

NASA/TM-2020-220440



Architecture and Information Requirements to Assess and Predict Flight Safety Risks During Highly Autonomous Urban Flight Operations

*Steven Young, Ersin Ancel, Andrew Moore, Evan Dill, Cuong Quach, John Foster,
Kaveh Darafsheh, Kyle Smalling, Sixto Vazquez, and Emory (Tom) Evans
Langley Research Center, Hampton, Virginia*

*Wendy Okolo, Matteo Corbetta, John Ossenfort, Jason Watkins,
Chetan Kulkarni, and Lilly Spirkovska
Ames Research Center, Mountain View, California*

January 2020

NASA STI Program . . . in Profile

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

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

- **TECHNICAL PUBLICATION.** Reports of completed research or a major significant phase of research that present the results of NASA Programs and include extensive data or theoretical analysis. Includes compilations of significant scientific and technical data and information deemed to be of continuing reference value. NASA counter-part of peer-reviewed formal professional papers but has less stringent limitations on manuscript length and extent of graphic presentations.
- **TECHNICAL MEMORANDUM.** Scientific and technical findings that are preliminary or of specialized interest, e.g., quick release reports, working papers, and bibliographies that contain minimal annotation. Does not contain extensive analysis.
- **CONTRACTOR REPORT.** Scientific and technical findings by NASA-sponsored contractors and grantees.

- **CONFERENCE PUBLICATION.** Collected papers from scientific and technical conferences, symposia, seminars, or other meetings sponsored or co-sponsored by NASA.
- **SPECIAL PUBLICATION.** Scientific, technical, or historical information from NASA programs, projects, and missions, often concerned with subjects having substantial public interest.
- **TECHNICAL TRANSLATION.** English-language translations of foreign scientific and technical material pertinent to NASA's mission.

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

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

- Access the NASA STI program home page at <http://www.sti.nasa.gov>
- E-mail your question to help@sti.nasa.gov
- Phone the NASA STI Information Desk at 757-864-9658
- Write to:
NASA STI Information Desk
Mail Stop 148
NASA Langley Research Center
Hampton, VA 23681-2199

NASA/TM–2020-220440



Architecture and Information Requirements to Assess and Predict Flight Safety Risks During Highly Autonomous Urban Flight Operations

*Steven Young, Ersin Ancel, Andrew Moore, Evan Dill, Cuong Quach, John Foster,
Kaveh Darafsheh, Kyle Smalling, Sixto Vazquez, and Emory (Tom) Evans
Langley Research Center, Hampton, Virginia*

*Wendy Okolo, Matteo Corbetta, John Ossenfort, Jason Watkins,
Chetan Kulkarni, and Lilly Spirkovska
Ames Research Center, Mountain View, California*

National Aeronautics and
Space Administration

Langley Research Center
Hampton, Virginia 23681-2199

January 2020

Acknowledgments

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

In addition, thanks to Program and Project Managers, Akbar Sultan, John Koelling, Misty Davies, and Kyle Ellis. Without their support, outside-the-box thinking, and constructive critiques, the concept exploration leading to this report would not have been possible.

Very special thanks to Jessica Nowinski and Kai Goebel. They set the stage for this report by accomplishing key prior research, establishing technically feasible objectives, and guiding the team along the way with insight and energy.

Key contributors to the R&D and testing were Portia Banerjee, George Gorospe, Gina Sierra Paez, Elinirina Robinson, Molly O'Connor, Indranil Roychoudhury, Russell Gilabert, Ed Hogge, Swee Balachandran, Nick Rymer, Matt Schubert, Ryan Condotta, Cesar Munoz, Maria Consiglio, and Max Friedrich. Thank you all for your dedication, creativity, and can-do spirit.

<p>The use of trademarks or names of manufacturers in this report is for accurate reporting and does not constitute an official endorsement, either expressed or implied, of such products or manufacturers by the National Aeronautics and Space Administration.</p>

Available from:

NASA STI Program / Mail Stop 148
NASA Langley Research Center
Hampton, VA 23681-2199
Fax: 757-864-6500

This report is available in electronic form at

<http://ntrs.nasa.gov>

Contents

1. Introduction	7
2. Architecture	12
3. Information Requirements	21
4. Uncertainty Management.....	27
5. Exchange Model and Protocols.....	28
6. Supporting Tests	30
7. Related Industry Developments	30
8. Summary and Plan for Updates	31
References	32
Appendix A: Enabling Technology R&D	37
Appendix B: Initial End-to-End Services Tested	46
Appendix C. Uncertainty Management Framework	57
Appendix D. Aerodynamic Modeling	64
Appendix E. More on In-Time Safety Assurance Functions	68
Appendix F. Test Summaries.....	70
Appendix G. Acronym List.....	78

1. Introduction

As aviation adopts new and increasingly complex operational paradigms, vehicle types, and technologies to broaden airspace capability and efficiency, maintaining a safe system will require recognition and timely mitigation of new safety issues as they emerge and before significant consequences occur. A shift toward a more predictive risk mitigation capability becomes critical to meet this challenge. In-time safety assurance comprises monitoring, assessment, and mitigation functions that proactively reduce risk in complex operational environments where the interplay of hazards may not be known (and therefore not accounted for) during design. These functions can also help to understand and predict emergent effects caused by the increased use of automation or autonomous functions that may exhibit unexpected non-deterministic behaviors. The envisioned monitoring and assessment functions can look for precursors, anomalies, and trends (PATs) by applying model-based and data-driven methods. Outputs would then drive downstream mitigation(s) if needed to reduce risk. These mitigations may be accomplished using traditional design revision processes or via operational (and sometimes automated) mechanisms. The latter refers to the ‘in-time’ aspect of the system concept.

This report comprises architecture and information requirements and considerations toward enabling such a capability within the domain of low altitude highly autonomous urban flight operations. This domain may span, for example, public-use surveillance missions flown by small unmanned aircraft (e.g., infrastructure inspection, facility management, emergency response, law enforcement, and/or security) to transportation missions flown by larger aircraft that may carry passengers or deliver products.

Caveat: Any stated requirements in this report should be considered initial requirements that are intended to drive research and development (R&D). These initial requirements are likely to evolve based on R&D findings, refinement of operational concepts, industry advances, and new industry or regulatory policies or standards related to safety assurance.

1.1. System concept

NASA’s Aeronautics Research Mission Directorate describes a strategic plan for investigating and advancing in-time system-wide safety assurance (ISSA) capabilities [1]. Within this plan, it is envisioned that advanced safety assurance tools can be introduced to take advantage of increasing availability of aviation system data. The identification of safety issues will focus on scaling currently available data mining methods to process a broad range of data; thereby enabling a disparate set of high-fidelity model-based information services that can inform and track the changing nature of risk during flights. By using these models and information services, combined with increased speed and accuracy of analysis tools, safety assurance can progress toward more timely identification of PATs, thereby maintaining acceptable safety margins.

As described in [1], three high-level functions are needed that can be tailored to a specific application domain and may span from the vehicle-level to the airspace system level (depending on the safety risks and risk tolerance for the domain). These functions are:

- **Monitoring** – A set of information services and an underlying architecture that allows for acquisition, integration, and quality assurance of heterogeneous safety-relevant data that may come from a diverse set of sources (including vehicles). Access to these services must recognize that some data may require protections that de-identify the source and defend against corruption by unauthorized or unauthenticated sources.

- Assessment – A set of tools and techniques that provide timely detection, diagnosis, and a predictive capability regarding changes in risk and hazard states. Assessment functions should be capable of spanning hazard types to judge how overall safety margin is changing based on current context, on recent (in-flight) cascading event sequences, and on longer-term trends that can become evident with access to historical data maintained by monitoring functions.
- Mitigation – A set of methods, tools, and procedures that provide for multi-agent or automated planning and execution of timely responses to hazardous events or event sequences when/if safety margins are observed or are predicted to deteriorate below acceptable levels.

A report published by the National Academies outlines challenges that must be addressed in development of a similar but broader capability – an In-time Safety Assurance Management System (IASMS) [2]. This capability is defined within the larger context of SMS [3], which covers all aspects of managing safety including organizational structures, accountabilities, policies, procedures, and business practices. As reported in [2], the committee’s vision for an IASMS is summarized in the following recommendation:

“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.”

For the remainder of this report, we focus on a specific operational domain (i.e., application domain) – highly autonomous low altitude flights near and over populated urban areas. These include flights such as are envisioned for some Urban Air Mobility (UAM) operations [4] and many use-cases for small Unmanned Aircraft Systems (sUAS).

1.2. Application domain

From an operational perspective, the in-time safety assurance concept can be thought of as an extension to the way current operations are conducted, with the provision that an information-sharing infrastructure will be in place. This infrastructure, with both on-board and off-board elements, will enable the collection and monitoring of safety-relevant information, the assessment of risk (including predictions), and mitigation option generation and/or automated control actions (as required). To illustrate the concept, consider three operational phases: pre-flight, in-flight, and post-flight.

Pre-flight – As part of a pre-flight checklist, a trained, qualified, and licensed operator ‘connects’ his/her vehicle(s) to one or more authorized safety-relevant information service providers. The operator may opt for generally-available information (publish-subscribe), or mission-specific information (request-reply). For the latter, the operator can send the flight plan or intended region of flight along with requested information types. In either case, the latest information (which may include a model and a forecast) is transmitted by the service provider. Upon receipt, the operator checks the information for validity, and then has the opportunity to check for any safety assessment results (e.g., high-risk areas) that may cause reconsideration of flight plans or launch window. Once these checks are completed, relevant information is loaded onto the vehicle system for use as the basis of on-board monitoring, assessment, and mitigation of risk as it evolves during the flight.

Such a pre-flight procedure is already being used for some UAS and sUAS operations for limited information types and services, and is consistent with the UAS Traffic Management (UTM) concept [5]. However, for the envisioned safety assurance system, additional safety-related information services would be available and associated service provider functions in operation.

In-flight – Once vehicle(s) are launched, the operator monitors flight status including risk(s) or other observables reported by the vehicle(s) and/or the information service providers. Monitoring functions may be executing in parallel at multiple locations: on-board the vehicle(s), at the ground control station(s) (GCS), and/or at the service supplier(s)/provider(s). Most likely each will be operating at different rates and with forecasts of different spatial and/or temporal resolutions and time horizons. The choice of where monitoring should occur can be based on operational safety requirements for a particular domain (i.e., the mission/vehicle/operational environment three-tuple), the risks therein, and the bandwidth limits of links between locations. Risk assessment and mitigation functions would be implemented in a similar manner. They may execute on-board, at the GCS, and/or at the service provider during flight. On-board mitigation options for UAS would consist of automated selection and execution of fail-safe contingency maneuvers under certain situations (e.g., hold-in-position, return-to-launch point, maneuver-to-safe-zone, land immediately, or launch abort). For UAM, an appropriately trained operator may be on-board and would also have a role to play in mitigation.

The above describes a concept with only one human in-the-loop during operations, the operator. This person would be responsible for oversight and supervision of one or more vehicles. It is possible that other humans will be (at least initially) required to ensure safety. For example, a remote safety pilot may be part of the mitigation function under some circumstances.

Post-flight – After each flight, the primary activity to perform relative to in-time safety assurance is to off-load all flight data recorded during the flight. These data, along with any data recorded at the GCS, will be uploaded to the relevant service providers to support updating and validating of their services and models. Performance anomalies can be reported which may lead to design changes or maintenance actions. The operator may also report safety-relevant observations or metadata to help providers understand the data and/or the operational context of the flight. This process may be highly automated and supported by appropriate tools such that post-flight procedures can be completed in a timely manner. Other post-flight activities may include active probing of flight-critical equipment with ground-based inspection tools to determine any deterioration not sensed during flight.

To better illustrate the concept of operations, it can be helpful to walk through scenarios that utilize these constructs. Use-cases will vary with complexity and boundary conditions, from simple point-to-point sUAS missions (e.g., the transport of goods/supplies and infrastructure inspection), to complex roaming sUAS missions (e.g., emergency/fire response and law enforcement support), to manned UAM missions (e.g., air taxi services). As a low-complexity example, the transport of medical specimens from a suburban medical office to a large downtown laboratory for testing at a hospital has been used to help expose requirements. This scenario is described in [6], and there are similar use-cases that have been operationally approved [7][8].

1.3. Urban flight environment hazards and risks

A set of safety-critical risks to low altitude urban flight were initially identified to help derive information requirements, particularly for the Monitoring function. These were selected as a representative set based on previous work by NASA and others in industry. They include: flight outside of approved airspace; unsafe proximity to air traffic, people on the ground, or property; critical system failures (including loss of link, loss or degraded positioning system performance, loss of power, and engine failure); loss-of-control due to envelope excursion or flight control system failure; severe weather encounters (including wind gusts); security-related risks (cyber or physical); and human factors-related risks. The latter includes for example procedural errors of omission/commission that could lead to loss of safety margin in the best case or accidents in the worst case. Recent policy by the FAA [9] identifies UAS ‘common hazards’ as: technical issues within the UAS, deterioration of external systems supporting the UAS, human error, adverse operating conditions, and inability to detect and avoid. Outcomes listed in this same policy all involve collisions (e.g. with other aircraft, people on the ground, or infrastructure). Although not specific to highly-autonomous low altitude urban flights, there is good agreement between those given in the FAA policy and those identified here as initial drivers for in-time safety assurance system concept development.

It should be recognized that the above hazards/risks may not be comprehensive and can involve disparate contributing factors as the intended mission, vehicle, and/or environment changes. New hazards may also be exposed due to mismatches in vehicle and operational assumptions used during design that prove to be invalid (or bounded) during operations; vulnerabilities exist even though the system is operating as designed. Hazards of this type (i.e., the unknown unknowns) are particularly relevant to the in-time safety assurance concept as it is intended in part to help identify them. There are multiple structured processes that have been used in the past to help expose the broadest possible set of hazards that may be encountered (e.g., [10] and [11]). In terms of risk assessment for a specific application domain and set of assumptions, process guidance is given in [9] (for UAS), and the Safety and Operational Risk Assessment (SORA) process can be used as well [12]. Guidance for UAM hazard analysis is given in [13].

1.4. Scope and approach

The three topics above determine the scope of the requirements and considerations described herein. These are the in-time safety assurance system concept, the application domain, and the set of identified safety-critical risks. Within this scope, keep in mind that one purpose of the system concept is to identify, track, and predict ‘unknown unknown’ safety risks or hazards (i.e., the discovery of vulnerabilities that were not known at design time). Because historically these have occurred due to unforeseen combinations, cascades, or contextual dependencies among known safety risks (hazards), we believe they will more likely be observable by a system that can look across their indicators. We denote this class of observables as precursors, anomalies, and trends (PATs). Of course, the more risks/hazards that can be addressed individually, the more likely the unknown unknowns can be expected to be detected, assessed, and mitigated in a timely manner by the system. To this end, there should be provisions that enable reporting of human observations of unsafe situations/occurrences that have developed (e.g., via the Aviation Safety Reporting System (ASRS), the Aviation Safety Action Program (ASAP), and other methods practiced within effective Safety Management Systems (SMS)).

The approach taken in this document is to describe the system concept by function and data flow. The physical architecture can vary, with the UTM construct and ecosystem used as an example herein and for initial testing. Existing systems, processes, and standards are strongly leveraged which will ultimately affect the design to some degree. For example, System-Wide Information Management (SWIM) [14], SWIM services, evolving UTM services, and the Aviation Safety Information Analysis and Sharing (ASIAS) data environment and analytics [15] can be a basis for the envisioned system. More on leveraging existing systems and processes is discussed in Sections 2 and 3.

The organization and representation of information requirements uses existing standards as a template or metaphor where possible, since many existing standards/requirements and information services are applicable here. In some cases, further research is needed to determine requirements. In these cases, we present factors that should be considered when making these determinations.

1.5. Relevant standards

The following standards are relevant and may be cited in various parts of this report. Relevance arises from the fact that many information services and standards already exist for the domain of commercial air transportation. For these, the information types and/or uses overlap, or the processes for exchanging and assuring the quality of information can be similar or identical.

RTCA DO-200B, Standards for Processing Aeronautical Data

RTCA DO-201B, User Requirements for Navigation Data

RTCA DO-272D, User Requirements for Aerodrome Mapping Data

RTCA DO-276C, User Requirements for Terrain and Obstacle Data

RTCA DO-291C, Exchange Requirements for Terrain, Obstacle, and Mapping Data

RTCA DO-324, Safety and Performance Requirements (SPR) for Aeronautical Information Services (AIS) and Meteorological (MET) Data Link Services

RTCA DO-349, Architecture Recommendations for Aeronautical Information and MET Data Link Services

RTCA DO-364, Minimum Aviation System Performance Standards for Aeronautical Information and Meteorological Data Link Services

RTCA DO-369, Guidance for the Usage of Data Linked Wind Information in ATM Operations

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 Unmanned Aircraft Systems Containing Complex Functions

There are also existing or evolving standards from the European Union Aviation Safety Agency (EASA), EUROCONTROL, ARINC, and the Open Geospatial Consortium (OGC) that may be relevant.

1.6. Assumptions

There are two important classes of safety risk management functions that are not directly covered by the system concept presented herein. These are related to air traffic (e.g., functions that provide for separation assurance) and airspace access (e.g., functions that coordinate and authorize airspace usage). We assume that associated safety risks will be covered in part by a set of ATM services and functions that can be interoperable with (and complementary to) the services and functions described here. For example, ATM functions that enable trajectory-based operations or merging and spacing flow sequencing into shared landing sites. An approach to enabling this type of interoperability is part of ongoing research based on the UTM ecosystem.

We also assume there will be a system similar to today's NAS that can provide some of the required information (e.g., AIS, weather, and flight information). This will likely be via SWIM-like services or 3rd-party services managed by ICAO States, local/municipal governments, or industry. Many such services and functions already exist or are in development as part of UTM. These include for example those provided by Flight Information Management Systems (FIMS), UAS Service Suppliers (USS), and Supplemental Data Service Providers (SDSPs). In subsequent sections we provide more information on some of the most relevant of these information sources.

Per the ConOps described previously, we assume auto-pilot-based flight and as such there may not be a remote pilot flying "stick and rudder" as occurs today for many sUAS flights. However, we also assume that there will be at least one human (operator) at a ground location who is responsible for overseeing and supervising flights. This individual will be able to issue high-level commands such as uploading a new flight plan or sending an emergency land command. Further, a single individual may remotely oversee multiple air vehicles simultaneously. This change of role and responsibility of human(s) during operations will lead to derived requirements for effective interfaces, procedures, and training. We assume that the architecture and information requirements presented herein are sufficient to design these interfaces, procedures, and training. This is also assumed for UAM operations where there may be an onboard operator/pilot with limited traditional piloting skills or training.

We assume that some 'connected' urban infrastructure can and will exist (e.g., [16]), and some elements of this infrastructure may be designed and used for purposes other than to support aviation; hence requiring more attention to data quality when using this infrastructure as a data source. Finally, in order to achieve the full potential of the system concept, we assume some sharing of information among and across operators, manufacturers, and safety assurance service suppliers will be possible; and that this sharing can be done while protecting intellectual property and privacy (e.g., by de-identifying or otherwise anonymizing source data).

2. Architecture

A high-level functional view of the system concept is shown in Figure 1 and Figure 2, which are derived from [1] and [2], respectively. The three functions (monitor, assess, mitigate) can be applied within several architectural paradigms including the overarching National Airspace System (NAS) architecture and the evolving approach to SWIM [14]. Ultimately, design decisions regarding the allocation of functions across architectural elements (and locations), as well as how they can perform in a coordinated manner remains a subject of research. However, there are a set of principles and traits that should be adhered to when making these decisions. These are discussed below.

2.1. Guiding Principles and Overarching Traits

Decomposition of the high-level functions (into sub-functions) can take many forms and remain effective both in terms of performance and information requirements. This is also true of (a) the distribution of functions onto physical computing elements at the various locations; and (b) the various possible assignments of role and authority given to human(s) in the system (e.g., the ability to intervene and ‘take-over’ to mitigate risk in some situations). Based on the decades-long evolution of safety assurance best-practices for commercial airline-like operations, the following are some of the principles and traits we recommend when considering the architectural design space.

1. Service-oriented; scalable; building block approach
2. Open and extendible to address new risks or hazards as/if they are discovered
3. Leverages and interoperates with existing relevant systems, including SWIM and ANSP services
4. Transformative from the existing NAS; with a practical transition path
5. Applies techniques that assure appropriate levels of data/information integrity
6. Applies run-time assurance/verification (RTA/RTV) techniques (see Section 3.3 and Section 4)
7. Supports isolation of flight-critical functions onboard to meet higher fail-safe assurance levels
8. Supports techniques that can bound the behavior of non-deterministic functions (see Section 4)
9. Data and service providers can be authorized/certificated as ‘trusted source’
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 meeting quality requirements)
12. Provides mechanisms that can protect sensitive data (e.g., de-identification)
13. Combines SWIM-like connectivity/services with ASIAs-like analytics and processes
14. Applies design assurance methods for flight-critical elements (e.g., auto-mitigate functions)
15. Supports current SMS processes; including reporting of system failures back to designers
16. Provides an incremental step to the IASMS concept described by the National Academies [2]

Fortunately, many of these principles and traits are also intrinsic to the design and evolution of the National Airspace System (NAS), which includes for example UTM and SWIM.

For initial development and testing, a UTM-like ecosystem has been used [5]. Within this ecosystem, instances of the three high-level functions may exist at various locations (e.g., at the service provider(s)/supplier(s), at the GCS, and on-board). To begin to evaluate this design space and to check for compatibility with existing UTM service concepts, three locations have been used for initial testing (Figure 3). Within this architecture, three end-to-end services have been tested, as have several monitoring and assessment sub-functions. More details on this work and the underlying architecture are provided in Section 2.3 and in Appendices A, B, and F.

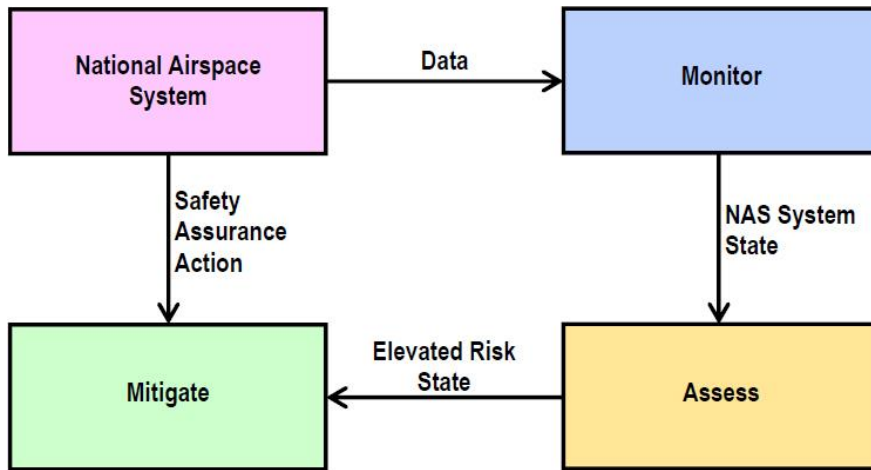


Figure 1. Functional elements and flow of information for an IASMS (as shown in [2])

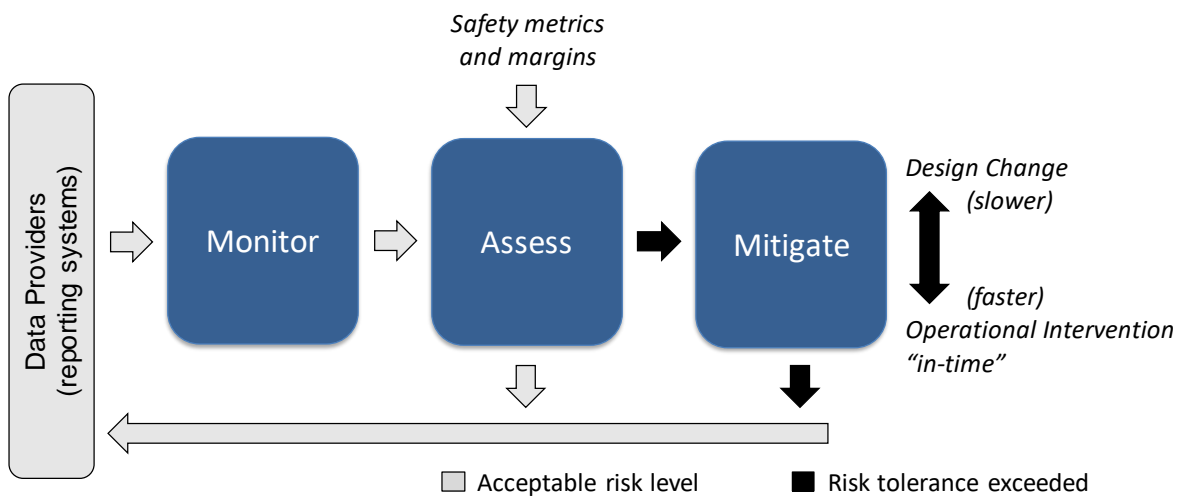


Figure 2. Functional elements and flow of information for an in-time safety assurance system

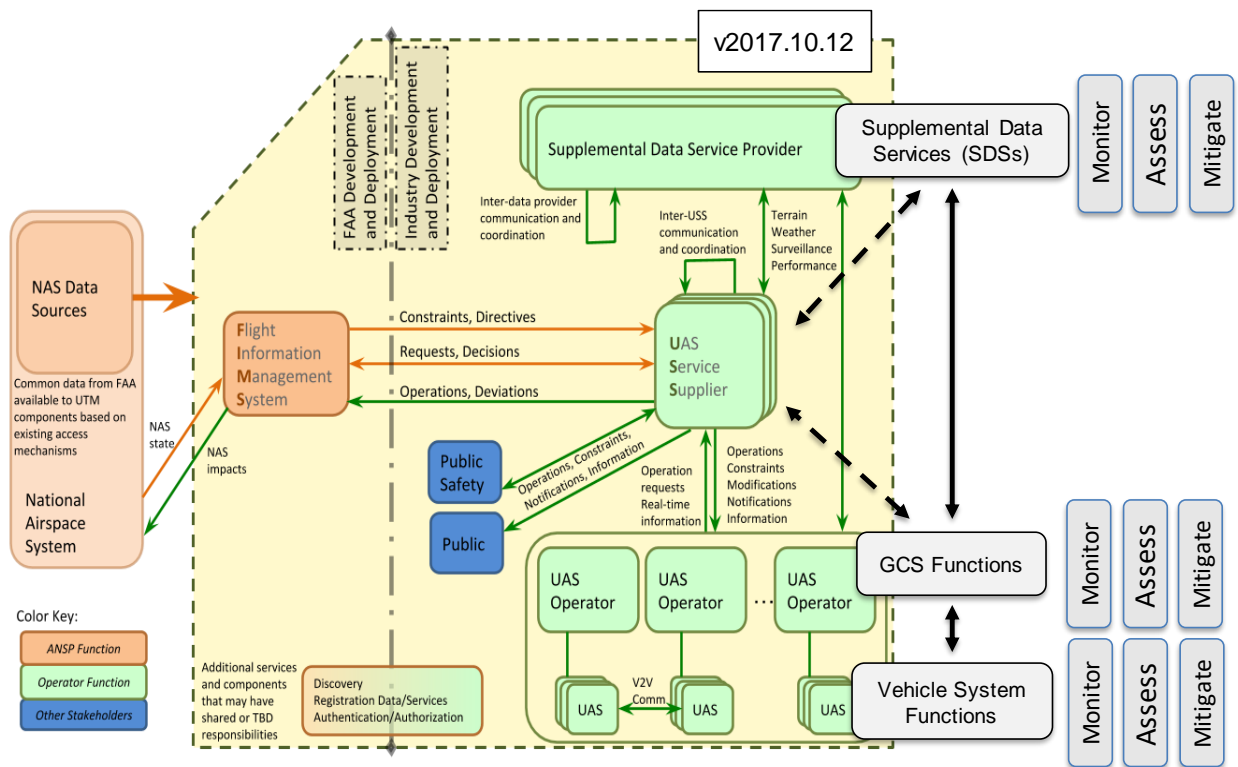


Figure 3. In-time safety assurance functions applied within the UTM ecosystem for initial testing [5][6]

2.2. SWIM and ASIAs Correspondences

SWIM is a framework for exchanging information regarding the state of airspace operations [14]. This framework consists of standards, infrastructure, and governance that enables both the management of information and its exchange between qualified parties via a set of interoperable services. The SWIM system operates through a flexible and secure service-oriented architecture where information providers and consumers interact through registries that list the services available and describes how to connect and use them. Information providers maintain and operate the services (e.g., Notices to Airmen (NOTAMs)), and consumers request and receive information. Requests can be on an as-needed basis (called 'request/reply') or by subscribing to receive information automatically (called 'pub/sub' or 'publish/subscribe') per the terms of an *a priori* agreement between the provider and consumer. To achieve interoperability, applications that employ SWIM services use standardized exchange models and protocols. To date, these are categorized as three service types. SWIM is extensible to other service types and this may provide a path to implement any new services that fall from the in-time safety assurance system concept presented here. The three existing SWIM service types are:

- Aeronautical information service (AIXM exchange model)
- Weather information service (WXXM exchange model)
- Flight information service (FIXM exchange model)

As will be described in Section 3, many information elements (and parameters) relevant to the in-time safety assurance system concept are already part of these services. In some cases, the content may require extension, while the underlying exchange protocol may be applicable (e.g., low altitude winds in urban areas). In addition, new SWIM services are becoming available to support specific needs of UAS operations.

Similar to SWIM, the ASIAs program (also referred to as the ASIAs system) collects and manages a large amount of operational data. But the types of data are different, as is the availability and intended use. The ASIAs program connects nearly 200 information sources from across government, industry, and the community, archives data from these sources, and then uses these data to monitor known risks, detect emerging risks, and evaluate the effectiveness of mitigations [15]. The correspondence with the aims of the system concept presented in this document is direct; with the primary differences being the method, the cycle time, and the operator community. The ASIAs-based method requires significant human involvement (e.g., subject matter experts) and ranges from months to years to complete the monitor-assess-mitigate cycle. This is largely because mitigations typically require changes to designs, policy, or training/maintenance. In contrast, the 'in-time' safety assurance concept presented here aims to shorten this significantly (e.g., a few seconds to a few hours) for some types of hazards or vulnerabilities. Both concepts aim to be proactive in terms of identifying PATs before accidents occur.

Contributors to ASIAs include the FAA plus more than 40 airline operators, many business jet operators, aircraft manufacturers, and maintenance/repair organizations. The resulting information covers approximately 99% of all U.S. air carrier commercial operations. There is no corresponding coverage of UAS operations (or urban UAS operations). However, there is an industry activity underway considering the efficacy and methods for creating a similar program for UAS [17]. Of the many information sources used by ASIAs, the following can be either directly utilized by the envisioned system concept, or can serve as a model or framework for a complementary capability for urban UAS (or UAM) operations of the future.

- ASAP (Aviation Safety Action Program)
- ATSAP (Air Traffic Safety Action Program)
- ASRS (Aviation Safety Reporting System)
- FOQA (Flight Operational Quality Assurance)
- LOSA (Line Operations Safety Audit) and M-LOSA (Maintenance LOSA)
- METARs and MORs (Meteorological Aviation Reports; Mandatory Occurrence Reports)
- NFDC (National Flight Data Center)

FOQA [18] is particularly relevant to the safety assurance system concept described in Section 1, as it covers the routine collection and analysis of flight data pertaining to individual flights as well as aggregated across many flights. Flight data are recorded onboard during flight, then off-loaded after flight. Over 200 parameters are recorded regarding the state of the aircraft and onboard systems. In terms of finding systemic issues that require mitigation, aggregation of data across flights has proven to be of greater value than analysis of single flights. Aggregated data allow analysts (as well as assessment tools) to look for trends and patterns. For example, [18] discusses how excessive descent rates can be identified across the fleet for a particular airport. This would perhaps suggest a change to the approach procedure at that airport. One important aspect of FOQA is the process for de-identification and

protection of data. Without assurances of these traits, sharing across the industry would not be possible.

Some UAS operators and manufacturers do retain and analyze flight data logs; however, nothing on the scale of FOQA exists. Such a capability would be ideal to support the Monitoring and Assessment functions of the safety system described in Section 1, particularly as/if the number of operations grows. The parameter set is well defined and many are the same as would be needed for urban sUAS operations and UAM (e.g., aircraft position, heading, and velocity). Although it is desirable to get some flight data in ‘real-time’ (via wireless link); off-loading post-flight can support some of the envisioned monitoring and assessment functions. In addition, it is likely that some of the tools used by FOQA for managing large-scale information sets and analyzing these sets to look for vulnerabilities (e.g., PATs) may be translatable to ‘in-time’ highly automated settings and cycle times.

In summary, although not operating in ‘real-time’, ASIAs offers many correspondences to the information needs and functions embodied by the system concept presented in this document. These should be leveraged as much as possible as development progresses.

2.3. Architecture Supporting Initial Testing

Figure 4 illustrates the architecture used for concept exploration and preliminary testing within a UTM ecosystem. For this instantiation, an initial set of in-time safety assurance services were defined as were two types of Supplemental Data Service Providers (SDSPs), a research Ground Control Station (GCS), and a test aircraft hosting an onboard research platform. Using this architecture, representative physical, logical, and functional designs were tested to support requirements exposure and validation during this phase of R&D. These tests are discussed further in Section 6, as well as in the Appendices.

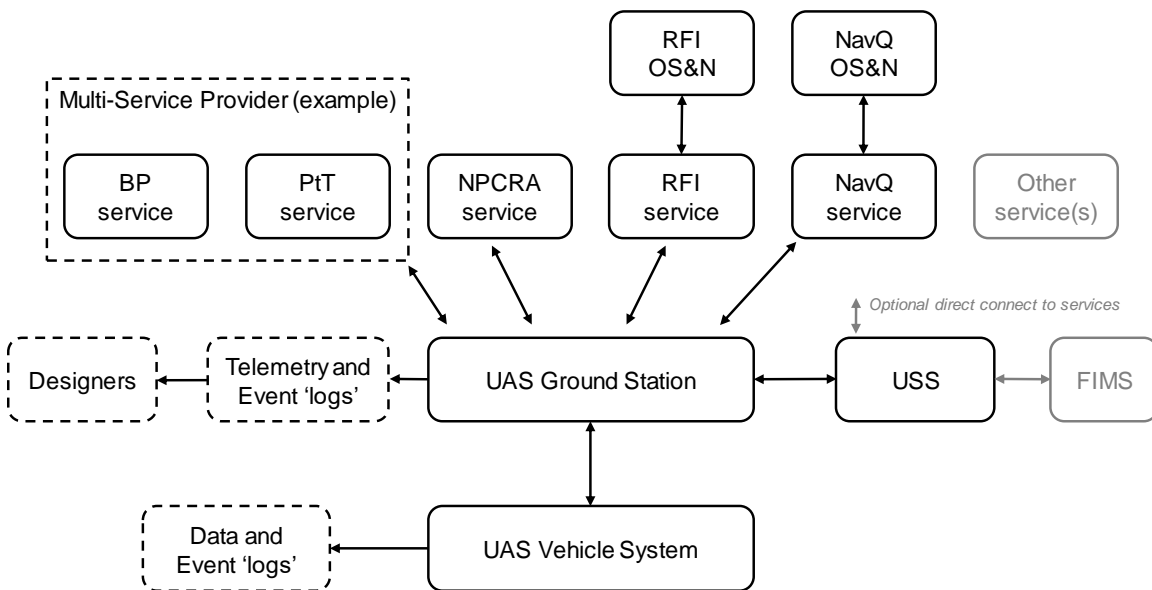


Figure 4. Architecture used for developmental testing

Several terms and acronyms are used in Figure 4 to label architectural elements. These are defined below. Additional details can be found in Appendix A and B.

- Multi-Service Provider. In UTM, Supplemental Data Service Providers (SDSPs) may be providers of individual services or multiple services. In the test architecture, we wanted to evaluate both types of providers. Here two services are combined in terms of information exchange with the UAS ground station.
 - BP, Battery Prognostics service
 - PtT, Proximity to Threat service
- NPCRA, Non-Participant Casualty Risk Assessment service (single-service provider)
- RFI, Radio Frequency Interference service
 - Utilizes information provided by the RFI OS&N (Observation Stations and Network)
- NavQ, Navigation System Quality service
 - Utilizes information provided by the NavQ OS&N

Urban Infrastructure and Ground-based Elements

The two OS&N elements allow for testing and evaluation to determine the efficacy of using urban infrastructure to help to reduce risk associated with hazards in the flight environment (i.e., supporting better Monitoring and Assessment functionality). More specifically, in-situ observations of the RF environment at relevant frequencies can be used for model validation/updates and to see in-time disturbances that may lead to loss of link if continuing on the same flight plan or trajectory.

Similarly, utilizing GPS or other navigation system receiver observables from appropriately positioned stations within the urban area can help to validate predictive models regarding navigation system performance (e.g., with respect to assumptions of multi-path effects at low altitudes). An added benefit of access to GPS observables from a network of receivers is the potential to apply ‘corrections’ that remove common errors (e.g., due to atmospheric attenuation); this could enable a form of differential GPS to be applied to improve performance [19]. Lastly, a NavQ service can leverage and provide data from terrestrial-based Alternate Positioning, Navigation, and Timing (APNT) system(s) that may be available in urban areas. For this testing, two such APNT system were implemented and are being evaluated as part of this service: Locata™ [20] and NextNav™ [21].

Although not tested here, the OS&N concept can also be used to provide weather observables within urban areas (e.g., winds, temperature, and visibility) similar to the way Automated Weather Observing Systems (AWOS) work at commercial airports [22]. This capability would likely be required for UAM verti-ports where all-weather operations are desired.

NASA’s version of a UAS Service Supplier (USS) was used to test interoperability with UTM as well as to access inherent safety-related assurance capabilities provided by UTM elements such as air traffic and airspace management functions. Although not tested to date, this would include functions like provided by the Low Altitude Authorization and Notification Capability (LAANC) service [23] and other FIMS or USS services (which in turn may provide connectivity to SWIM services). Further, the USS may provide USS-specific data products applicable to the envisioned safety assurance system functions. Some have suggested combining GCS and USS functions, USS/SDSP connectivity, and direct USS-to-vehicle communications during flights. These concepts were not tested but are supported by the architecture.

safety assurance functions and sub-functions are at various levels of maturity and will mature at different rates going forward as the research progresses.

Among other things, cFS allows independently-executing functions to access a common virtual ‘shared’ information bus. More specifically, the framework coordinates bus access and enforces memory access permissions so that functions may read or write information to this bus with little overhead, much like ‘apps’ interface to cloud-based data storage. cFS has matured over many years and is in widespread use across many domains where real-time OS performance can be mission- and safety-critical. As such, it provides the stable and robust platform we require for conducting R&D on each of the envisioned functions, as well as the aggregate system-of-systems aimed at in-time safety assurance. For example, we can create an asynchronous ‘app’ associated with each of the monitoring sub-functions mentioned previously, as well as for any automated or autonomous assessment and mitigation functions we may want to evaluate. This also allows each ‘app’ to be designed to unique data quality requirements (DQRs), design assurance levels (DALs), data processing assurance levels (DPALs), and/or Specific Assurance and Integrity Levels (SAILs) [29][30][12].

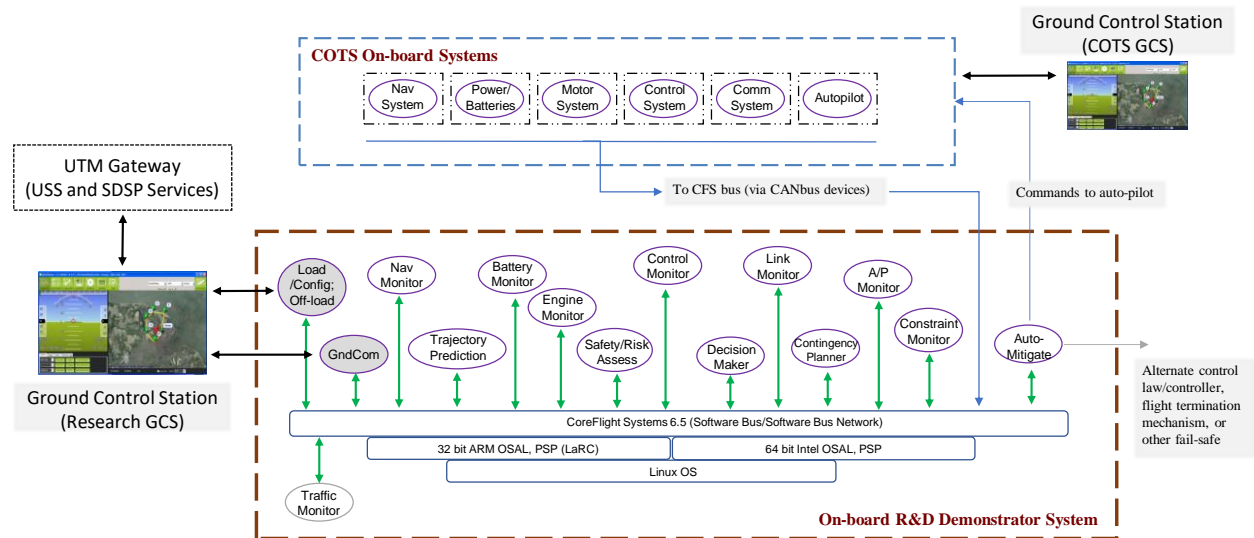


Figure 6. Platform for testing onboard functions using CoreFlight System [6][27][28]

Two caveats should be mentioned with respect to the functional elements shown (in Figure 6) as connected to the cFS bus. First, only limited auto-mitigation control functions have been tested. This is because research has primarily focused on monitoring and assessment to date. Some testing of auto-mitigation has been done via ICAROUS [31][32], however this was accomplished by signaling the COTS auto-pilot when monitoring or assessment thresholds were exceeded, and providing guidance commands via that signaling. For cases where the COTS auto-pilot is not able to respond appropriately, an alternate control law (or controller), or other fail-safe mechanism may be required. Second, monitoring and assessment functions may not span all of the hazard types shown in this experimental system; and ultimately, there may also be some grouping. For example, vehicle health or Electric Power Train (EPT) monitoring could combine battery and engine/motor monitors. In addition, some of this functionality may become embedded within the COTS sub-systems (e.g., to achieve a higher DAL).

The ‘Constraint Monitoring’ function is based on a capability originally conceived and implemented as Safeguard [33][34]. Safeguard was designed to be an independent highly assured system that warns (either the autopilot or a remote pilot) of impending violations of geo-spatial constraints (e.g., stay-in or stay-out areas). Here, the Constraint Monitor function is a more general-purpose independent monitor that can watch for impending violations of these constraints as well as other operator-specified or ATM-defined constraints. These include for example airspace restrictions, range limits, path deviations, envelope excursions, terrain/obstacle separation, and altitude/airspeed restrictions. Predicted violations can trigger actions by the remote operator, contingency management functions, and/or auto-mitigation functions (including the auto-pilot/flight controller). This function can also provide a form of behavioral bounding such as described in [35]. As such, flight controller non-determinism can be constrained and enable learning of safe limits of behavior. As long as this function is an independent system and highly-assured, it can be the ‘teacher’ in this regard; mitigating the risk of non-deterministic behavior.

The on-board architecture shown in Figure 6 was selected based on the guidelines and principles laid out earlier in this section; while also allowing for investigation of the trade-offs regarding on-board ‘in-time’ monitoring, assessment, and mitigation of risk versus ground-based versus a mix of both. Preliminary testing involves two forms of safety/risk assessment functions and both are designed to execute on-board as well as off-board (see Appendix B). Findings from these tests are to be published, including characterizing the efficacy of these two and other on-line assessment methods.

3. Information Requirements

Given an in-time safety assurance concept that applies ‘big-data,’ data-driven, and model-based predictive capabilities, the more high-quality and relevant data that can be accessible as inputs to the system, the greater the potential for the system to reduce risk. This is particularly true when trying to identify PATs that can result from unforeseen or unexpected condition combinations or cascades. This is a lesson-learned over decades, and applied today in SMS [3] and ASIAs [15] for commercial air transport-category operations. However, as with ASIAs, there may be challenges with integrating across heterogeneous data sets as well as with sharing some types of data across manufacturers, operators, and those who develop/manage infrastructure systems. Exacerbating this issue for emerging urban operations is the likelihood that some infrastructure and services may not be designed specifically to support aviation and meeting aviation system performance standards (e.g., urban environment monitoring systems).

In addition, some information classes or parameters may not be required for some application domains (i.e., mission/vehicle types and flight environments). For example, urban sUAS missions and vehicles are expected to be very diverse, as are the flight profiles; whereas UAM operations are likely to be more homogeneous. Risk assessments such as SORA can help to determine the scope of information required for specific missions/vehicles and flight environments.

With this in mind, below we discuss the span of considerations that are relevant in order to provide the data inputs to the envisioned safety assurance system (i.e., the far left box of Figure 2).

3.1. Content and Classes

A set of 16 classes of information has been identified that can enable the Monitoring and Assessment functions envisioned for the in-time safety assurance system and the selected application domain. This set spans a broad range of observables related to known safety risks, while also allowing for tailoring to user/operator preferences and risk tolerance. It is recognized that several issues (such as described above) may hinder or otherwise affect the availability of some of these classes or parameters. However, as mentioned previously, the in-time safety assurance system ConOps and architecture are scalable, and in this case, can be scaled to utilize the information available; keeping in mind that with less data, there will be reduced capability to identify and mitigate some classes of vulnerabilities (e.g., PATs).

The set of identified information classes are shown in Figure 7. Parameters within these classes follow in Table 1. For many entries in the table, there are existing relevant standards (which may or may not need to be revised) and existing sources, services, or capabilities that may be extendible to provide the information. For classes marked with a (*), external environment data is needed at a minimum for the launch site(s). It is desirable to also have data for landing site(s) and for locations or volumes within the urban area and near planned flight route(s). Metadata requirements are described separately (see 3.3).

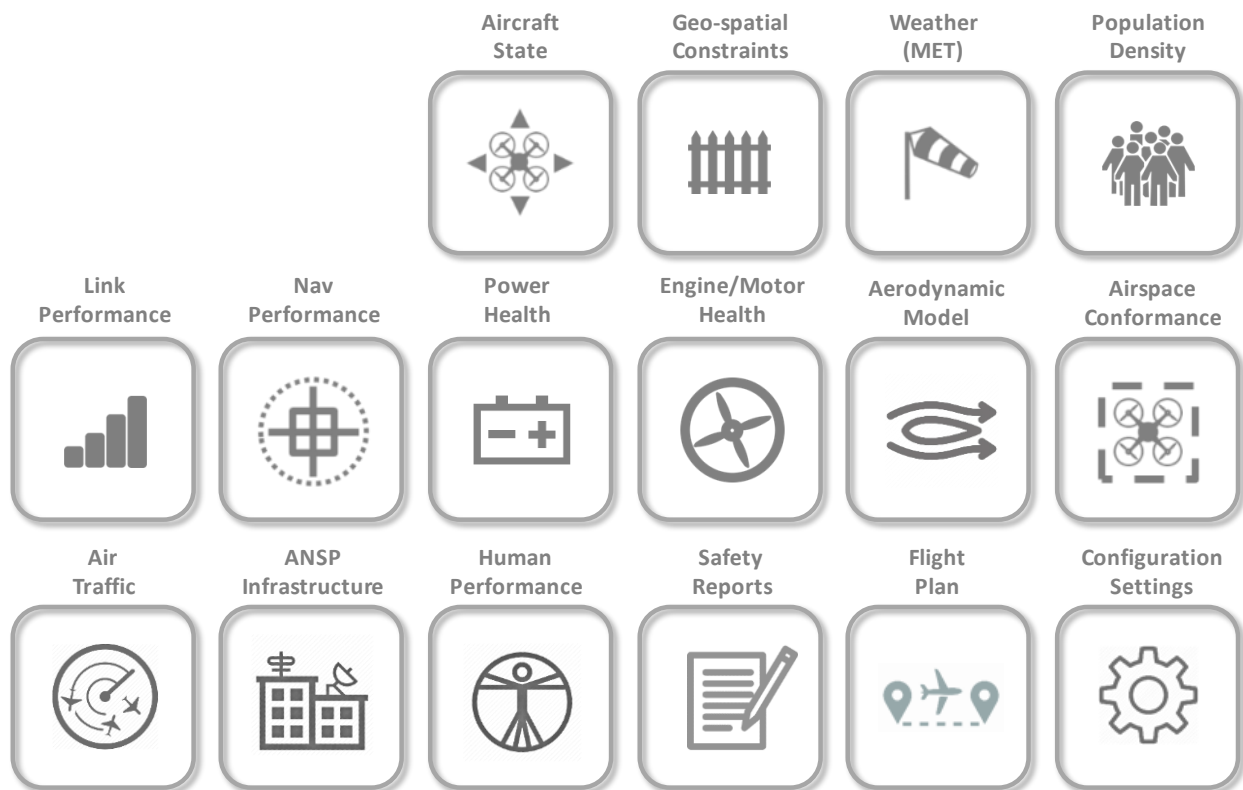


















Figure 7. Information classes relevant to in-time safety assurance functions

Table 1. Information classes and parameters.

Info Class	Parameters
 Aircraft State	Position (latitude, longitude, altitude)
	Attitude (pitch, roll, yaw)
	Heading
	Track
	Airspeed
	Groundspeed
	Vertical speed
	Acceleration (x,y,z)
 Geo-spatial Constraints*	Flight-critical system states (incl. flight controller state and auto-pilot mode)
	Airspace boundaries (e.g., Classes A-G)
	No-fly zones (e.g., Temporary Flight Restrictions (TFRs))
	Obstacles (type, location, extent)
	Vertical structures (some may also be Obstacles)
	Terrain (Area 2, 3, and 4, See [41][43])
 Weather*	Operator-defined geofenced areas (e.g., Stay-in regions)
	Wind speed and direction
	Visibility
	Air Temperature
	Barometric pressure
	Precipitation
	Relative humidity
Cloud ceiling	
 Population density*	Forecast model – Weather forecast database or model with set (or subset) of weather parameters above and for a defined coverage volume and time window (See MET/WIXM information types [25])
	Person position observables (e.g., from camera-based technologies)
	Person position reports (e.g., from cell phone-based applications)
	Forecast model – Population density database or model with estimated #people in each cell of an (x,y) grid across a defined coverage area and for defined time epochs (preferably correlated with 2/3-D building footprints)
 Link performance* (at relevant frequencies)	Signal strength observables (e.g., RSSI)
	Channel occupancy rate
	Message drop count and type
	Forecast model – Link performance database or model with set (or subset) of parameters above and for a defined coverage volume and time window
 Nav performance*	GPS receiver observables (e.g., DOPs, SVs) (ephemerides)
	INS/IMU observables
	Magnetometer (or other magvar measure)
	Augmentation system corrections (if available)
	Alternate nav system observables (if available)
	Forecast model – Navigation system performance database or model with set (or subset) of parameters above and for a defined coverage volume and time window

Power system performance 	Battery voltage (each pack)
	Battery current (each pack)
	Battery temperature (each pack)
	Battery model (derived from calibration procedure) (each pack)
Engine/motor performance 	Vibration level (each motor)
	Temperature (each motor)
	Rotor current (each motor)
	Engine/motor model (derived from calibration procedure) (each motor)
Aerodynamic model 	Information to develop initial model and flight data to validate or otherwise improve the model (see Appendix D)
Airspace conformance 	Authorizations (e.g., as if from LAANC)
	Airspace-related warnings (e.g., from ATM/ANSP/USS)
	ATC communications (if available)
Air traffic 	Identification and location reports (e.g., ADS-B/Remote ID or radar-based)
	Intended flight plan
	Schedule information (e.g., departure/arrival and waypoint slot times)
	Air traffic-related constraints (e.g., procedures and restrictions)
	Air traffic-related warnings (e.g., from ATM/ANSP/USS)
ANSP infrastructure (AIS) 	Airport/heliport/vertiport locations (see [42])
	Airport/heliport/vertiport feature information (see [42])
	ANSP infrastructure availability and status (e.g., NOTAMs of outages) Augmentation systems availability and status (e.g., GBAS, SBAS, LOCD-IN) Alternate nav systems availability and status
	See AIS/AIXM information types [25][36][41]
Human performance 	Communications (voice/text between participants)
	Participant inputs (e.g., operator commands sent to vehicle)
	Time on duty (of each participant)
	Training recency and history (of each participant)
	Direct physio measures; eye-tracking; workload measures

Safety reports 	ASRS reports (updated for UAM and urban UAS)
	ASAP/ATSAP reports (updated for UAM and urban UAS)
	MORS/PIREPS (updated for UAM and urban UAS)
	Error and failure logs for equipment and functions
	Maintenance logs (incl. age/history of critical components)
Configuration settings 	User or operator-defined risk tolerance (e.g., thresholds, safety margins)
	User or operator-define constraints (e.g., geo-fences, speed limits)
	User or operator input of vehicle specs (incl. MTBF estimates)
	Contingency policies (e.g., if loss of link, trigger auto-pilot LAND mode)
Flight plan 	Flight plan waypoints (incl. ETA or airspeed at waypoints)
	Flight plan mode changes
	Takeoff and landing info (e.g., descent and climb rates)

3.2. Models and Databases

One of the most desirable traits of the system concept is to provide predictive capability. Models and/or databases for some classes of information can help to enable this capability. Further, because of the ‘big-data’ data-driven approach, model validation and quality can improve over time. Model updates can be based on flight data from previous flights as well as data provided by observation stations within the region of flight. As a result, predictive uncertainty can reduce by closing the gap between the validation domain and the application domain for each model [37]. Based on prior similar work and the expected short duration of flights in this domain, it is anticipated that model exchanges do not need to occur during flights. Instead, exchange is needed as part of a pre-flight procedure and checklist, to check for model updates and ‘load’ the latest version(s) into the operational system. Similarly, the post-flight procedure should allow for forwarding relevant data back to model designers and service providers (see Figures 1, 2, and 4).

Ten types of models (or databases) are envisioned as supportive of the concept (see Table 1).

- Aircraft aerodynamic model
- Geo-spatial feature model (including terrain and obstacles)
- Weather forecast model*
- Population density model*
- Link performance model*
- GNC system performance model (incl. Nav Quality model*)
- Battery performance model
- Engine performance model
- Power estimation model
- Mean time between failure (MTBF) models (for critical components)

For highly autonomous low altitude urban flight, there are R&D challenges for some of these model types (see examples in Appendix A); however, there are efforts underway to address them by industry, academia, and government agencies. More details on aerodynamic modeling are given in Appendix D.

The model types above with the (*) could benefit from having a common representation in a spatio-temporal reference frame. In other words, estimates or predicted (forecast) values of parameters may be provided at (x, y, z, t) increments over a user-specified range. This is the approach used for some existing weather products and SWIM services [38][39]. For the models noted above to be useful to safety assurance during low-altitude urban flight operations, it is to be determined appropriate values for horizontal/vertical resolution (i.e., cell size), forecast horizon (or look-ahead time), and forecast resolution. This issue and other information quality issues are addressed further below.

3.3. Quality

Well-defined quality procedures facilitate effective data exchange by allowing data producers to clearly specify the quality of the data produced, and by allowing data users to determine the extent to which the data meets their requirements. Data quality should be achieved and maintained in accordance with DO-200B, “Standards for Processing Aeronautical Data” [29]. This standard covers all aspects of quality management and has been successfully applied in commercial aviation for decades, with revisions twice over this timeframe to accommodate the new types of data and information services used in aviation systems over the intervening years.

As described in DO-200B [29]:

- Data Quality is defined as the degree or level of confidence that the data provided meets the requirements of the user of the data.
- Each data user has the responsibility to define his/her data quality requirements based on the intended use of the data.
- Quality requirements cover both the processing and management of data throughout the ‘aeronautical data chain’; this chain includes all exchanges from data origination to end use.
- DQRs are described using seven quality characteristics or traits: (1) Accuracy, (2) Resolution, (3) Assurance Level, (4) Traceability, (5) Timeliness, (6) Completeness, and (7) Format.

As stated in [29], “The degree that a data element meets the data quality requirements determines its fitness for the intended use.” Data processing requirements, including data protections/security, are also covered in this standard.

Some relevant quality standards have been established by ICAO and should be sufficient for the domain considered here. For example, [40] provides accuracy recommendations for weather observations and forecasts. Examples relevant to low altitude urban flight include: mean surface wind (direction, +/- 10 deg; speed, +/- 0.5 m/s (1 kt) to 5 m/s (10 kts), +/- 10% above 5 m/s (10 kts)); visibility (+/- 50 m up to 600 m); runway visual range (i.e., visibility at the surface) (+/- 10 m up to 400 m); air temperature (+/- 1 deg C); and pressure value (+/- 0.5 hPa). Other relevant examples of numerical quality requirements can be found in [41], which covers geo-spatial features such as would be provided on charts or in databases used by flight systems. Examples include terrain data (horizontal accuracy of 5 m; vertical accuracy of 3 m), obstacle data (horizontal accuracy of 5 m; vertical accuracy of 3 m), and heliport feature data (horizontal accuracy of 0.5 m; vertical accuracy of 0.5 m). Geo-fencing boundaries (i.e., no-fly zones) can apply the requirements specified for similar polygonal features at airports (e.g., horizontal accuracy

requirement is 1 m for apron boundaries and construction areas). These and other relevant numerical requirements for quality can also be found in RTCA and EUROCAE standards (e.g., [42][43][44]).

Because the system concept aims to provide a level of safety assurance, data integrity can be a critical characteristic that will either enable or constrain the degree to which risk to safety can be mitigated. In terms of existing quality standards, data integrity is considered part of the Assurance Level characteristic (e.g., DPAL value) [29]. Any data element (or parameter) that is an input to a flight-critical function should have a high DPAL associated with it. Further, for higher DPALs, additional processes and methods must be employed to assure the data has not been altered or otherwise corrupted prior to end-use. In other words, the data must come from a trusted source and be trustworthy. DO-200B provides guidance on processes to utilize to achieve various DPALs. In addition, there are system/technological approaches that can be employed as needed, such as applying redundant or dissimilar data sources, cyber-security protection mechanisms (e.g., [45]), and RTA/RTV techniques (e.g., [46]-[50]). A general framework for information management aimed at achieving data integrity is described in [51]. In this framework, a span of design intervention options are described that can be applied depending on the required integrity level. These options include for example augmentation services and techniques such as are employed for navigation systems today [52][53][54]. The framework also considers the role humans can play with regard to data integrity assurance.

Quality becomes particularly important for predictive functions (e.g., trajectory prediction) and functions that combine outputs of other functions (e.g., assessments across hazard monitors). In these cases, care must be taken to identify and understand how the quality of all the input data can affect the quality of derived measures and analytic tool products. This process we denote as uncertainty management and is discussed further in the next section.

4. Uncertainty Management

Within the holistic view of a safety assurance system, consideration of uncertainty management (UM) is essential, particularly for in-time predictive capabilities. Information and operational data are collected through both sensor networks and autonomous functions, each of which can suffer from resolution limitations, noise, and external forces like environmental conditions. The latter are intrinsically uncertain, being driven by complex physical phenomena that are difficult to predict in complex domains (e.g., wind tunneling effects in urban canyons [55]). Moreover, the variety of vehicle types and mission profiles expected during the low-altitude operations (e.g., [4][5][56][57]) requires UM methods that can accommodate heterogeneous vehicle performance, un-modeled events and effects, and adjust predictions accordingly. Appendix C describes a generic framework for UM focused on identification of uncertainty sources, specifically for in-time vehicle tracking and monitoring, and a formal method for uncertainty quantification (UQ). Generally speaking, UQ encompasses the study of uncertainties in input parameters as well as those derived from design simplifications that can affect the output or response of a process or function. An important facet of UQ is the proper characterization and treatment of input uncertainties. This characterization and treatment of input uncertainties is part of UM. Because of the span and diversity of information types that may be used by in-time safety assurance systems, a structured approach or framework for UM is essential.

Input parameter uncertainties can be divided into two classes: aleatoric and epistemic uncertainty [37]. Aleatoric uncertainty is the inherent variation associated with a parameter and is often referred to as

irreducible or stochastic uncertainty. An example of aleatoric uncertainties are sensor measurements. Sensor manufacturers often provide an accuracy specification as an estimate of the uncertainty to be expected when using a particular sensor (e.g., mean value, standard deviation, and probability distribution function). This type of uncertainty can also be quantified by users to some extent through a calibration or benchmarking process. Aleatoric uncertainties exist on other quality characteristics as well (e.g., timeliness; which includes update rate and latency). In contrast, epistemic uncertainty results from imperfect knowledge or ignorance of the behavior of a system, function, or process that produces a parameter or value. These can often be identified and accounted for through effective verification and validation processes, and then appropriate process controls as data is generated over time during operations and more is learned regarding system behavior in various contexts. RTA/RTV techniques in particular can help to identify and reduce epistemic uncertainty once a system has become operational (e.g., [46]-[50]). With respect to the potential for non-deterministic behavior (e.g., as may be associated with complex autonomous functions), a 'simplex' architectural approach can be used to manage or bound this type of epistemic uncertainty [58][59]. This approach is employed for example by the conformance monitor design described in [33] and [34]. A good UM framework must recognize that both types of uncertainties (aleatoric and epistemic) can occur and provide for a means of propagating them into a measure or bound on predictive uncertainty. More details on this complex issue can be found in [37].

To date, for risk assessment functions we have applied a generalized point-collocation non-intrusive polynomial chaos expansion (PCE) method as part of an underlying UM framework (Appendix C). Polynomial chaos is a surrogate modeling technique based on a spectral representation of uncertainty. This approach allows for the generation of uncertainty estimates without modification to underlying source code of the process or function being modeled. In addition, estimates for sensitivities and confidence intervals can be found analytically without significant increase in computational costs. Sensitivity estimates discovered by application of this method can guide future research and resource investments (e.g., re-design of function or acquisition of better sensors). These can then drive down the overall uncertainty in the assessment and prediction of safety risk. Also, the estimation of confidence intervals can give insight into the non-determinism of predictions. These models are extremely computationally efficient in comparison to traditional UQ approaches such as Monte Carlo simulation.

The PCE methodology is initially being applied to different (3-DoF and 6-DoF) off-nominal trajectory and impact point predictive models to better understand the input parameter sensitivities for parameters such as heading, ground speed, wind velocity, wind direction, roll, pitch, and yaw at varying altitudes. One initial goal is to identify a ceiling altitude where the 3-DoF modeling estimations can be sufficient for pre-flight risk assessment. The analysis will also help identify sensitive input parameters where additional testing and/or enhanced sensors or instrumentation might be beneficial. More on this element and the underlying framework is provided in Appendix C.

5. Exchange Model and Protocols

The Aeronautical Information Exchange Model (AIXM) [25] enables the management and exchange of aeronautical information and has generally been adopted for future aviation-related information support systems. The current version includes for example airport/heliport information, airspace structures, waypoints, navigation aids, arrival/departure procedures, routes, and flight restrictions. AIXM is one of a family of conceptual data models developed by the FAA and EUROCONTROL to

facilitate global interoperability and information exchange. Two others are the Weather Information Exchange Model (WXXM) and the Flight Information Exchange Model (FIXM). WXXM enables interoperable meteorological information exchange. FIXM facilitates the exchange of flight schedules and flow information in a globally standardized format. The Aerodrome Mapping Exchange Model (AMXM) was developed specifically to support applications of aerodrome (i.e., airport) mapping data.

Collectively, these models enable platform-independent information collection, dissemination, and transformation through the data chain to the end-user or system. Further, the content and quality standards previously mentioned were used as the basis for these models. Each consists of a conceptual model of the information domain and an XML encoding schema. The conceptual model catalogs the features and properties of the information using the Unified Modeling Language (UML). The XML encoding schema allows exchange of the information in digital XML format. This format is similar to the JSON format previously discussed and used for the preliminary testing within the UTM ecosystem.

AIXM includes nearly 300 features, or classes of aeronautical information, many of which are relevant to low altitude urban operations. Each feature/class is broken down into attributes and associations (e.g., a runway has a surface type associated). Each association in turn can have further associations. Thus many layers of information can be defined. AIXM was developed to be extensible to meet the needs of a community of interest or application domain. This can be done by either extending the core classes to include new attributes and/or associations, or by defining new classes. For example, consider the AIXM feature class 'Airport/Heliport' [25]. This feature class comprises 11 associated features and 26 attributes. Examples of the associated features include the *TouchDownLiftoff* point, the *Apron* area, and *RulesProcedures* that apply. Examples of attributes include *fieldElevation*, *transitionAltitude*, and whether it is for *privateUse*. This class could be extended/adapted to model required UAM vertiport information which should be similar. This is the recommended approach for the new domain in general (i.e., build on top of the existing exchange models – extending relevant feature classes, attributes, and associations; and creating new classes as needed).

As with the testing performed to date, data exchange can be instantiated through AIXM-like feature services such as the OGC Web Feature Service, which enables the direct provision AIXM features [25][60]. Other relevant standards and exchange models can be found in [61][62][63]. As discussed, there are many correspondences with SWIM and where possible, SWIM feeds should be leveraged. This is another reason why a common and accepted exchange model is recommended for the new domain.

Lastly, we envision primarily request-reply type communications. Pre-flight communication between operator(s) and service provider(s) would consist of requests for the latest information available (current and forecast). Further, if contract-based, these exchanges may be automated to improve efficiency. Operators would then load onto the aircraft relevant data as part of setup. In-flight exchanges between the aircraft and the GCS (and perhaps directly with service providers) would be limited and would primarily encompass aircraft systems state information sent to the GCS (or service provider) via a telemetry link. Post-flight exchanges would involve off-loading data recorded onboard and sending relevant elements back to service providers (or designers) for quality improvement and for analysis regarding PATs that may only be identifiable by looking across many flights. Because both XML and JSON are bandwidth inefficient, binary encoding (e.g., MavLink [64]) may be needed for some of these exchanges. The above approach is the one we used for the test architecture described in Section 2.3 and Figures 4 to 6, and for the preliminary testing summarized below and later in Appendix F.

6. Supporting Tests

Several tests were conducted during 2018-2019 with the following objectives:

- Expose and validate requirements
- Evaluate the efficacy and feasibility of the envisioned information system
- Demonstrate interoperability (and compatibility) within a UTM ecosystem
- Collect data to support R&D of on-line analytics tools (e.g., for anomaly detection)
- Verification and technology maturation for selected elements
- Inform decisions regarding R&D priorities and plans going forward

For these tests, the architectural principles and constructs described in Section 2 and illustrated in Figures 4-6 were applied (e.g., a UTM-based ecosystem was used as a basis). Two sets of the tests were simulation-based and two sets were flight test-based using sUAS platforms. Simulation testing occurred at NASA Ames Research Center using two different simulation facilities, tailored somewhat to urban sUAS operations and UAM operations, respectively. Flight tests were conducted at NASA Langley Research Center using the City Environment for Range Testing of Autonomous Integrated Navigation (CERTAIN) and multiple sUAS aircraft equipped as shown in Figure 6. During the flight tests, the system spanned and connected SDSP servers and the USS at NASA Ames with aircraft, GCSs, and an SDSP server operating at NASA Langley. More details on these supporting tests are provided in Appendix F.

7. Related Industry Developments

Within the target domain there are relatively few commercial operations today. UAM is still in a concept development stage, although some in industry are working aggressively to achieve operational capability in the near-term (e.g., [4]). As an initial step, reference vehicle designs have emerged and are being developed (e.g., [65]). As for safety assessments, at least one company has published results of a failure modes and effects analysis [66]. In contrast, sUAS flights have become somewhat ubiquitous with many manufacturers of aircraft and developers of supporting systems. However, due in part to safety concerns, operations typically avoid flight over people and urban areas, particularly at night or in bad weather conditions. Most also involve a remote pilot and remain in visual line-of-sight of this pilot and/or visual observer(s). However, there are many existing industry products and systems that are used for sUAS operations or related fields that can be leveraged to help achieve the envisioned safety assurance functions. Some were discussed in prior sections; additional examples are given below.

GCS software and mobile ‘apps’ support sUAS operators in the field for configuration, flight planning, tracking, command and control, and data recording/analysis. Most of these connect to a network and data is routinely and automatically returned to the manufacturer or service provider(s) to support product improvement. Connections may occur during pre-flight, in-flight, and/or post-flight, and various commercial links and networks are used to make these connections. Some products also provide access to services like those alluded to here as needed for safety assurance (e.g., LAANC and AIS/TFR). One company in particular asserts 15+ services available within its product; most to help during mission planning and when making go/no-go decisions. Similarly, several companies have developed USS systems per the UTM ecosystem concept (in the US) and U-space (in Europe). These can be directly applicable and enabling of future in-time safety assurance functions such as are described in Section 1.

As mentioned previously, operational approval has been granted for limited package deliveries in urban/sub-urban settings (e.g., [7][8]). Lower-cost fault-tolerant architectures have been productized by

at least one sUAS manufacturer. Detect-and-avoid and sense-and-avoid (DAA/SAA) avionics for UAS have been the subject of standards and product development. Pilot programs have been sponsored by the FAA that include industry and local municipalities working together to explore ways to enable more routine operations near and over populated areas without compromising safety. Results are informing new rulemaking aimed at enhancing both capability and safety. One relevant example is 'Remote ID'; a transponder-like capability for identifying and tracking UAS in the U.S. [67]. As described previously, aircraft location information is needed to fully achieve the in-time safety assurance system concept.

Some insurance companies have begun to collect vast amounts of UAS operational data and at least one company maintains component reliability data. There are several examples of urban infrastructure and connectivity being developed for non-aviation purposes that may indirectly benefit urban aviation safety in the future (e.g., [16][21]).

The Unmanned Aircraft Safety Team (UAST) is a government/industry group that is developing data-driven consensus-based recommendations for safety enhancements [17]. One of their initiatives is to explore the extent to which data sharing across industry (such as is done for ASIAs) can have positive effect with respect to the safety goals of the UAS community. The UAST is modeled after the Commercial Aviation Safety Team (CAST), which has successfully defined and implemented >200 safety enhancements for commercial airline operations over the past 20+ years; including the ASIAs program.

These are just a few examples of developments by an innovative and fast-moving industry. Safety assurance will likely be the enabler or the constraint to future operations that are routine, frequent, all-weather, and highly-autonomous in urban environments. In other words, it may be the throttle or the brake on the train crossing this frontier. It seems industry recognizes this, and is moving in a positive direction toward enabling on-line and predictive capabilities such as suggested by the concept described herein. It remains however somewhat to be determined how these capabilities can complement or advance current SMS practices and design-time safety assurance processes used in the aviation sector.

8. Summary and Plan for Updates

This report comprises architecture and information requirements, recommendations, and considerations toward enabling in-time and predictive safety assurance capabilities within the domain of low altitude highly autonomous urban flight operations. This broad class of operations can include many types of missions, vehicles, human/system roles, and flight environment conditions. For this reason, any stated requirements should be considered initial requirements that can be used to drive R&D. Over the course of R&D by industry, academia, and government agencies, ConOps will mature for both urban flight operations and in-time safety assurance systems (e.g., [68]). Industry solutions and FAA policies will advance. It is also expected that additional hazards/risks will be identified, in particular for UAM, where function allocation, roles/responsibilities, vehicle designs, airworthiness requirements, and acceptable levels of safety are still being defined.

To align with this evolution, this document and any associated research plans, standards, and developments will be updated in the future.

References

- [1] National Aeronautics and Space Administration, Aeronautics Research Mission Directorate, *Strategic Implementation Plan (2017)*, [Online] <https://www.nasa.gov/aeroresearch/strategy>, 2019.
- [2] National Academies of Sciences, Engineering, and Medicine, *In-time Aviation Safety Management: Challenges and Research for an Evolving Aviation System*, 2018.
- [3] International Civil Aviation Organization, *Safety Management, Standards and Recommended Practices*, Annex 19 to the Convention on International Civil Aviation, 2nd edition, July, 2016.
- [4] Uber Elevate Summit, "Fast-Forwarding to a Future of On-Demand Urban Air Transportation," White Paper, October 27, 2016, [Online] <https://www.uber.com/us/en/elevate/vision/>, 2019.
- [5] Aweiss, A., et. al., "Unmanned Aircraft Systems (UAS) Traffic Management (UTM) National Campaign II," Proceedings of AIAA SciTech Forum, AIAA Infotech @ Aerospace, Kissimmee, FL, January 8-12, 2018.
- [6] Young, S.; Quach, C.; Goebel, K.; and Nowinski, J.; "In-Time Safety Assurance Systems for Emerging Autonomous Flight Operations," 37th AIAA/IEEE Digital Avionics Systems Conference, London, UK, September 23-27, 2018.
- [7] "FedEx Completes First Commercial Drone Delivery," [Online] <https://www.ttnews.com/articles/fedex-completes-first-commercial-drone-delivery> , Oct 21, 2019.
- [8] "FAA Allows UPS to Deliver Medical Packages Using Drones," Sandra Garcia, NY Times, Oct 2, 2019.
- [9] FAA, "Unmanned Aircraft Systems Safety Risk Management Policy," FAA Order 8040.6, Oct 4, 2019.
- [10] Belcastro, C. M., Newman, R. L, Evans, J. K., Klyde, D. H., Barr, L. C., and Ancel, E.; "Hazards Identification and Analysis for Unmanned Aircraft System Operations," 17th AIAA Aviation Technology, Integration, and Operations Conference, Denver, CO, June 5-9, 2017.
- [11] Belzer, J; et. al.; "Wide-Scale Integration of Unmanned Aircraft Systems into the National Airspace System through a Fault Tree Analysis Approach," 36th AIAA/IEEE Digital Avionics Systems Conference, St. Petersburg, FL, September 17-21, 2017.
- [12] Joint Authorities for Rulemaking of Unmanned Systems, "Guidelines on Specific Operations Risk Assessment," JARUS Document JAR-DEL-WG6-D.04, June 26, 2017.
- [13] Neogi, N., Graydon, M., and Wasson, K.; "Guidance for Designing Safety into Urban Air Mobility: Hazard Analysis Techniques", AIAA Scitech Forum, Orlando, Florida, January 6-10, 2020.
- [14] ICAO, *Manual on System Wide Information Management (SWIM) Concept*, ICAO Doc 10039, 2015.

- [15] Federal Aviation Administration, *Aviation Safety Information Analysis and Sharing Program Fact Sheet*, Apr 2016, [Online] https://www.faa.gov/news/fact_sheets/news_story.cfm?newsId=18195.
- [16] National Institute of Science and Technology, *Smart Cities and Communities*, 2019, [Online] <https://www.nist.gov/el/cyber-physical-systems/smart-america/global-cities> .
- [17] Unmanned Aircraft Safety Team, *Mission and Safety Enhancements*, 2019, [Online] <https://www.unmannedaircraftsafetyteam.org/>
- [18] Federal Aviation Administration, *Flight Operations Quality Assurance (FOQA)*, FAA Advisory Circular AC 120-82, April 12, 2004.
- [19] Gilabert, R., Dill, E., and Uijt de Haag, M., "Evaluation of Improvements to the Location Corrections through Differential Networks (LOCD-IN)," Proceedings of the 32nd International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GNSS+), Miami, FL, Sep 16-20, 2019.
- [20] Rizzos, C., "Locata: A Positioning System for Indoor and Outdoor Applications Where GNSS does not Work," Proceedings of the 18th Association of Public Authority Surveyors Conference, 2013.
- [21] Meiyappan, S., Raghupathy, A., and Pattabiraman, G., "Positioning in GPS Challenged Locations – The NextNav Terrestrial Positioning Constellation," Proceedings of the Institute of Navigation's GNSS+ Conference, 2013.
- [22] Federal Aviation Administration, *Surface Weather Observation Stations*, 2019, [Online] https://www.faa.gov/air_traffic/weather/asos .
- [23] Federal Aviation Administration, *UAS Data Exchange and the Low Altitude Authorization and Notification Capability*, 2019, [Online] https://www.faa.gov/uas/programs_partnerships/uas_data_exchange/
- [24] Watkins, J., Teubert, C., and Ossenfort, J., "Prognostics As-A-Service: A Scalable Cloud Architecture for Prognostics," Annual Conference of the Prognostics and Health Management Society (2019), Scottsdale, AZ, September 21-26, 2019.
- [25] EUROCONTROL, *Aeronautical Information Exchange Model (AIXM)*, 2019, [Online] www.aixm.aero . Related information available for flight information (<https://www.fixm.aero>), weather information (<http://wxm.aero>); and extensions (<http://www.aixm.aero/document/aixm-511-extensions>).
- [26] International Standards Organization, *Controller Area Network, ISO 11898-1 and 11898-2*, 2016.
- [27] Lowry, M., et. al., "Autonomy Operating System for UAVs: Pilot-in-a-Box", 17th AIAA Aviation Technology, Integration, and Operations Conference, Denver, CO, June 5-9, 2017.
- [28] National Aeronautics and Space Administration, Goddard Space Flight Center, "Core Flight System Background and Overview," 2019, [Online] <https://cfs.gsfc.nasa.gov/> and <https://cfs.gsfc.nasa.gov/cFS-OverviewBGSlideDeck-ExportControl-Final.pdf>

- [29] RTCA, *Standards for Processing Aeronautical Data*, RTCA Document DO-200B, June 2015.
- [30] RTCA, *Software Considerations in Airborne Systems and Equipment Certification*, RTCA Document DO-178C, December 2011.
- [31] Moore, A., Balachandran, S., Young, S.D., Dill, E.T., Logan, M.J., Glaab, L.J., Munoz, C. and Consiglio, M., "Testing enabling technologies for safe UAS urban operations," 18th AIAA Aviation Technology, Integration, and Operations Conference, Atlanta, GA, June 25-29, 2018.
- [32] Consiglio, María, et al; "ICAROUS: Integrated configurable algorithms for reliable operations of unmanned systems," 35th AIAA/IEEE Digital Avionics Systems Conference, Sacramento, CA, September 25-29, 2016.
- [33] Dill, E., Hayhurst, K., Young, S., and Narkawicz, A., "UAS Hazard Mitigation through Assured Compliance with Conformance Criteria," AIAA SciTech Forum, Kissimee, FL, January 8-12, 2018.
- [34] Dill, E., Hayhurst, K., and Young, S., "Safeguard: An Assured Safety Net Technology for UAS," 35th AIAA/IEEE Digital Avionics Systems Conference, Sacramento, CA, September 25-29, 2016.
- [35] ASTM International, *Standard Practice for Methods to Safely Bound Flight Behavior of Unmanned Aircraft Systems Containing Complex Functions*, ASTM F3269-17, 2017.
- [36] Federal Aviation Administration, *Aeronautical Information Services*, 2019 [Online] https://www.faa.gov/air_traffic/flight_info/aeronav/.
- [37] Oberkampf, W., and Roy, C., *Verification and Validation in Scientific Computing*, Cambridge University Press, 2010.
- [38] Federal Aviation Administration, *Common Support Services - Weather (CSS-Wx)*, 2019, [Online] <https://www.faa.gov/nextgen/programs/weather/csswx/>.
- [39] National Oceanic and Atmospheric Administration, *High-Resolution Rapid Refresh (HRRR) Model*, 2019, [Online] <https://rapidrefresh.noaa.gov/hrrr/>.
- [40] International Civil Aviation Organization, *Standards and Recommended Practices for Meteorological Service for International Air Navigation*, ICAO Annex 3, 20th edition, July 2018.
- [41] International Civil Aviation Organization, *Standards and Recommended Practices for Aeronautical Information Services*, ICAO Annex 15, 16th edition, July 2018.
- [42] RTCA, *User Requirements for Aerodrome Mapping Information*, RTCA Document DO-272D, November 2015.
- [43] RTCA, *User Requirements for Terrain and Obstacle Data*, RTCA Document DO-276C, Nov 2015.
- [44] RTCA, *User Requirements for Navigation Data*, RTCA Document DO-201B, December 2018.

- [45] Gautham, S., et. al., "A Multilevel Cybersecurity and Safety Monitor for Embedded Cyber-Physical Systems," Proceedings of the 10th ACM/IEEE International Conference on Cyber-Physical Systems, Montreal, CA, April 16-18, 2019.
- [46] Clark, M., et. al., "A Study on Run Time Assurance for Complex Cyber Physical Systems," Air Force Research Lab, Report No. ADA585474, April 2013.
- [47] Goodloe, A., "Challenges in High-Assurance Runtime Verification," 8th International Symposium on Leveraging Applications of Formal Methods, Verification, and Validation (ISoLA 2016); Corfu, Greece, October 10-14, 2016.
- [48] Pike, L., et. al., "Copilot: A hard real-time runtime monitor," In Runtime Verification (RV), volume 6418, pages 345–359, Springer, 2010.
- [49] Goodloe, A., and Pike, L., "Monitoring distributed real-time systems: A survey and future directions," NASA/CR-2010-216724, July 2010.
- [50] Schierman, J., et. al., "Run Time Assurance for Complex Autonomy," Barron Associates, Presented at the Safe and Secure Systems and Software Symposium, Dayton, OH, June 2015.
- [51] Duan, P., et. al., "Human-In-The-Loop Evaluation of an Information Management and Notification System to Improve Aircraft State Awareness", Proceedings of the AIAA SciTech Forum, Kissimmee, FL, January 5–9, 2015.
- [52] European Space Agency, "Receiver Autonomous Integrity Monitoring and Integrity Architectures for GPS," 2019, [Online] <https://gssc.esa.int/navipedia/index.php/RAIM>.
- [53] *Understanding GPS/GNSS: Principles and Applications*, 3rd Edition, edited by Elliot Kaplan and Christopher Hegarty, Artech House, ISBN-13: 978-1-63081-058-0, May 2017.
- [54] *Position, Navigation, and Timing Technologies in the 21st Century: Integrated Satellite Navigation, Sensor Systems, and Civil Applications*, edited by Jade Morton, Frank van Diggelen, James Spilker Jr., and Bradford Parkinson, IEEE and Wiley, 2019 [in press].
- [55] Adkins, K., "Urban flow and small unmanned aerial system operations in the built environment," International Journal of Aviation, Aeronautics, and Aerospace, Vol. 6, Issue 1, 2019.
- [56] Kopardekar, P., Rios, J., Prevot, T., Johnson, M., Jung, J., and Robinson, J., "Unmanned Aircraft System Traffic Management (UTM) Concept of Operations," AIAA Aviation Forum, Washington, DC, June 13-17, 2016.
- [57] Kopardekar, P., "Unmanned Aerial System (UAS) Traffic Management (UTM): Enabling low-altitude airspace and UAS operations," NASA Technical Report, TM-2014-218299, 2014.
- [58] Sha, L., "Using simplicity to control complexity," IEEE Software, vol. 18, no. 4, pp. 20–28, 2001.

- [59] Baky, S., et. al., "Real-Time Reachability for Verified Simplex Design," AFRL PA case number 88ABW-2014-4185, September 2014.
- [60] Open Geospatial Consortium, "OGC Standards Support Aviation Information Management," 2019, [Online] <https://www.opengeospatial.org/domain/aviation>.
- [61] RTCA, *Minimum Interchange Standards for Terrain, Obstacle, and Aerodrome Mapping Data*, RTCA Document DO-291C, September 22, 2015.
- [62] RTCA, *Minimum Aviation System Performance Standards (MASPS) for Aeronautical Information/Meteorological Data Link Services*, RTCA Document DO-364, December 15, 2016.
- [63] Open Geospatial Consortium, *City Geography Markup Language (CityGML) Encoding Standard, v2.0*, 2019, [Online] <https://www.opengeospatial.org/standards/citygml>.
- [64] Tridgell, A. and Dade, S., "Mavproxy: a UAV ground station software package for MAVLink based systems," Ardupilot Project, 2016.
- [65] Silva, C., et. al., "VTOL Urban Air Mobility Concept Vehicles for Technology Development," AIAA 2018-3847, AIAA, June 2018.
- [66] Darmstadt, P., et. al., "Hazards Analysis and Failure Modes and Effects Criticality Analysis (FMECA) of Four Concept Vehicle Propulsion Systems," NASA Contractor Report, NASA/CR—2019-220217, The Boeing Company, June 2019.
- [67] Federal Aviation Administration, *Remote Identification of Unmanned Aircraft Systems*, Notice of Proposed Rule Making, Federal Register, Vol. 84, No. 250, December 31, 2019.
- [68] Ellis, K., and Krois, P.; "Stakeholder Engagement for an Emerging Operation's Safety Management System," Information Session, AIAA SciTech Forum, Orlando, FL, January 6-10, 2020.

Appendix A: Enabling Technology R&D

A range of models, sub-functions, and enabling technologies are under development where gaps exist with respect to the envisioned information system. A synopsis of relevant recent NASA activities is given here. Additional activities are planned, including for example, Cyber-security Threat Monitoring; Auto-Pilot and Control System Monitoring; Automated Assured Contingency Planning and Execution, and Effective Interfaces for Human Oversight and Supervision. Many enablers are also being advanced by industry, academia, and other government agencies. Some of these are mentioned in Section 8.

Geo-spatial feature models and databases

Geospatial features (e.g., buildings, power lines, and trees) are collision hazards when flying at altitudes just above ground level. Techniques to avoid these obstacles are typically sensor-based or model-based or a combination of the two. Model-based approaches enable collision risk to be mitigated while planning the flight (proactively) and/or during the flight (reactively) if the horizontal and vertical extent of these obstacles are known (e.g., via surveying and timely updating). Before flight, an operator can choose flight plan waypoints that maintain a safe distance from obstacles that have been modeled and included in a database. During flight, onboard autonomy can compare the vehicle's current location and predicted trajectory to the modeled features and if necessary maneuver to avoid collision in the event that the vehicle has strayed off-course due to off-nominal conditions (e.g., high winds).

Although decades of R&D have led to quality geo-spatial model products and processes for maintaining, delivering, and using them in various domains, there are two modeling challenges we focus on with respect to the in-time safety assurance system concept and our domain of interest (i.e., low altitude urban operations). These we feel are gaps in state-of-the-practice. First, accurate and complete surveys of obstacle boundaries are required for some operations, and second, the obstacle boundaries must be represented compactly for efficient use by the higher level Monitor and Assessment functions. Aerial surveys of ground structures in the form of LIDAR point clouds [A1] can map geospatial features with decimeter-level accuracy and resolution. Compact representation of obstacle boundaries is needed, however, because detailed three-dimensional (3D) LIDAR surveys generate enormous data sets. The raw data size can overwhelm both visualization software used to plan flights and the onboard computing [A2] used for inflight automated avoidance. Naïve data reduction methods such as down-sampling prior to boundary determination risks the removal of critical features.

Representing ground structures with bounding polyhedra instead of point clouds greatly reduces the data size and can enable effective obstacle avoidance, as long as the bounding geometry envelopes the structures with high spatial fidelity. There is a tradeoff between boundary complexity and compactness. Simple 2.5D boundaries are more than an order of magnitude more compact than 3D boundaries, but enclose more empty space than high-fidelity 3D 'shrink wrap' boundaries (Figure A-1, [A3]). Unless the interstitial airspace within the footprint of a ground structure is needed for contingency maneuvers (or to complete a mission, as in bridge and power line inspection flights), 2.5D models are adequate for collision avoidance.

Survey data from satellite photogrammetry is now readily obtainable at low cost; and the AIS/AIM process provides many of the required features, particularly near airports. Commodity satellite-based surveys provide spatial accuracy as good as 3m (e.g., [A4]), which is about ten times worse than LIDAR-based surveys. The spatial sampling of satellite-based surveys limits their precision to about 50cm,

which is about five times worse than LIDAR-based surveys. Since both sub-meter spatial sampling and accuracy are required to resolve and map small structures (e.g., power lines, guy wires and road signs), current satellite photogrammetry is suitable only for larger obstacles (e.g., buildings and trees).

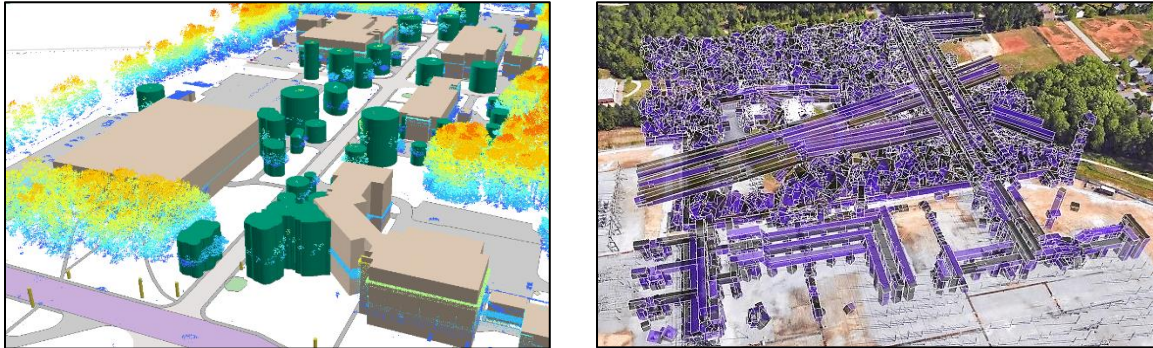


Figure A-1. Levels of model fidelity and cost for geospatial features. **(1)** At present, most geospatial feature sets available are akin to the brown building geometries at left. Since they can be constructed at high accuracy and with little effort from manual surveys or from processing lidar surveys or satellite image, this kind of model is predominant in ‘smart city’ geospatial databases. **(2)** The collision boundaries of trees (green cylinders at left) are the next most expensive kind of model. As long as human-drawn ground footprints exist, extruding the footprints to the height of raw lidar (blue-to-red colored dots, color gradient varied according to elevation) is fast and inexpensive. **(3)** Full 3D ‘shrink-wrap’ models (purple geometry at right) are the most accurate, yet the most expensive. The software to compute them at city scales is not widespread and requires accelerated processors. **(4)** Inexpensive satellite survey data cannot resolve fine features such as light poles (yellow structures, foreground left) and power lines (linear structures at right). Full-fidelity geospatial features require investment in collecting, archiving, and processing voluminous lidar survey data.

Population density models and databases

All non-participant casualty estimation models require a population density representation within the area surrounding the flight path. Based on the application, such population density representations can be obtained using average arbitrary values for rural, suburban, and urban settings; commercially acquired high-resolution historical population activity density values; data collected by on-board sensors/cameras; or by (hypothetically) utilizing real-time population density data gathered by cellular phone towers. In the cases where real-time data is employed (sensor or cell-phone tower driven), the population density data can be used directly in casualty estimation calculation as they represent actual population on the ground. On the other hand, historical population density values can be used to feed population density models. For example, employing one city’s average hourly population density values to represent another metropolitan area with similar population. Another approach would be to create surrogate population density representations from available data (e.g., utilizing data from a Monday in June to represent other non-holiday Mondays during the summer). The commercially available population activity density data used for testing provides hourly-expected population values within a 10m x 10m area and is based on cell-phone usage activity. The resolution of the population density data is used to inform the accuracy requirements of the impact point estimation, which is leveraged by the

use of 6-DoF trajectory models. Monthly data for City of San Francisco, Reno, Corpus Christi, and Dallas Fort Worth, TX were acquired from AirSage, Inc. and are currently being used for pre-flight and in-flight risk assessment simulations. An example of this data is shown in Figure A-2, and applied as discussed in Appendix B and [A5].

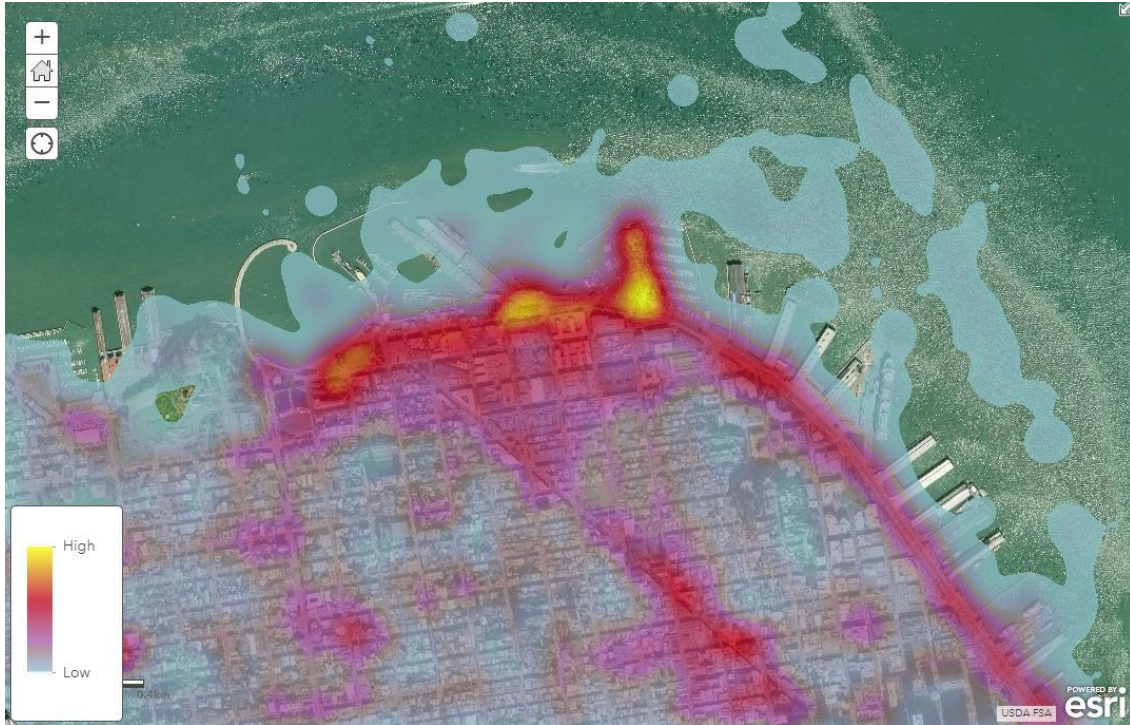


Figure A-2. Sample population density data for the City of San Francisco [A5]

Navigation system performance models and augmentation services

For commercial air transportation, positioning, navigation and timing (PNT) data of sufficient quality is (or can be) provided during all phases of flight. This data is provided by high-quality sensors (often employed redundantly), and a myriad of available dissimilar PNT systems (e.g., IMU/INS, VOR, DME, GPS). For GPS in particular, various forms of augmentation systems have been deployed as well (e.g., GBAS, SBAS, and ABAS [53]). All to achieve a desired Required Navigation Performance (RNP) for a particular class of operations. Unfortunately, many of these systems are terrestrial-based and become increasingly unavailable as operational altitude decreases. Thus, low altitude flights, such as those for sUAS or UAM, will not have the access to the full suite of deployed PNT system options. For these low altitude operations, PNT sources are typically limited to inertial (IMU/INS) and GPS. In some cases, there may also be an Alternative PNT (APNT) system, but the coverage volume and performance of each such system will need to be considered [20][21].

Due to the importance of high-integrity PNT data for flight operations, combined with the scarcity of adequate solutions for low altitude urban flight, a navigation system performance (or quality) service is envisioned to support both flight planning and in-flight contingency management. This service would provide three types of information: (1) quality estimates and a forecast model of PNT performance (e.g.,

for GPS); (2) corrections from available reference station(s) positioned within the urban environment to enable differential positioning; and (3) access to PNT estimates from any available APNT systems for the operational area. This concept is referred to as the NavQ service in Section 2 (Figure 4). The forecast model portion provides a means of predicting the quality and availability of PNT information for a given area. This model would be driven by characteristics of a PNT system (e.g., beacon location(s), transmit power, frequency, and receiver sensitivity) combined with a 3D terrain/obstacles model coupled with a model of multi-path and attenuation effects associated with the terrain/obstacles model.

For most of these systems, GPS included, accounting for the effects of the terrain on signals becomes increasingly important in complex operational environments (e.g., urban canyons) due to RF effects such as shadowing, multipath and signal attenuation. Further refinement of this model can be accomplished if real-time measurements of a PNT system can be obtained from known locations in the area of interest. These can be used to update the prediction as well as to validate the model over time. Measurements can be obtained from various sources including vehicles operating in the area of interest as well as fixed 'stations' positioned on the ground and via a network, continuously quantifying the PNT systems performance at these known locations. This would be similar to the way in which the Continuously Operating Reference Stations (CORS) network operates across the U.S. Additionally, the resulting model can support a temporal component to account for time-vary performance that can result from non-fixed beacon locations for some PNT systems (e.g., orbiting satellites in GPS) and/or from changing environmental conditions. The output of this model is envisioned as a discretized 4D cube covering a given volume with estimates of the availability and accuracy of PNT systems for each grid cell and time increment. This reference frame could be similar or equivalent to that of other models used by other services or functions (e.g., a population density model, weather/wind model(s), an RFI model, and terrain/obstacle models).

In cases where the aforementioned fixed stations are available to monitor GPS performance, measurements from these stations can also be used to improve positional accuracy of GPS receivers in the area. Network-based sharing of raw measurements (i.e., pseudorange, code phase, and carrier phase) from a set of such stations was developed and tested as the LOcation Corrections through Differential Networks (LOCD-IN) system [A6]. LOCD-IN was created as a means of enhancing GPS-based positioning accuracy without adding to the Size, Weight, Power and Cost (SWaP-C) as would be required for traditional methods. LOCD-IN utilizes numerous signal processing methods as well as adaptations of techniques used for differential GPS, Real-Time Kinematic (RTK) GPS and the Ground Based Augmentation System (GBAS) to remove errors common to the measurements of both devices (the vehicle and base station) resulting in increased accuracy of position estimates [A7]. Figure A-3 shows an example of the performance improvement seen for a set of tests performed on NASA's CERTAIN range.

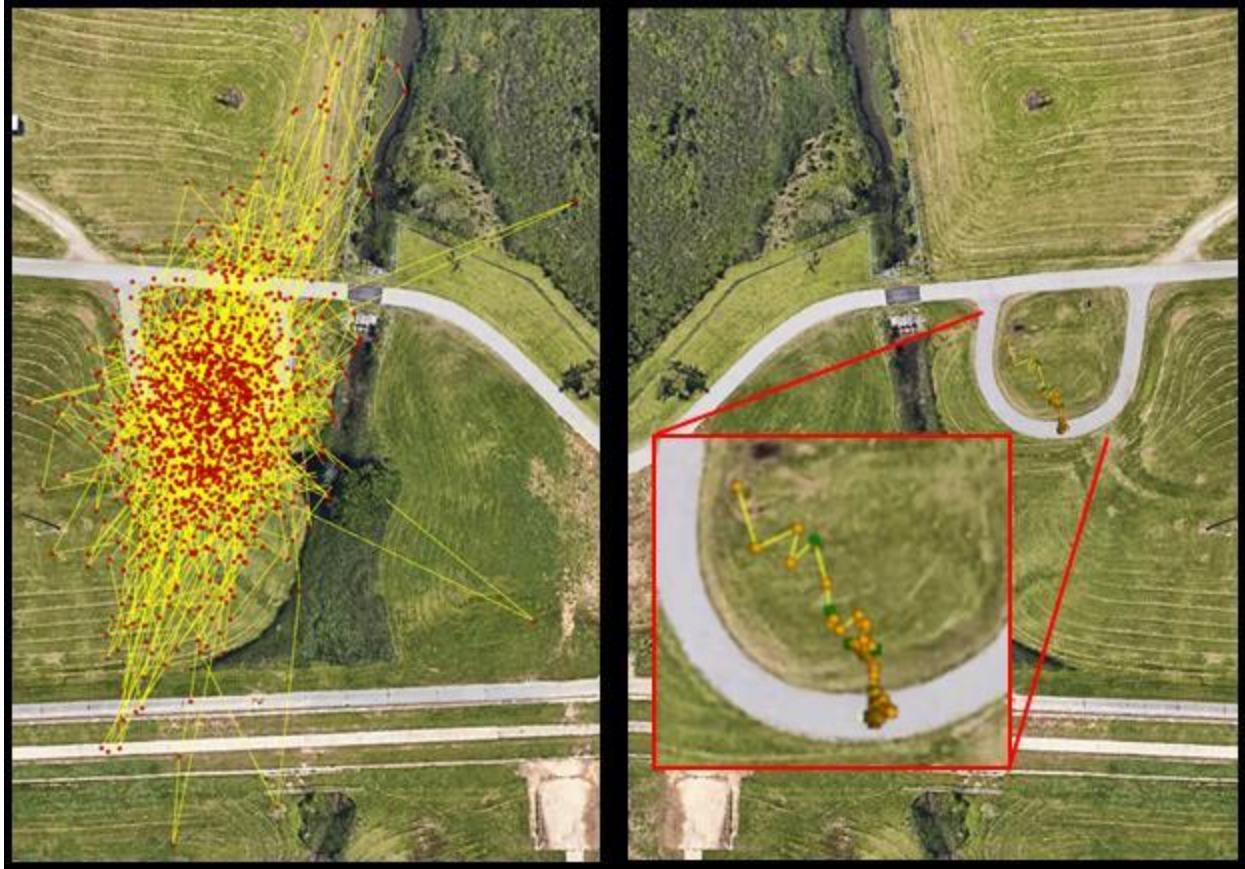


Figure A-3. Example of GPS accuracy improvement using LOCD-IN [A7]
 (Left, Ave Error (6m), Stdev (19m); Right, Ave Error (30cm), Stdev (1.5m))

Link and Radio Frequency Interference (RFI) modeling

Link and RFI modeling addresses hazards arising from RFI that can: (1) degrade or inhibit command and control (C2) and other communications links between the vehicle and ground station(s), and/or (2) couple into on-board electronic components to create performance anomalies in the avionics systems. Although both types of hazards are RF-related, they have different manifestations and thereby require different inputs and modeling approaches. The common information requirements to model both hazards for a defined airspace region is (a) geo-spatial data for objects in the region and (b) information about the RF characteristics of these objects as well as any equipment used within the system (e.g., on-board avionics).

On-going work applies traditional computational electromagnetic (CE) modeling techniques supplemented by updates received from airborne and ground-based measurements to produce radiation 'maps' of the flying area. Various CE tools can be used to generate maps such as those illustrated in Figure A-4. Much like small-scale weather maps, these radiation maps can be used during pre-flight to verify that the flight plan does not take the vehicle into areas that exceed the vehicle's susceptibility level; or they could be used in-flight when/if it becomes necessary to re-route unexpectedly.

Modeling link performance in an operating area requires knowledge of the power budget for the communication link(s) and RF visibility between the vehicle and its ground station. Combining this information with the GIS model and flight plan information allows for estimation of link margin along the planned flight track. During pre-flight, this information help to maximize the link margin and reduce likelihood of link loss. Monitoring link performance during flight adds another layer of capability. It can sense directly a complex and time-changing RF environment that can result from spectrum crowding at the lower altitudes of urban flight. These interactions are extremely difficult to model fully.

Modeling for RF energy hazards requires also knowing the coupling susceptibility of the vehicle (and its equipage) over a broad range of frequencies. The effects of RF coupling into electronics is, at best, difficult to detect and quantify. Exacerbating this issue is the difficulty of accounting for all sources that may emit RF energy into the operational airspace, and the dynamic nature of sources that may have directional gains (e.g., satellite beam pattern dispersions or radars operating near facilities).

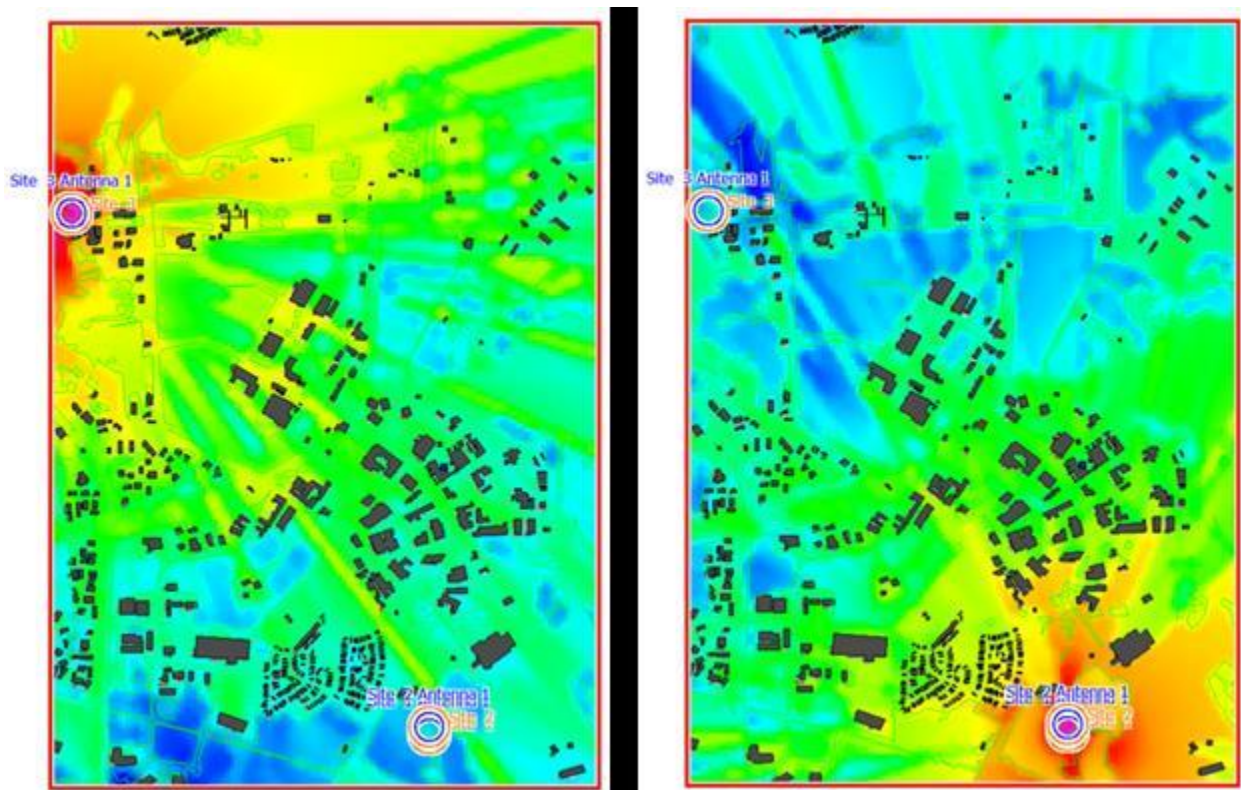


Figure A-4. RF emission models for two sites at NASA LaRC. (Left) Transmitting antenna is at upper left of image at top of 180 ft structure; (Right) Transmitting antenna is at lower right of image at top of 50 ft building. Red indicates high received signal strength; Blue indicates low received signal strength; Black indicates no received signal strength (e.g., inside building structures).

Battery and EPT modeling and prognostics

In order to predict end-of-discharge as defined by a voltage cutoff, the battery model estimates the voltage as a function of time given the current drawn from the battery. The approach taken employs a lumped-parameter ordinary differential equations form of the battery, so it is efficient and usable for

on-line prognostics, yet still incorporates key electrochemical processes. Model parameters are specific to the batteries used on the vehicle; however, the model remains general enough that with some modifications it may apply to different battery chemistries. The vehicles under test have four such battery packs in series parallel configuration to get the required voltage and current. Each pack has its own model running in parallel to observe changes in the state-of-charge and report it back to the server.

To identify an initial set of parameters, the battery is subjected to very low current close to open circuit voltage (OCV). Based on these curves the parameters for Nerst equations are identified. In the second step the Butler-Volmer equation parameters are identified wherein the battery is subjected to a 1C discharge.

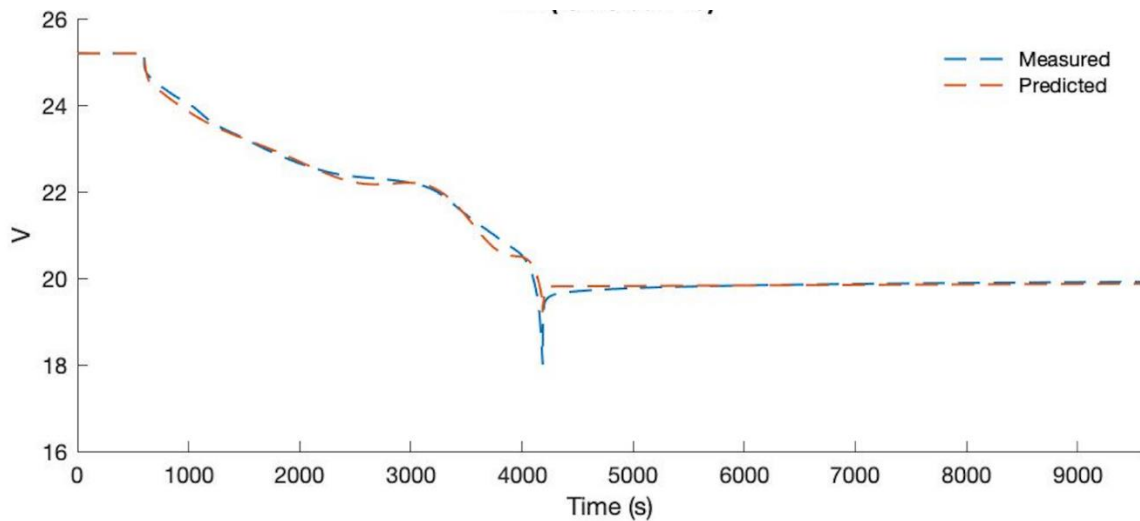


Figure A-5. ABC model validation with constant discharge (1C) profile

In the final step, the model is validated against a variable loading discharge profile. The experiment simulation profile includes variable loading and captures the max and min load values to validate if the model is able to track it well within the error range.

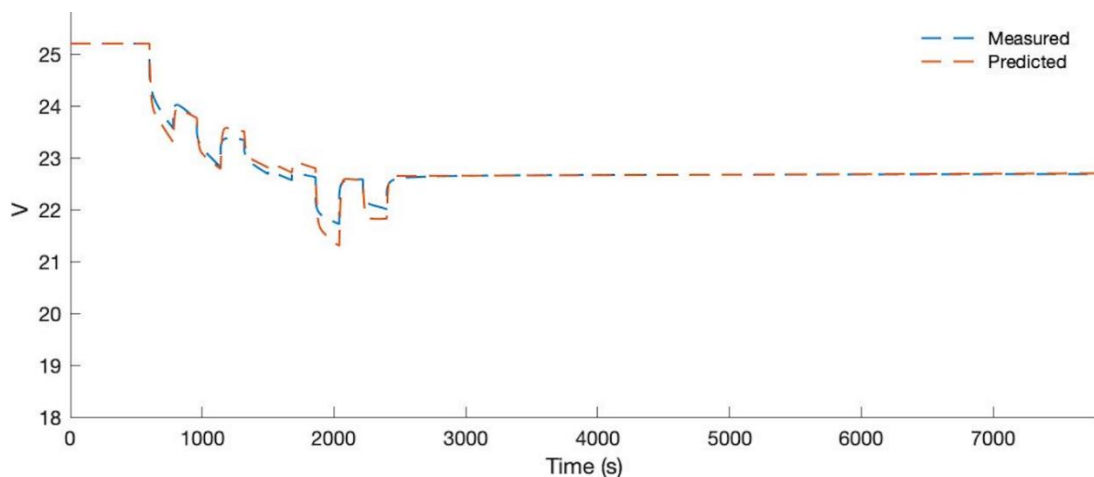


Figure A-6. ABC2 model validation with variable loading profile

A model-based prognostics architecture is then implemented [A8] in which there are two sequential problems:

- (1) The estimation problem, which requires determining a joint state-parameter estimate $p(x(k), \vartheta(k) | y(k_0:k))$ based on the history of observations up to time k , $y(k_0:k)$; and
- (2) The prediction problem, which determines at k_P , using $p(x(k), \vartheta(k) | y(k_0:k))$, a probability distribution $p(k_E(k_P) | y(k_0:k_P))$. The distribution for Δk_E is computed from $p(k_E(k_P) | y(k_0:k_P))$ by subtracting k_P .

As shown in the prognostics architecture (Figure A-7), at discrete time k the system is provided with inputs, u_k (e.g., voltage and current) and provides measured outputs, y_k . The estimation module uses this information, along with the battery system model, to compute an estimate $p(x(k), \vartheta(k) | y(k_0:k))$. The prediction module uses the joint state-parameter distribution and the system model, along with hypothesized future inputs, to compute the probability distribution $p(k_E(k_P) | y(k_0:k_P))$ at given prediction times k_P .

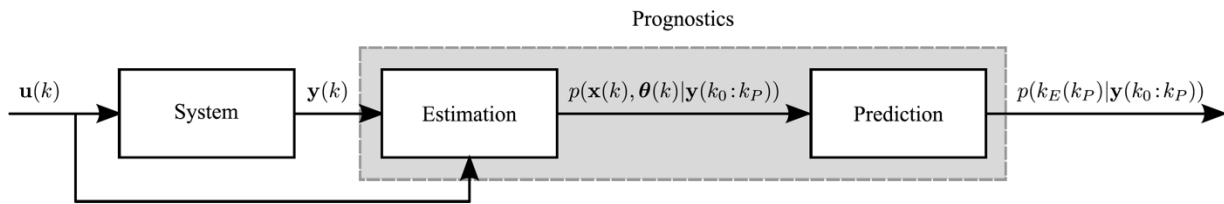


Figure A-7. Generalized Prognostics Architecture

In addition to the battery prognostics, a framework is being developed to do system level prognostics for the entire electric power train (EPT). This includes battery packs, speed controller, power electronics and motors. Each underlying sub-system degrades and fails at different rates. Since the systems are very much inter-dependent their degradation and failures can lead to cascading effects which are being considered in the framework development. As envisioned, all sub-systems can use a model-based diagnostics and prognostics architecture such as discussed above and in [A9].

References

- [A1] Wehr, A. and Lohr, U., 1999. Airborne laser scanning—an introduction and overview. ISPRS Journal of photogrammetry and remote sensing, 54(2-3), pp.68-82.
- [A2] Moore, Andrew J., Matthew Schubert, Nicholas Rymer, Swee Balachandran, Maria Consiglio, Cesar Munoz, Joshua Smith, Dexter Lewis, and Paul Schneider. "UAV Inspection of Electrical Transmission Infrastructure with Path Conformance Autonomy and Lidar-based Geofences NASA Report on UTM Reference Mission Flights at Southern Company Flights November 2016." NASA Technical Memo 2017-219673 (2017).
- [A3] Moore, Andrew J., Matthew Schubert, Terry Fang, Joshua Smith, and Nicholas Rymer. "Bounding Methods for Heterogeneous Lidar-derived Navigational Geofences." NASA Technical Memo 2019-22399 (2019).
- [A4] Vricon point cloud. <https://www.vricon.com> . Accessed 2019-7-10

[A5] Ancel E, Capristan F., Foster, J.V., and Condotta, R. (2019) In-Time Non-Participant Casualty Risk Assessment to Support Onboard Decision Making for Autonomous Unmanned Aircraft, AIAA Aviation 2019. (AIAA 2019-3053).

[A6] Gilabert, R., Dill, E., and Uijt de Haag, M., "Progress and Test Results for the Location Corrections through Differential Networks (LOCD-IN)," Proceedings of the 31st International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS+), Miami, FL, September 2018.

[A7] Gilabert, R., Dill, E., and Uijt de Haag, M., "Evaluation of Improvements to the Location Corrections through Differential Networks (LOCD-IN)," Proceedings of the 32nd International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GNSS+), Miami, FL, September 2019.

[A8] M. Daigle and C. Kulkarni, "Electrochemistry based Battery Modeling for Prognostics", Annual Conference of the Prognostics and Health Management Society (PHM 2013), October 2013, New Orleans, LA.

[A9] M. Corbetta and C. Kulkarni , "An approach for Uncertainty Quantification and Management of Unmanned Aerial Vehicle Health", Annual Conference of the Prognostics and Health Management Society (PHM 2019), September 2019, Scottsdale, AZ.

Appendix B: Initial End-to-End Services Tested

To help to expose potential requirements for the system concept described in Section 1, three services were developed, tested, and evaluated in 2018-2019. These are considered stepping stones to the larger concept and illustrative of the functions and sub-functions ultimately envisioned.

Non-Participant Casualty Risk Assessment

The current implementations of the non-participant casualty risk assessment (NPCRA) capability consists primarily of monitoring available parameters and estimating the probability/risk of experiencing casualties on the ground following the aircraft experiencing a failure. The NPCRA capability is comprised of on-board and ground components, derived from the UTM Risk Assessment Framework (URAF) [B1] which outlines various models (population density, off-nominal trajectory and impact point model, probability of casualty estimation model, mishap likelihood model). The pre-flight implementation, called Ground Risk Assessment Service Provider (GRASP) is a server-based SDSP that assists operators with flight planning to understand and minimize the associated casualty risk of alternative flight plans [B2]. Figure B-1 is an example GRASP product for a flight plan over the area with the population density modeled as shown in Figure A-2. In this example, red dots indicate locations along the flight path where the casualty risk is estimated/predicted to be the highest. Given this information, the operator may choose an alternate flight plan (or time of day); then re-run GRASP to see if the risk is reduced.

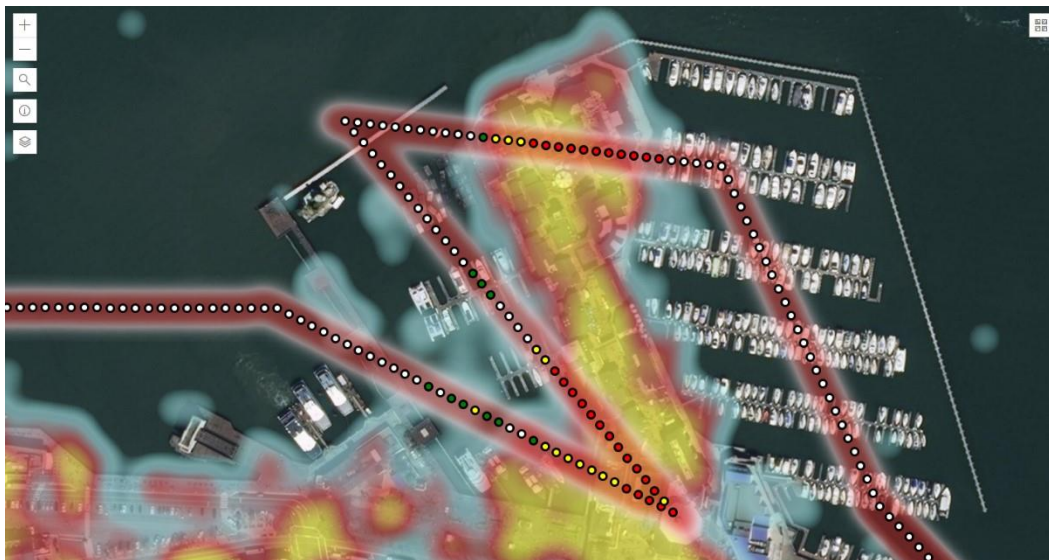


Figure B-1. Example casualty risk assessment for flight plan over the City of San Francisco [B2]

The onboard implementation (called Real-time Risk Assessment (RTRA)) is designed to operate on cFS-based aircraft and support autonomous on-board decision making by providing current and future ground casualty risk for projected paths, eventually aiding with mitigation re-routes in off-nominal conditions [B3]. Within the in-time safety assurance concept, future applications of NPCRA will bridge the on-board and server-based risk assessment capabilities to assist aircraft during all phases of flight as described in Application Domain section.

This Assessment function is intended to estimate, track, and predict the risk of impacting populated areas in the event of critical system failure or loss-of-control. The function has been implemented in

various forms, supporting both pre-flight and in-flight applications. The pre-flight tool simulates the flight via the flight plan (waypoint) file and provides potential non-participant casualty risk assuming a critical system failure every ~15-20 meters where the NPCRA tool is running at the remote SDSP servers (Figure B-2) [B2]. In contrast, the real-time risk assessment function uses models loaded prior to flight in conjunction with real-time observables regarding aircraft state, system states, and the changing flight environment. The real-time implementation can take three forms. (1) The in-flight risk assessment tool aids the GCS operator with the NPCRA software solely operating on the GCS computer using downlinked flight parameters from the vehicle (Figure B-3a) [B1]. (2) The in-flight risk assessment tool executes on on-board computers with assessment results downlinked to the GCS for information purposes with the goal of assisting autonomous decision making and risk mitigation (Figure B-3b) [B3]. (3) The in-flight risk assessment tool supports airborne aircraft remotely via an Aircraft-GCS-SDSP link in a fully autonomous flight scenario (Figure B-3c).

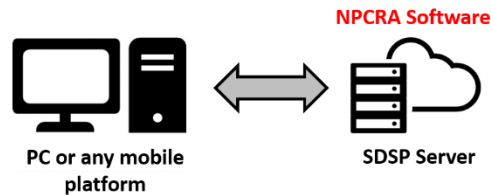


Figure B-2. Pre-flight NPCRA Access

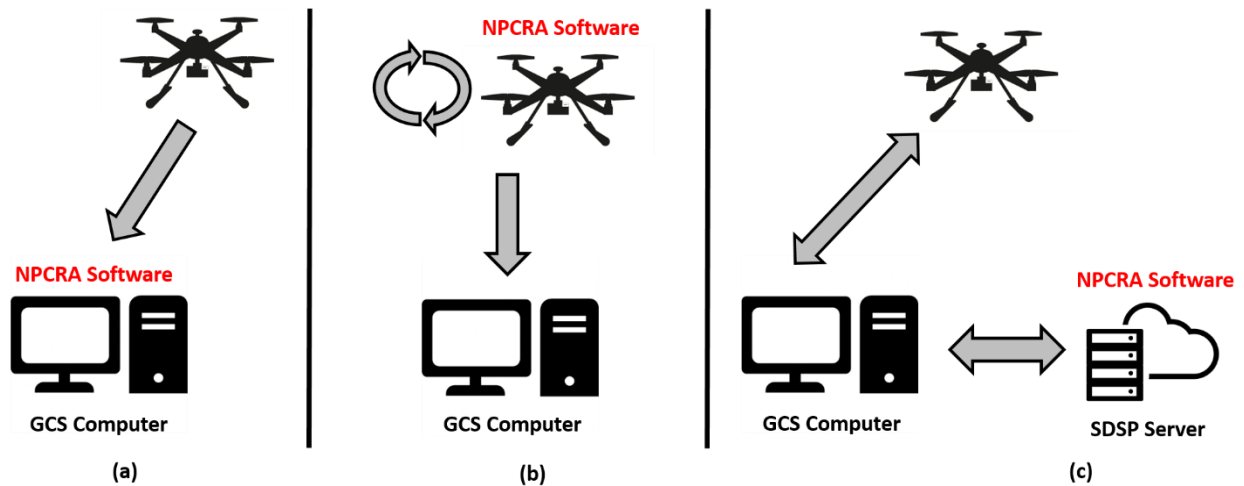


Figure B-3. Real-time NPCRA access options

Based on the implementation, the outputs of this assessment function include:

- Casualty probabilities (pre-flight applications)
- GUI with color coded impact location/area visualizations (pre-flight applications)
- Casualty risk (mishap likelihood and casualty probability estimates) (in-flight application)
- Mishap likelihood and recommended action (abort, land, RTL, continue) (in-flight application)

The fidelity of the risk assessment is dependent upon the assessment type (pre-flight vs. in-flight) and the location where the software is executed (on-board, GCS, or SDSP). The pre-flight risk assessment exercise inherently carries more assumptions and yields to a lower fidelity and limited set of results. In particular, the pre-flight implementation runs a 3-DoF trajectory and impact point prediction model and only provides casualty probabilities, assuming the mishap is eminent at each time step since detailed aircraft state vectors are not available to inform a 6-DoF model. The pre-flight assessment is aimed to help operators minimize non-participant casualty probability during the planning phase and the risk assessment is expected to be updated throughout the flight. On the other hand, depending on the implementation, the in-flight applications can employ real-time vehicle health and state data that feeds the detailed Hugin Bayesian Belief Network (BBN) models and 6-DoF off-nominal trajectory models. Coupled with high-resolution population density data, the 6-DoF trajectory model should provide more accurate representation of the risk. Based on the current NPCRA implementation, data type and requirements are given in the Table B-1.

Inputs: See Information Requirements section below.

Testing: UTM TCL-3/4 Sprint sims (2019); CERTAIN flight tests (2018, 2019); UAM X2 sim (2019)

Access: Hosted on SDSP Server, with migration to AWS planned. The GUI is hosted at the GCS and as such available to operators to support pre-flight planning and go/no-go decisions.

For more information:

[B1] Ancel E, Capristan F., Foster, J.V., and Condotta, R. (2017) Real-Time Risk Assessment Framework for Unmanned Aircraft System (UAS) Traffic Management (UTM), AIAA AVIATION Forum, 17th ATIO Conference (AIAA 2017-3273)

[B2] Ancel E, Helsel, T., Heinich, T. (2019) Ground Risk Assessment Service Provider (GRASP) Development Effort as a Supplemental Data Service Provider (SDSP) for Urban Unmanned Aircraft System (UAS) Operations, AIAA/IEEE DASC 2019, San Diego, US. Sept. 9-12, 2019

[B3] Ancel E, Capristan F., Foster, J.V., and Condotta, R. (2019) In-Time Non-Participant Casualty Risk Assessment to Support Onboard Decision Making for Autonomous Unmanned Aircraft, AIAA Aviation 2019. (AIAA 2019-3053)

Table B-1. Model parameters vs. NPCRA implementation types

Risk Assessment Variation	Mishap Likelihood Assessment	Trajectory and Impact Point Estimation	Probability of Casualty Estimation	Population Density Model	Building Footprint Data	Vertical Wind Profile
Pre-Flight Casualty Assessment (Fig B-2)	N/A (no real-time flight parameters to assess aircraft health or mishap likelihood)	3-DoF (point-mass model)	Probability of causing one or more casualties [B3]	Acquired hourly Activity Density data (see input requirements)	N/A (can be expanded to include)	User-provided (SDSP acquired in the future)
In-Flight computed on the GCS (Fig B-3a)	Hugin BBN model which tracks limited downlinked MAVLink sensor data	Differential of ballistic and point-mass models to include uncertainty	Expected number of casualties [B1]	Modeled Local population data (e.g., LaRC)	Modeled building footprint data (e.g., LaRC GIS)	Locally measured values (e.g., Langley AFB tower data)
In-flight computed on-board (Fig. B-3b)	Hugin BBN model tracking detailed a/c health parameters & BHM/ vehicle prognostics via-SDSP	6-DoF [B3]	Probability of causing one or more casualties [B3]	Acquired hourly Activity Density data (see input requirements)	Planned expansion	Locally measured or User provided
In-flight provided by SDSP (Fig. B-3c)	Hugin BBN model tracking downlinked health parameters (bandwidth limited)	3-DoF or 6-DoF (based on the availability of aircraft state vectors)	Probability of causing one or more casualties [B3]	Acquired hourly Activity Density data (see input requirements)	Planned expansion	Locally measured, user provided or SDSP acquired

Battery Prognostics

This Monitor and Assessment service/function is intended to estimate, track, and predict state-of-charge (SOC) and remaining useful life of onboard power source(s). Outputs provide the estimated time when end of discharge (EOD) will be reached; the estimated remaining flight time available; and the probability of reaching EOD before the end of the mission.

In a manner analogous to a fuel gauge, SOC is provided on a linear scale (percentage) of available power, as well as a projected SOC at each waypoint along the planned trajectory. To estimate when EOD will occur, the service/function employs a battery model to track the available energy in the battery and executes the model open loop to predict the EOD based on projected power consumption rates. The function also uses a separate motor system power model to estimate the required power for each flight segment, allowing for prediction of SOC at each waypoint in the flight plan.

The function requires periodic measurements of battery voltage and current in order to update SOC and RUL predictions on-the-fly. This allows the prognostic algorithm to adjust for changes in trajectory and flight conditions. Data is streamed from sensors on the vehicle down to the ground station and forwarded on to the SDSP (see Figure B-4). This is similar to the NPCRA service (Figure B-3), but connecting to a different server.

During pre-flight, the battery prognostic models are initialized with the vehicle parameters, the intended flight plan, as well as the battery parameters. Once initialized, the algorithms calculate the prognostic metrics (SOC, RUL, EOD) as the stream of battery voltage and current data is delivered. During the flight phase, the service provider expects regular updates of the voltage and current measurements (e.g., Figure B-3). A request/reply protocol is implemented so the ground station or other safety monitoring applications can request the battery prognostic information from the SDSP server. The battery prognostics is currently deployed with the PtT service and reachable directly from the GCS. Future work will allow access indirectly via AWS-based connection to the NASA USS (or other USSs).

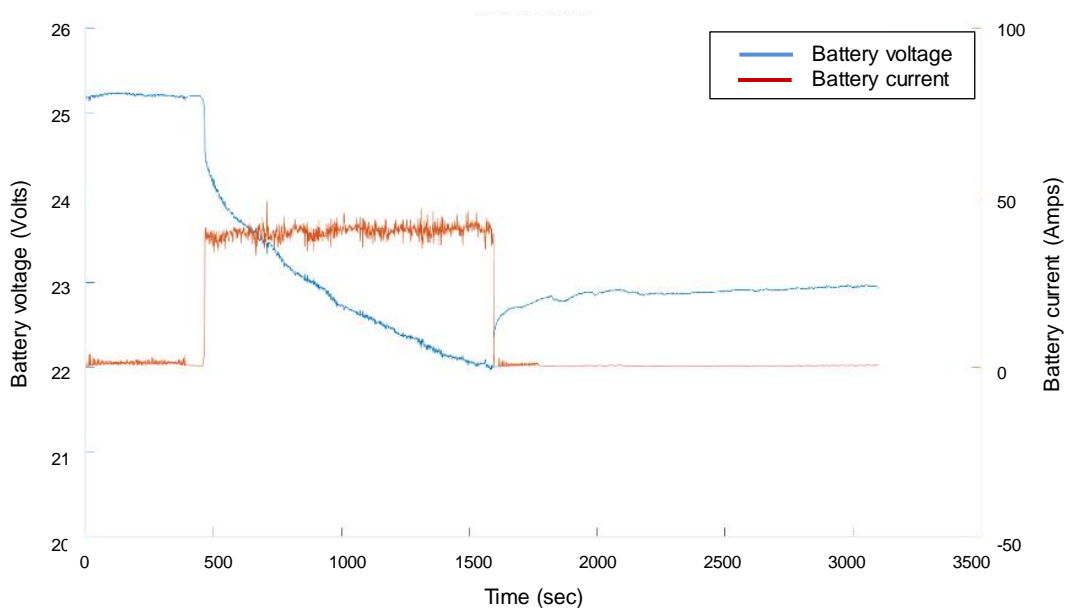


Figure B-4. Example of battery pack voltage and total current draw as sent to the SDSP at ~1Hz

Inputs: See Information Requirements below.

Testing: UTM TCL-4 Sprint 4 sim (2019); CERTAIN flight tests (2018, 2019); UAM X2 sim (2019)

Access: Hosted on SDSP server, access via AWS-based connection to NUSS and/or GCS.

For more information:

[B4] Kulkarni, K., Corbetta, M. Health Management and Prognostics for Electric Aircraft Powertrain. AIAA/IEEE Electric Aircraft Technologies Symposium, 2019.

[B5] Kulkarni, K., Corbetta, M. A Hybrid Battery Model for Prognostics In Small-Size Electric UAVs. Annual Conference of the Prognostics and Health Management Society, 2018.

[B6] G. Sierra, M. Orchard, C. Kulkarni, K. Goebel. Flight Tests of a Remaining Flying Time Prediction System for Small Electric Aircraft in the Presence of Faults. Annual Conference of the Prognostics and Health Management Society, 2017.

[B7] Kulkarni, Chetan; Schumann, Johann; Roychoudhury, Indranil (2018) On-Board Battery Monitoring and Prognostics for Electric-Propulsion Aircraft, AIAA/IEEE Electric Aircraft Technologies Symposium (EATS); July 09, 2018 - July 11, 2018; Cincinnati, OH; United States, 2018.

[B8] Goebel, Kai; Gorospe, George; Kulkarni, Chetan; Schumann, Johann; Cuong Chi, Quach 'Patrick'; Hogge, Edward (2019) Health Monitoring and Prognostics for More Electric Aircrafts, More Electric Aircrafts Europe 2018; October 23, 2018 - October 25, 2018; Hamburg; Germany, October 23, 2018.

[B9] Edward F. Hogge, Brian M. Bole, Sixto L. Vazquez, Chetan S. Kulkarni, Thomas H. Strom, Boyd L. Hill, Kyle M. Smalling, Cuong C. Quach (2018) Verification of Prognostic Algorithms to Predict Remaining Flying Time for Electric Unmanned Vehicles, International Journal of Prognostics and Health Management; Vol 9 (1) 021, pages: 15, 2018.

[B10] Kulkarni, Chetan; Hogge, Edward; Quach, Cuong C. (2018) Remaining Flying Time Prediction Implementing Battery Prognostics Framework for Electric UAV's, AIAA Propulsion and Energy; July 09, 2018 - July 11, 2018; Cincinnati, OH; United States, July 09, 2018.

[B11] Edward F. Hogge, Chetan S Kulkarni, Sixto L. Vazquez, Kyle M. Smalling, Thomas H. Strom, Boyd L. Hill, and Cuong C. Quach (2017) Flight Tests of a Remaining Flying Time Prediction System for Small Electric Aircraft in the Presence of Faults, Annual Conference of the Prognostics and Health Management Society 2017; August 16, 2017.

Proximity to Threats

Awareness of the proximity of conditions that may cause damage, harm, or operational interruption – “threats” – to a proposed or active flight plan is critical for safe operations. Threats as defined for this service may be:

- Static physical objects with vertical extent (e.g., buildings, poles, trees, or terrain)
- Transitory non-physical objects (e.g., restricted airspaces, areas of adverse weather/winds, areas of expected RF interference or low signal strengths, areas of degraded navigation sensor performance, or sensitive ground locations/areas (e.g., school yards during recess))

Proximity to threats such as these should be considered during preflight planning and monitored during flight to allow for contingency execution (i.e., mitigation) in the event of unexpected unplanned off-nominal conditions. If the vehicle approaches a threat closer than a predefined threshold, holistic threat awareness is required to change the flight path to maintain a safe proximity to threats, even under the uncertainty inherent in operations.

The initial implementation of this service considers proximity to buildings, poles, and trees. It takes as input the locations of these threats, pre-defined threshold(s) for closest allowed approach distance, a predicted flight path or trajectory, and a desired confidence that the flight will remain within that path. As output, the service provides locations along the flight trajectory at which the safety margin is predicted to fall below 100% of the minimum-allowed approach distance.

For example, assume an aircraft must remain at least 5m laterally and 2m vertically from buildings and 3m laterally and 1m vertically from trees; these are approach distance thresholds the operator can define as a configuration setting prior to flight. For testing, we created a 3-D database of building and tree locations pulled from LIDAR point clouds (for trees) and OpenStreetMap (for buildings). Building data consisted of perimeter footprints and a maximum height. Tree data consisted of tree canopy coverage and a maximum height. Although the current version of the service relies on a database or model of geo-referenced threats, it is designed to be agnostic to the source of threat information. For example, data may be sensor-derived or come from another service. For example, the existing and previously-mentioned AIS [36] can provide some of the required information. Although not yet ready for testing, the RFI and NavQ services may also be able to provide data in the form needed by the PtT service in cases where the operator would like to include these threats in this safety margin metric.

Next, a nominal 4-D trajectory is generated based on the waypoints of a given flight path. A trajectory prediction is then created based on a gaussian distribution for the path, given the uncertainties of winds aloft, the onboard flight controller behavior, and other factors [C7]. For the final input, the aircraft operator selects a desired confidence level for the flight path assessment. For example, selecting 75% would task the service to compute (and track) the proximity of threats that cover 75% of the possible trajectories the flight may take given the considered uncertainties.

As mentioned previously, the service uses these parameters to compute a safety margin between predicted flight trajectories and threats defined as above, outputting the time of occurrence when the predicted margin is below 100%. Figure B-5 shows an example situation illustrating one output of the service (i.e., the safety margin metric).

As with the battery prognostic (BP) service, the initial version of the Proximity to Threat service is reachable directly from the GCS via a request/reply protocol. Future versions will be accessible indirectly via AWS-based connection to the NASA USS (or other USSs or SDSPs).

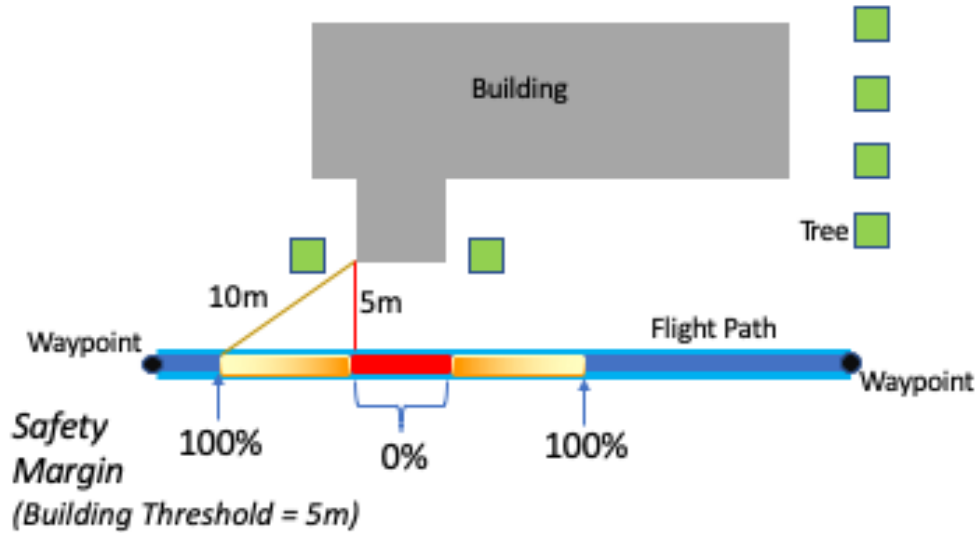


Figure B-5. Safety margin for a flight path near trees and buildings. Safety margin is computed using the percent error formula, that is, $SM_{proximity} = \frac{(distance - threshold)}{threshold} * 100$, capped at 0% and 100%. Thus, a margin of 0% means the flight path is closer to the object than the given threshold, i.e., there is no margin. A margin of 100% means the flight path is at least twice as far from the object as the given threshold. As an example, with a threshold of 5m, a point on the flight path that is 7m from a building has a margin of 40%, or 2m more than the closest allowed approach distance.

In summary, this Assessment function is intended to estimate, track, and predict proximity metrics (time and distance) to geo-referenced features that represent threats along or near the flight path. The example used for testing has been the perimeter of fixed vertical features (e.g., buildings); but these could also represent no-fly zones or other hazardous areas defined by operators or ATM/UTM service providers. Outputs indicate those portions of the vehicle trajectory that are predicted to violate proximity thresholds to these threats. These include start/end points; nearest approach point; distance to nearest approach point; and severity of violation. As with NPCRA, this assessment can be done prior to flight using a flight plan, or in-flight using a trajectory prediction that is continuously updated during the flight.

Inputs: See Information Requirements below.

Testing: UTM TCL-4 Sprint 4 sim (2019); CERTAIN flight tests (2018, 2019); UAM X2 sim (2019)

Access: Hosted on SDSP server, access via AWS-based connection to NUSS and/or GCS.

Information Requirements (as tested)

For these three services as tested, required input data is summarized below based on whether needed pre-flight or in-flight.

Pre-flight info type	NPCRA	BP	PtT	Comment
Configuration settings	X	X	X	e.g., Thresholds for warnings
Vehicle information	X	X	X	e.g., Size, weight, model, #rotors/engine
Aerodynamic model	X		X	e.g., Drag coefficient
Flight plan	X	X	X	4D preferred (can be waypoint file)
Battery model		X		Calibration procedure (every 8-10 flights)
3D geo-feature database	X		X	Buildings/obstacles/geo-fenced areas (polygons); terrain model (optional)
Population density database	X			Stored at the server
Wind vector (or 3D model)	X		X	3D model preferred
Flight day/time	X			

In-flight info type (@ 1 Hz or better)	NPCRA	BP	PtT	Comment
Aircraft state	X	X	X	Position, velocity, attitude, heading
Battery state	X	X		For each battery pack: voltage, current, temp
Engine/motor state	X			For each motor: current, temp, RPM
Auto-pilot state	X			e.g., auto, manual, land, RTL 'mode'

Nav system state	X			e.g., GPS SVs and DOPs
Comm system state	X			e.g., RSSI

Vehicle Information (pre-flight)

- Number of rotors (required)
- Length of each arm (vehicle center to rotor center) (required)
- Dimensions of center body (desirable)
- Rotor diameter (desirable)
- Angle between each arm if not axial-symmetric (desirable)
- Mass (total) (required); Mass (rotors and arms) (desirable); Mass (battery(s)) (desirable)
- Mass (payload) (desirable)
- Battery pack configuration (serial /parallel)
- Battery maximum discharge rating
- Battery rating for discharge (nominal operation); Battery rating for charging

Flight plan (pre-flight) (in-flight, if updated during flight)

The following values are needed for each waypoint in the flight plan. Flight plans may be provided pre-flight, or updated in-flight.

Element	Data Type	Units	Frequency	Description
Latitude	double	degrees	N/A	Current latitude position in degrees
Longitude	double	degrees	N/A	Current longitude position in degrees
Altitude	double	feet	N/A	Current altitude position in feet, WGS84
Eta	int64	microseconds	N/A	Expected time of arrival at waypoint, UNIX time
desired flight speed	double	feet/s	N/A	Cruise, climb and descent. This can be used as an alternative to ETA, if expected ETA is not known.
hold time at waypoint	TBD	TBD	N/A	Hold time at each waypoint. Required if ETA is not provided
Proximity radius from waypoints	double	feet	N/A	The minimum radius from each waypoint such that when the UAV enters within that radius, it is considered to have reached that waypoint location. This enables smooth trajectories. In case these values are unavailable, specify the trajectory type: smooth or with sharp turns.

Trajectory prediction data (in-flight)

The trajectory prediction is built on a simple physics-based model of the vehicle, and generates the necessary predicted future states for proactive risk assessments.

Element	Data Type	Units	Frequency	Description
timestamp_ms	uint32	millis	1 Hz	Timestamp (milliseconds since UNIX epoch)
vehiclePositionLat_deg	double	decimal degrees	1 Hz	vehicle position in latitude, in decimal degrees
vehiclePositionLon_deg	double	decimal degrees	1 Hz	vehicle position in longitude, in decimal degrees
vehicleWGS84Alt_ft	double	feet	1 Hz	vehicle WGS-84 altitude
rpm_rotor		rpm	1 Hz	Rotor speed (rpm). Ideally RPM of each rotor. If not an average of all the rotors.
groundSpeed_ftPerSec	float	feet/sec	1 Hz	Ground Speed in (ft/s)
heading_deg	float	degrees	1 Hz	Heading (deg, True North)
trueAirspeed_ftPerSec	float	feet/sec	1 Hz	True airspeed in (ft/s)
verticalSpeef_ftPerMinute	float	feet/min	1 Hz	vertical speed in feet per minute, negative indicates descent
groundCourse_deg	int16	degrees	1 Hz	Ground course, also known as track (degrees, true north)

Battery telemetry (in-flight)

Outputs from the battery telemetry calculations give estimated time when EOD will be reached (or est. remaining flight time) and probability of reaching EOD before end of mission.

Element	Data Type	Units	Frequency	Description
timestamp_ms	uint32	ms	1 Hz	Timestamp (milliseconds since system boot)
temp_amb	uint16	degrees C	1 Hz	Temperature outside the vehicle, in centigrade
voltage_pk	uint16	volts?	1 Hz	Battery voltage of each pack
current_pk	uint16	amperes	1 Hz	Battery current of each pack
temp_pk	uint16	degrees C	1 Hz	Temperature of the battery, in centigrade
voltage_cell	uint16[10]	volts	1 Hz	Battery voltage of each pack/ cells
current_cell	uint16[10]	amperes	1 Hz	Battery current of each pack/cells

Aircraft state (in-flight)

Element	Data Type	Units	Description
time_boot_ms	uint32	millis	Timestamp (milliseconds since system boot)
pos_lat	int32	degrees	Current latitude position in degrees * 1E7
pos_lon	int32	degrees	Current longitude position in degrees * 1E7
pos_alt	float	meters AMSL	Current altitude position in meters, AMSL

Appendix C. Uncertainty Management Framework

A formal approach to uncertainty quantification is proposed, identifying four main sources of uncertainty. Then, those uncertainty sources map within a *predictive estimation process*, modified from [C1], which outlines input-output relationships of the predictive framework and helps modeling of uncertainty within its elements. Uncertainty sources and predictive process architecture define the critical elements necessary for meaningful uncertainty quantification. Thus, frameworks for quantitative in-time safety predictions should always include those critical elements, or a sub-set of them, to enable reliable prognostics.

Uncertainty Sources

The four macro-categories *model*, *method*, *measure*, and *input* have been chosen to represent uncertainty sources in the predictive estimation process. Each of them comprises of sub-categories that are depicted in Figure C-1, and are discussed below [C1][C2][C3][C4].

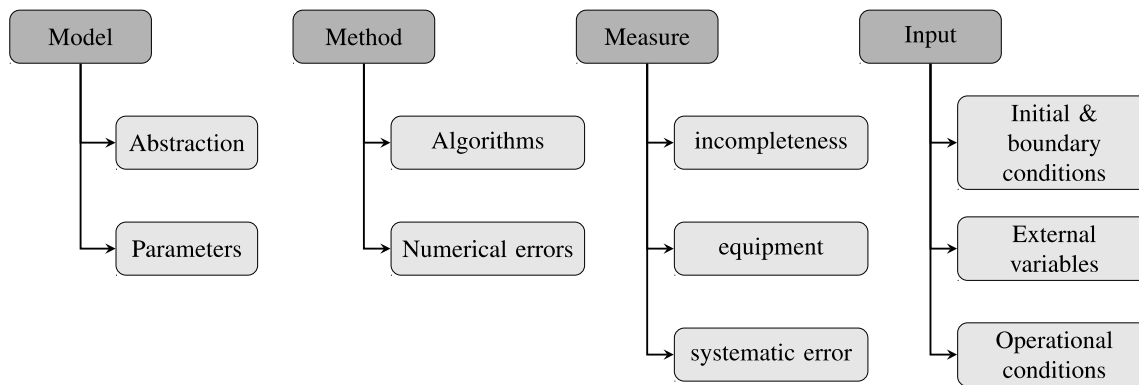


Figure C-1. High-level classification of uncertainty sources encountered in a predictive process

Model *abstraction* refers to the hypotheses introduced during model development with the intent of representing reality and physical processes through a set of equations. Model *parameters* include fixed or variable coefficients required to estimate the output quantities of interest (QoIs) from the model. Here, *methods* refers to the collection of algorithms and computation tools utilized to compute the QoIs, to interpolate or extrapolate input variables from input data, or to perform prediction by propagating information through models or in time domain. They have been divided into *algorithms* and *numerical errors*. Algorithms introduce uncertainty because they may converge to sub-optimal solutions trying to minimize errors or cost functions. As a result, different runs of the algorithms may generate different results because the algorithms remain trapped in local minima. Numerical errors include roundoff or discretization errors, which may be negligible for most of the applications. *Measures* includes measure *incompleteness*, uncertainty in measurement *equipment*, which typically translates into sensor resolution, accuracy and precision, and *systematic errors* generated by the measuring process, sensor installation and human error (if humans are involved in the measuring process). *Input* includes time-dependent variables, initial and boundary conditions, and exogenous forces that may interact with the system and therefore affects its dynamics. *Operational input* are defined according to the system's intended function. *External inputs* are generated by external forces or events which depend on the operational environment of the system, and are typically characterized by large uncertainty. *Initial* and *boundary conditions* refer to both

external and system’s variables. Table C-1 shows an exemplifying list of uncertainty sources first considered for in-time prediction of aircraft remaining trajectory and powertrain health assessment. The list should not be considered exhaustive, as involves only a subset of tasks for in-time safety assessment of the airspace. More, specific sources of uncertainty will be added as more research is performed and experimental evidence collected.

Table C-1. Example of uncertainty sources affecting the predictive process for in-time safety assessment. (Source type codes are Model (MI), Method (Md), Measure (Ms) and Input (I))

Type	Description
MI	Abstraction of vehicles operating in the airspace (e.g., complexity of vehicle models)
I/MI	Vehicle ability to execute desired kinematic profile
I/Ms	Weather conditions: temperature, air density, wind field over flight path
I/Ms	Dynamic obstacle size and location
I/Ms/MI	Initial conditions of the vehicle: state of health of safety-critical component and propulsion system, battery state of charge, etc.
Ms	Sensor precision, accuracy, resolution
MI/Md	Degradation progression: vehicle structural and dynamic properties
MI/Md	Degradation progression: vehicle powertrain system
MI/Md	Degradation progression: sensor degradation and sensor faults
Md	“Local minima effects” from numerical solutions of model equations
Md	Aleatoric variability hidden in the prediction process
Md	Anomaly detection capability for a variety of vehicles in the airspace

Architecture of the predictive process

Figure C-2 shows a diagram of the high-level predictive process structure proposed in [C3][C4]. From left to right, we introduce the measure space, which represents quantities that must be measured. The input space represents those variables not belonging to the system that is being monitored but affect the system’s dynamics. The input space overlaps with the measured space, since external variables must be, somehow, estimated or measured. Measured space and Input space variables feed the representation space, which comprises of system’s models and input models. While the introduction of the system’s model is self-explanatory, the reason for incorporating input models is twofold. Engineering systems are often described by differential equations or systems of equations, and input specifications may not be written in a form that is directly implementable into those equations. Input models play a relevant role also for external variables. Some external variables affecting the system’s dynamics may be hidden (not directly measurable), and therefore a model to extract the latent variable(s) from observations is necessary. Often, external variables are non-deterministic and affected by large uncertainty, and a model to perform quantification and look-ahead forecast becomes a necessity. The computing space includes numerical tools and models are combined to provide an estimation of the current QoIs of the system and their future values.

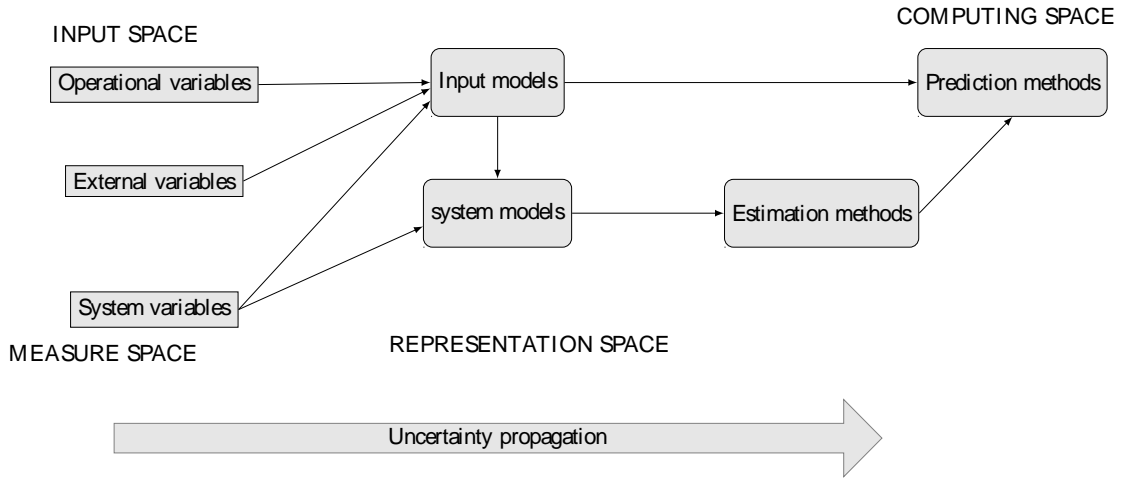


Figure C-2. Predictive process structure. The bottom arrow describing uncertainty propagation does not indicate that uncertainty is introduced only in the measure and input spaces, but it rather indicates that all the elements in the predictive process introduce uncertainty, which increases from left to right.

Case study 1 – Uncertainty Quantification applied to small UAV powertrain health monitoring

In this example, the UQ framework is applied to the design of a health monitoring system for electrical powertrain typically installed in small, low-cost UAVs. The health monitoring system consists of an electrochemistry model for Li-ion batteries developed in [C5], a model for the electronic speed controller (ESC) composed of a pulse-width modulation (PWM) system and six switches [C6], and the dynamic model of the brushless DC motor utilized to actuate rotors. Under some simplifying assumptions listed in [C3], the uncertainty affecting the powertrain elements is modeled as follows. The predictive process structure for powertrain health is depicted in Figure C-3.

The electrochemistry model for Li-ion batteries is modified to account for uncertain number of Li-ions moving from the positive sides of cell surface and bulk, as in Eq. (UM.1),

$$q_k = q_{k-1} + \dot{q}_{k-1}\Delta t + \sigma_q\sqrt{\Delta t} r \quad (\text{UM.1})$$

Where r is a random realization from the standard Normal distribution. The output voltage of the battery can then be estimated by propagating uncertainty through the model [C3]. The ESC model is shown in Eq. (UM.2).

$$\begin{bmatrix} v_{ab} \\ v_{bc} \\ v_{ca} \end{bmatrix} = V \begin{bmatrix} 1 & -1 & 0 \\ 0 & 1 & -1 \\ -1 & 0 & 1 \end{bmatrix} \begin{bmatrix} F_1 \\ F_2 \\ F_3 \end{bmatrix} \quad (\text{UM.2})$$

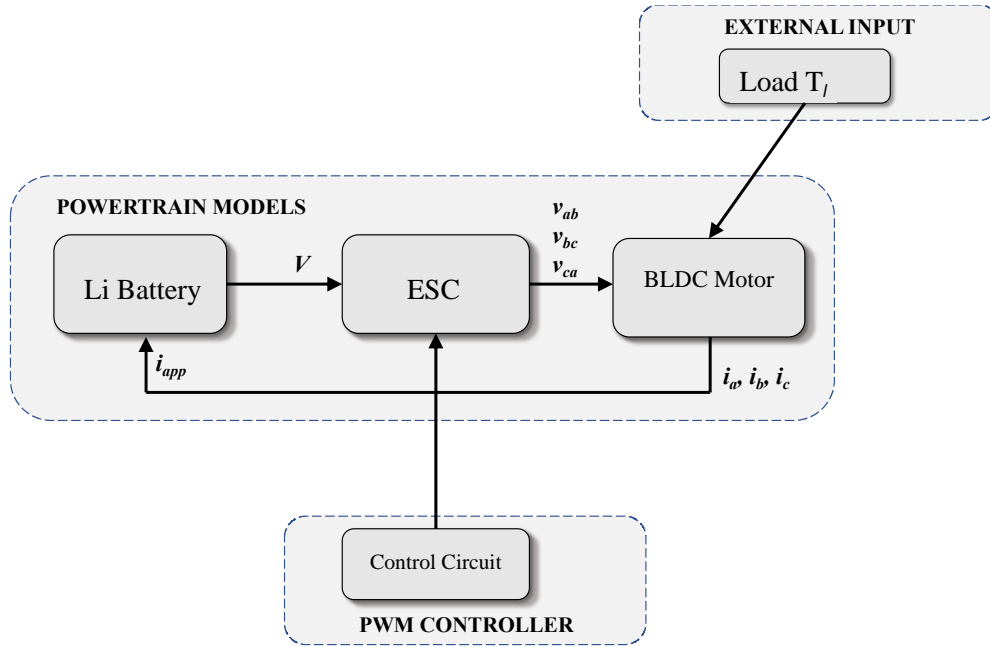


Figure C-3. