In-Time System-Wide Safety Assurance (ISSA)
Concept of Operations

Introduction, Risk Identification and Prioritization

Introduction

Emerging operations involving Urban Air Mobility (UAM) poses a challenge to safety assurance and accessibility to the 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 an In-time Aviation Safety Management System (IASMS) Concept of Operations (ConOps) for a scalable UAM along with a service-oriented architecture. This architecture would better focus safety investments for technological solutions that overcome safety related barriers for emerging operations. By working with industry, consensus can be reached on desirable system traits that are based on integration 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.

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. - (NAR pg 2)

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 (NASA, 2017). 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 is defining the scope, functionality, and technical challenges required for an integrated IASMS. 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 that provide monitor, assess, and mitigate services to provide safety assurance of 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. NASA will survey stakeholders during the August Autonomy Workshop and solicit operational recommendations.

The scope of the ISSA ConOps and relative reference to other facets of air transportation safety is framed by the ICAO definition of the overall Safety Management System (SMS), as shown in Figure 1. This figure shows the relationships of IASMS and ISSA within the SMS as a whole.

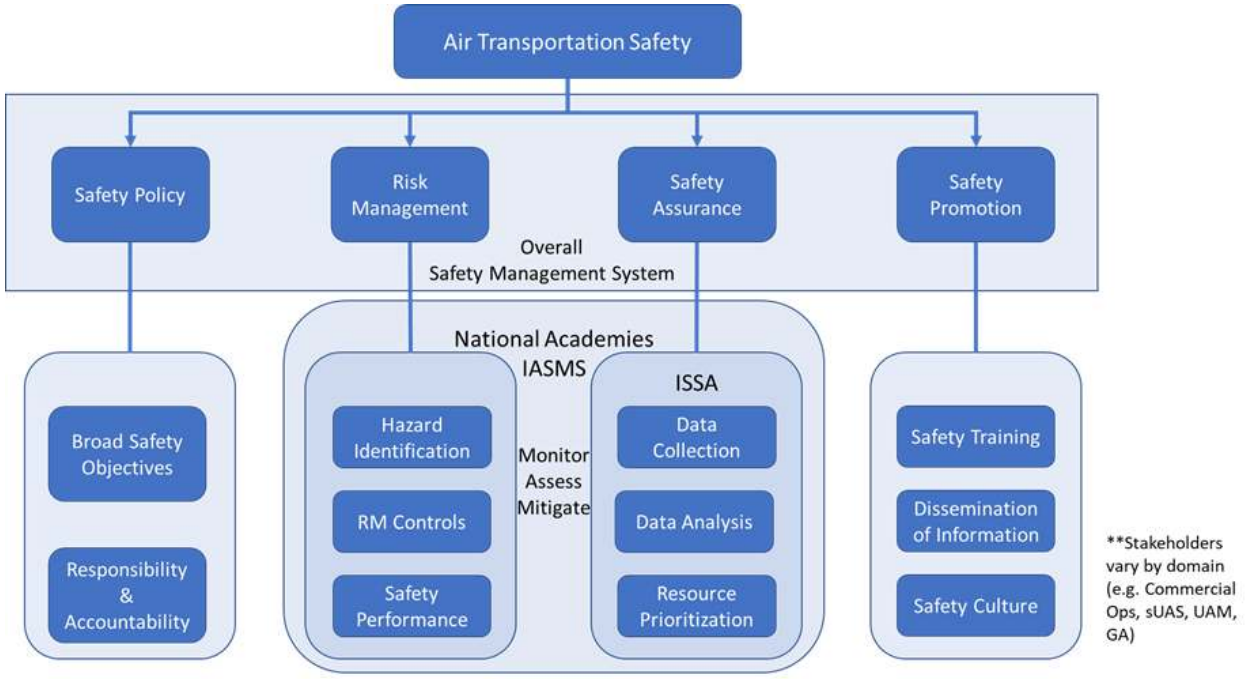

Figure 1. ICAO Safety Management System.

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 national airspace system, 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. - (NAR pg 3)

Vision of an In-time Aviation Safety Management System

1. 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 so on, and then assess that data, as follows:
    a. Assess data on a second-by-second, minute-by-minute, and hour-by-hour basis to detect or predict elevated risk states based on rapid changes in system status. (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.
    b. Assess data over periods of days to detect risks based on longer-term trends.
    c. Detect and predict elevated risk states that arise from a confluence of factors, none of which by itself would be noteworthy.
    d. Assess data in the context of 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.
    e. Assess system outputs over long periods of time to identify emergent risks that in some cases should be added to the list of risks that the system is designed to monitor.

2. 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. An IASMS will not be designed to recommend safety assurance actions that would occur over a period of weeks, months, or longer, such as changes to pilot training programs, operational procedures, equipment design, or the content of scheduled maintenance checks. The output of an IASMS, however, may be useful to those who are responsible for these longer-term areas of interest.

3. Safety assurance actions generated by an IASMS may take the form of recommendations that operators take action. In some cases when urgent action is required, IASMS may be designed to initiate safety assurance actions on their own.

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 identify 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 the future ISSA system will operate on a functional level and will define the issues that an IASMS will address. The ISSA ConOps will identify the key technical and policy issues that may impact the industry's ability to develop and integrate IASMSs in the existing NAS and its operational sub-elements. Most importantly, the primary intent of the ISSA ConOps is to manage the cost/complexity of IASMSs, primarily through prioritization of risks requiring mitigation. 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 this ISSA ConOps includes consideration of aircraft types, including new entrants across aviation domains (i.e. traditional scheduled operations, small UAS, etc). Across aircraft type and operational domains, the ISSA ConOps considers the data requirements necessary to enable an effective prototypical IASMS, and to identify known and emergent risks. Other considerations include cross-references to other ConOps: including the UTM ConOps (published reference) and the UAM ConOps (currently in development) to incorporate future operations in 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 scalability of the proposed systems. This means that the ConOps must be iterative in nature so that future adaptations may be made as technology advances to solve increasingly complex system challenges. Scalability includes 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.

The ConOps takes further consideration of the following:

- Ability to collect, share, protect, manage, and assure the quality of required data
- Architecture and NAS evolution
- Effectiveness comparing costs and benefits
- Human performance limitations and human-machine roles
- System authority vis-a-vis human performance capabilities and limitations
- Interoperability with legacy ATM systems and procedures

- Interoperability with legacy ATM systems and procedures
- Interoperability with legacy Flight Deck systems and procedures
- Transition path, SMS to IASMS
- Technical capabilities
- Uncertainties associated with each functional element of the generic ConOps
- Verification, validation, and certification

Users of the ISSA Concept of Operations

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 (FAA, 2018).

