# TRUSTED INFORMATION INTEGRITY AS AN ENABLER OF AUTONOMOUS AVIATION SYSTEMS

**Alexander R. Murray**

*(Aerospace Solutions Architect and Research Lead – Noblis, Inc.)*

**Andrew R. Lacher**

*(Director, Aerospace Systems Research Center – Noblis, Inc.)*

Information integrity becomes increasingly critical as automated systems become less reliant on human oversight and their ability to ensure information is suitable for its intended use. As more responsibility is delegated to autonomous agents, there will be a need to calibrate trust of the information used to conduct intended functions. Information integrity is key to trust and any reduction in integrity needs to be factored into an autonomous agent's decision logic. This paper presents the need and concept for establishing an information integrity framework to enable increasing autonomous aviation systems in an environment with multiple information service providers that may include both trusted and unknown providers. This paper introduces five pillars of information integrity.

## INTRODUCTION

There are efforts across the aviation community to increase the level of automation associated with operations, whether it be to simplify flight controls of piloted aircraft or eventually to have unmanned aircraft automatically delivering parcels and eventually people. This future will be enabled by increased automation both on-board aircraft and on the ground. Ground systems will include Air Navigation Service Provider (ANSP) systems, systems managed by the aircraft operator (e.g., fleet operations systems), and third-party automation systems [e.g., Unmanned Aircraft System (UAS) Traffic Management – (UTM)]. These distributed decision systems will be sharing information in real time. More importantly, they will depend upon information shared with them and from their own sensors to make decisions and take actions that could impact the safety of flight.

Fundamental to ensuring trust in increasingly autonomous flight operations will be the integrity of information flowing among distributed decision-making entities including aircraft, ground infrastructure, and human decisionmakers. Autonomous machines, or agents, require information to support their decision-making processes just as humans do. Integrity of the information exchanged between agents, both machine and human, is critical to the ability for such agents to make trustworthy decisions. An agent that makes decisions on information with poor integrity can result in uncertain and undesired outcomes leading to mistrust in the system. Mayers et al. states that "the relationship between integrity and trust involves the trustor's perception that the trustee adheres to a set of principles that the trustor finds acceptable." [Mayers et al., 1995] While Mayers et al. is speaking to the trust relationship between people, the same relationship exists in the exchange of information in machine-to-machine and human-to-machine relationships. The

 

integrity-trust relationship depends on the adherence to a predefined set of principles that is deemed acceptable.

This paper discusses the current efforts to enable and integrate autonomous flight operations into the National Airspace System (NAS) as detailed in the Federal Aviation Administration (FAA) and National Aeronautics and Space Administration (NASA) operational concepts for UTM, Urban Air Mobility (UAM), and Upper E Traffic Management (ETM). In all these concepts there is a dependency on the use of third-party, i.e., non-governmental, service suppliers which further increases the importance of information integrity. A framework for ensuring information integrity necessary to enable autonomous flight operations is then presented. The information integrity framework includes methods to describe the integrity of information obtained from various sources and provides autonomous and/or human agents with a means to ensure information is applied according to required performance criteria or adapt its operation to ensure safety is maintained.

## CURRENT ARCHITECTUAL CONCEPTS FOR UAS NAS INTEGRATION

Efforts to integrate remotely piloted and highly automated aircraft systems into the National Airspace have been in process for more than a decade. Organizations including NASA, FAA, academia, standard bodies, and industry have been working on how to initially accommodate with a path to full integration. Within the last year or so, NASA and the FAA have released several concepts of operation to accommodate UAM, UTM, and routine operations in Class E airspace above Class A (aka 'Upper E'). One thing all these concepts have in common is that they propose a new paradigm for how air traffic and air navigation information services (e.g., separation/deconfliction, terrain and obstacle data, specialized weather data, surveillance, constraint information) are provided to operators in the system where third-party suppliers deliver the required services for safe and efficient operations instead of the FAA. [FAA 2020, FAA 2020a, FAA 2020b, NASA-Deloitte 2021]

