Defining Services, Functions, and Capabilities for an Advanced Air Mobility (AAM) In-time Aviation Safety Management System (IASMS)

Ellis, K.[1], Krois, P.,[2] Koelling, J.,[1] Prinzel, L.,[1]
Davies, M.[3], Mah, R.[3] and Infeld, S.[4]

[1] *NASA Langley Research Center, Hampton, VA*
[2] *Crown Consulting Inc., Aurora, CO*
[3] *NASA Ames Research Center, Mountain View, CA*
[4] *Analytical Mechanics Associates, Hampton, VA*

I. Introduction

NASA's vision for Advanced Air Mobility (AAM) Mission is to help emerging aviation markets to safely develop an air transportation system that moves people and cargo between places previously not served or underserved by aviation. The integration of new operational paradigms and vehicle classes in this system requires a transformation of the National Airspace System (NAS) that includes substantive changes critical for assuring safety. These changes are compelled by unique challenges posed by AAM to the safety management system (SMS). These challenges were assessed by committees of the National Academies in their reports on a vision for an In-time Aviation Safety Management System (IASMS) and a blueprint for AAM [1, 2]. In their description of an IASMS, the top recommendation was development of a concept of operations (ConOps) for IASMS.

This paper describes the high-priority recommendations from the National Academies for its IASMS vision and how they are addressed through a distributed system-of-systems architecture. The IASMS architecture is structured on the services, functions, and capabilities (SFCs) necessary for In-time System-wide Safety Assurance (ISSA) initially developed for urban air mobility (UAM). The paper then posits where these SFCs would reside across vehicles, airspace, or service suppliers such as Supplemental Data Service Providers (SDSPs), and how SFCs scale with increasing complexity in design and operations of AAM. SFCs are foundational building blocks for a system that targets an individual or family of risks using a Monitor-Assess-Mitigate risk paradigm for anomalies, precursors and trends. An IASMS could be conceived that uses a portfolio of SFCs for AAM in general or prioritizes SFCs for a specific domain or operation.

A. National Academies AAM High-Priority Recommendations

The vision of the National Academies considered the IASMS to continuously Monitor the NAS to collect data on the status of aircraft, air traffic management (ATM) systems, airports, weather and other status data [1]. The IASMS would Assess these data based on different parameters of time (seconds, minutes, hours, or days) to detect or predict elevated risk states. Different elements of a safety assurance system would operate on different time scales exclusive of emergencies caused by catastrophic failures. The assessment would detect and predict elevated risk states that arise from multiple factors, none of which by itself would necessarily be noteworthy. This assessment of risk states would incorporate nominal performance patterns of systems and operators, the fault tolerance of the NAS and its key elements, and historical data on the occurrence and consequence of any off-nominal situation. The assessment

would also examine long-term trends to identify emergent risks that in some cases should be added to the list of risks the system monitors.

It was also recommended that the IASMS should focus on risks requiring safety assurance action prior to flight or in-flight. Preflight safety assurance action could include a decision to delay or cancel a flight such as due to adverse weather or equipment status. The National Academies noted that an IASMS would not be designed to recommend safety assurance actions that would take weeks to months or longer to implement. These actions having a longer time horizon could involve changes to pilot training, operational procedures, equipment design, or maintenance checks. It was noted that the outputs of an IASMS could be useful to those having responsibilities in these areas. As part of the IASMS concept, NASA is working to define SFCs that could bridge these areas requiring responsive time horizon in order to provide more proactive in-time risk management and safety assurance. This could mean that as operational experience reveals emergent risk that there is a loop to inform training, procedures, and equipment design for timely changes. This information could also support showing means of compliance for Part 121 air carriers that are required to implement an SMS [3].

Lastly, an IASMS would take safety assurance actions to mitigate risk that could be in different forms ranging from recommended actions that operators should take, to time-critical situations in which the IASMS initiates a safety assurance action on its own. The above IASMS functions of Monitor, Assess, and Mitigate use an integrated set of SFCs to accomplish these risk mitigation and safety assurance responsibilities.

B. Pillars of SMS

At a high level, the International Civil Aviation Organization (ICAO) defined four pillars of a Safety Management System (SMS) that include Risk Management and Safety Assurance [4]. An IASMS will require these Risk Management and Safety Assurance pillars to integrate and work seamlessly together. This concept is shown in Figure 1. This integration requires developing SFCs that can quickly exchange data to detect and manage risk with reduced levels of human interaction and dramatically increased responsiveness for in-time safety.

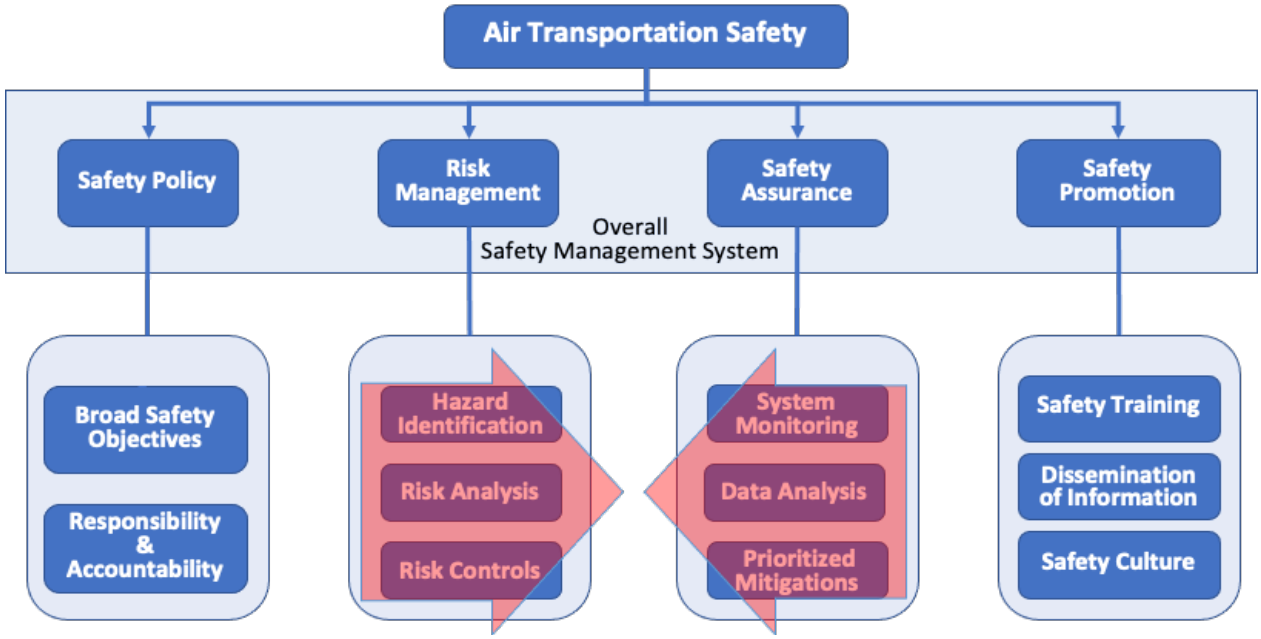

Fig. 1 Achieving Aviation Safety Today and with AAM—ICAO Annex 19.

C. IASMS and SFCs

As a step toward developing the IASMS ConOps, an initial In-time System-wide Safety Assurance (ISSA) approach was developed with industry and academia focused on the functionality, risk priorities, and use case scenarios for safety assurance in the UAM domain [5]. In contrast, the IASMS ConOps integrates risk management and safety assurance across multiple domains to assure safety including commercial operations, unmanned aircraft system (UAS) and small UAS (sUAS), UAM, air taxis, General Aviation (GA), cargo, and space launch and return. Building an IASMS that supports the safety case begins with identifying safety critical risks through an appropriately rigorous

hazard analysis. The safety case would address known risks by defining requirements for IASMS SFCs. The design of SFCs, the architecture, and data requirements would be scaled to address the complexity, uncertainty and risk criticality of the envisioned operation with the appropriate level of autonomation and autonomy.

Through the lens of an IASMS, SFCs are used today to assure safety. For example, during flight, known risks are addressed by SFCs represented by Traffic Alert and Collision Avoidance System (TCAS), Enhanced Ground Proximity Warning System (EGPWS), the air traffic control (ATC) conflict probe called the User Request Evaluation Tool (URET), flight deck information displays such as advanced vision systems and cockpit display of traffic information (CDTI), and various weather information products and displays using weather radar and wind shear detection. Safety is assured today post-flight using archived data and mining algorithms to identify precursors, anomalies, and trends. Programs serving this purpose include the industry Aviation Safety Information Analysis and Sharing (ASIAS) program and the different data bases on which it is based such as Flight Operations Quality Assurance (FOQA), Aviation Safety Action Program (ASAP), and the Air Traffic Safety Action Program (ATSAP). Other safety data bases include the NASA Aviation Safety Reporting System (ASRS) and Line Operations Safety Audit (LOSA).

In AAM, risks that are identified or emerge during life-cycle phases of design-time or operations-time explain why SFCs need to be provided by the vehicle, airspace, SDSP, and other actors in the architecture. A *Service* has been defined as a system providing information or data to a user who subscribes to that service [5]. Examples of Services include Non-Participant Casualty Risk Assessment (NPCRA), Proximity to Threats (PtT), and Battery Prognostics (BP). A *Function* is defined as one or more actions that translates a set of inputs to a desired set of outputs. A Function can detect, generate, validate, integrate, or distribute information that may or may not be included in a Service. On-board vehicle functions can include autopilot and digital communication. A *Capability* is defined as the ability to perform a set of Functions to achieve certain outcomes. On-board vehicle capabilities include trajectory prediction, navigation monitor, link monitor, constraint monitor, and contingency planner. SFCs use or consist of data falling into different information classes, as shown in Figure 2 [6].

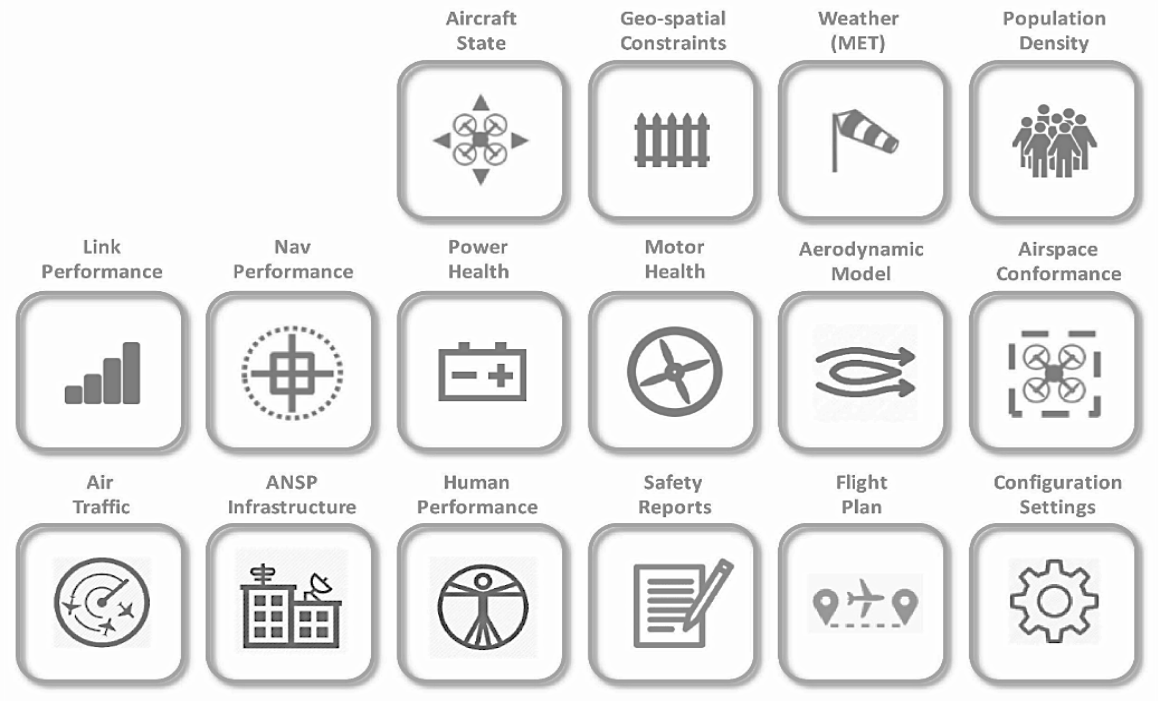

Fig 2. IASMS Information Classes.

SFCs rely on generation and exchange of digitized data. Digitization of data involves quality considerations that include availability, latency, update rates, integrity, security, formats, implementation and service costs, bandwidth utilization, and standards. Digitization should follow a common architecture and suite of SFCs although relevant standards and principles may not yet exist and represent an area of future work. There may be several instances where data standards and guidance may not yet exist and represent a critical area of research to enable AAM.

A key challenge to the IASMS architecture is having the ability to scale as AAM and the NAS become more complex. Today's NAS is already constrained because operations are labor-intensive, and its design is bounded with limited ability to scale with increased use of automated systems. Consequently, SFCs become the coin of the realm to assuring safety with these increasingly complex systems.

II. AAM Safety Landscape

In order to maintain the current level of safety, the transformed NAS represents a landscape of expanded and new safety mechanisms and protections compared to today's system. To enable a safe, transformed NAS, development of an IASMS needs to identify the technical hurdles that safety must overcome. This can be accomplished in part by leveraging research on AAM as well as traditional operations to inform safety requirements for emerging operations.

The AAM ecosystem contains operational risks that the IASMS manages from pre-flight, en route, and post-flight. The risks, complexities, and constraints of operations that must be addressed are shown as an operational view in Figure 3.