1. **Public consumers of UAM businesses**.
2. **UAM 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 UA 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 UA. 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 aircraft at different, but sequential times during the flight, provided at least one person is responsible for the operation at any given time. The RPIC may be located at a **Ground Control Station (GCS)**.
4. **USSs.** A 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. 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, and (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 network of USSs to provide cooperative management of low altitude operations without direct FAA involvement. USS services support operations planning, aircraft de-confliction, 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 mostly likely their supporting USSs share data or interact with one another (e.g., USS makes intent (or other) information available to all of the other USSs). 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 de-confliction 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.
6. **SDSPs**. USSs can access 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., public/private internet sites**).**
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 is the UTM component the FAA will build and manage to support UT0M operations.
8. **FAA.** The FAA is the federal authority over aircraft 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) 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**
11. **Pilots, e.g., commercial, GA, rotorcraft**
12. **Maintenance personnel**
13. **Weather forecasters**
14. **Vehicle and system design engineers, and test engineers**
15. **Members of Standards Committees**
16. **IASMS safety experts (e.g., ASIAS-like analysts for post-flight data fusion and analysis)**
17. **FAA Air Traffic Organization personnel (e.g., air traffic controllers, airspace and procedures specialists)**
18. **State and local officials**

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.

Our delineation of ISSA safety critical risks was informed by an integration of multiple sources of expert reference. These sources of expert reference represent different perspectives on UAM and IASMS. Some identified risks were common across two or more sources, while in other instances a source because of its unique perspective identified additional risks. Young (2018) classified these risks as safety risk outcomes or causal/contributing factors to those outcomes.

The three safety risk outcomes identified by Young and others (2018) are shown in Table 1.

Table 1. Identification and Alignment of Safety Risk Outcomes from Different Sources.

Source of Expert Reference	**Safety Risk Outcome Examples**		
DASC Paper - Young et. al., 2018 **and** **ConOps Dev Team**	*Flight Outside of Approved Airspace*	*Unsafe Proximity to People or Property or Other Vehicles*	*Societal Risk Outcomes:* Lack of Public Trust -> Limited access to airspace Increased regulations Reduced/Limited Market Growth Increased Operational Costs Litigation
National Academies report	Known Risk	Known Risks	Societal Risks due to societal concerns. This most commonly occurs after a high-profile accident.
Autonomy Workshop Group	Differences in how static and dynamic hazards may be displayed (things might not show up on google maps --> dynamic) Clearing the airspace due to an emergency	Loss of detect and avoid systems (UAS, people, obstruction) Midair collisions at a low altitude (rogue UAS, obstruction) Ground based collision (UAS, people, obstruction)	
FAA UTM Concept of Operations		Collision Avoidance - In the UTM environment, BVLOS UAS share responsibility with other BVLOS UAS	

		and manned aircraft for collision avoidance TCLs - are staged based upon four risk-oriented metrics: the number of people on the ground, the amount of property on the ground, the number of manned aircraft in close proximity to the UAS operations, and the density of the UAS operations.	
Webinar - Risk ID Sept 26th			

The causal or contributing factors are shown in Table 2a through 2f. The first three factors were identified identified by Young et.al., (2018) and the remaining three factors were identified in a mix of the National Academies report (2018) and the Autonomy Workshop Group.

Table 2a. Identification and Alignment of Causal or Contributing Factors for Critical System Failures.

Source of Expert Reference	**Causal or Contributing Factors:** **Critical System Failures**
DASC Paper - Young et. al., 2018 and ConOps Dev Team	Including loss of link, loss or degraded GPS, loss of power, and engine failure.
National Academies report	Known Risks
Autonomy Workshop Group	
FAA UTM Concept of Operations	
Webinar - Risk ID Sept 26th	Long list of failsafe conditions - take a look at these. There are some related to rotorcraft and others. FAA handbook. Historical data collection methods - is there a need to collect UAS/UAM FOQA type data? Sensor failures - Weather interaction and relative vehicle performance - general weather, micro weather in urban environment (city winds) - need for new weather models. Data collection of -> Icing, battery performance impacts, precipitation impacts,

	Do we need the raw data or do we need performance capability information to drive the system? The vehicle based IASMS can be owned by the operator and not share but perhaps they must simply communicate their capabilities based on their own assessment. Environmental - Risk to People (pop density under the flight path) modeling the movement of people on the ground. Sensors/data/model required? NASA is working this on some level. Environmental and Airspace concerns/risks are a more easily agreed upon thread to work as opposed to vehicle. Focus on Performance Goals and Metrics to collaboratively define reqs. Are these error rates or metric thresholds to meet? Analogy to commercial ops… discuss contingencies etc to dispatch is a req. The sharing of the performance specifics is not required to be shared. The USS or Operator itself will be responsible for hosting the appropriate IASMS capability and share the analyzed output to discuss performance and alternatives with appropriate agents within the overall system. There is an expectation that a service will be available to handle flow management in the airspace/terminal/vertiport area. Is it possible to have a shared model across the agents… a partitioned IASMS. Vendor - User - USS to share information to create a model to do the necessary function of the IASMS. Modelling needs for system performance - battery, aerodynamic, weather interactions/effects, RIsk: Machine Learning certification and capabilities definition/assurance. Non-deterministic system certification in general - G34 committee. Human Automation Teaming - The balance between operational authority in automation vs human and who is responsible.

Table 2b. Identification and Alignment of Causal or Contributing Factors for Loss-of-Control.

Source of Expert Reference	**Causal or Contributing Factors:** **Loss-of-Control**
DASC Paper - Young et. al., 2018 and ConOps Dev Team	Including envelope excursions and flight control system failures.
National Academies report	
Autonomy Workshop Group	
FAA UTM Concept of Operations	
Webinar - Risk ID Sept 26th	

Table 2c. Identification and Alignment of Causal or Contributing Factors for Cyber Security Risks.

Source of Expert Reference	**Causal or Contributing Factors** **Cybersecurity Related Risks**
DASC Paper - Young et. al., 2018 and ConOps Dev Team	Cybersecurity related risks - referenced but unspecified
National Academies report	CYBERSECURITY RELATED RISKS: Emerging Risks like cyberattacks Breach of data management firewall exposing PII
Autonomy Workshop Group	Security Issues Digital Hijacking Cybersecurity attack Crypto key management Phishing attack directed at operators (easiest thing for a hacker to do)
FAA UTM Concept of Operations	Security - refers to the protection against threats that stem from intentional acts (e.g., terrorism, or unintentional acts, such as human error or natural disasters affecting aircraft, people, and/or property in the air or on the ground).
Webinar - Risk ID Sept 26th	

Table 2d. Identification and Alignment of Causal or Contributing Factors for Physical Security Risks.