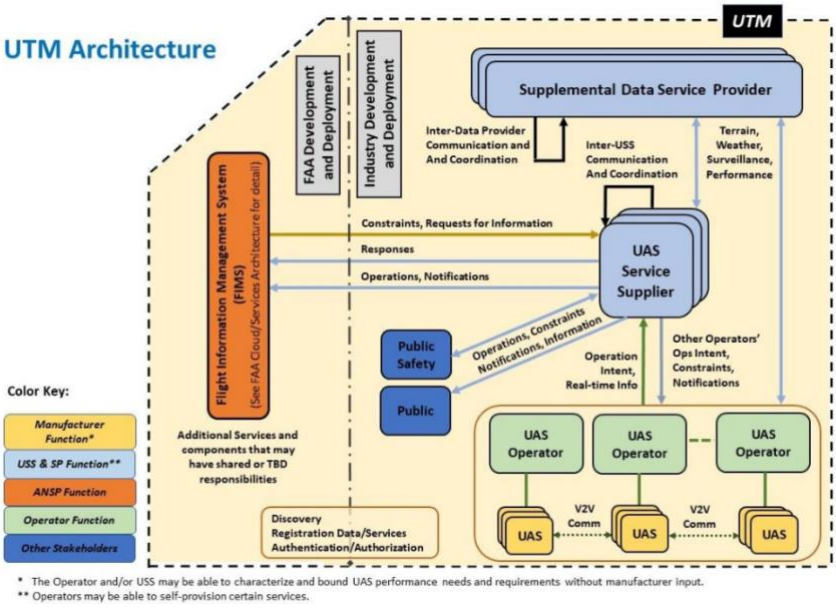


**Figure 1 - UTM Architecture from FAA UTM ConOps v2**

The FAA UTM ConOps v2 states that UAS Service Suppliers (USS) "provide the operator with information about planned operations in and around a volume of airspace so that operators can ascertain the ability to safely and efficiently conduct the mission." In this new approach, the

 

responsibility for the FAA shifts to developing rules, regulations, policy, and procedures as required to maintaining 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 primary reason for this shift is due to the fact the existing Air Traffic Management (ATM) system infrastructure and associated resources cannot cost-effectively scale to deliver services for small UAS operating below 400 feet Above Ground Level (AGL). The FAA UTM Architecture, shown in Figure 1, illustrates this shift from the FAA providing the majority of flight services to UAS Service Suppliers. [FAA 2020]

Urban Air Mobility (UAM) or the more expansive Advanced Air Mobility (AAM) is a concept for future mobility eventually involving fully autonomous aircraft transporting passengers and freight using electric vertical takeoff and landing (eVTOL) aircraft. Through engagement with NASA, industry, and community stakeholders, the FAA developed the UAM ConOps v1.0 which "describes the envisioned operational environment that supports the expected growth of flight operations in and around urban areas." Unlike UTM, UAM will need to support operations at altitudes higher than 400 feet AGL and need routine access in controlled airspace including Classes B, C, and D. The FAA's initial approach to enabling UAM operations is through using UAM corridors that leverage existing helicopter routes. Helicopter routes use locally charted airspace structures to simplify the interactions between a helicopter Pilot-In-Command (PIC) and Air Traffic Control (ATC). The key differences in how helicopters operate in these routes today and how UAM operations intend to function within UAM corridors is that UAM operations will not require clearances nor interaction with ATC and operations may be limited according to their ability to meet performance and participation requirements. [FAA 2020b, National Academy of Sciences 2020]

To enable UAM operations without the support of FAA Air Traffic Service, the FAA envisions an ATM solution very similar to UTM described previously. In the FAA's UAM ConOps v1.0, they present a Notional UAM architecture to support the services required for safe and efficient UAM operations; shown in Figure 2. The FAA's Notional UAM Architecture proposes the use of Providers of Services for UAM (PSU)sit as the means to provide UAM operators with the services needed to meet the UAM operational requirements for safety, efficiency, and security. PSUs support UAM operators through the exchange of information with other PSUs, Supplemental Data Service Providers, UAS Service Suppliers, the FAA, and other stakeholders such as first responders. UAM operators may obtain information not provided through PSUs directly with supplemental data service providers as needed to support their operations.

To describe the evolution of UAM, NASA developed the UAM Maturity Level (UML) framework for the transition of UAM operations from isolated and sparse to routine and numerous. UMLs are grouped into three states (initial, intermediate, and mature) across six levels (UML-1 to UML-6) and split among three organizational frameworks and barriers (aircraft, airspace, and community). Each level in the UMLs provide for a stepwise increase in air traffic density, operational complexity, and reliance on automation. The NASA UML framework shown in Figure 3 illustrates that increasingly autonomous operations will be likely as the number of UAM operations scale up. Level 4 in Figure 3 is highlighted to indicate the scope of NASA's UAM Vision ConOps. With the combination of increased autonomy and reliance on information from multiple third-party sources of both known and unknown pedigree, the need for a means to ensure information integrity becomes critical to ensure safe, efficient, and secure flight operations. The next section further discusses the need for ensuring information integrity through exploring its impact on the decision-making processes, both human and machine, and how increased automation presents a challenge in the ability to identify, adjust, or discount information of poor integrity. [NASA-Deloitte 2021]

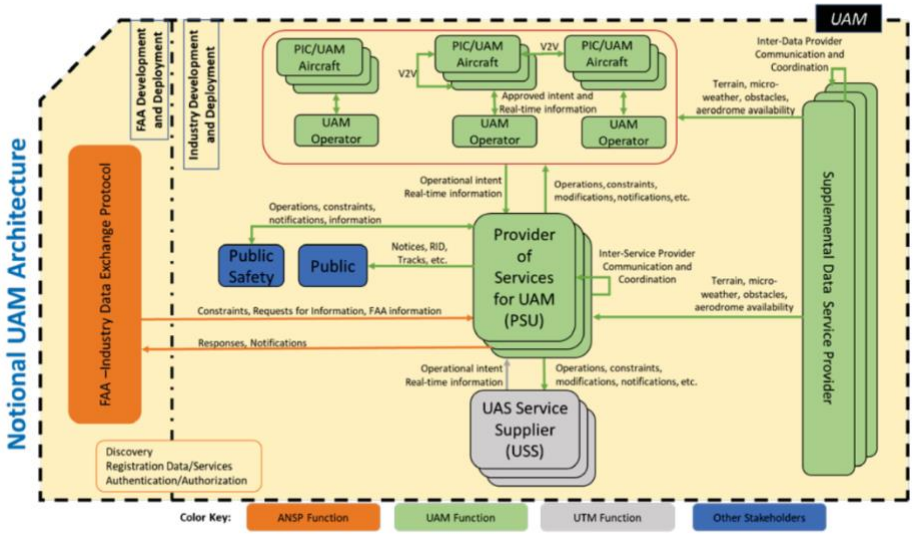


**Figure 2 - Notional UAM from FAA's UAM ConOps v1.0**

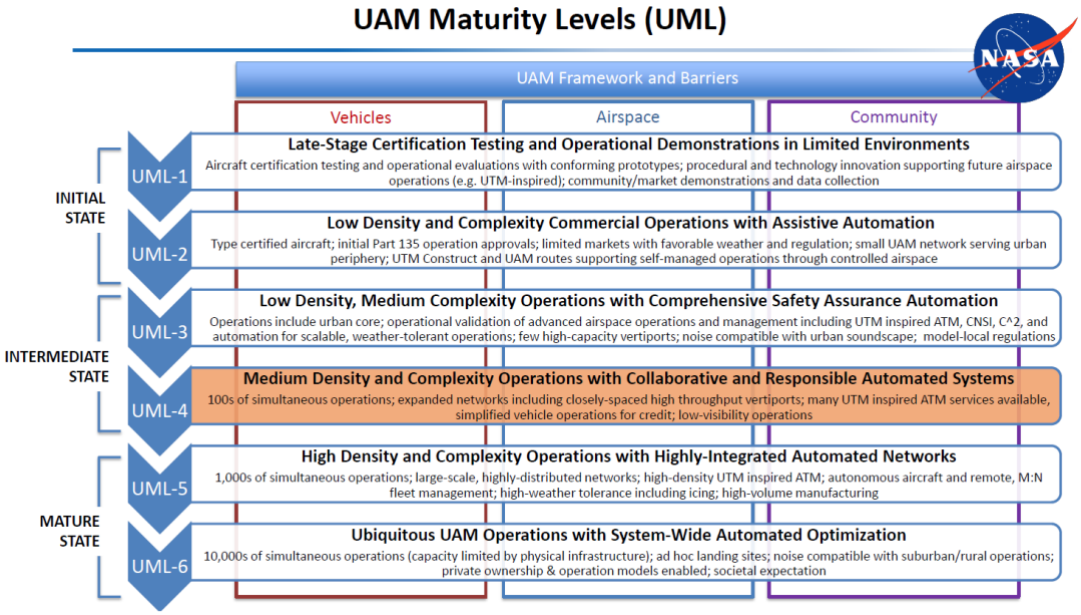


**Figure 3 - NAS UAS Maturity Levels (UML)**

## CASE FOR INFORMATION INTEGRITY

For an automation system to be trusted by regulators, operators, users, passengers, and the public, it must function as intended within acceptable levels of risk. The key to functioning as intended is for the system to appropriately monitor and assess the situation, decide on the appropriate course of action, and execute accordingly. Accurate monitoring and situation assessment are the keys to good decision-making. [Orasanu 1998, Endsley 1995, Klein 1993]

For humans, monitoring and assessing situations begins with the sensation of information received through the visual, auditory, olfactory, tactile, and kinesthetic sensory systems followed by the processing of the sensory data into perceived information. Perceived information is then used to support tasks such as monitoring, decision making, and developing situation awareness. Consider a pilot, their visual system provides information needed to perceive the environmental conditions (e.g., weather), assist with navigation (e.g., monitoring GPS position on moving map), and look for potential hazards (e.g., other aircraft or wildlife); their auditory system provides information such a correctly operating engine; the olfactory system can detect potential anomalies (e.g., fires or fuel leaks); and their kinesthetic sensory inputs support the perception of aircraft orientation (e.g., ensuring a coordinate turn). Humans integrate all this information to appropriately perceive the situation and make an assessment. Humans can discount information that is inconsistent or based upon their experience may be less reliable (e.g., less accurate). They do this through the formulation of mental models which are shaped by their experience, knowledge, bias, training, and situational context; see Figure 4 for a simplified illustration of how humans perceive information and develop an assessment of their environment ultimately supporting their decision-making processes. Figure 4 follows the IDEF0 process modeling approach to demonstrate that inputted information is perceived by using mental models effected by experience, context, bias, knowledge, and training to assess a situation. While humans do this instinctively, we need to ensure that automated processes have the necessary integrity information to achieve the same effect.

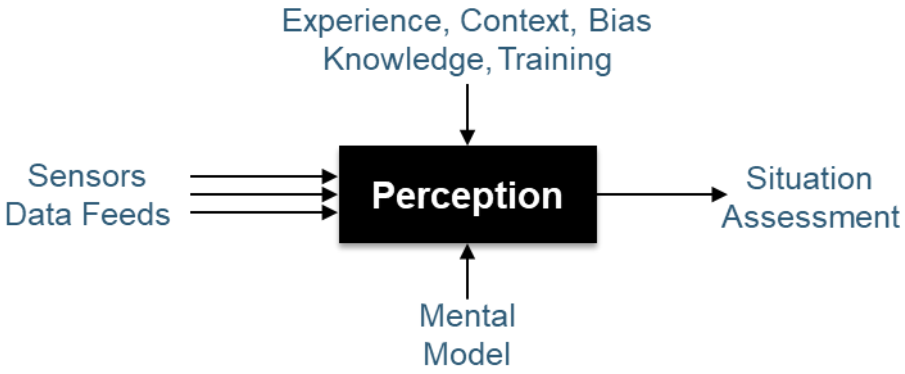


**Figure 4 - Process Model of the Perception. For Humans, sensors are sensory inputs and data feeds are processed information received from displays, gauges, alerts, or spoken word**

To further explain how humans discount unreliable information, think of the instrument rated pilot's process to establish their physical orientation in instrument meteorological conditions. Instrument pilots are specifically trained to ignore sensory inputs (e.g., what they see out the window or how they feel the aircraft is oriented) and focus instead on the information provided through scanning their instrument panel. For pilots in training, this requires deliberate thought and contributes to their cognitive workload. As pilots gain experience and proficiency, the ability to discount and ignore direct sensory inputs and rely instead more heavily upon the processed information from the instruments to perform situation assessments becomes second nature.

There are times where the processed information being presented to pilots can present challenges. Consider the following example from 2010 where a flight crew noticed a 2000 foot discrepancy between the pilot and co-pilot's altimeters on a Pilatus PC12 flying in the Bordeaux flight information region. Unaware of which altimeter was reporting correct information, the flight crew attempted to check with ATC who in-turn checked with military controllers in an attempt to cross-validate the correct altitude. Due to a misunderstanding of the civilian and military

controller's altitude source, the flight crew received an erroneous confirmation of which altitude was correct. The misunderstanding was that the altitude used by both FAA and the military controllers was sourced by the aircraft's own transmission of the faulty altimeter by the Mode S transponder. The erroneous altitude information provided by the aircraft's faulty altimeter was thus being used by ATC for separation services, by the Traffic Collision Avoidance System (TCAS) for collision alerting, and by the flight crew to maintain altitude. This situation resulted in a near miss with an Airbus 318 that was assigned an altitude of which the pilots of the Pilatus were unknowingly cruising. The example described illustrates how all the decision processers involved including the flight crew, air traffic controllers, and automation (e.g., autopilot and TCAS) were relying upon this inaccurate information. Luckily in this case tragedy was averted.

