A Concept of Operations (ConOps) and Design Considerations for an In-time Aviation Safety Management System (IASMS) for Advanced Air Mobility (AAM)

Kyle Ellis[1], Paul Krois[2], John Koelling[1], Lawrence Prinzel[1],
Misty Davies[3], and Robert Mah[3]

1. *NASA Langley Research Center, Hampton, VA 23681*
2. *Crown Consulting Inc., Aurora, CO 80016*
3. *NASA Ames Research Center, Moffett Field, CA 94035*

The National Academies provided a vision for transformation of the future airspace system for Advanced Air Mobility (AAM) which is an In-time Aviation Safety Management System (IASMS). The IASMS integrates safety assurance, which is the foundation for In-time System-wide Safety Assurance (ISSA), with traditional risk management. The IASMS and its distributed architecture scales in relation to innovations in the Unmanned Aircraft System (UAS) and an increasingly complex AAM ecosystem comprised of an expanding mix of small UAS, air taxis, traditional operations, new supersonic aircraft, and space launch systems. Design of an IASMS builds on the In-Time System-wide Safety Assurance (ISSA) concept that mitigates risks before they can lead to an incident or accident using an architecture that integrates shared operational and IASMS-unique Services, Functions, and Capabilities (SFCs). The design of the IASMS architecture couples SFCs in both traditional and innovative ways to more effectively identify patterns in precursors, anomalies and trends and validate known-knowns, manage unknown-knowns, analyze known-unknowns, and discover unknown-unknowns that pose risk to AAM solutions.

I. Introduction

The accelerated growth of new emerging operations involving Advanced Air Mobility (AAM) necessitates development of an In-time Aviation Safety Management System (IASMS) as advocated by the National Academies [1]. In response to the top recommendation in the National Academies report, NASA developed a Concept of Operations (ConOps) for In-time System-wide Safety Assurance (ISSA) that is the foundation for the IASMS ConOps [2]. The IASMS ConOps provides an integrative approach complementing the broad vision defined by the National Academies.

This work derives from the NASA Aeronautics Research Mission Directorate (ARMD) Strategic Thrust 5 focused on ISSA. The objective is to proactively mitigate risks and demonstrate innovative solutions while ultimately ensuring safety to the community on the ground and in the National Airspace System (NAS). ISSA is enabled by three functions of Monitor, Assess, and Mitigate consisting of domain-specific safety monitoring and alerting tools, integrated predictive technologies with domain-level applications, and in-time safety threat management.

The transformed NAS involves emerging innovations in Unmanned Aircraft System (UAS) and an increasingly complex ecosystem comprised of an expanding mix of small UAS (sUAS), air taxis, traditional operations, General Aviation (GA), new supersonic aircraft, and space launch systems. This evolving aviation system improves our quality of life by moving anyone or anything, anywhere, and more quickly using a growing set of transportation options. The transformation also enables operations into applications not traditionally serviced by aviation, such as extended infrastructure inspections, emergency response, and surveillance in ways that can be safer, economical and more agile compared to today’s operations.

The challenge for the IASMS ConOps is to assimilate future innovations and remaining agile while maintaining levels of safety compatible with operational and certification requirements of the NAS. The National Academies vision and the IASMS design approach incorporate the multiple aircraft operational domains foreseen to participate in a future transformed NAS.

The purpose of the IASMS ConOps is to define a design approach to providing safety assurance and accessibility that supports integrating emerging aircraft domains into the NAS. Emerging operations involving Urban Air Mobility (UAM) pose a unique challenge to safety assurance and accessibility to the NAS. In particular, the public has a low tolerance for accidents, incidents, and risk in aviation and current NAS operations tend to be labor-intensive with limited ability to scale for operations such as UAM. In response to this landscape, NASA collaborated with industry to develop use cases and define the initial ISSA ConOps that provides a scalable distributed architecture for UAM [2].

The initial ISSA ConOps developed thus far described functional capabilities comprising safety assurances in terms of classes of information that would be monitored and assessed to identify the highest priority issues to help focus resources. The ISSA ConOps reflected collaboration with industry in development of operationally relevant use cases that showed the integration of data and leveraging automated systems to identify and more proactively manage operational risk. The IASMS ConOps expands on this by adding identification and mitigation of hazards using risk management controls and validating safety performance. IASMS does this integration across multiple aircraft domains to ensure seamless safety assurance, e.g., commercial operations, sUAS, UAM, GA, and space launch and return.

This paper describes the IASMS distributed architecture and how it provides safety assurance. The paper starts off by providing an operational view of the IASMS. A summary of the recommendations and concerns from the National Academies is then presented identifying what must be addressed to enable a safe transformed NAS. The structure of IASMS in the context of the overall Safety Management System (SMS) framework is then described. This is followed by outlining the IASMS safety functions of Monitor, Assess, and Mitigate and describing the IASMS architecture along with factors that determine its complexity. Lastly, conclusions and further work are discussed.

II. IASMS Operational View

The AAM ecosystem provides transportation that is on-demand, fast, affordable, and safe. Users work collaboratively to manage operational risks with a federated architecture. The risks, complexities, and constraints of operations that must be addressed in the architecture are shown as an operational view in Figure 1.

The IASMS is designed to mitigate undesirable outcomes. It checks the route of flight to prevent unsafe proximity to air traffic, people on the ground, and property including obstructions. Automated systems mitigate possible flight outside of approved airspace. These systems also mitigate the potential for possible hull loss for vehicles carrying passengers, precious cargo or having high kinetic energy.

The IASMS is based on requirements that reduce or eliminate causal factors. Requirements address the handling of critical system failures including loss of link, loss or degraded positioning system performance, loss of power, and engine failure. Loss-of-control risk due to envelope excursions or flight control system failure is mitigated. Mitigation of risk also involves the physical environment and weather encounters such as wind gusts. Safety risks ensuing from cybersecurity infractions and malicious threats by people on the ground are also included as part of the IASMS design requirements.

The high-priority safety risks shown in the IASMS Operational View are paired with corresponding example SFCs and mitigations in Table 1.

Safety risks can emerge from patterns in precursors, anomalies, and trends. These risks may appear as validated concerns known to designers and operators and known to be detected and mitigated by safety assurance SFCs (i.e., known-knowns). Emergent risks may be unknown to designers and operators (e.g., an unexpected and surprising situation) but SFCs could understand, adapt, and manage them through machine learning or artificial intelligence (i.e., unknown-knowns). Other risks could be recognized by designers or operators even though these are outside the envelope for safety assurance SFCs to detect and mitigate them (known-unknowns). Lastly, there could be unforeseen risks that are not recognizable by designers or operators or by safety assurance SFCs and await discovery (unknown-unknowns). In application, an SFC designed to manage unknown-known risk such as GPS Degradation Modeling involves the SFC actively monitoring the quality of the GPS signal and reporting.

