

Questions:
How would an airspace operations management system allow for a graceful degradation of UAM operations in reaction to unintended disruptions to UAM services (e.g., loss of GPS, flight services, CNSI, and/or weather information; UAM Port issues; cyber security attacks).

IASMS Use Case Capabilities: Time-Based Flow Management

Narrative:

The UAM-inspired ATM system provides time-based flow management (TBFM) capability to safely minimize flight time and maximize vertiport throughput in the UAM airspace under most weather conditions. TBFM requires all U4-SS vehicles to participate including by providing flight intent and position information for all phases of flight during VLOS and BVLOS operations. TBFM requires vehicles to be equipped for performance-based navigation (PBN) that enables trajectory-based operations (TBO). Congestion management involves sequencing and spacing of arrivals to a vertiport for vehicles already en route and vehicles waiting at the departure vertiport for a departure time.

Questions:

What level of RNP accuracy is required for PBN in a UAM operational environment, e.g., would a circle with a radius of 0.05 hundredth of a NM as RNP 0.05 be sufficient (back in the 1960s would be considered half the length of a city block)?
What IASMS services will be required to execute TBFM?
Where will the envisioned IASMS services reside? What services would be necessary to ensure resilience for TBFM operations?

Summary and Plan for Updates

This report provides an industry-based ISSA ConOps as an approach to in-time safety assurance of fully autonomous UAM operations. The report responds to the National Academies top recommendation for developing a concept of operations that defines the scope and architecture of the three main system functions of monitor, assess, and mitigate while enabling scalability and accessibility for emerging operations. Vehicles, airspace, vertiports, weather and other aspects of the UAM operational environment would be monitored by sensors

and systems collecting data organized into different information classes. These data would be assessed for anomalies, precursors, and trends that together enable more proactive management of operational risks. Risks could be mitigated by the vehicle or USS such as on the bases of predetermined operations, artificial intelligence by autonomous systems, or human intervention when appropriate. The ISSA ConOps poses a distributed architecture where functions, services, and data exchange reside with vehicles, GCSs, operators, USSs, SDSPs, and FAA. UAM users work together as a federated community under regulation from the FAA.

Futurum Consilia

The next phase in the evolution of the ISSA ConOps would be accomplished through further industry engagement to integrate risk management and safety assurance for an IASMS ConOps. This could involve the use of real-world operational walk-throughs of Use Cases in the AAM ecosystem examining different functions and capabilities. Opportunities for access to real-world operational data could be assessed using different types of partnerships or agreements. This could provide important lessons and outcomes for safety assurance involving data collection and analysis as well as use of resources. Further research is needed on methods for safety assurance including use of SORA.

The ISSA ConOps establishes a conceptual foundation that builds on the National Academies recommendation to expand the traditional notion of safety assurance in the operational context (i.e., “in-time functions”) to incorporate facets of risk management. Further conceptualization is needed on defining requirements and assumptions for risk management in order to integrate hazard identification and risk management controls and evolve ISSA towards full IASMS capability.

While the ISSA ConOps is established as a high-level set of concepts that aggregate into a future-generation safety management system that acts “in-time”, the details regarding the integration of monitor, assess, and mitigate functions must consider the operational domain in which it is applied. These details may vary such as relative to Part 121 wide-body transport, Part 135 UAS drone delivery, or UAM taxi services and the other operations with which it may interact. All operations can and will have interactive effects that must be considered.

The applicability of the ISSA ConOps into the operational systems of other countries’ airspace must also be considered along with assumptions and barriers. While many systems function similarly on a conceptual level, small implementation differences may be difficult to manage when evaluating efficacy of IASMS in mixed and transitioned airspace (i.e., international operations with varying aircraft types).

Towards an IASMS ConOps

The IASMS ConOps could focus on emerging operations and span innovations in Unmanned Aircraft System (UAS) and an increasingly complex ecosystem comprised of a widening mix of vehicles and technologies, Urban Air Mobility (UAM) with industry-federated services, traditional operations, as well as new supersonic aircraft and space launch systems. The challenge for the IASMS ConOps is to be broad to encompass innovations in the coming years and decades

while agile to ensure levels of safety compatible with operational and certification requirements of the National Airspace System (NAS). Addressing these challenges provides a robust addressing of the National Academies recommendation for the IASMS ConOps.

Development and integration of the IASMS ConOps with other on-demand and air mobility concepts would facilitate identifying and defining additional IASMS risks, functions, and data and architecture capabilities. In addition, the IASMS ConOps could identify roles and responsibilities for different participants/users.

Path to Certification - Assurance of Autonomy

IASMS capabilities will need to be validated and verified in an effective way. This poses a unique challenge as the envisioned operations leverage increasingly autonomous systems that may be non-deterministic. However, there are few appropriate methods to assure such non-deterministic systems can consistently achieve a prescribed level of performance. This need highlights a substantial gap in the field of assurance of autonomy and the development of a new and effective certification path for such systems (amplify on overcoming operational barriers with use of autonomy and certification of autonomous design including for contingency management). Certification methods used for today's UAM systems should be assessed for how they might provide a path to certification of more highly autonomous systems. Considerations should be given as to how an autonomous system will be assured at the beginning of the design phase of the autonomous system.

Model and Database Development

Further research is needed on weather and wind in urban environments. Development of models related to vehicle performance should be linked to risk assessment. Adaptive Threat Management is a more proactive approach when there is an imminent threat.

It was noted that some businesses do not have data mining as part of their business model as a cost factor. This could possibly be offset by having businesses share data post-flight for subsequent aggregation and analysis. While a large business may not share its data, other smaller firms might consider selling their data. There could be different avenues for collecting data, analyzing performance, and developing models, e.g., planned demonstration or test programs by government and industry in real operational settings or laboratory simulation

References

[1] NASA, "NASA Aeronautics Strategic Implementation Plan," NASA, Washington DC, 2017.

[2] International Civil Aviation Organization, "Safety Management, Standards and Recommended Practices - Annex 19," in Convention on International Civil Aviation, 2nd Edition, 2016.

[3] National Academies of Sciences, Engineering, and Medicine, "In-Time Aviation Safety Management: Challenges and Research for an Evolving Aviation System," The National Academies Press, Washington, DC, 2018.

[4] P. Kopardekar, J. Rios, T. Prevot, M. Johnson, J. Jung and J. Robinson, "Unmanned Aircraft System Traffic Management (UTM Concept of Operations," in AIAA Aviation, Dallas, TX, 2016.

[5] Federal Aviation Administration, "Unmanned Aircraft Systems (UAS) Traffic Management (UTM) Concept of Operations v2.0," FAA, Washington, DC, 2020.

[6] S. Young, C. Quach, K. Goebel and J. Nowinski, "In-Time Safety Assurance Systems for Emerging Autonomous Flight Operations," in AIAA/IEEE Digital Avionics Systems Conference, London, UK, 2018.

[7] Deloitte, NASA, "UAM UML-4 Concept of Operations," NASA/TM-2020-000000, Washington DC, In-Press.

[8] National Academies of Sciences, Engineering, and Medicine, "Assessing the Risks of Integrating Unmanned Aircraft Systems (UAS) into the National Airspace System," The National Academies Press, Washington, DC, 2018.

[9] National Academies of Sciences, Engineering, and Medicine, "Advancing Aerial Mobility: A National Blueprint, Prepublication Copy" The National Academies Press, Washington, DC, 2020.

[10] National Transportation Safety Board, “U.S. Aviation Fatalities Increased in 2018,” NTSB News Release, 11/14/2019, last accessed on 4/16/2020 at https://www.ntsb.gov/news/press-releases/Pages/NR20191114.aspx.

[11] B. Adams, L. Bruyn, S. Houde, and P. Angelopoulos, “Trust in Automated Systems Literature Review,” DRDC Toronto No. CR-2003-096, Toronto, Canada, 2003, last access on 5/6/2020 at https://cradpdf.drdc-rddc.gc.ca/PDFS/unc17/p520342.pdf.

[12] National Institute for Standards and Technology, "Autonomy Levels for Unmanned Systems," NIST, 2019.

[13] Federal Aviation Administration (2012). Helicopter Flying Handbook. FAA-H-8083-21H, 2012.

[14] E. Ancel, J. Foster and R. Condott, "In-Time Non-Participant Casualty Risk Assessment to Support Onboard Decision Making for Autonomous Unmanned Aircraft," in AIAA Aviation, Dallas, TX, 2019.

[15] Joint Authorities for Rulemaking of Unmanned Systems, "Guidelines on Specific Operations Risk Assessment," JARUS, 2017.

[16] E. Denney, G. Pai and M. Johnson, "Towards a Rigorous Basis for Specific Operations Risk Assessment of UAS," in IEEE Digital Avionics Systems Conference, London, 2018.

[17] J. Nowinski, First Meeting of the Aviation Safety Assurance Committee, 2016.

[18] UBER, "Fast-Forwarding to a Future of On-Demand Urban Air Transportation," 2016.

[19] S. Young, E. Ancel, A. Moore, E. Dill, C. Quach, J. Foster, K. Darafsheh, K. Smalling, S. Vasquez, E. Evans, W. Okolo, M. Corbetta, J. Ossenfort, C. Kulkarni and L. Spirkovska, "Architecture and Information Requirements to Assess and Predict Flight Safety Risks During Highly Autonomous Urban Flight Operations," NASA/TM-2020-220440, Hampton, VA, 2020.

[20] RTCA, "DO-364, Minimum Aviation System Performance Standards for Aeronautical Information/Meteorological Data Link Services," RTCA, Washington DC, 2016.

[21] RTCA, "DO-200B, Standards for Processing Aeronautical Data," RTCA, Washington DC, 2015.

[22] L. Spirikovska, I. Roychoudhury, M. Daigle and K. Goebel, "Real Time Safety Monitoring: Concept for Supporting Safe Flight Operations," in AIAA Aviation, Denver, CO, 2017.

[23] J.L. Rios, I.S. Smith, P. Venkatesen, J.R. Homola, M.A. Johnson, and J.Jung, UAS Service Supplier Specifications, NASA/TM-2019-220376, Moffett Field, CA, 2019.

[24] ASTM, Standard Practice for Operational Risk Assessment of Small Unmanned Aircraft Systems (sUAS), West Conshohocken, PA: ASTM International, 2016.

[25] ASTM, Standard Practice for Methods to Safely Bound Flight Behavior of Unmanned Aircraft Systems Containing Complex Functions, West Conshohocken, PA: ASTM, 2017.

[26] Federal Aviation Administration and NASA, Cover Letter - UTM RTT CWG Concept and Use Cases Package #2, NASA, 2018.

[27] Federal Aviation Administration and NASA, Cover Letter - UTM RTT CWG Concept and Use Cases Package #2 Addendum, 2018.

[28] Federal Aviation Administration and NASA, Concept and Use Cases Package #2: Technical Capability Level 3, Version 1.0, Washington DC: FAA and NASA, 2018.

[29] S. Bradford, Conference Panelist, Cooperative Separation of Stratospheric Operations. ICAO DRONE ENABLE/3,2019.

List of Acronyms

ADS-B	Automatic Dependent Surveillance - Broadcast
AIAA	American Institute of Aeronautics and Astronautics
AIS	Aeronautical Information Services
ANSP	Air Navigation Service Provider
AOC	Airline Operations Center
AOM	Airspace Operations Management
AOSP	Airspace Operations and Safety Program
ARC	Ames Research Center
ARMD	Aeronautics Research Mission Directorate
ASAP	Aviation Safety Action Programs
ASIAS	Aviation Safety Information Analysis and Sharing
ASRS	Aviation Safety Reporting System
ATC	Air Traffic Control
ATM	Air Traffic Management
CAST	Commercial Aviation Safety Team
CNSI	Communication, Navigation, Surveillance and Information
ConOps	Concept of Operations
CPC	Certified Professional Controller
DOP	Dilution of Precision
EF	Escalation Factor
EFB	Escalation Factor Barrier
ETA	Estimated Time of Arrival
eVTOL	Electric Vertical Take-Off and Landing
FAA	Federal Aviation Administration
FIMS	Flight Information Management Systems
FOQA	Flight Operations Quality Assurance

GA	General Aviation
GAJSC	General Aviation Joint Steering Committee
GCS	Ground Control System
IASMS	In-Time Aviation Safety Management System
ICAO	International Civil Aviation Organization
ID	Identification
IM	Inertial Measurement
IMU	Interval Management Unit
INS	Inertial Navigation System
IPP	Implementation Pilot Program
ISAM	Integrated Safety Assessment Model
ISSA	In-Time System-Wide Safety Assurance
JARUS	Joint Authorities for Rulemaking of Unmanned Systems
LAANC	Low Altitude Authorization and Notification Capability
LaRC	Langley Research Center
MASPS	Minimum Aviation System Performance Standard
MOPS	Minimum Operational Performance Standard
MOR	Mandatory Occurrence Reports
MTBF	Mean Time Between Failures
NARI	NASA Aviation Research Institute
NAS	National Airspace System
NAV	Navigation
NIA	National Institute of Aerospace
NIST	National Institute for Standards and Technology
NTSB	National Transportation Safety Board
NFZ	No Fly Zone
ODM	On-Demand Mobility
OEM	Original Equipment Manufacturer

OR	Operating Range
PBN	Performance Based Navigation
PII	Personal Protected Information
PIREP	Pilot Report
PRA	Probabilistic Risk Analysis
RC	Remote Control
RFI	Radio Frequency Interference
RNP	Required Navigation Performance
RPIC	Remote Pilot In Charge
RSSI	Received Signal Strength Indicator
RTCA	Radio Technical Commission for Aeronautics
RTT	Research Transition Team
RTRA	Real-Time Risk Assessment
SAA	Special Activity Airspace
SDSP	Supplemental Data Service Provider
SDSS	Supplemental Data Service Supplier
SMS	Safety Management System
SORA	Specific Operations Risk Assessment
SUA	Special Use Airspace
sUAS	Small Unmanned Aircraft Systems
SWIM	System-Wide Information Management
SWS	System-Wide Safety
TBFM	Time-Based Flow Management
TFR	Temporary Flight Restriction
TBO	Trajectory Based Operations
U4-AOM	U4-Airspace Operations Management
U4-SS	UTM Maturity Level 4 – Service Supplier
UAM	Urban Air Mobility

UAS	Unmanned Aircraft Systems
URAF	UTM Risk Assessment Framework
USS	UAS Service Suppliers
UTM	UAS Traffic Management
VTOL	Vertical Take-Off and Landing