Automation systems can be especially vulnerable to erroneous information. Consider the Maneuvering Characteristics Augmentation System (MCAS) on the Boeing 737 MAX. The original MCAS (the system on the aircraft involved in the two fatal accidents Lion Air Flight 610 in October 2018 and Ethiopian Airlines Flight 302 in March 2019) only consumed data from a single angle-of-attack sensor. If that sensor's readings were faulty, the assessment of the aircraft's situation would also be faulty, and the automatic trim system would cause the aircraft to pitch down [Travis 2019]. Erroneous information led to an incorrect situation assessment that ultimately resulted in a wrong decision/action and thus the automation was brittle to faulty information. While Boeing did have an option for an angle-of-attack disagree warning, few airline customers (approximately 20 percent) purchased that option. [Gelles and Kitroeff 2019]

As automation becomes primarily responsible for situation assessment, how are the appropriate mechanisms included to capture the value humans add to operational processes by being the arbiter of information integrity? This is especially important when information is not only coming from sensors directly connected to the automation but from information processed by other automation systems and received over communications links and networks. With a human no longer in the information processing flow, there need to be a means to ensure the function humans perform through cross-checking information, leveraging context, and baselining assumption off of experience with different sources of information under different conditions is maintained. These other automation systems could include systems maintained and operated by aviation authorities or from systems certified by aviation regulators (e.g., another aircraft); however, information sources could also include third party automation systems (e.g., UTM).

For increasingly autonomous aviation operations to be trusted by regulators, operators, users, passengers, and the public, a mechanism to expose the pedigree of information so that it could be processed and used appropriately will be needed. To ensure the appropriate situation assessment is reached, a means for considering the integrity of information received from sensors and data feeds will be needed to incorporate contextual information as well as capturing the equivalent of experience and knowledge used by humans to discount or ignore information from potentially unreliable sources. A means for appropriately associating information integrity with the information itself as it flows through distributed automation systems is likely going to be necessary.

## FRAMEWORK FOR ENSURING INFORMATION INTEGRITY

The progression towards increased autonomy and reliance on information from multiple third parties require us to re-assess how the integrity of information used in decision-making processes of both human-machine and machine-machine relationships is established. This will be essential to ensuring safe, efficient, and secure flight operations. This section presents a framework for ensuring information integrity that provides a methodology for systems to adjust functional performance based on the calibration of information integrity to ensure the trustworthiness of increasingly

autonomous aviation systems. Five pillars of information integrity are presented and provide the foundations to the integrity framework. These pillars state that information integrity is known and maintained when it is accurate, performant, transparent, authentic, and monitored. After establishing what is needed to ensure information integrity, an approach to trusted information management to enable increasingly autonomous flight operations is presented. This approach provides a methodology for systems to ensure information integrity through categorizing according to source pedigree, tagging with meta data for integrity analysis, determining alignment with established acceptable performance criteria, and then adjusting or discounting its use accordingly to support one or more desired functions.

**Five Pillars of Information Integrity**

There are five pillars of information integrity which ensure that it is accurate, performant, transparent, authentic, and monitored as depicted in Figure 5. This section discusses each of these pillars and associated methods that can be used to establish and maintain the integrity of information from sources of both known and unknown pedigree.


**Figure 5 - Five Pillars of Information Integrity**

*Accurate.* Accuracy is a key component to the integrity of information. Information can be considered accurate if it is a correct representation of reality (or truth) without error or that the error is known. The precision of a reported measurement should match the accuracy of the information and its error. It is important to ensure that information is either verified as accurate to an acceptable degree or the amount of error is known so the decision maker, human or machine, can calibrate its use accordingly. Some examples of methods that can be used to verify the accuracy of information include validation through independent sources, voting algorithms, statistical calculation, and range checks, among others. Accuracy checks in an information system can be performed either at the source or by a trusted third party and then provided with the information when sent to the end receiver. If the receiver does not trust the source, it can conduct its own verification of the accuracy through verification with other sources that provide the same or similar information or information that can be derived or estimated from other sources.