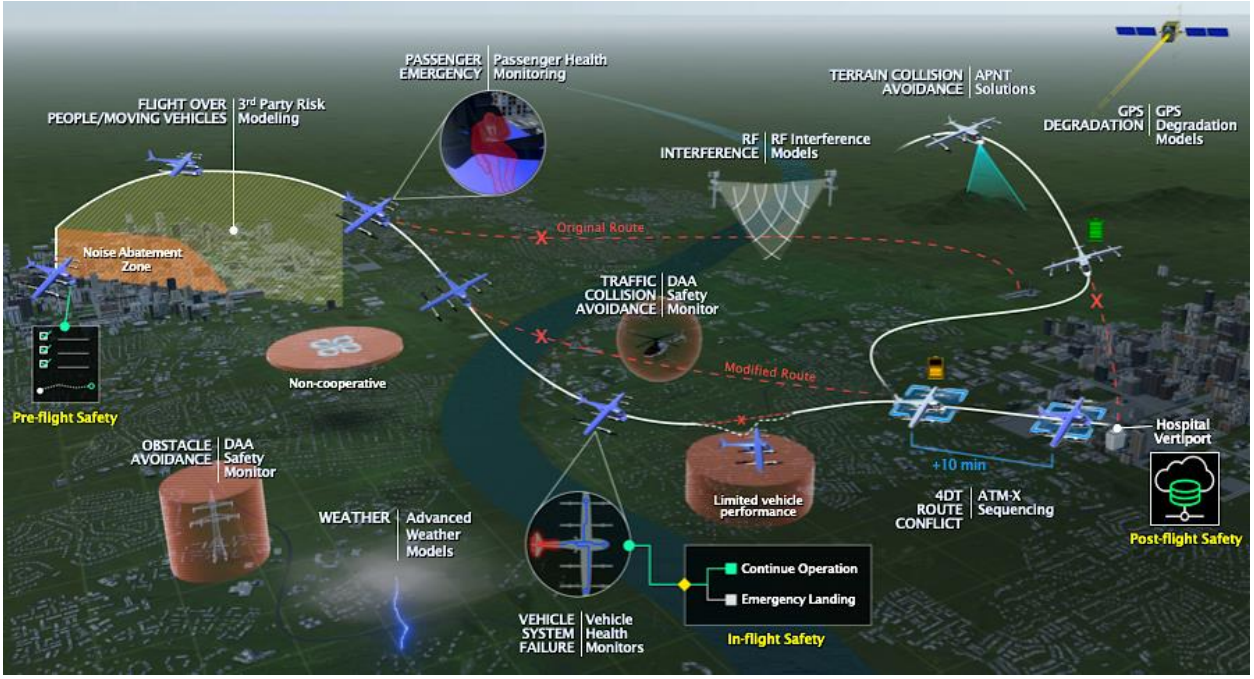
PASSENGER EMERGENCY | Passenger Health Monitoring
FLIGHT OVER PEOPLE/MOVING VEHICLES | 3rd Party Risk Modeling
TERRAIN COLLISION AVOIDANCE | APNT Solutions
RF INTERFERENCE | RF Interference Models
GPS DEGRADATION | GPS Degradation Models
Noise Abatement Zone
Original Route
TRAFFIC COLLISION AVOIDANCE | DAA Safety Monitor
Modified Route
Non-cooperative
Pre-flight Safety
OBSTACLE AVOIDANCE | DAA Safety Monitor
Hospital Vertiport
+10 min
Limited vehicle performance
4DT ROUTE CONFLICT | ATM-X Sequencing
Post-flight Safety
WEATHER | Advanced Weather Models
Continue Operation
Emergency Landing
In-flight Safety
VEHICLE SYSTEM FAILURE | Vehicle Health Monitors

Fig. 1 IASMS Operational View.

Risks	Example SFCs	Risk Mitigations
Flight Over People/ Moving Vehicles	3rd Party Risk Modeling	Vehicle maintains safe lateral distance around people and moving vehicles as established in its flight plan or as information is updated during flight, e.g., changes to route of flight or 3rd party risk assessment.
Obstacle Avoidance	DAA Safety Monitor	Flight plan accounts for known obstacles as specified on aeronautical charts and maps, and other geographic information products to ensure safe lateral and vertical distances. DAA systems monitor planned operational trajectory to detect unanticipated obstacles to be avoided.
Weather	Advanced Weather Models	Flight plan checked before departure for current and forecast weather including temperature, wind direction, strength and gust, convective weather, precipitation, and icing. Microweather forecasting for urban flight planning. Pilot weather reports used to update flight plan.
RF Interference	RF Interference Models	Operational systems monitor and assess RF interference for disrupting communications.
GPS Degradation	GPS Degradation Models	Operational systems monitor and assess RF interference for disrupting communications.
Vehicle System Failure	Vehicle Health Monitors	Vehicle health monitoring systems continuously assess performance of on-board operational systems, e.g., battery power and motor performance.
Traffic Collision Avoidance	DAA Safety Monitor	An on-board real-time operational system provides detect-and-avoid warning, determines maneuvers away from other airborne vehicles, and executes these maneuvers while communicating with other vehicles and USS/PSU/ANSP.
Terrain Collision Avoidance	APNT Solutions	An on-board real-time operational system provides detect-and-avoid warning and maneuvering away from terrain to avoid controlled-flight-into-terrain (CFIT).
Route Conflict	ATM-X Sequencing and Spacing	On-board and/or ground-based operational systems provide safe sequencing and spacing between flights going to the same destination vertiport/airport, as well as separation between vehicles having crossing trajectories including during climb/descent.

Table 1. IASMS Sample Set of Risks, SFCs, and Mitigations.

III. National Academies Safety Recommendations

The National Academies report provided a vision for an IASMS [1]. This vision posited 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 National Academies IASMS report noted that the NAS continually grows in complexity with the increase in commercial flights, modernization of air traffic control (ATC) systems, use of sophisticated flight deck automation, use of autonomous systems for aircraft and ground systems, and increasing prevalence of UAS.

The IASMS would assess data according to relevant parameters of time (i.e., second-by-second, minute-by-minute, or hour-by-hour, as required) to detect and predict elevated risk states especially those based on rapid changes in system status. Alternatively, data could be assessed over periods of days, weeks, or months to detect risks based on longer-term trends.

As part of their top recommendation for NASA to develop a ConOps and risk prioritization, the report described the IASMS functions of Monitor, Assess, and Mitigate to anticipate and detect anomalies, precursors and trends that can be predicted to lead to elevated risk states. Such trends can emerge from a confluence of factors, none of which by itself would be noteworthy, e.g., might be missed as a weak signal. The IASMS would continuously assess data through the lens of a thorough understanding of the nominal performance of systems and operators, tempered by historical data regarding both the occurrence and consequences of off-nominal situations, and calibrated by the fault tolerance of the NAS and its key elements. Over time, outputs from the IASMS could identify emergent risks that in some cases should be added to the list of risks managed primarily through design of automated systems or during operations, as appropriate.

The National Academies developed a national blueprint for AAM that emphasized the assurance of system safety by building safety into the system from the beginning of development [3]. Traditional hazard analysis and safety engineering modeling and analysis techniques were found insufficient to ensure safety in complex, software-intensive systems like UAM. The report indicated there needs to be a way of validating that software requirements ensure a safe system.

IV. IASMS in the Overall SMS Framework

The traditional framework of a SMS established by the International Civil Aviation Organization (ICAO) is shown in Figure 1 [4]. The two pillars involved with the IASMS are Risk Management and Safety Assurance. The initial ISSA ConOps focused on the scope, functionality, and risk priorities of the UAM domain with relevant use cases developed with industry input and built on a service-oriented architecture of UTM. The IASMS ConOps integrates Safety Assurance and Risk Management that together identify and mitigate emergent risks and hazards much more rapidly in-time than today, using less labor, and able to scale for increased complexity.

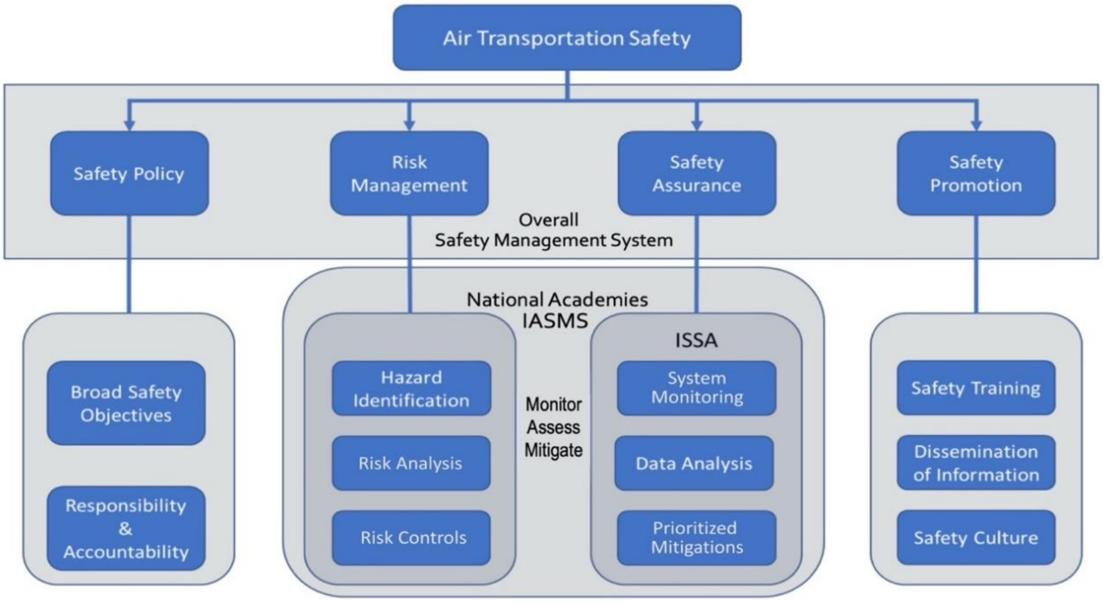

Fig. 2 SMS Framework for IASMS and ISSA.

The SMS framework contained in the Federal Aviation Administration (FAA) Advisory Circular 120-92B is shown in Figure 3 [5]. The approach integrates the processes for risk management and safety assurance [6]. Risk management involves early identification of hazards and ensuring controls are designed to manage hazards at an acceptable level. Safety assurance monitors how controls are used operationally and continues to mitigate risk as intended.

The IASMS ConOps poses that Risk Management and Safety Assurance functions need to merge together to more rapidly identify emergent risks and hazards and mitigate them by alerting the human operator to take action or directly mitigate the risk using automated systems much more quickly than today. That is, in some cases, when urgent action is required, the IASMS may be designed to initiate safety assurance actions on its own.

The IASMS accomplishes the Risk Management and Safety Assurance functions through an architecture that integrates shared operational and IASMS-unique SFCs. These SFCs perform in an integrated manner the 6 key elements of Risk Management and Safety Assurance. Increased use of automated and autonomous systems may reduce levels of human interaction and dramatically increased responsiveness (In-Time), particularly so when handling larger scales of operations and data.

In addition, the IASMS through the SMS framework informs safety policy with operational and performance data and understanding for improvements to safety objectives as well as ensuring responsibility and accountability. The IASMS also informs safety promotion for improvements to safety training, dissemination of safety information, and promoting the safety culture.

The monitoring, assessment, and response time of an IASMS can range from seconds to minutes such as for Detect-and-Avoid, to a longer period of time such as weeks to months or longer for mining of anomalous trends in post-flight safety databases such as is currently done with the Flight Operations Quality Assurance (FOQA) program. In addition, pre-flight safety assurance action may include a decision to postpone or cancel a flight until, for example, weather conditions change, or equipment is repaired. Longer time frames using data from IASMS services may have implications to changes such as in pilot training programs, flight 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.

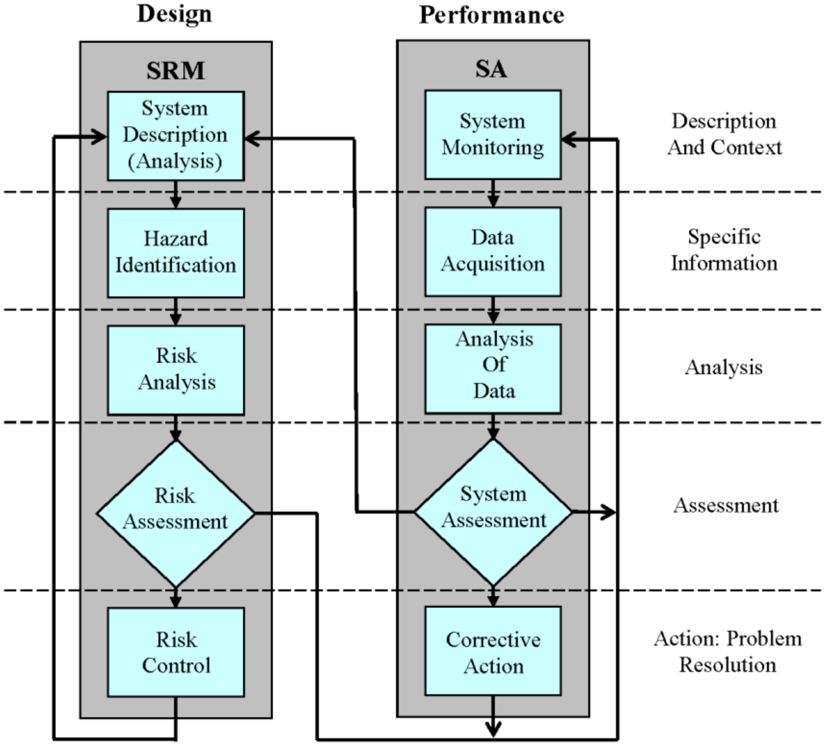

Fig. 3 FAA SMS Framework for Part 121 Air Carriers (from AC 120-92B, Figure 2.1).

Incorporating safety in the design and operation of a complex AAM system involves multiple considerations representing a layered approach [7]. Safety is positioned as a cross-cutting factor spanning the five pillars of NASA's UAM concept that are Airspace and Fleet Operations Management, Airspace System Design and Implementation, Aircraft Development and Production, Individual Aircraft Management and Operations, and Community Integration, Considerations include that there would be more exacting safety requirements for passenger-carrying missions compared to cargo transport, ensuring safety through design and operation of aerodrome takeoff and landing areas/pads and ground services, and the balance of roles and responsibilities between human operators and automated systems including for safety-critical services and functions.

The Specific Operations Risk Assessment (SORA) was developed by the Joint Authorities for Rulemaking of Unmanned Systems (JARUS) to model risk with unmanned airborne mobility [8, 9]. At a higher level, SORA uses risk modeling to assess risk (harms) and their mitigations (barriers). Research poses that SORA could be used to measure qualitative assumptions by which risk under uncertainty can be more carefully examined [10].

An incident or accident can occur when a hazard or error occurs that penetrates across all the relevant safeguards, such as in an adaptation of the notional Swiss Cheese model [11]. The safeguards are designed and implemented based on an assessment of known-knowns and can by extension mitigate known-unknowns and unknown-knowns. It could be hypothesized that the safeguards are sufficiently comprehensive and robust to be able to identify and mitigate risks considered to be unknown-unknowns.

An analysis of known-knowns and known-unknowns for sUAS was based on assessment of current hazards shown in sUAS mishaps and extension to future hazards through analysis of sUAS use cases [12]. Known-unknowns were reflected in categories of future hazards such as multi-UAS operations.

V. Design of SFCs

The ability of the NAS to use data to monitor its system state, to assess and identify an elevated risk state, and to mitigate risk through safety assurance action is predicated on design of SFCs. SFCs take data from requisite sources and fuse that data to feed into the Monitor-Assess-Mitigate functions.

A Service involves a system providing information or data to a user who subscribes to that service. Services use data collected from infrastructure elements as well as vehicles operating in the airspace. Services important to risk management include Non-Participant Casualty Risk Assessment (NPCRA), Proximity to Threats (PtT), Battery Prognostics (BP), radio frequency emitters and interference (RFE/RFI), and weather/wind data and forecasts. A Function is a process or action that integrates streams of information and data. On-board vehicle functions can include autopilot, communications, and navigation. A Capability uses technology including sensors and models that detect, generate, validate, and distribute information and data for use by Functions and Services. Capabilities important to risk management on-board the vehicle could include link monitor, constraint monitor, trajectory prediction, and contingency planner.

The IASMS architecture design couples SFCs together in ways to validate known-knowns, uncover known-unknowns, and discover unknown-unknowns that pose risk to AAM solutions. Use of traditional SMS methods and data are used to sustain today's safety target. Innovations in technology and models can lead to new approaches to assessing data with machine learning and artificial intelligence that can lead to identifying emergent risks. These traditional and innovative methods intend to maintain the margin of safety through both proactive and reactive approaches.

The IASMS through the SFCs can quickly manage known risks, quickly identify unknown risks, and quickly inform that system design changes are needed. These risks include flight outside of approved airspace; unsafety proximity to air traffic, people on the ground, terrain, or property; critical system failures including loss of link, loss or degraded positioning system performance, loss of power, flight control failure and engine failure; loss-of-control as envelope excursions; environmental and physical risks such as weather encounters (e.g., wind gusts) and malicious threats; and, cyber security risks.

There could be additional risks that the predictive and prognostic SFCs have not yet identified. As the complexity of automated systems increases, the SFCs could identify unknown risks, inform system designers about these risks for mitigations such as changes to requirements and specifications of automated systems, and increase the effectiveness of human operators to manage operational risks such as through improved procedures and training.

The IASMS leverages the array of open data sources in the NAS. This open architecture incorporates current data bases and compels development of new data sources as the architecture evolves and expands in complexity. Data could be sourced from the vehicle, airspace, Supplemental Data Service Suppliers (SDSP), System-Wide Information Management (SWIM)/Flight Information Management System (FIMS), and other sources. Sixteen information classes were identified involving specific types of data, shown below in Figure 4 [13]

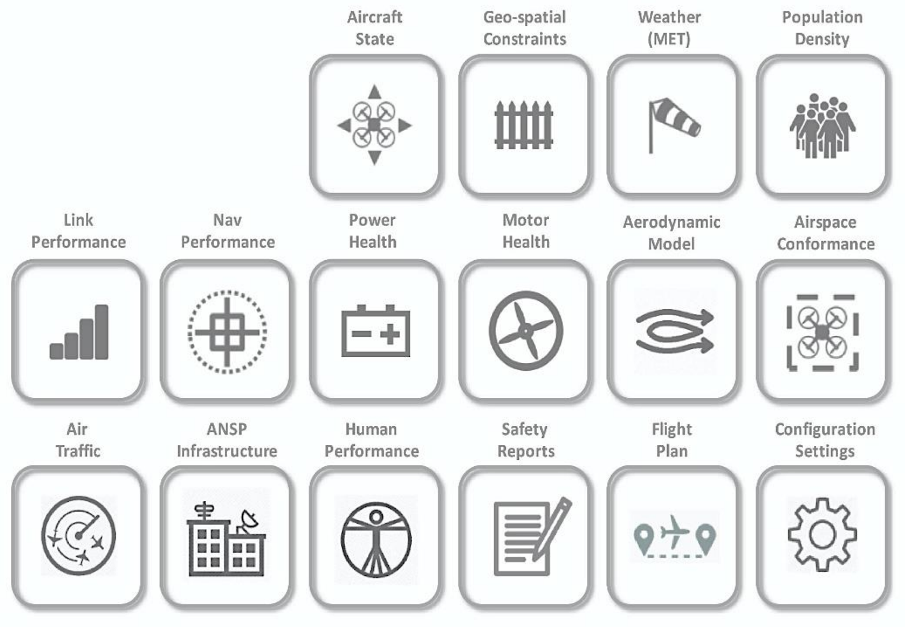

Fig 4. IASMS Information Classes [13]

The IASMS would evolve as the AAM architecture scales so that the IASMS functions assimilate cross-domain SFCs. That is, interoperability of SFCs between domains would grow in importance relative to providing fast, seamless, and safe transitioning of operations in different types of airspace (e.g., mixed AAM and traditional operations, and mixed operations of different AAM vehicles).

Data quality considerations include availability, latency, update rates, integrity, security, formats, implementation and service costs, bandwidth utilization, and standards. Standards, principles and overarching traits are pertinent to the development of the data architecture required for the design of the SFCs. These principles and traits reflect best practices from software engineering as applied to aviation and include use of a building block approach that is service-oriented and scalable. The architecture should be open and extendible to address new risks or hazards as/if they are discovered, leverage and interoperate with existing relevant systems (e.g., system-wide information management and air navigation service supplier services), and transformative from the existing NAS such that it does not involve a clean-slate design approach. The American National Standards Institute (ANSI) reviewed existing standards and standards in development, identified gaps and issue areas including research needs, and developed recommendations regarding airworthiness, flight operations, and personnel training, qualifications, and certification [14].

Assurance of an IASMS and its sub-systems is critical to meet the target level of safety for an envisioned operation. SORA represents an approach to identify the risks to an operation and qualitatively outline the requisite assurance at both the component and system-level to satisfactorily build the safety case for a particular operation. Each identified risk to an operation would be addressed by one or several SFCs and each SFC must be assured through an appropriate process based on an accepted risk assessment, such as SORA [10].

VI. IASMS Safety Functions

The Monitor, Assess, and Mitigate functions are linked with Services and Capabilities. In the architecture the SFCs are distributed across vehicles, airspace, and SDSPs. SFCs are individual services, functions or capabilities that, in terms of safety, are foundational building blocks that target an individual risk or family of risks. A set of coordinated and collaborative safety SFCs make up an IASMS. One can imagine an IASMS that is relatively simple and rudimentary or very complex and capable.

A. Monitor Function

IASMS capabilities will 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 the expected and/or nominal state. To achieve this, multiple sets of data will be monitored, and the analysis of that data will generate key assessments of known hazards as well as emergent, unknown hazards that threaten operational safety. The IASMS capability would monitor its state to detect anomalies, precursors, and trends as the leading indicators.

The Monitor function collects data and checks its quality before it undergoes data fusion. Data would be distributed across the architecture through services that are subscribed to by users. Data sources would include operational vehicles and their flight plans, as well as safety data bases that would check current performance data with nominal performance profiles.