Source of Expert Reference	**Causal or Contributing Factors** **Physical-Security Risks (Intentional OR Unintentional)**
National Academies report	PHYSICAL SECURITY RELATED RISK: Emerging Risks like instability of human operators, an emergent risk could mimic one or more known risks, and new entrants (UAS, ODM, commercial space)
Autonomy Workshop Group	Heterogeneity of Vehicles and Algorithms (different vehicles work in different ways, different hardware & software) Counter drone systems used by malicious operators Weather/wake issues Inexperienced Pilots/poor training Physical Hijacking Cargo weight, size, shape Inflight medical emergency (psychological vs. physical), passengers & crew Hostile property owners (get out of my airspace) & people on the ground (possibly fixed by dedicated emergency landing zones) Amateur/non-communicating operator flying in controlled airspace Vandalism: Teenagers throwing things / intentional damage to vehicle/operational system Lasers

FAA UTM Concept of Operations	
Webinar - Risk ID Sept 26th	

Table 2e. Identification and Alignment of Causal or Contributing Factors for Regulatory Risks.

Different Sources	**Causal or Contributing Factors** **Regulatory Risks**
National Academies report	Referenced at high level
Autonomy Workshop Group	Position certification requirements: Manning operator certification New entrants without appropriate aircraft type designations Drone umbrellas Intentionally ignoring or violating regulations Lack of enforcement capability
FAA UTM Concept of Operations	
Webinar - Risk ID Sept 26th	What is the appropriate safety margin for UAS/UAM operations? For vehicle, for USS, for people on the ground… What is the right role for NASA here? -> Determining safety margins for operational IASMS capabilities. MASPS for UAS / UAM.

Table 2f. Identification and Alignment of Causal or Contributing Factors for Safety Culture.

Different Sources	**Causal or Contributing Factor for Safety Culture**
National Academies report	
Autonomy Workshop Group	Profitability vs. Safety trade-off Aggressive business model Culture shift/clash
FAA UTM Concept of Operations	
Webinar - Risk ID Sept 26th	

Prioritizing Risks

The National Academies IASMS report underscored the importance of prioritizing risks, with the risks having the most impact on system safety commensurate. Addressing higher priority risks balances the safety benefit with the cost of risk mitigation while considering the complexity of the system.

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.

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 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.

The National Academies report provided a set of IASMS criteria for risk prioritization. These criteria can be applied to the Causal and Contributing Factors. The use of the IASMS criteria for rating the level of uncertainty with the set of 3 Causal or Contributing Factors is shown in Table 3. In this assessment, uncertainty can range from low with a score of 9 to high with a score of 27.

Table 3. IASMS-Based Criteria for Prioritization of Causal and Contributing Factors (levels of risk uncertainty: 1=low, 2=medium, 3=high).

	Causal and Contributing Factors (Example using Steve Young's DASC paper)		
IASMS-Based Criteria	Critical System Failures (including loss of link, loss or degraded GPS, loss of power, engine failure)	Loss-of-Control (including envelope excursions and flight control system failures)	Security Threats - Cybersecurity Related Risks Physical-security Related Risks (Intentional OR Unintentional)
Traditional: Consequence	H (if outside USS but M if within US)	H	H
Traditional: Probability	M (need data)	M	M
Experience with Hazard	M (for some experience; how much is experience with GA & commercial applicable to UAS?)	M	H
Detectability by monitoring data to detect elevated risk	L (assume GPS data to USS)	M	H
Mitigation Viability	L (for voice)	L	H
Cost of mitigation	M (for auto landing)	L	H
Undesirable secondary effects	L	H	H
Societal risk	H (for airport intruder or rogue)	H	H
Other for ISSA	H (for Pop-up)	M	M
Priority Score	18	19	25

Risk Discussion

Overall, the above tables respond to the recommendation within the National Academies report that NASA identify and prioritize the risks assessed and mitigated by the ISSA system. Tables 1 and 2 identified the risks with UAM. Tables 3 provided an initial assessment of the priority of these risks based on the levels of uncertainty with risk information and assessment.

This information is important in developing the ISSA concept of operations including the data and architecture necessary for the functions comprising ISSA. With this information NASA can continue to collaborate with industry 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.

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 is to derive the necessary services to enable operations in the "most challenging case at the highest level of autonomy". Therefore, the scope of possible IASMS services pertains to the domain of low-altitude urban flight. 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' is OK to 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

What the services do? These services provide real-time information and data on vehicle state, known hazards, safety risks, and causal and contributing factors to safety risks.

When the services do this? 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, and days to months depending on the data monitored, risks assessed, and actions required for mitigation.

Who uses these services? These services are envisioned to be used in their entirety or in part by any of the entities listed in section XX above called *Users of the ISSA Concept of Operations*. Some of these entities and their definitions are taken from the UTM Concept of Operations (FAA, 2018).

1. **Public consumers of UAM businesses**.
2. **UAM operators, e.g., cargo carriers.**
3. **Remote pilot in charge (RPIC)**. The RPIC may be located at a **Ground Control Station (GCS)**.

4. **USSs.**
5. **USS Network**.
6. **SDSPs**.
7. **Flight Information Management System/FIMS.**
8. **FAA.**
9. **Ancillary Stakeholders.**
10. **Vertiport operators**
11. **Pilots, e.g., commercial, GA, rotorcraft**
12. **Maintenance personnel**
13. **Weather forecasters**
14. **Vehicle and system design engineers, and test engineers**
15. **Members of Standards Committees**
16. **IASMS safety experts (e.g., ASIAS-like analysts for post-flight data fusion and analysis)**
17. **FAA Air Traffic Organization personnel (e.g., air traffic controllers, airspace and procedures specialists)**
18. **State and local officials**

Key IASMS Services

Three service categories were identified by Young and others (2018) as key to an effective IASMS consisting of monitor, assess and mitigate. These categories span the three functions comprising the IASMS concept described in the National Academies IASMS report (2018).

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 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 (*known and unknown*) 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.

Several relevant information classes exist that are necessary to provide the data necessary to enable the IASMS capabilities. Figure 2 below identifies the information classes available; data classes either singularly or in combination can be used to generate an IASMS capability. These services and capabilities are described in greater detail below as part of the Monitor, Assess, and Mitigate functional services. The monitoring function is comprised of information services that provide data from the classes listed below in Figure 2. The assess function leverages tools and techniques to create models that can judge changes to operational safety margins. applied to the monitored data based on the overall system requirements and data architecture. The mitigate function is the method for multiple agents or

automated capabilities to execute a timely response when safety margins fall below acceptable levels. (Young., et al, DASC 2018).

The timeline of each service and corresponding IASMS capability depends on the type of safety assurance action necessary and will vary depending on the source of information available. When considering the timeline, there are three categorical types of services that address the critical needs for safety assurance, which are referred to as SDS-R, SDS-X, and SDS-S. 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.

SDS-R type services are near real-time services. 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. All three service categories are capable of interacting independently but function more effectively through interconnectivity of shared information.

SDS-S type services include post-flight data analytics that range from services that exist today such as Flight Operations Quality Assurance (FOQA) and the Aviation Safety Reporting System (ASRS), to future prognostic capabilities. Future capabilities may evolve to evaluating system-wide operational trends in increasingly near-real time, as well as validate performance models that leverage increased levels of autonomy.

Inclusion of 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 ingests power health information as well as aircraft model data and population density can leverage all 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. To account for safety assurance amidst the growing scale and complexity of operations, IASMS service capabilities must at a minimum communicate between other IASMS service capabilities or include multiple information classes to take informed mitigation responses. Therefore, it is envisioned that the risk reduction of an IASMS capability is on a continuum that corresponds with the information it ingests and the possible mitigation responses it can generate.

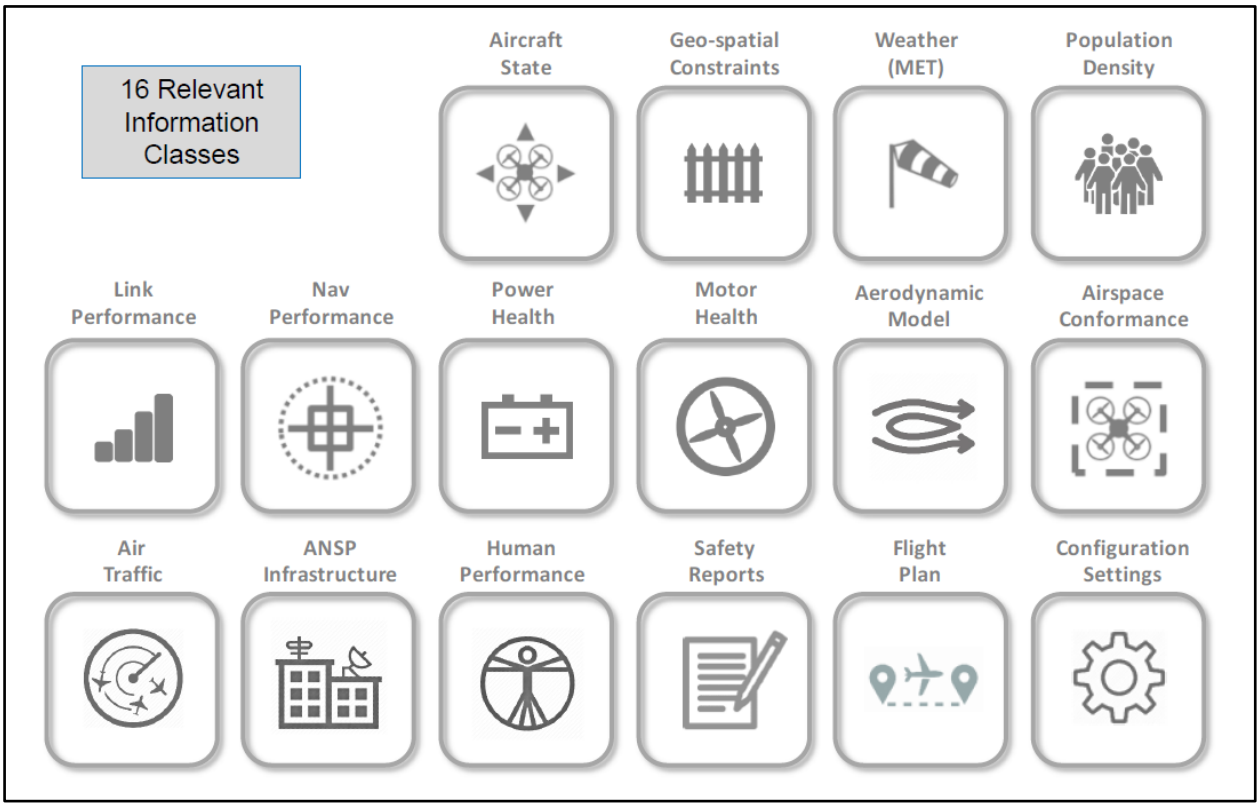

Figure 2. Information classes to generate IASMS service capabilities (Young., et al, In-Press 2019).

Monitor Function and Data Services - Categories of Service Types

The Monitor Function and Data Services are used by predictive models addressing each safety critical risk. These models can operate at different update rates and data resolutions (e.g., level of accuracy), 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 (Uber, 2016).
- 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's 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 (2019) specified several models that would be part of the ISSA ConOps. These models consist of the following:

- Aircraft aerodynamic model
- Geo-spatial feature model
- Weather forecast model
- Link performance model
- Navigation system performance model
- Battery performance model
- Engine performance model

The specification of predictive models and data including synchronization and interaction between services may vary based on operational state of 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 on IASMS (2018) posed use of IASMS data and large-scale data analytics to monitor for systemic or anomalous changes to the NAS. Data resources include 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 class source include:

- **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 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 be referenced such as DO-364, Minimum Aviation System Performance Standards for Aeronautical Information/Meteorological Data Link Services Services (RTCA, 2016), and DO-200B, Standards for Processing Aeronautical Data (RTCA, 2015). 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 will be necessary to provide the necessary design criteria and guidance. As the complexity of operations in the NAS evolves, different approaches should be examined ranging from relatively simple methods based on exceedance criteria to more complex model-based methods, conformance methods, and statistical methods. 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.

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.

<u>Assess Function and Data Services</u>

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 reported by Spirkovska and others (2017) as a parallel to the FAA's Integrated Safety Assessment Model (ISAM).

Three Assess function categories were identified by Young and others (2018):

- SDS-R performs a continuous and rapid real-time risk assessment on the scale of seconds to minutes and based primarily on aircraft state, vehicle system states, weather factors, and population density in the region of flight. UTM Services could include Registration Service and Discovery Service along with Separation Services involving Strategic Deconfliction, Conformance Monitoring, Conflict Advisory and Alert, and Dynamic Reroute Services (FAA, 2018). 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 (Rios, 2018).
- SDS-X provides information relative to air traffic and airspace constraints on the time scale of seconds to minutes to hours. This capability is more oriented towards the airspace and may include position reports, warnings, and/or advisories. The information would be part of the UTM design with information and data provided by the USS. New SMS capabilities would be added as UTM operations evolve. UTM Services could include Airspace Authorization, Restriction Management, and Flight Planning Services (FAA, 2018). An additional service could include Tactical Separation Provision – Surveillance Service, Ground Surveillance, Detect and Avoid (Rios, 2018).
- SDS-S is envisioned as a service that would provide an overarching report and assessment of the evolution of safety risk vis-à-vis a desired safety margin. SDS-S would be on a time scale of hours to days to months reflecting system-wide assessments. This capability would use outputs from multiple services 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 ASIAS, FOQA, and ASRS. 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 noncausal 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. Computational architectures will need to be developed for data input and output devices, processing capabilities, and storage. These architectures will need to be able to work with high-volume and high-speed streaming of data from multiple data sources as well as meet the requirements of the consumers of various components of the data.

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.

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.

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.

Regarding the IASMS multi-dimensional view that shows how services interplay with risks, phase of flight, levels of autonomy, hazards, vehicle state, and transition paths, these comments included the following:

- A comment was that the material was well laid out and interpretable. A concern was raised about how compliance will be measured in terms of the thresholds to trigger risks.
- A concern was raised about what separation standard will be used for mixed aircraft operations. For this airspace no radio communication is required.
    - Separation could be based on pre-declared trajectories such as with the use of terminal STARS airspace. This could lead to an RNP-like requirement such as for use of corridors.
    - The recent Berkeley UAS conference addressed closer separation as a way to manage traffic to vertiports.
- The concept of operations should consider the ecosystem of the vehicle with the increased aggregation of services.
- It was noted that the transition paths shown at the bottom of the slide represent categories of change.
- The Mitigate and Implement Services are important to safety assurance and could include contingency operations to deconflict localized conflicts.
- Mixed aircraft operations could include use of a best equipped, best served approach.
    - Legacy operators such as tour helicopters would want equitable treatment, which could be another transition path.
    - 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.
- It was noted that a requirement is needed to fill the gap for weather effects.
- Participants addressed the question about what NASA's role should be in addressing these issues including by noting that government does not need to address all the questions whereas public-private partnerships could be used.

Regarding safety risks addressed by IASMS functions, these comments included the following:

- There was discussion whether the ConOps should include emergency conditions such as failed motor or uncontained engine failure.
- Consider whether the ConOps identifies additional risks such as from mitigation of risk from use of RNP.
- The recent Berkeley UAS conference addressed vehicle sovereignty vs ground systems in terms of where software capability is located. Vehicles should as an end state have the software and models to operate independent of ground systems.

- 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 comm system would need to change. Further, other nearby vehicles may also lose their comm 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), these comments included the following:

- A question was whether the Monitor services should include independent surveillance.
- It was noted that services similar to the 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. For example, what data are needed for a common situation awareness among operators.
- NASA noted that UTM is not intended to be the UAM traffic management approach. Rather, NASA is imagining a more service-oriented ATM sometimes referred to as "UTM-inspired ATM" as a more sophisticated 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 as an emergency condition use of a parachute such as if the UAS was carrying an elderly person.
- 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.
- Need to account for traffic load, route loading, and capacity changes to improve safety for vertiports.
    - Need a measure of risk for vertiports including to show how quickly it can change and the effects of mitigations.

Regarding information requirements between people, systems, and monitors, these comments included the following:

- Need to identify minimum capabilities for systems and equipment. Need to consider interconnectivity between services.
    - Change "Equipment Monitors" to "Monitor Services."
- Consider how Detect and Avoid would be added to the information requirements.

Data Requirements and Architecture

The National Academies IASMS report 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 IASMS report 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 approach 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. 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.

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 IASMS 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. 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. As part of these 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.

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 IASMS report noted that viable and effective methods should be developed for the timely detection and mitigation of elevated risk states for particular risk areas.

In sum, the National Academies IASMS report identified a complex landscape of data requirements and architecture necessary to in-time identification of critical risks safety and sufficient relative to operational complexity and cost effectiveness.

Principles and Traits

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

1. Use of a building block approach that is service-oriented and scalable.

2. The architecture should be open and extendible to address new risks or hazards as/if they are discovered.

3. Leverages and interoperates with existing relevant systems (e.g., SWIM and ATM/ANSP services).

4. Transformative from the existing NAS such that it does not involve a clean-slate design approach.

5. The approach should apply techniques that assure appropriate levels of data/information integrity.

6. Applies run-time assurance techniques including the reporting of system failures back to designers.

7. Supports isolation of flight-critical functions onboard to meet higher fail-safe assurance levels.

8. Supports functions that can bound the behavior of autonomous functions.

9. Service providers can be certifiable as “trusted sources.”

10. Minimizes exposure to cyber threats, e.g., by minimizing in-flight exchanges of critical data.

11. Data exchanges are protected and link agnostic (as long as exchanges meet quality requirements).

12. Combines SWIM-like connectivity and services with ASIAS-like analytics and processes.

13. Supported by a safety case for flight-critical elements, e.g. auto-mitigate functions.

14. Provides an incremental step to the larger IASMS concept described in National Academies report.

15. Supports current SMS processes.

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.

Notional Architecture

The notional architecture for the ISSA Concept of Operations is shown in Figure XX. The UAS Ground Station has a pivotal role as the conduit between the USS and other services with the vehicle itself. The vehicle provides data and event "logs" to the UAS Ground Station.

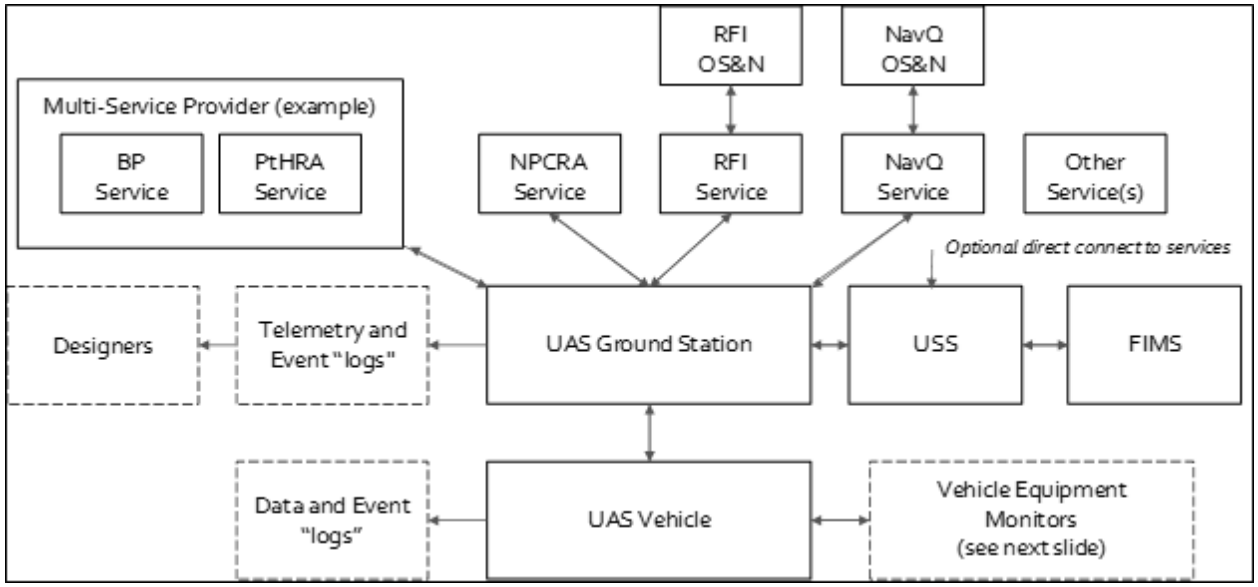

Figure XX. ISSA notional architecture.