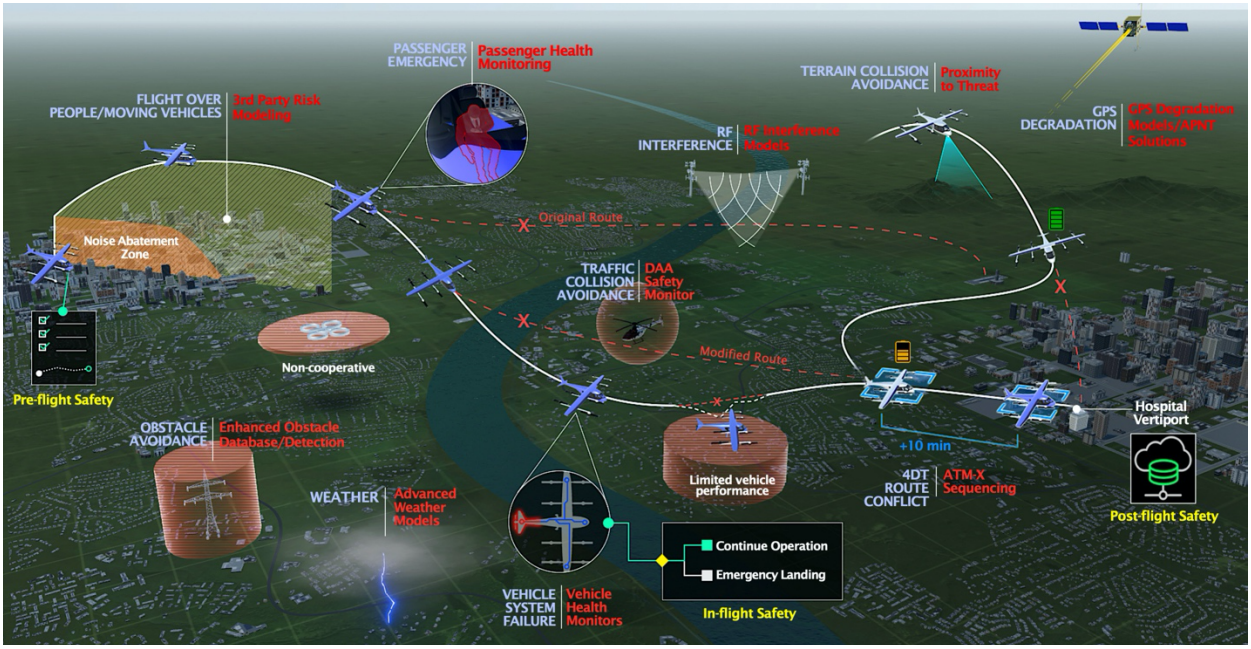

Fig. 3 IASMS Operational View.

The high-priority safety risks shown in the IASMS Operational View are paired with corresponding classifications of SFCs, the risk mitigations, and current reference SFCs in Table 1.

Risks	Risk Mitigations	SFC Classification	Reference SFCs
Critical System Failure	Vehicle health monitoring systems continuously assess performance of on-board operational systems, e.g., battery power and motor performance.	Vehicle Flight / Contingency Management – (Vehicle Health Monitors, System Health Monitor)	Battery Health Prognostics FOQA-type data services Semaphores (space domain solution)–longest interval for critical agent to function as specified
Cyber Risks	Cybersecurity threats or malfunctions can be identified and mitigated through proactive and reactive methods; private networks and protocols can be standardized and segmented to limit potential spread of this risk	Systems-Level (Networks)	Several industry solutions–DoD reference solutions for Remotely Piloted Vehicles Network monitoring Nodal/segmented network architectures

Flight Outside of Approved Airspace	Vehicle conforms to approved airspace or follows approved filed flight plan.	Airspace (Airspace Conformance)	Safeguard
Flight Over People/ Moving Vehicles	Vehicle maintains safe lateral distance around people and moving vehicles as established in flight plan or as information is updated during flight, e.g., changes to route of flight or 3rd party risk assessment.	Environmental Hazard (3rd Party Risk)	Proximity to Threat Service, Non-participant Casualty Risk Assessment, ICAROUS-Route conflict resolution module, Safe2Ditch
GPS Degradation	Operational systems monitor and assess RF interference for disrupting communications.	Environmental Hazard (GPS Degradation)	GPS Degradation Modeling, APNT Services
Noise abatement	Procedural adjustments and/or limitations based on noise modeling and acceptance testing for various aircraft types.	Environmental Hazard (Noise)	RVLT noise models for various vehicle types Community testing
Obstacle Avoidance	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.	Environmental Hazard (Geographic)	ICAROUS Route conflict resolution module (vehicle) Enhanced Geographic Database Services (SDSP)
Physical Risks	Wildlife (bird strike, etc.) and/or malicious agents can be avoided with greater sources of information exchange and sensor capabilities	Environmental Hazard (projectiles)	Locality reporting
Procedural Risks	Unintended consequences resulting in safety risks can be detected by systems-level data analysis to inform new safety enhancements	Systems-level (Predictive and prognostic risk assessment)	MKAD–multi-kernal anomaly detection Adaptive security procedure development
RF Interference	Operational systems monitor and assess RF interference for disrupting communications.	Environmental Hazard (RF Interference)	RF Interference Modeling
Route Conflict	Pre-flight 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.	Airspace (Routes)	Dynamic Density Metric Trajectory Generator ATM-X Sequencing and Spacing NOTAMS TFR Enhanced
Terrain Collision Avoidance	An on-board real-time operational system provides detect-and-avoid warning and maneuvering away from terrain to avoid controlled-flight-into-terrain (CFIT).	Environmental Hazard (Terrain)	Proximity to Threat Service EGPWS-type solutions APNT Solutions
Traffic Collision Avoidance	ANSP real-time operational system provides detect-and-avoid warning, determines trajectories	Airspace (Traffic)	xTM-based deconfliction service: Conflict detection

	away from other airborne vehicles, and communicates these maneuvers while communicating with other vehicles and USS/PSU/ANSP network.		Conflict resolution Dynamic Density Metric Trajectory Generator
Traffic Collision Avoidance	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.	Environmental Hazard (Traffic)	Vehicle-based ICAROUS DAA Module
Weather	Flight plan checked before departure for current and forecast weather including temperature; wind direction, strength and gust; convective weather; precipitation; and icing. Micro-weather forecasting for urban flight planning. Pilot weather reports to update flight plan.	Environmental Hazard (Weather)	Cellphone-based or other non-traditional weather data solutions Hyper-local integrated weather modeling Locality infrastructure sensors & modeling

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

The IASMS posits that the timeliness by which complex aviation systems are managed by humans and automation can be improved by providing in-time safety assurance for known risks. The IASMS also serves to enable increasingly proactive detection and management of previously unknown emergent risks. In today's system, known risks are handled a priori during design using defined mitigations integrated in automated system design or that could be part of operations involving flight planning or following standard operating procedures and flight rules. Unknown risks are handled as they are encountered during flight based on the expertise and skill of operators, pilots, and controllers as quick operational fixes. Unknown risks may be discovered post-flight through the mining of operational performance and safety databases including analysis of accidents, incidents, and safety reports, which in today's system can eventually lead to either operational or design fixes.

In contrast, changes with the future IASMS system will quickly detect and identify previously unknown operational and design risks and mitigate those risks for in-time safety assurance. Emergent risks will be identified at least initially following known patterns to detect emergent precursors, anomalies, and trends in safety data such as weak signals based on an initially limited number of data points but enough to trigger further monitoring. As the IASMS matures, it will use artificial intelligence and machine learning to detect and interpret deviations from known patterns.

Adaptive and scalable systems will overcome limitations with today's systems and operations. For smaller operations, such as Part 135 on-demand carriers, flight data monitoring could be augmented with supervisory SFCs (sSFCs) that intelligently scale for checks that are continuous, periodic or manually initiated. The architecture of sSFCs would operate at a baseline frequency and make slight adjustments by increasing the frequency of relevant sSFCs when certain data start to show deviations from nominal patterns. That is, an IASMS could be scaled that manages itself using sSFCs and makes adjustments based on its own sensitivity analysis. The IASMS would inform the human operator when adjustments would be made and the associated unexpected variation from patterns of performance.

III. Ecosystem Architecture

The current UTM architecture is shown in Figure 5 [7]. 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.

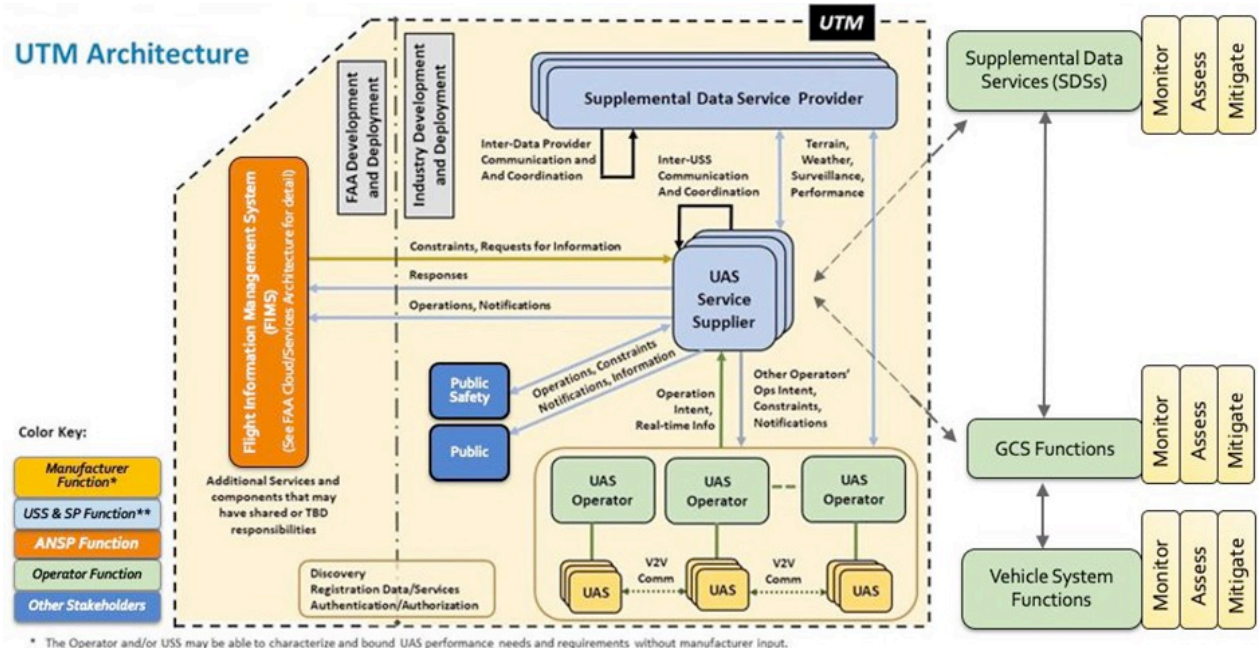

Fig. 5 UTM Architecture.

The distributed architecture of the IASMS reflects where the SFCs reside. This is shown in Figure 6 that includes the classes of information collected and used by the SFCs for safety assurance and risk management. This architecture shows the NAS is continuously monitoring different actors for risk.

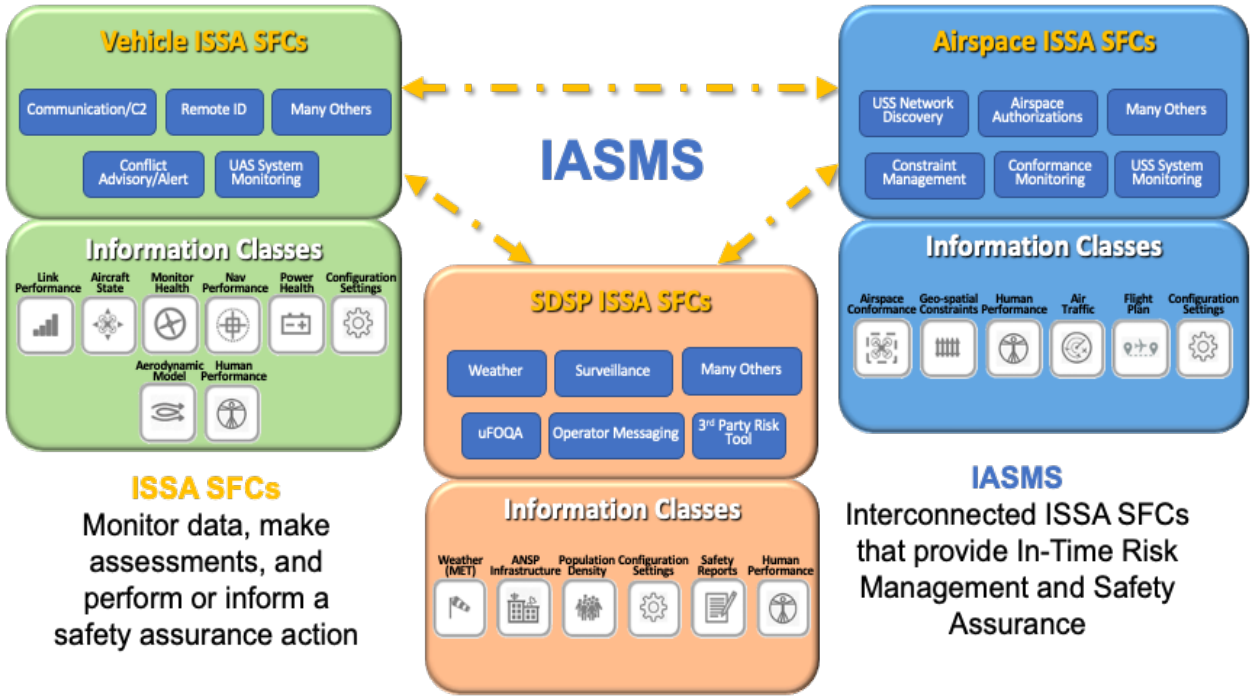

Fig. 6 SFCs and Information Classes.

The SFCs can be organized according to different network architectures. As shown in Figure 7, SFCs can be organized as operational or are part of the IASMS, and some SFCs can be both operational and part of the IASMS. SFCs can also be organized according to where they are located as part of the overall system, i.e., common NAS network with SWIM/FIMS, ATC/USS network, operator network, vehicle network, or SDSP network.

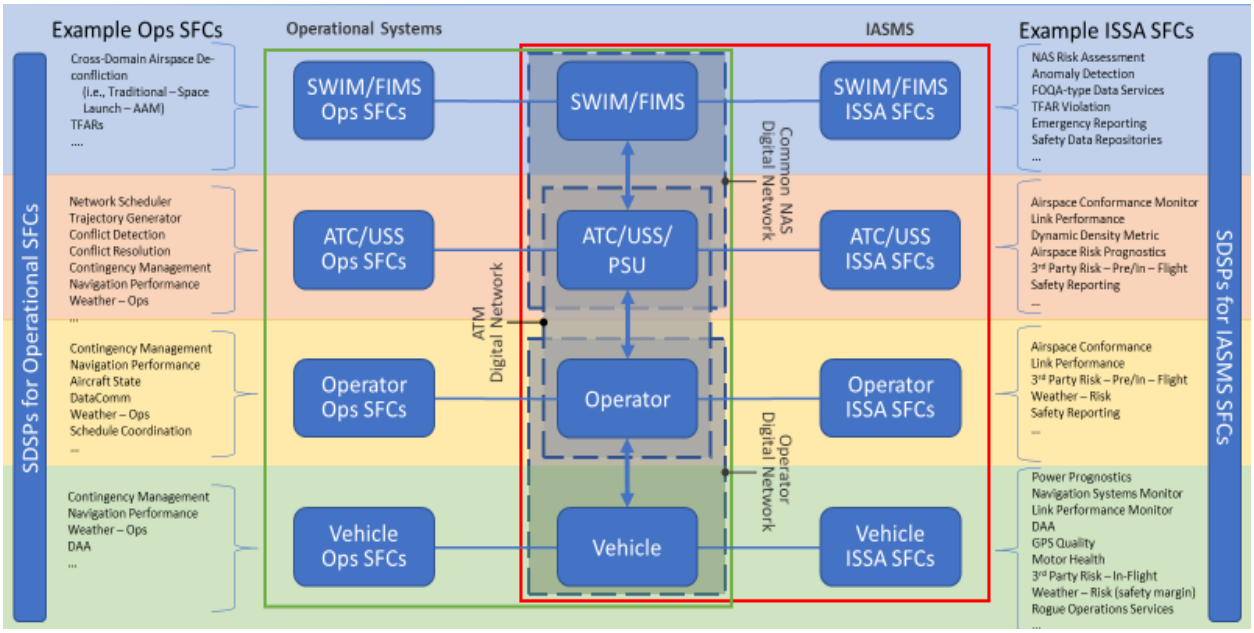

Fig. 7 Network Architectures of SFCs.

Development and evolution of the above architecture would meet requirements and standards that are specific to types of operations. Across the different levels, the IASMS and operational SFCs would meet safety assurance and certification requirements. SFC-level cybersecurity requirements would also be developed at each level.

IV. Assuring Safety in AAM

In tomorrow's system, safety will be assured by quickly identifying and managing known operational risks, quickly detecting and assessing unknown risks, and quickly informing system design for targeted improvements. These improvements could involve changes to system specifications, procedures, or operator training. Safety assurance will be scaled relative to operational complexity including that SFCs will be aligned to risks pertinent to intended or actual operations such as developed and assessed with operational use case scenarios.

Considering that design and operations will be assured through SFCs, SFCs should be adaptable to meet the requirements of particular operations. These operations would be represented by select use case scenarios. SFCs will be certified using assurance-based arguments as a suitable means of compliance. The flow by which SFCs would be assured is shown in Figure 8. One approach for assuring SFCs could involve use of sSFCs that monitor the performance of SFCs in a supervisory manner.

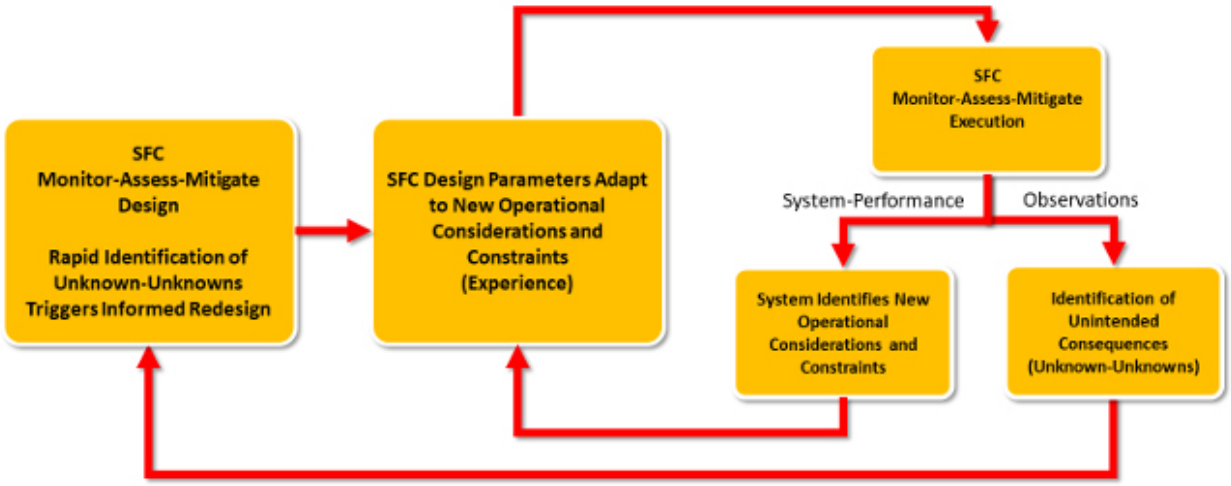

Fig. 8 Assurance of SFCs.

Development and evolution of the above architecture would meet requirements and standards that are specific to the intended types of operations. Across these different use cases, the IASMS and operational SFCs would have to meet safety assurance and certification requirements. SFC-level cybersecurity requirements could also be developed for each type of operation.

The SFC high-level network architectures shown in Figure 7 correspond with the roles and responsibilities that the safety agents have for managing IASMS risks. Table 2 shows a concept for the distribution of roles and responsibilities for risk management, based in part on how they are characterized in the FAA UTM ConOps V2 [7]. Some roles and responsibilities may be shared or partitioned across different safety agents such as for failover and redundancy to establish resiliency for safety critical systems.

	Safety Agents				
IASMS Risks	**Vehicle**	**Operators**	**ATC/USS**	**SWIM/FIMS (FAA)**	**Vertiport**
Cybersecurity	Detection and mitigation	Detection and mitigation	Detection and mitigation	Detection and mitigation	Detection and mitigation
Flight Outside of Approved Airspace	Detection and mitigation	Detection and mitigation	Decision confirmation	Exception notification	
Flight Over People/ Moving Vehicles	Data, modeling and mitigation	Data, modeling and mitigation	Exception notification	Exception notification	
GPS Degradation	Data (sensors)	Data, modeling and mitigation	Data and modeling	Exception notification	Data, modeling and mitigation
Obstacle Avoidance	Detection and mitigation	Detection and mitigation	Decision confirmation	Exception notification	
Physical Security	Detection and mitigation	Exception notification	Exception notification	Exception notification	Detection and mitigation
RF Interference	Data (sensors)	Data, modeling and mitigation	Data and modeling	Exception notification	Data, modeling and mitigation
Route Conflict	Detection and mitigation	Detection and mitigation	Decision confirmation	Exception notification	Exception notification
Terrain Collision	Detection and mitigation	Decision confirmation	Exception notification	Exception notification	
Traffic Collision	Detection and mitigation	Decision confirmation	Exception notification	Exception notification	
Vehicle System Failure	Detection and mitigation	Decision confirmation	Exception notification	Exception notification	
Weather	Data (sensors)	Data, modeling and mitigation	Data and modeling	Exception notification	Data, modeling and mitigation
	↑	↑	↑	↑	
	SDSP (Local/Regional/National) – Data and Modeling				

Table 2. Roles for Managing IASMS Risks.

A key premise of IASMS is that its functionality is assured by SFCs. These SFCs mitigate risks with an acceptable level of certainty, correctly identify unknown anomalies and hazards in the system, and correctly assess performance and any deficiencies in the existing system design. Assurance requirements are specific to risk criticality, flight rules, and operational complexity. SFCs would be assured to an appropriate level via an acceptable process involving suitable means of compliance. These relationships are shown in Figure 9. Challenges with this approach are that the efficiency of traditional assurance methods will need to be improved, assuring systems could make increased use of machine learning and artificial intelligence, and future systems as they mature will learn and adapt within operation cycles.

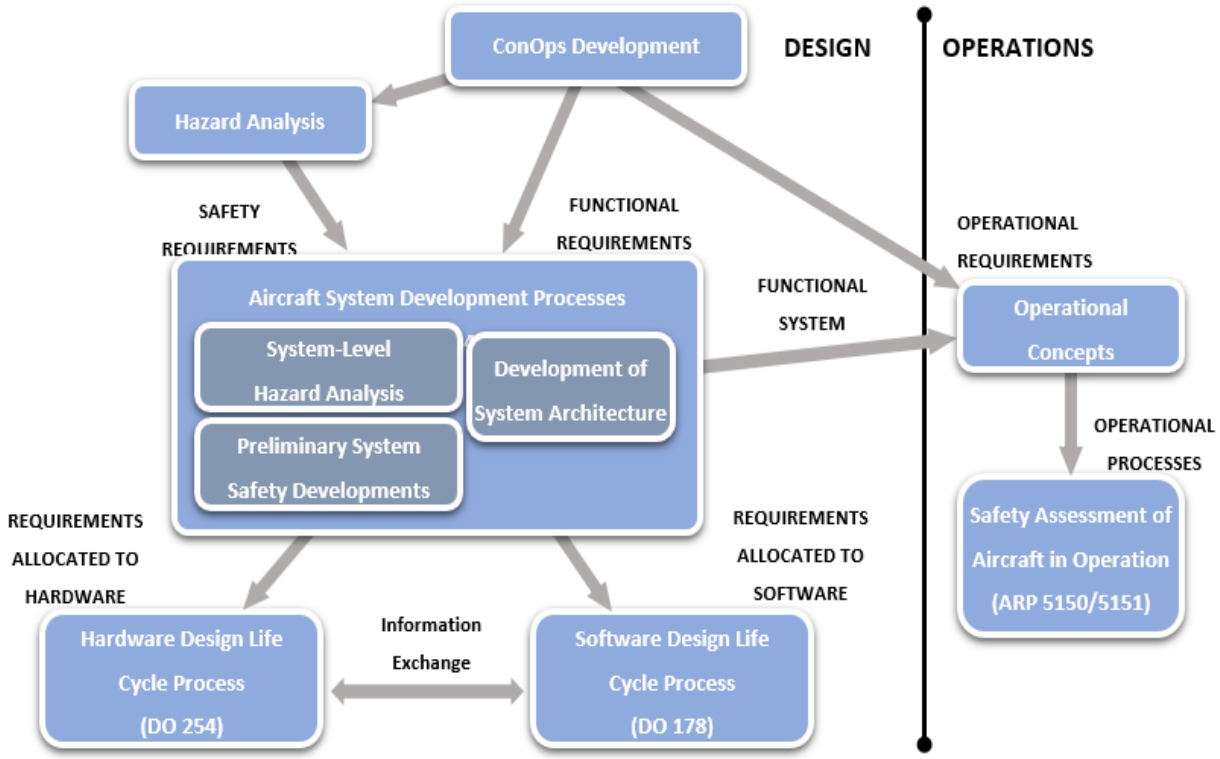

Fig. 9 Assurance of SFCs.

V. Operational Factors of Complexity

The IASMS architecture of SFCs scales with increasing complexity in operations. As complexity increases, new SFCs would be identified and become required and many SFCs would be inherited from the previous lower level of complexity or antecedent condition. These inherited SFCs might be retained without change and some may change. A similar pattern may occur with sSFC. It would be unlikely that an existing SFC required at one level of complexity would not be carried forward up into the next higher level in the same or similar form since it may be required such as for redundancy or failover when a component degrades or fails.

Previously, four factors were identified for scaling operational complexity of the AAM ecosystem consisting of Vehicle Flight Management, Environment, Airspace, and Contingency Management [8]. These factors provide a notional design to represent the changes that become more important as operations become more complex and how increased complexity corresponds with design of systems that are increasingly automated. As shown in Figure 10, for operations in today's AAM ecosystem, Vehicle Flight Management involves the human pilot managing the flight in a closed loop with simplified control. The Environment for the flight is completely known, controlled, and predictable such as involving suitable weather conditions and an infrastructure capable of handling any degradation. The Airspace is dedicated to AAM vehicles, so it does not have to be monitored for VFR aircraft. Contingencies are managed by the human pilot including detecting and avoiding rogue aircraft and being supported with automated alerting for off-nominal conditions.

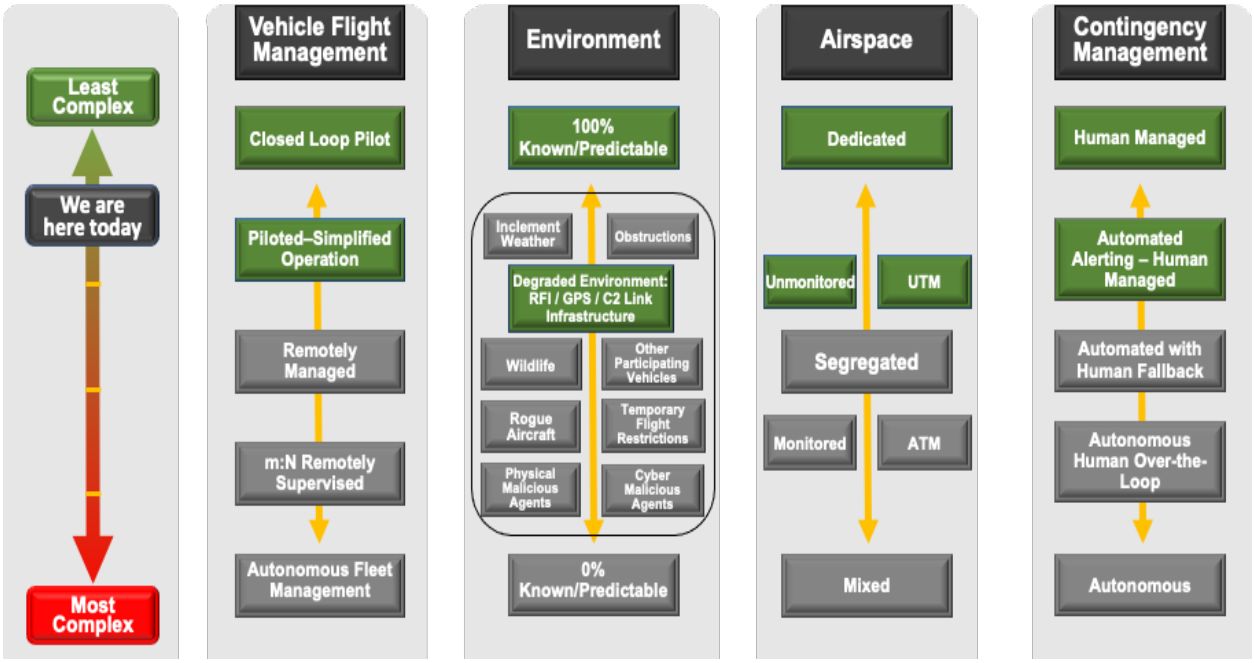

Fig. 10 Complexity Factors for Today's Operations.

The complexity of an envisioned future operation could entail changes along all four factors, as shown in Figure 11. Vehicle Flight Management could involve autonomous fleet management beyond one remote pilot being responsible for a coordinated swarm or monitoring multiple independently operating vehicles with each vehicle having its own flight plan. The Environment during pre-flight and at departure involves partially known conditions (e.g., changing weather forecasts) mixed with unknown and unpredictable considerations (e.g., presence of rogue aircraft and cyber threats). The Airspace combines monitored and unmonitored aircraft using an integrated ecosystem of air traffic management (ATM) and UAS traffic management (UTM). These increasingly complex operations necessitate autonomous Contingency Management with very limited monitoring by humans due to the high volume of traffic posing possible safety risks that require timely mitigation.

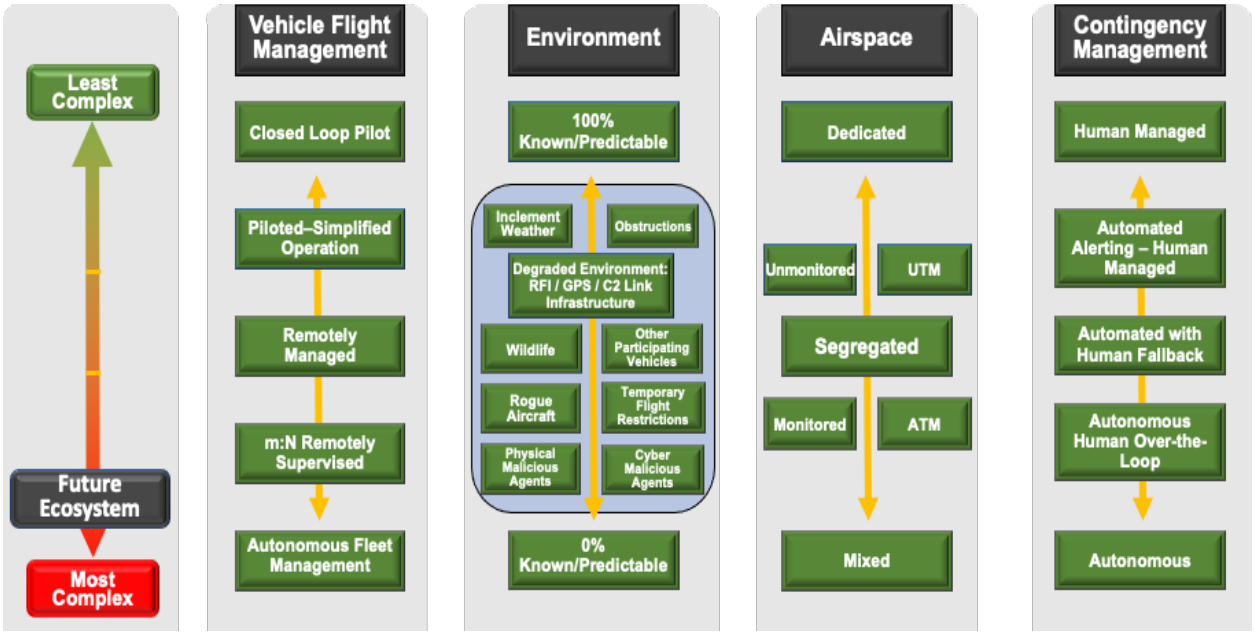

Fig. 11 Complexity Factors for an Envisioned Future Operation.

VI. Safety Management Across Architecture Epochs

The different factors of complexity described in the previous section can be overlaid atop a series of notional Epochs that represent the transformation of the NAS associated with integration of AAM technologies and airspace capabilities, as shown in Figure 12. Epochs increase in complexity based on vehicles, environment, airspace, and contingency management. Epochs also correspond to introduction of emerging safety risks that need to be identified and mitigated during design and operations. Across Epochs, the integrated architecture of SFCs would evolve in size and complexity as the roles of humans and automated systems change with automation taking on more authority and responsibility. These SFCs would be distributed and layered across the network architectures according to the requirements of each Epoch.

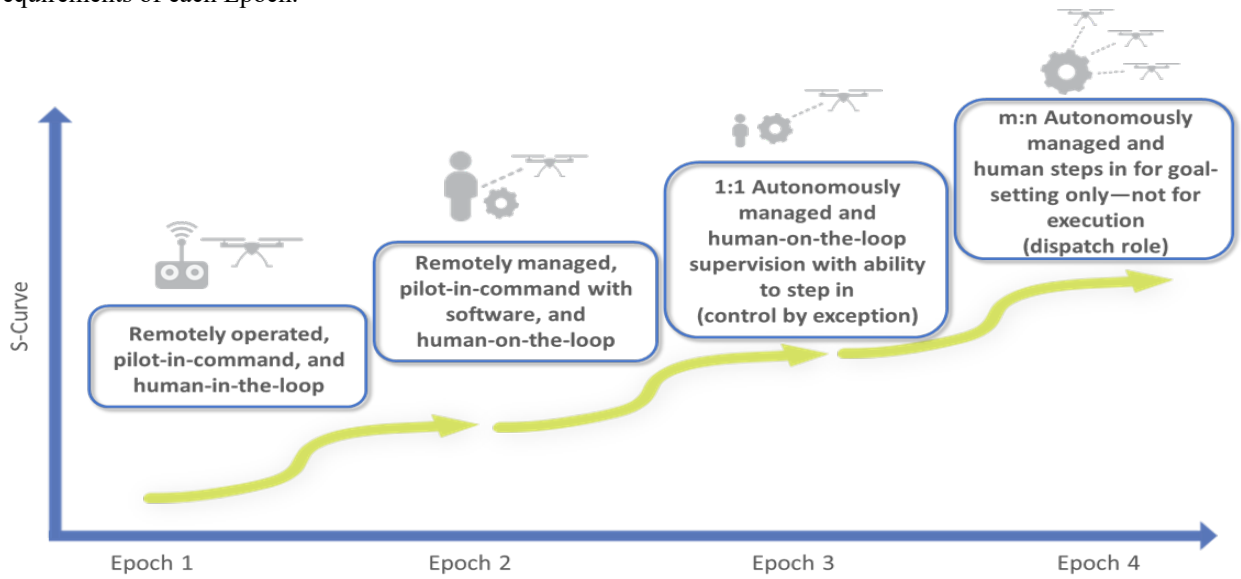

Fig. 12 Epochs Representing Evolution of the NAS.

Epoch 1 represents today's simplified UAS operations with the pilot in a closed loop. Operations occur in only dedicated UTM airspace that is not monitored by the Federal Aviation Administration (FAA). The environment is completely predictable with no known degradations in surveillance or communication links. Risks are alerted to the human pilot who is responsible for their mitigation. Contingencies for other off-nominal conditions may also involve automated alerting and are managed by humans.

Epoch 2 involves a remote pilot in-charge (RPIC) managing the vehicle using an in-the-loop control structure. The pilot is responsible for a single vehicle, and SFCs would alert the pilot to unsafe conditions.

Epoch 3 involves an autonomous vehicle with one operator (1:1) who has supervisory responsibility and monitors and manages the vehicle using an on-the-loop approach with the ability to step in as required (control by exception). Automated systems are designed to monitor and detect non-normal conditions and assess whether operations should be adjusted accordingly. Risk mitigation can occur according to a sliding scale, balancing responsibility between the human operator and automation. For example, an automated system that has assessed a risk may present the operator with information about a risk; the system or the operator then decides what action to take, or the automation may execute an action and the operator can intercede and override the system when necessary.

Epoch 4 involves multiple autonomous vehicles with several operators working in an over-the-loop dispatch capacity (m:n). Risk mitigation and contingency management would be executed by autonomous systems with the operator responsible for goal setting for flight outcomes and not for changing an individual vehicle's flight plan that would be amended by automated systems.

The increasing complexity represented by the Epochs corresponds to changes in the roles and responsibilities of the safety agents as previously shown in Table 2. Those changes can be represented by levels of automation for human-autonomy teaming (HAT). Table 3 shows one concept proposed for HAT [9]. This concept shows how roles move from the human operator to the computer as the level of automation changes from manual control to full automation. An assumption is that the SFCs would change as HAT progresses towards full automation and automated systems are designed to take full operational responsibility for monitoring, assessing, and mitigating known and unknown emergent risks.

	ROLES			
LEVEL OF AUTOMATION	MONITORING	GENERATING	SELECTING	IMPLEMENTING
Manual Control	Human	Human	Human	Human
Action Support	Human/Computer	Human	Human	Human/Computer
Batch Processing	Human/Computer	Human	Human	Computer
Shared Control	Human/Computer	Human/Computer	Human	Human/Computer
Decision Support	Human/Computer	Human/Computer	Human	Computer
Blended Decision Making	Human/Computer	Human/Computer	Human/Computer	Computer
Rigid System	Human/Computer	Computer	Human	Computer
Automated Decision Making	Human/Computer	Human/Computer	Computer	Computer
Supervisory Control	Human/Computer	Computer	Computer	Computer
Full Automation	Computer	Computer	Computer	Computer

Table 3. A Concept for Levels of Automation.

The AAM ecosystem architecture would be designed to operate with agility and resilience suited for different domains. These different domains, such as small UAS and UAM, could have safety risks in common but differences between domains could also necessitate different SFCs to address unique safety risks and criticalities.

In sum, IASMS SFCs including the underlying ISSA SFCs become increasingly capable and complex across the Epochs as the architecture scales to meet operational requirements. The design of SFCs enables complex automated systems to perform the key elements of risk management and safety assurance with reduced levels of human interaction and dramatically increased responsiveness of automated systems.

VII. Future Challenges

Maturation of the IASMS ConOps continues to progress as understanding and insight are gained across today's challenges and the future needs emerging from the different domains that comprise the AAM ecosystem. The IASMS ConOps provides an approach for assuring safety as AAM transforms the NAS.

Today's challenges include two safety recommendations identified by the National Transportation Safety Board (NTSB) in its *2021-2022 Most Wanted List of Transportation Safety Improvements* having implications for the IASMS [10]. One recommendation is to require and verify the effectiveness of SMS in all revenue passenger-carrying aviation operations. The SMS should comply with Advisory Circular 120-92B called *Safety Management Systems for Aviation Service Providers* [3]. This recommendation involves Part 135 commercial, non-scheduled private air charters, air taxi flights, and package delivery by drone, and Part 91 General Aviation that includes living flight history experience (LHFE) flights as reflected in the NTSB accident investigation report on a B-17 crash. It found the operator had an ineffective safety management system (SMS), which had failed to identify and mitigate safety risks [11]. The second recommendation was that all Part 135 operators should have flight data recording capabilities supporting a flight data monitoring program and require operators to establish a structured flight data monitoring program that reviews all available data sources to identify off-nominal deviations and other potential safety issues.

Future needs include developing further understanding and insight into the risks that need to be addressed by SFCs that are scaled as the ecosystem and its associated architecture evolve towards increasing complexity. This can be progressed through different use case scenarios that involve different risks, assess SFCs that may be common across use cases, and design and operational conditions that could drive requirements for SFCs unique to particular use cases.

Further development of the IASMS ConOps and the distributed architecture of SFCs could examine implications of how increasing complexity would change human-automation teaming. For example, SFCs could include safety nets with buffers to define and protect the envelope of human performance capabilities and limitations as well as the cognitive requirements derived from different levels of complexity.

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] 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.

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

[4] International Civil Aviation Organization, "Safety Management, Standards and Recommended Practices–Annex 19," in Convention on International Civil Aviation, 2nd Edition, 2016.
[5] 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.
[6] 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.
[7] Federal Aviation Administration, "Unmanned Aircraft Systems (UAS) Traffic Management (UTM) Concept of Operations v2.0," FAA, Washington, DC, 2020.
[8] Ellis, K., Krois, P., Koelling, J., Prinzel, L., Davies, M., Mah, R., "A Concept of Operations (ConOps) and Design Considerations for an In-time Aviation Safety Management System (IASMS) for Advanced Air Mobility (AAM)," AIAA SciTech, 2021.
[9] Endsley, M. R., & Kaber, D. B. (1999). "Level of automation effects on performance, situation awareness and workload in a dynamic control task." *Ergonomics, 42*(3), 462-492. https://doi.org/10.1080/001401399185595
[10] National Transportation Safety Board, "2021-2022 Most Wanted List of Transportation Safety Improvements." Accessed at www.ntsb.gov/safety/mwl/pages/default.aspx.
[11] National Transportation Safety Board, "Aviation Accident Final Report." Accident Number: ERA20MA001, Washington, DC, 2021.