The Monitor function would provide data to predictive models addressing each safety critical risk. These models could operate at different update rates, data resolutions and 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 (GCS), the UAS Service Supplier (USS), or SDSP. These model services include aircraft state information and aerodynamic models, aircraft trajectory data, positioning system state information, and performance model (i.e., what the UAS is doing in terms of flight performance). The model services also include population density information, vehicle system health, aeronautical information services, and communications system state information.

Key factors regarding the collection of data from each information source include availability of data originating from the vehicle and its systems as well as data from performance models, latency of data, and accuracy of data collected from different sources. The data lags, different resolutions of data, and other variations in key parameters can limit data correlation and fusion. Moreover, the update rates can be synchronous and asynchronous between information classes. Other important factors are the integrity of data from NAS communications, navigation, and surveillance networks, security of data (i.e., issues unique to 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), and formats of data from the heterogeneous sources (the differences can constrain data correlation and synthesis of data with timing and other characteristics).

In addition, 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. The implementation and service costs are important to the business case for the IASMS. It is important to evaluate 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. Another important factor is spectrum regulation and bandwidth utilization to provide sufficient bandwidth for data services considering the update rates, latencies, and resolutions of data from multiple sources.

B. Assess 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, the USS/Provider of Services for UAM (PSU)/Air Navigation Service Provider (ANSP), and/or even at the overall FIMS/SWIM level. Outputs from the Assess function may focus on an individual risk or family of risks or may be integrated into an overall IASMS risk assessment. The Assess function relies on prognostics and prediction.

The Assess function could model flight plan data and assess real-time operational data to ensure safety of flight. Innovations in data mining techniques could be applied to archival safety data bases to improve detection of leading indicators and other weak signals related to safety issues.

Models built on complex algorithms could apply machine learning to safety data to improve predictive accuracy. The IASMS uses data mining techniques for pinpoint risk analysis as well as safety trend analysis. Design elements of the IASMS can be used to identify improvements to the performance of safety models, which could occur over a longer time span to validate these improvements. Decision techniques such as deep neural networks and fuzzy logic could be used to minimize false positives involving predicted airspace conflicts.

The Assess function and its sub-functions and their models can scale within each domain 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).

C. Mitigate Function

The Mitigate function can take time-dependent action triggered automatically based on decision criteria and required performance thresholds. The function could also alternatively be based on operational procedures, and possibly augmented with a decision support tool as an assistive agent for the human operator.

The Mitigate function would be designed to resolve either current or impending operational situations that exceed a defined safety threshold. A key challenge will be defining roles and responsibilities between human(s) and machine for the distribution of authority and autonomy [15]. 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.

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.

As a feedback loop, the monitoring and assessment functions ultimately determine how well mitigation can occur for any safety-adverse situation that develops. There could be a provision that the mitigation would change in-flight such as to adjust the course in order to maintain a safety buffer with a rogue vehicle and report the location of the rogue vehicle to the IASMS system at-large.

VII. IASMS Architecture

The current FAA UTM architecture is shown in Figure 5 [16]. The figure has been adapted to show that the Monitor, Assess, and Mitigate functions can be distributed across SDSPs, GCS functions, and vehicle system functions. The Monitor, Assess, and Mitigate functions could also directly reside with the USS systems.

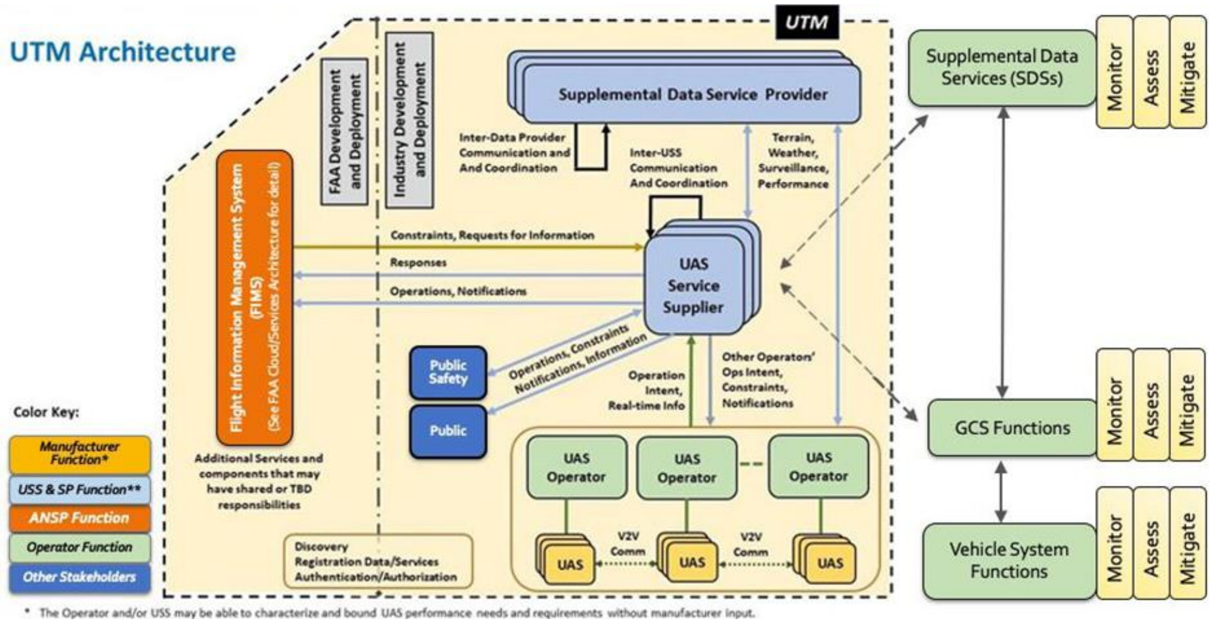
UTM Architecture
UTM
FAA Development and Deployment
Industry Development and Deployment
Supplemental Data Service Provider
Inter-Data Provider Communication and And Coordination
Inter-USS Communication And Coordination
Terrain, Weather, Surveillance, Performance
Flight Information Management System (FIMS)
(See FAA Cloud/Services Architecture for detail)
Constraints, Requests for Information
Responses
Operations, Notifications
UAS Service Supplier
Public Safety
Public
Operations, Constraints Notifications, Information
Operation Intent, Real-time Info
Other Operators' Ops Intent, Constraints, Notifications
Additional Services and components that may have shared or TBD responsibilities
Discovery
Registration Data/Services
Authentication/Authorization
UAS Operator
UAS Operator
UAS Operator
UAS
UAS
UAS
V2V Comm
V2V Comm
Color Key:
Manufacturer Function*
USS & SP Function**
ANSP Function
Operator Function
Other Stakeholders
Supplemental Data Services (SDSs)
GCS Functions
Vehicle System Functions
Monitor
Assess
Mitigate
Monitor
Assess
Mitigate
Monitor
Assess
Mitigate
* The Operator and/or USS may be able to characterize and bound UAS performance needs and requirements without manufacturer input.

Fig 5. UTM Architecture (adapted from [16]).

In-time safety management can be approached as a system-of-systems for which the National Academies posited an architecture having the three key functions of Monitor, Assess, and Mitigate (M-A-M). This architecture is shown in Figure 6. The high-level architecture defines what has to be done and the ConOps provides a framework for how the architecture will work. On the bases of this architecture, the NAS is continuously monitored for risk through the assessment of data that it has collected, and then, as necessary, designated risk mitigation actions are either recommended or initiated. These actions are monitored and assessed to ensure the intended outcome is achieved.