*Performant.* Information that meets the required performance criteria for a specific use is considered performant. Performance is a key aspect of information integrity when decisions must be made in a timely manner. Performance criteria metrics and thresholds that impact information integrity are dependent on the task for which the information is to be used. Three examples of common performance metrics in real-time decision systems are availability, latency, and update frequency. In this case, information could be said to have integrity, considering all other integrity factors discussed as met, if it can be assessed when needed (available), delivered in an acceptable time (latency) and is refreshed in the timeframe required (update frequency) to meet the performance criteria of the task at hand.

*Transparent.* When assessing the integrity of information, details of what could impact integrity are needed to derive a confident assessment. To judge information as to be accurate and performant, meta data associated with accuracy (e.g., error rate) and performance (e.g., latency) are necessary for the decision maker (whether human or an autonomous agent) to determine if it meets their required integrity thresholds and/or to calibrate its use accordingly. Additionally, the source of

 

information and any alterations that occurs through its lifecycle (i.e., provenance) is an important factor when assessing the integrity of information. Determination of integrity can be greatly influenced by knowing where information came from if the source is both trusted and known to be reliable. Meta data and provenance associated with a set of information provides the transparency needed to establish integrity and can be provided by the source, calculated at time of use, or provided by an independent trusted third party.

*Authentic.* Authenticity of information is vital to security and can have a significant impact to its integrity. Authenticity of information can be achieved by verifying the identity of the source and ensuring it is not altered between generation and delivery. This can be achieved using X.509 certificates to create digital signatures in combination with validation through a trust authority, either local or remote. Digital signatures provide the ability for an end receiver to both verify the source and content of a piece of information. They also provide the ability for the sender to verify the acknowledgement of receipt is authentic and provides for non-repudiation if needed. It is also important to ensure sources can only provide information for which they are authorized. This can be done through Rule Based Access Control (RBAC) or Attribute Based Access Control (ABAC). RBAC determines if a user/system has permissions to perform a function associated with a pre-defined role (e.g., a weather provider role could be approved to submit wind, cloud height, temperature) where ABAC determines permission based on defined attributes (e.g., a weather provider could be authorized to just provide wind and restricted from providing cloud height and temperature). Authorization can be performed at the time of information submission, effectively preventing the information from distribution, or it can be done at the time of use, the end user controls if it authorizes the use.

*Monitored.* Integrity of information is multi-faceted and dynamic, once established it needs to be monitored to ensure it is maintained. This can be performed at the system using the information, via a third-party, or by an enterprise service. Monitoring integrity parameters provides in-time assessment of the information services to identify anomalies, inconsistencies, and sub-system performance to alert appropriate agents. If the established integrity of information changes, systems need to be aware and modify its use accordingly. This could be a component of the In-time System-wide Safety Assurance (ISSA) for scalable UAM currently in research by NASA. [NASA 2020]

**Trusted Information Integrity Management Framework**

Successful integration of increasing autonomous flight operations into the NAS will require the ability to determine the integrity of information used to make decisions, both by human and autonomous agents. To address this issue, a Trusted Information Integrity Management Framework (TIIMF) is proposed. The TIIMF methodology provides agents, human or machine, with the information needed to determine the level of integrity a piece of information retains so to adequately adjust or discount such information according to the task at hand. The framework is split into four layers (Source, Meta Data, Performance, Functional) associated with the information use life cycle (Collection, Exchange, Analysis, and Operational); depicted in Figure 6.

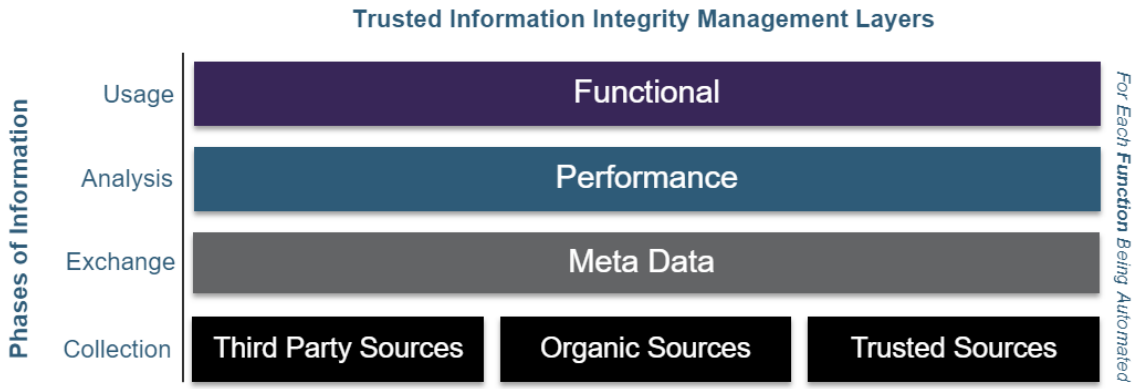


**Figure 6 - Trusted Information Integrity Management Framework (TIIMF)**

*Source.* The Source layer of TIIMF segregates information according to pedigree as either Organic, Trusted, or Third Party. Organic sources are those that originate from elements directly connected to the system (e.g., dedicated sensors). Trusted sources are those that originate from entities inherently trusted because of certification or other means that involve a degree of validation/substantiation (i.e., pedigreed source), e.g., Mode S transponder replies from another aircraft and Notice to Airmen (NOTAMS) directly provided by the FAA through System Wide Information Management (SWIM). All other sources of information fall into the Third-Party category (e.g., weather from a commercial provider). While the information provided by third-party sources can be valuable or even necessary, they require a higher level of integrity validation prior to their use (e.g., non-certified weather sensor). The source of information needs to be taken into consideration determining the level of integrity validation necessary to ensure system performance consistently meets required threshold for safe, efficient, and secure operations.

*Meta Data.* The Meta Data layer of the TIIMF is the most important layer as it provides the data required to conduct a correct integrity assessment of the information in question. Meta data is anything associated with a piece of information that can be used to determine its accuracy, performance, and authenticity. Meta data is key to transparency. Meta data can either be included with the information when sent by the source; or added while information is exchanged or accessed via an external provider. Examples of key meta data that are required to determine the integrity of information include timestamps, error approximations, confidence estimates, and source authenticity. As end systems receive information and prepare for use, they use meta data in the analysis phase of information processing to ensure it meets established performance criteria required for the intended function of use which comprises the final two layers of the TIIMF.

*Performance.* Prior to using information to conduct a specific function, it should be analyzed to ensure the expected performance will meet the established performance criteria required for such function's tasks. This is accomplished through gathering supporting integrity data associated with the information as provided by the meta data layer of TIIMF. Additionally, outside sources may be required to obtain enough supporting data to conduct performance validation. This is critical when the information in question does not have sufficient meta data associated with it to adequately determine its integrity. Several methods can be used to accomplish this including cross-validation through independent sources, use of voting algorithms and statistical calculations to assess integrity over time, range checks to ensure reported values are within acceptable tolerances, and checksums on communication to ensure no errors have been introduced during transit.

*Functional.* Once the performance integrity of information is established, the system then adjusts its use of the information as needed to meet specific functions, or tasks. Each system function should have a pre-defined performance criterion in which information must meet to ensure the output of an action, or set of actions, is of high predictability. If the integrity of information to be used for a specific function does not meet the established performance criteria, the system can adjust to ensure the desired level of performance is maintained; similar to how an instrument-rated pilot has been calibrated to ignore their own sensory perception and rely instead on information from their instruments.

### A Practical Example for a Trusted Information Integrity Framework

A simple but powerful example for the need of a TIIMF is in the execution of an automated collision avoidance function of an autonomous flight system. The collision avoidance function is responsible for ensuing clearance from obstacles such as terrain, man-made structures, other aircraft, airspace status, and special operations (e.g., skydiving). To perform this function effectively and efficiently, the autonomous system must collect information from multiple sources including onboard sensors, ground sensors, position information from other aircraft in the vicinity, terrain databases, obstacle data (e.g., towers), Notices to Airman (NOTAMs), and status of airspace and special operations to name a few. Each one of these pieces of information originates from different sources and has a varying level of integrity. Inadequately or incorrectly identifying the integrity of any of these sources could result in an incident or accident with the potential for a serious outcome, including loss of life. Through the adoption of the TIIMF, the integrity of information available would be known and the autonomous decision-making entity would be able to mitigate any identified degradations in integrity through adjusting how it makes decisions to operate accordingly. In summary, if the information used to execute a collision avoidance function is of poor integrity, the resulting decisions of the function can be producing inconsistent results that are detrimental to safe, efficient, and secure operations.

## CONCLUSION

This paper discussed the shift away from a single governmental entity providing air traffic services to a distributed multi service-provider model to enable emerging UTM, UAM, and Upper-E flight operations. Further discussed was the importance of information integrity in increasing autonomous systems and the need for a means to ensure and actively manage information integrity within these systems. The paper describes five pillars of information integrity and presents a Trusted Information Integrity Framework as mechanism to discuss potential mitigations for the lack of humans' intrinsic ability to discount uncertain information. While the approach offered is one way to address this issue, it is the strong belief of the authors that ensuring information integrity is a critical requirement to the safe, efficient, secure, and successful integration of emerging autonomous flight operations into the NAS. Failing to effectively account for information integrity will likely result in the increased potential for systematic failures that could result in unintended consequences, including the unnecessary loss of life.

## ABOUT THE AUTHORS

**Alexander R Murray** is an innovator and thought leader in aviation and has been working in the industry for the past 15 years. After initially starting off as a flight instructor, he became exposed to the engineering side of aviation and quickly pivoted his interest to solving complex problems facing the future of aerospace. He has led and supported multiple research projects focused towards advancing aviation in the areas of autonomy, unmanned systems, and information management for NAS integration. He is an expert in aviation information service with a focus enterprise architecture to support disperse interconnected systems.

 

**Andrew R Lacher** has 35 years of experience in aviation and transportation systems and is an expert on safety and security of unmanned/autonomous systems. He is currently the director of Aerospace Systems Research Center with a prominent role in shaping Noblis' aerospace and autonomous systems research. He was senior manager for Autonomous Systems Integration at Boeing where he shaped their approach to integration, BVLOS, and airspace management. Andy retired from MITRE after 30 years where he was responsible for unmanned/autonomous systems integration and adoption.

## REFERENCES


Bureau d'Enquêtes et d'Analyses (BEA), 2011, Incident on 2 June 2010 Bordeaux FIR, OLRAK Point between the A318 registered F-GUGJ operated by Air France and the PC 12 registered EC-ISH, Ministère de l 'Écologie, du Développement durable, des Transportsetdu Logement.

Endsley, M.R. 1995, *Toward a Theory of Situation Awareness in Dynamic Systems*, Human Factors Journal 37(1), 32-64.

Federal Aviation Administration (FAA) 2020, Unmanned Aircraft System (UAS) Traffic Management (UTM) Concept of Operations V2.0, NextGen, Washington, DC.

Federal Aviation Administration (FAA) 2020a, Upper Class E Traffic Management (ETM) Concept of Operations V1.0, NextGen, Washington, DC.

Federal Aviation Administration (FAA) 2020b, Urban Air Mobility (UAM) Concept of Operations V1.0, NextGen, Washington, DC.Gelles D. and Kitroeff, N., 2019, *Boeing Believed a 737 Max Warning Light Was Standard. It Wasn't*, New York Times. May 5, 2019, https://www.nytimes.com/2019/05/05/business/boeing-737-max-warning-light.html?

Klein, G.A., Orasanu, J., Calderwood, R., and Zsambok C.E., 1993, *Decision Making in Action: Models and Methods*, ABLEX Publishing Corporation, Norwood, New Jersey.

Mayer, R. C., Davis, J. H., & Schoorman, F. D. 1995, An Integrative Model of Organizational Trust. The Academy of Management Review, 20(3), 709. https://doi.org/10.2307/258792

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.

National Aeronautics and Space Administration (NASA) 2020, In-time System-wide Safety Assurance (ISSA) Concept of Operations and Design Considerations for Urban Air Mobility (UAM), Washington, DC.

National Aeronautics and Space Administration (NASA) and Deloitte 2021, UAM Vision Concept of Operations (ConOps) UAM Maturity Level (UML) 4, Washington, DC.

Orasanu, J. and Martin, L, 1991, *Errors in Aviation Decision Making: A Factor in Accidents and Incidents*, HESSD 1998.

Travis, G., 2019, *How the Boeing 737 Max Disaster Looks to a Software Developer*, IEEE Spectrum, https://spectrum.ieee.org/aerospace/aviation/how-the-boeing-737-max-disaster-looks-to-a-software-developer



** This paper was presented at AUVSI XPONENTIAL 2021*