The associated vehicle system monitors and their interactions are shown in Figure XY. These monitors collect data from vehicle systems and send it by downlink to the UAS Ground Station. Weather and other data can be uplinked to the vehicle directly depending on the service used by the operator.

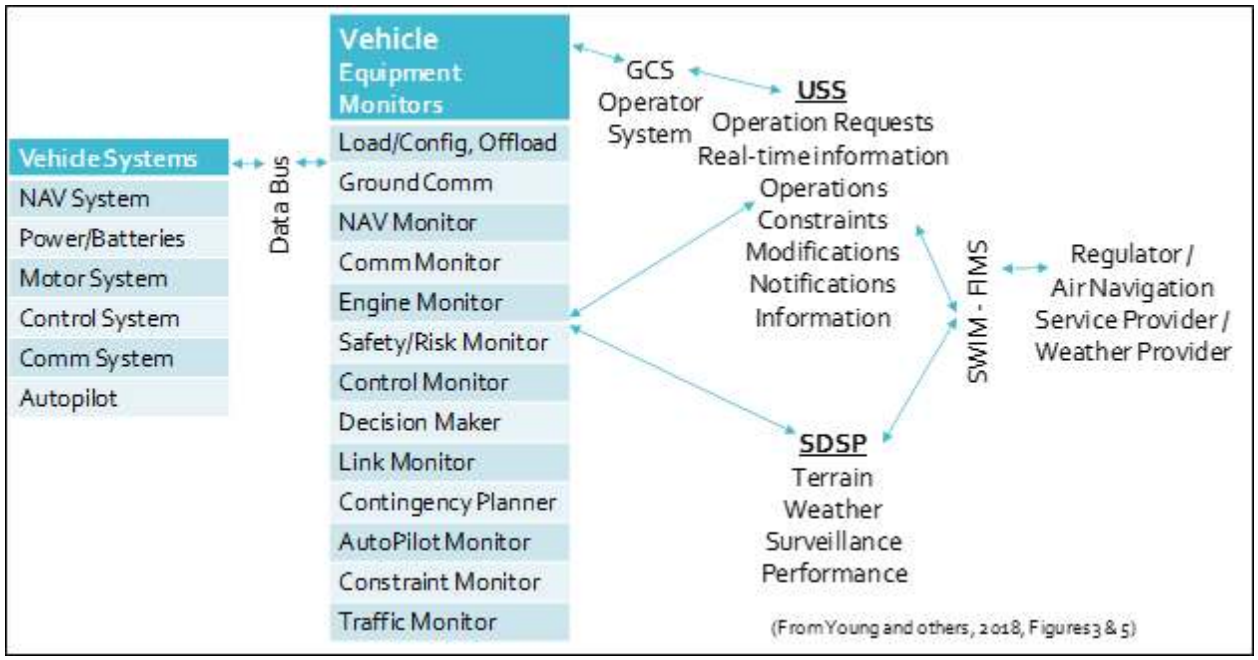

Figure XY. Vehicle equipment monitors and their interactions.

Integration with Existing ConOps Architectures

To accommodate to the identified principles and traits of IASMS capabilities, the notional architecture described above for the connected services should leverage the existing architectures that are already in place as well as those in development. Existing ATM architectures that are already in use today as well as the safety management systems that operate within that architecture provides 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 [RefX]. This leads to a UTM inspired ATM concept that IASMS capabilities and the functional services that drive them can operate across through system-wide networked services such as SWIM and FIMS. IASMS capabilities should be tailored to function within individual elements within notional architectures, such as the vehicle itself, the ground control station, the USS or AOC/IOC and have the built in responsibility to share operational risk assessment information and mitigation actions to the necessary stakeholders in the operational system it is operating within.

Depending on the operation, the vehicles and the managing USS or AOC/IOC 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. It is not expected that any operator subscribe to one pre-defined model for deployment of safety assurance services. It is the intent that the nature of

the operation should necessitate the need for the requisite level of operational assurance. Additionally, the level of acceptable risk as defined by the governing regulatory body will prescribe the necessary responsibilities to be addressed by an IASMS capability that reduces the operational risk for a given operation. For example, an operation that delivers lightweight packages has a different level of acceptable as opposed to an operation that is delivering an organ transplant. The level of operational and safety assurance of the latter operation is much more strict 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 and regulatory requirements.

Figure XX below depicts the interactive connections across the NAS and the traffic management 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 provide services for both scheduled and unscheduled services 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 of all traditional and emerging operations.

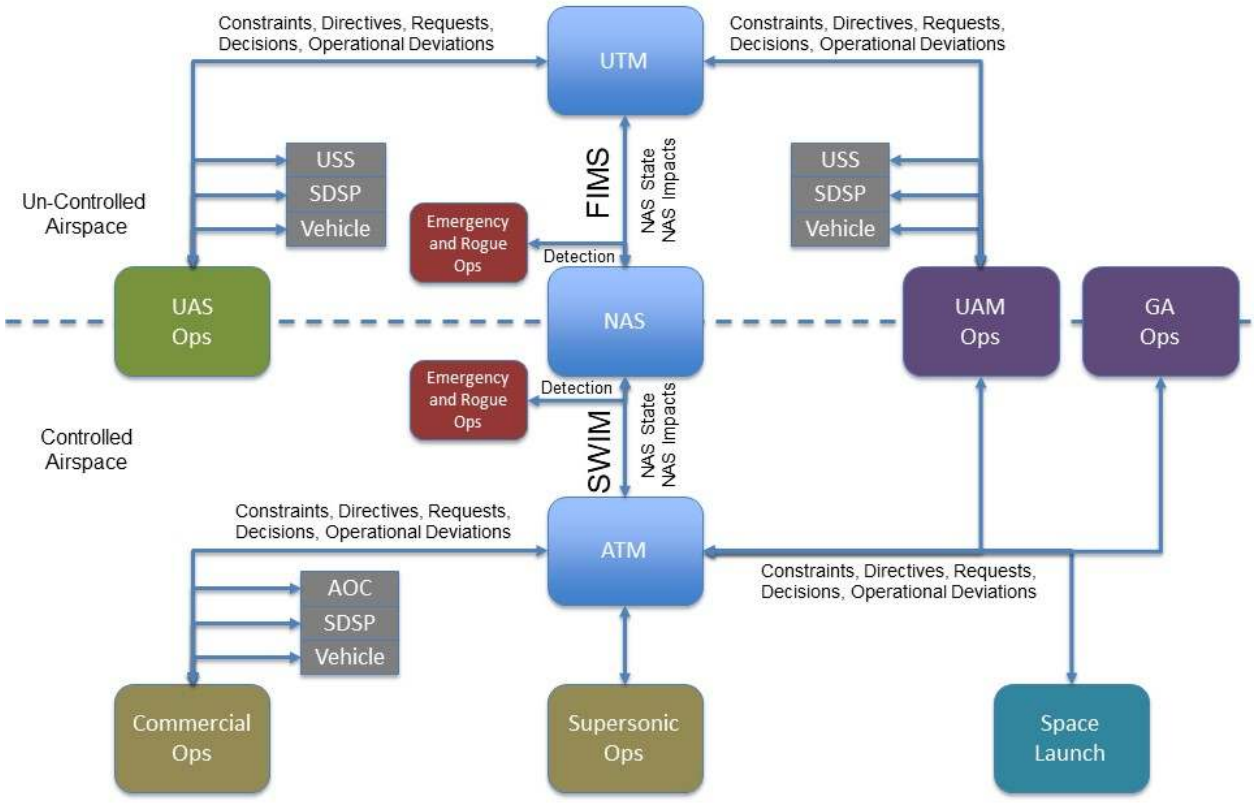

Figure xx. UTM inspired ATM for the National Airspace System

Figure XX below shows an example of distributed locations where IASMS capabilities may reside within the UTM architecture. The decision of when and where to place specific IASMS capabilities and which assortment of IASMS capabilities is driven by several factors. A limited list of the factors that inform the logical deployment of an IASMS capability is listed below:

- 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

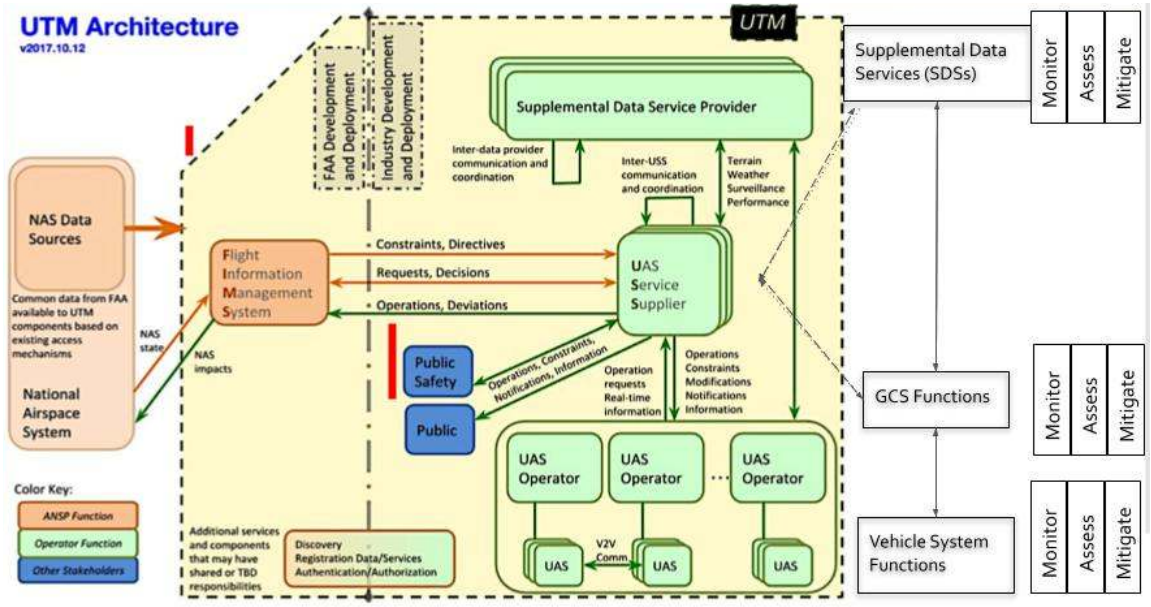

Figure xy. UTM Architecture with distributed IASMS Capabilities

A proposed model currently in use at NASA follows figure xy below. 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 necessary that is made available and is accessible to the monitor and assess functions of an IASMS capability. It is also assumed that for operations in mixed airspace that demand a more structured approach to scheduled operations, a connection to more traditional ATM will be required.

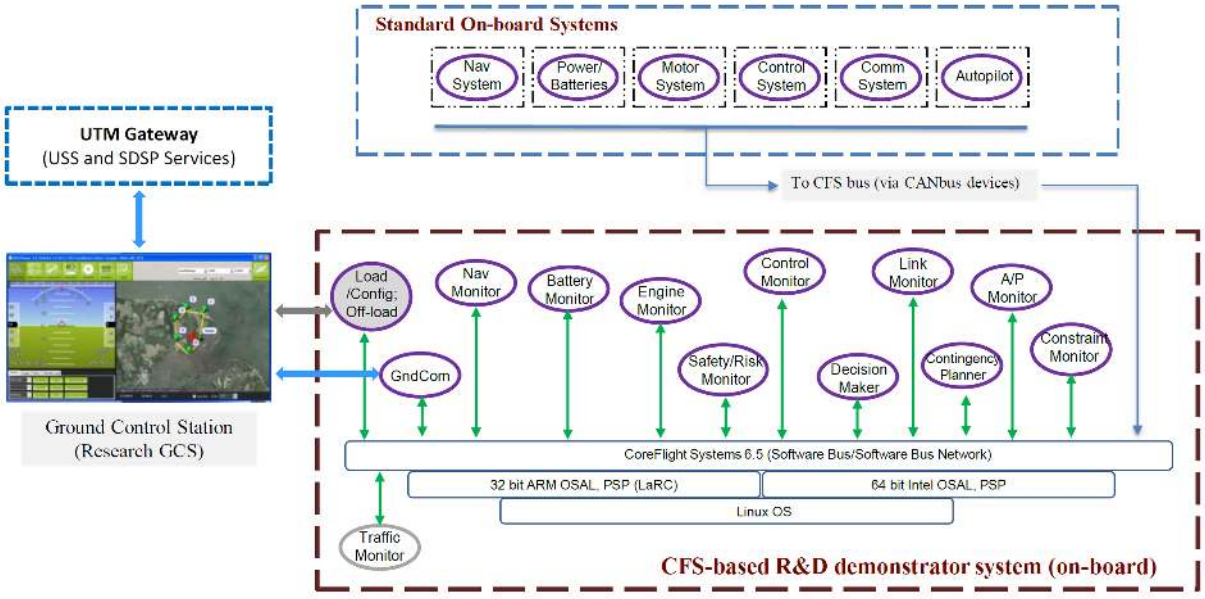

Figure xy. Vehicle system to GCS to UTM Gateway architecture for Testing In-Time System-Wide Safety Assurance Concepts [Ancel, et al 2019]

Information Requirements

Databases and Models

For the monitor and assess functions of an IASMS capability to function properly, several databases and models are required. The need for 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 and SDSP and made available as a monitor and assessment service, or it can simply be integrated into the 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 increasing density, 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, 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. A minimal set of various functional models are listed below:

- **Aircraft aerodynamic model**
- **Geo-spatial feature model**
- **Weather forecast model**
- **Population density model**
- **Link performance model**
- **Navigation system performance model**
- **Battery performance model**
- **Engine performance model**

The models indicated above address a variety of ISSA risks that should be considered when considering future emerging operations as identified in the Identification of Safety Critical Risks section.

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 a criteria to design toward. It is not expected to define the Minimum Aviation System Performance Standards (MASPS) and other recommendations or advisories (DO documents or Advisory Circulars) should be developed for safety critical IASMS capabilities and should address the following:

- **data quality requirements,**
- **redundancy requirements,**
- **verification and validation requirements**

There are several existing committees and organizations that are collaboratively working the standards and recommendations that regulatory bodies are seeking informed responses from.

Data Quality (and other relevant standards):

- **DO-200B, Standards for Processing Aeronautical Data**
- **DO-201B, User Requirements for Navigation Data**
- **DO-272D, User Requirements for Aerodrome Mapping Data**

- **DO-276C, User Requirements for Terrain and Obstacle Data**
- **DO-291C, Exchange Requirements for Terrain, Obstacle, and Mapping Data**
- **DO-324, Safety and Performance Requirements (SPR) for Aeronautical Information Services (AIS) …**
- **DO-349, Architecture Recommendations for AIS and MET Services**
- **DO-364, Minimum Aviation System Performance Standards for AIS and MET Services**
- **DO-369, Guidance for the Usage of Data Linked Forecast and Current Wind Information**
- **FAA Advisory Circular, AC 00-45H, Aviation Weather Services**
- **ICAO Annex 3, Meteorological Service for International Air Navigation**
- **ICAO Annex 15, Aeronautical Information Services**
- **ISO-9000 series, Quality Management Systems**
- **ASTM, F3269-17, Standard Practice for Methods to Safely Bound Flight Behavior of UAS**
- **[Others from FAA, ASTM, EASA, OGC, and ARINC}**

Use Cases

As described by Young and others (2018), use cases help illustrate the concept of operations and how its associated constructs are used. They noted that UAM and urban sUAS-based use-cases can vary with complexity and boundary conditions. Examples include the transport of goods/supplies, infrastructure inspection, fire department and law enforcement support, and air taxi. They used, as a low-complexity example to illustrate the concept of operations, the transport of medical specimens from a suburban medical office to a large downtown laboratory for testing at a hospital.

Use cases were also part of the FAA UTM Concept of Operations (2018). 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 (2018a; 2018b). 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.

References

Federal Aviation Administration (2012). Helicopter Flying Handbook. FAA-H-8083-21H.

Federal Aviation Administration (2018). Unmanned aircraft systems (UAS) traffic management (UTM) concept of operations v. 1.0. Retrieved from https://utm.arc.nasa.gov/docs/2018-UTM-ConOps-v1.0.pdf September 18, 2018.

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.

National Aeronautics and Space Administration (2017). NASA Aeronautics Strategic Implementation Plan. Retrieved from https://www.nasa.gov/sites/default/files/atoms/files/sip-2017-03-23-17-high.pdf.maspa

National Institute of Standards and Technology, Cognition and Collaboration Systems Group. Autonomy Levels For Unmanned Systems. Retrieved from https://www.nist.gov/el/intelligent-systems-division-73500/cognition-and-collaboration-systems/autonomy-levels-unmanned September 30, 2019.

Radio Technical Commission for Aeronautics (2016). DO-364, Minimum Aviation System Performance Standards for Aeronautical Information/Meteorological Data Link Services Services. Retrieved from https://global.ihs.com/doc_detail.cfm?document_name=RTCA%20DO-364&item_s_key=00701504.

Radio Technical Commission for Aeronautics (2015). DO-200B, Standards for Processing Aeronautical Data. Retrieved from https://standards.globalspec.com/std/9950777/rtca-do-200.

Rios, J. (2018). UAS Service Suppliers: Development of specifications, tests, and implementations in parallel. Presentation at the FAA V&V Summit, September 16, 2018. Retrieved from https://www.faa.gov/about/office_org/headquarters_offices/ang/offices/tc/library/v&vsummit/v&vsummit2018/presentations/3%20Joseph%20Rios%202018%20V+V%20Summit%20v20180916.pdf

Spirikovska, L., Roychoudhury, I., Daigle, M., and Goebel, K. (2017). Real Time Safety Monitoring: Concept for Supporting Safe Flight Operations. Proceedings of AIAA AVIATION 2017, AIAA-2017-4494, Denver, CO, June 5-9, 2017. Retrieved from https://ntrs.nasa.gov/archive/nasa/casi.ntrs.nasa.gov/20180006997.pdf

Uber Elevate (2016). Fast-Forwarding to a Future of On-Demand Urban Air Transportation. October 27, 2016. Retrieved from https://www.uber.com/elevate.pdf

Unmanned Aircraft System Traffic Management (UTM) Research Transition Team, Concept Working Group. (2018a). Concept & Use Cases Package #2: Technical Capability Level 3, Version 1.0. FAA and NASA.

Unmanned Aircraft System Traffic Management (UTM) Research Transition Team, Concept Working Group. (2018b). Concept & Use Cases Package #2 Addendum: Technical Capability Level 3, Version 1.0. FAA and NASA.

Young, S.D., Quach, C.P., Goebel, K., and Nowinski, J. (2018). In-Time Safety Assurance Systems for Emerging Autonomous Flight Operations. 37th AIAA/IEEE Digital Avionics Systems Conference, London, UK, September 23-27, 2018.

Ancel, E., Foster, J., and Condott, R. (2019). In-Time Non-Participant Casualty Risk Assessment to Support Onboard Decision Making for Autonomous Unmanned Aircraft. AIAA Aviation, Dallas, TX, 17-21 June, 2019.

List of Acronyms

RTT	Research Transition Team
UAS	Unmanned Aircraft System
UTM	Unmanned Aircraft System Traffic Management