The IASMS will live across all agent entities in the system and these entities will need to interconnect all Operators, Operations Centers, Service Suppliers, SDSPs, and so forth. The challenge is that all entities will need to speak the same language, have shared expectations, and exchange their operational data to the extent possible relative to any proprietary limitations.

Below the level of the IASMS, an ISSA Capability at its lowest level represents a system that monitors data, assesses data, and performs or informs a mitigating action for a particular risk or family of related risks. An IASMS consists of interconnected ISSA capabilities that together provide an integrated approach to in-time risk management and safety assurance. ISSA capabilities are shown in Figure 7.

The classes of data underlying the architecture provide status on quantitative parameters important to control and ensuring the safety of flight [13]. These classes represent the different types of vehicle, airspace, UAM/UTM/ATC ecosystem, safety reports, and configuration settings as information important to safety assurance. A risk that emerges during life cycle phases of design-time or operations-time explains why a service needs to be provided by the vehicle, USS, operator, or another actor in the architecture. For example, vehicle information can be decomposed to lower levels as aircraft state and include position (latitude, longitude, altitude), attitude (pitch, roll, yaw), heading, track, airspeed, groundspeed, vertical speed, auto-pilot mode, and acceleration. These information classes either singularly or in combination can be used to generate an ISSA capability.

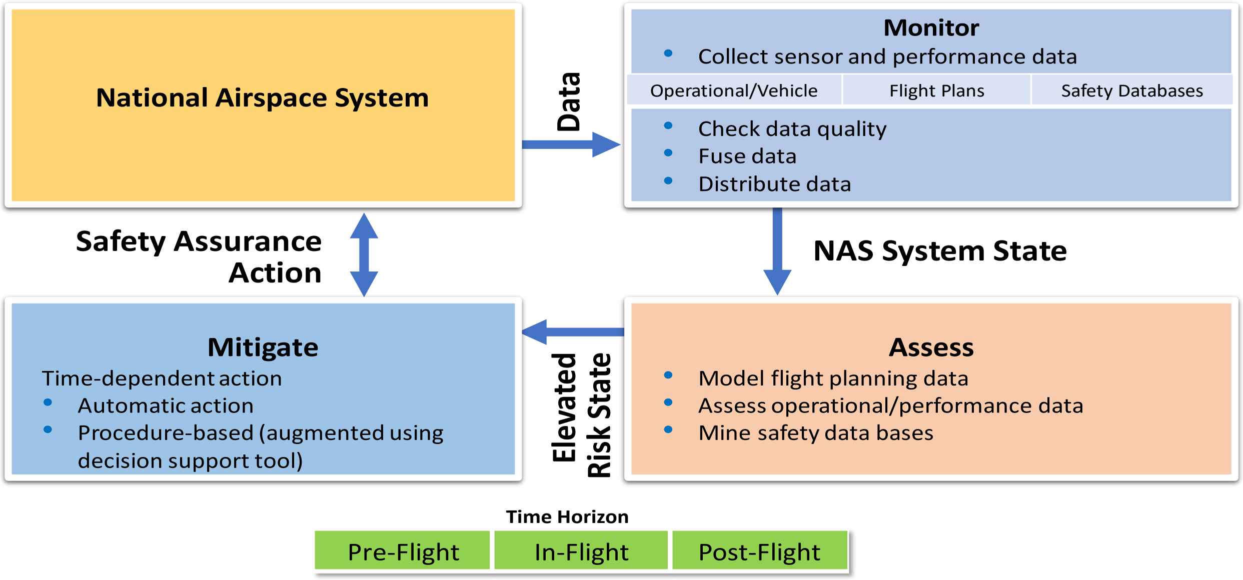

Fig. 6 IASMS High-Level Architecture.

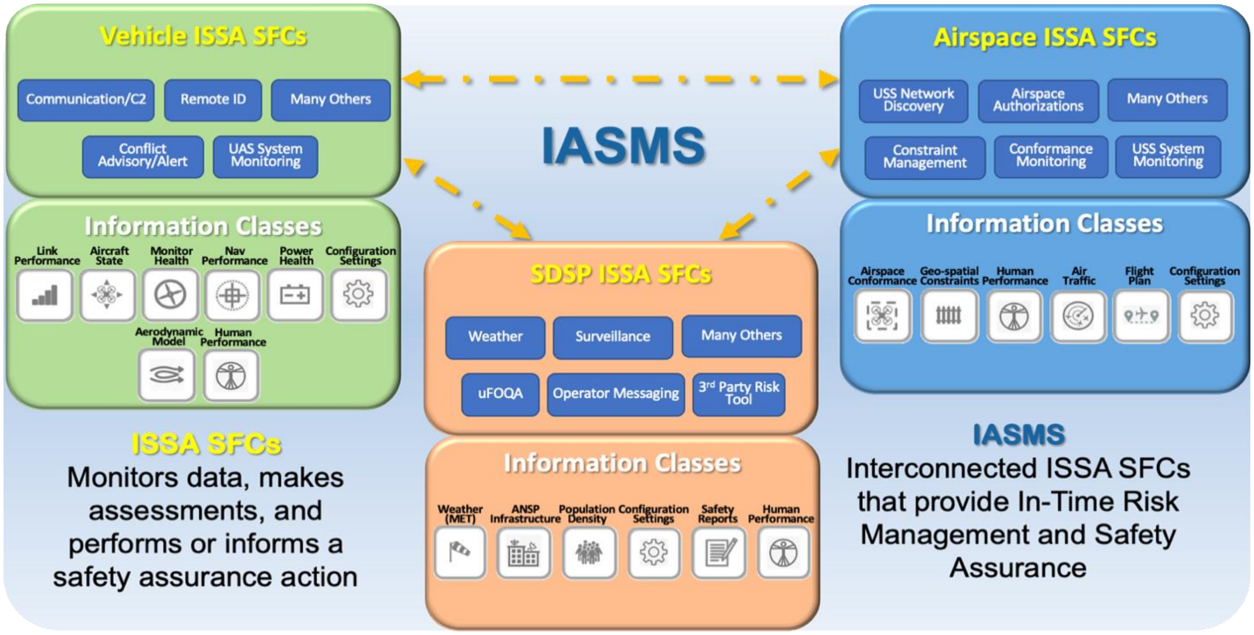

Fig. 7 IASMS Comprised of ISSA Capabilities.

The IASMS high-level architecture is embedded in the AAM ecosystem architecture that is the mainstay for all operational domains. As shown in Figure 8, the IASMS connects across different operational systems and operators in the AAM ecosystem architecture based on the suite of SFCs. As shown at the sides of the figure, SFCs are either operational or IASMS in nature. SFCs provided by the SDSPs are also either operational or IASMS in nature.

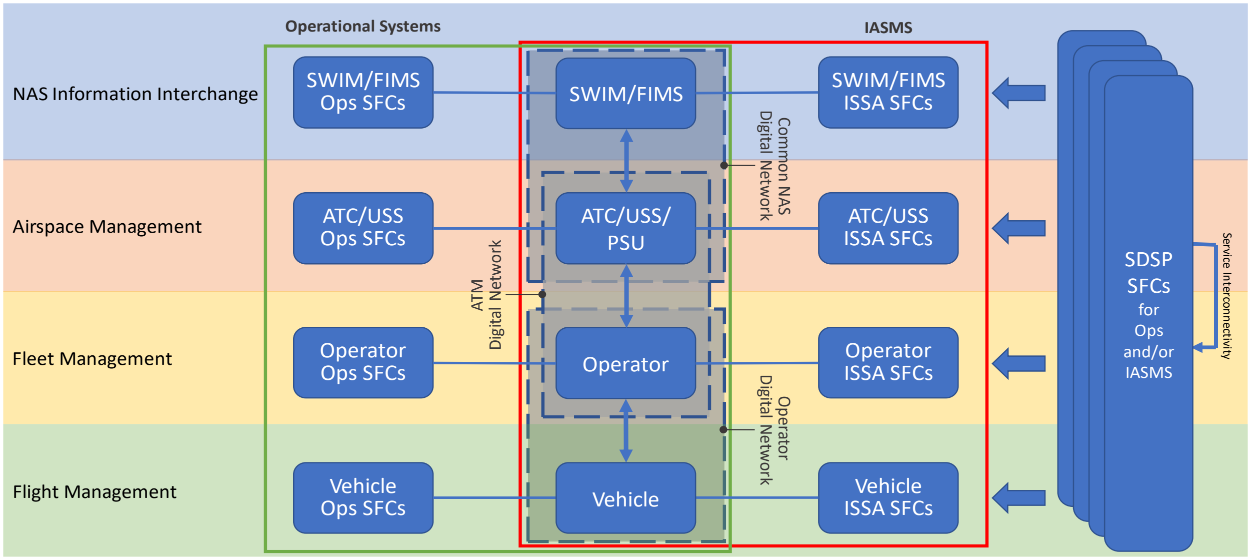

Fig. 8 AAM Ecosystem Architecture.

Example operational and IASMS SFCs are shown in Table 2 across categorizations of the IASMS architecture. Any one SFC could uniquely fit as either operational or IASMS within an architecture category or could fit in multiple categories. This one-to-one or one-to-many alignment reflects the interdependencies among SFCs in use of data and information and how risk is mitigated.

Architecture Categories	Operational SFCs	IASMS SFCs
NAS Information Exchange	Traditional-Space Launch-AAM Cross-Domain Airspace De-confliction TFAR	NAS Level Risk Assessment Anomaly Detection FOQA-type Data Services TFAR Violation Emergency Reporting Safety Data Repositories
Airspace Management	Network Scheduler Trajectory Generator Conflict Detection Conflict Resolution Airspace Contingency Management	Airspace Conformance Monitor Link Performance Dynamic Density Metric Airspace Risk Prognostics 3rd Party Risk – Pre/In-Flight Safety Reporting
Fleet Management	Fleet Ops Contingency Management Navigation Performance Fleet Monitor DataComm Weather – Operational Planning Schedule Coordination	Airspace Conformance Link Performance 3rd Party Risk – Pre/In-Flight Weather – Risk and Reporting Safety Reporting
Flight Management	Flight Ops Contingency Management Navigation Performance Weather – Flight Operations Powertrain DataLink DataComm Detect and Avoid (DAA)	Power Prognostics Navigation Systems Monitor Link Performance Monitor GPS Quality Motor Health 3rd Party Risk – In-Flight Weather – Risk (safety margin) Detect and Avoid DAA – Rogue Operations Services

Table 2. Examples of Operational and IASMS SFCs.

SFCs would be coupled together in the IASMS architecture with the design using both traditional and innovative methods and data. Machine learning and artificial intelligence pose avenues for research leading to identifying patterns with precursors, anomalies and trends that pose risk to AAM solutions. In this manner, known-knowns can be validated while known-unknowns are uncovered. In addition, new unknown-unknowns could be discovered.

As previously discussed, SFCs would be designed to meet operations-specific certification requirements and standards. These requirements and standards would provide SFC-level safety assurance. Additional requirements and standards would also provide SFC-level and systems-level cybersecurity. Requirements and standards for both assurance and cybersecurity represent a large body of industry consensus yet to be established.

VIII. Architecture Complexity Factors

For the purpose of the IASMS, operational complexity increases along four key factors. These factors reflect the complexity of the AAM ecosystem that would increase in complexity with the evolution of added capabilities including sensors, automated systems, performance models, and controls.

Vehicle Flight Management represents the extent that a human pilot manages the flight, for example, there could be one pilot per vehicle, or one pilot would be responsible for a swarm of multiple, independent vehicles. The Environment ranges from being 100% known to completely unknown, with things like weather, rogue aircraft, and malicious agents adding uncertainty to operations. Airspace can be dedicated to AAM vehicles that are under the purview of UTM or be mixed with VFR aircraft like GA and medical helicopters. Contingency Management represents the classical allocation of functions ranging from the human who is responsible for handling exceptions, setting dynamic constraints, and making strategic risk decisions to autonomous systems that use deep system understanding for tactical heuristic and probabilistic contingency management. Parameters nested below each of these complexity factors are shown in Figure 9.

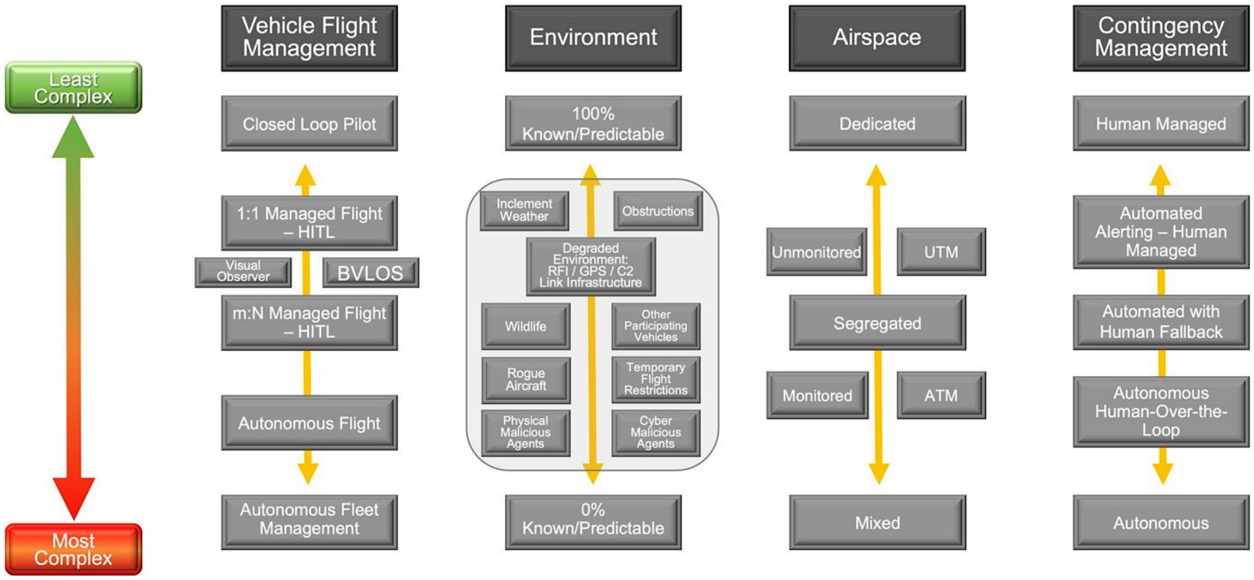
Least Complex
Most Complex
Vehicle Flight Management
Closed Loop Pilot
1:1 Managed Flight – HITL
Visual Observer
BVLOS
m:N Managed Flight – HITL
Autonomous Flight
Autonomous Fleet Management
Environment
100% Known/Predictable
Inclement Weather
Obstructions
Degraded Environment: RFI / GPS / C2 Link Infrastructure
Wildlife
Other Participating Vehicles
Rogue Aircraft
Temporary Flight Restrictions
Physical Malicious Agents
Cyber Malicious Agents
0% Known/Predictable
Airspace
Dedicated
Unmonitored
UTM
Segregated
Monitored
ATM
Mixed
Contingency Management
Human Managed
Automated Alerting – Human Managed
Automated with Human Fallback
Autonomous Human-Over-the-Loop
Autonomous

Fig. 9 Factors Driving Architecture Complexity.

These factors of complexity can be assessed to characterize where AAM exists today. Current operations involve the pilot in-the-loop with a visual observer. The environment is controlled and predictable with continuous monitoring such as for possible degradation of the command and control (C2) link. Flight occurs in dedicated UTM airspace or flying in unmonitored airspace, and contingencies are manually managed by the remote pilot of each vehicle.

Each of these factors can be comprised of multiple sub-factors that contribute to increasing complexity. For example, Airspace at a lower level of complexity could be dedicated to UTM operations that are unmonitored in dedicated airspace, and at a higher level of complexity could involve mixed UTM and ATM operations with heterogeneous vehicle types operating within the same airspace.

As operations become more complex, these factors scale to autonomous flight in unpredictable environments with mixed traffic and contingencies managed by automation. The National Academies noted that scalability is bounded by the limitations of human operators and their ability to safely manage increasingly complex operations. This highlights the interdependencies between these different factors. As Vehicle Flight Management, the Environment, and Airspace become more complex, there needs to be a commensurate shift towards increased automation to be able to manage the growing scale of complex contingencies. By the same token, with the human providing fallback, or in a supervisory over-the-loop role, concerns could include how difficult it could be for the human operator to intervene when time is short to resolve a safety issue.

It is worth noting that another approach to defining safety functions built on functional decompositions related to overcoming barriers necessary for increased use of automation with airspace management, and heavily automated and autonomously piloted aircraft [17]. Increasing levels of complexity necessitate development of data models and databases for safety assurance across a widening span of UAM applications such as flight inspection and use of metadata for pattern and anomaly detection.

IX. Conclusion

The IASMS ConOps describes an approach to the design of an architecture that integrates ISSA SFCs to address a risk or family of risks. Interdependencies across multiple factors, including increased use and complexity of automated systems, fewer skilled operators, increasingly complex operational environments, and airspace management with mixed aircraft and equipage pose a multi-dimensional space for design of an IASMS that provides safety assurance and risk management. The design of the IASMS architecture couples SFCs together for identifying anomalies, precursors, and trends using both traditional and innovative ways. This approach serves to validate known-knowns, uncover known-unknowns, and discover unknown-unknowns that pose risk to AAM solutions.

The IASMS ConOps 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. Data in different information classes 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 or artificial intelligence by autonomous systems or be mitigated by human intervention when appropriate.

Further development of the IASMS SFCs could correlate the data in different information classes that would be used to manage operational risks with an acceptable level of certainty. SFCs could also be assessed for informing system design to ensure life cycle product improvements by correctly assessing performance and deficiencies of the existing design. SFCs could also detect unknown risks by correctly identifying unknown anomalies and hazards in the system. Validation of SFCs could entail the development of specific use cases for detecting, assessing and mitigating risk for operational scenarios at different levels of operational complexity.

Acknowledgments

The authors thank Laura Bass for her excellent work in developing the figures and other contributions in development of this paper. We would like to thank NASA's Aeronautics Research Mission Directorate (ARMD) for their support of this effort. Multiple entities within ARMD have directly and indirectly supported this work, as well as several industry members from the broader aviation stakeholder community. We are grateful for the engagement of all who participated in the various workshops, seminars and conference sessions that contributed to the development of the IASMS concept of operations. This effort was led by members of NASA ARMD's System-Wide Safety project within the Airspace Operations and Safety Program.

References

[1] National Academies of Sciences, Engineering, and Medicine. 2018. *In-time Aviation Safety Management: Challenges and Research for an Evolving Aviation System*. Washington, DC: The National Academies Press. https://doi.org/10.17226/24962.

[2] Ellis, K., Koelling, J., Davies, M., and Krois, P., "In-time System-wide Safety Assurance (ISSA) Concept of Operations and Design Considerations for Urban Air Mobility (UAM)," NASA/TM-2020-5003981, Hampton, VA, 2020.

[3] National Academies of Sciences, Engineering, and Medicine. 2020. *Advancing Aerial Mobility: A National Blueprint*. Washington, DC: The National Academies Press. https://doi.org/10.17226/25646

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

[5] Federal Aviation Administration, “Safety Management Systems for Aviation Service Providers,” AC No. 120-92B, 2015.

[6] Stolzer, A.J., Halford, C.D., and Goglia, J.J., Safety Management Systems in Aviation, Ashgate Studies in Human Factors for Flight Operations, Burlington, VT, 2010.

[7] Patterson, M.D., Isaacson, D.R., Mendonca, N.L., Neogi, N.A., Goodrich, K.H., Metcalfe, M., Bastedo, B., Metts, C., Hill, B.P., DeCarme, D., Griffin, C., and Wiggens, S., “An Initial Concept for Intermediate-State, Passenger-Carrying Urban Air Mobility Operations,” AIAA Sci Tech, 2021.

[8] Joint Authorities for Rulemaking of Unmanned Systems, “Guidelines on Specific Operations Risk Assessment,” JARUS, 2017.

[9] Farner, M., “SORA Risk Assessment for Unmanned Airborne Mobility,” Workshop Intelligent and Autonomous Technologies in Aeronautics, September 2017.

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

[11] Shappell, S.A. and Weigmann, D. A., “The Human Factors Analysis and Classification System – HFACS,” DOT/FAA/AM-00/7, 2000.

[12] Belcastro, C.M., Newman, R.L., Evans, J.K., Klyde, D.H., Barr, L.C., and Ancel, E., “Hazards Identification and Analysis for Unmanned Aircraft System Operations,” AIAA Aviation 2017 Forum.

[13] Young, S. Ancel, E., Moore, A., Dill, E., Quach, C., Foster, J., Darafsheh, K., Smalling, K., Vasquez, S., Evans, E., Okolo, W., Corbetta, M., Ossenfort, J., Kulkarni, C., and Spirkovska, L., “Architecture and Information Requirements to Assess and Predict Flight Safety Risks During Highly Autonomous Urban Flight Operations,” NASA/TM-2019-000000, Hampton, VA, 2020.

[14] American National Standards Institute, “Standardization Roadmap for Unmanned Aircraft Systems, Version 1.0,” December 2018.

[15] Holbrook, J.B., Prinzel, L.J. III, Chancey, E.T., Shively, R.J., Feary, M.S., Dao, Q.V., Balin, M.G., and Teubert, C., “Enabling Urban Air Mobility: Human-Autonomy Teaming Research Challenges and Recommendations,” AIAA Aviation 2020 Forum.

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

[17] Feary, M., “A Decomposition Framework for Describing Advanced Air Mobility Mission Functions,” AIAA Aviation 2020 Forum.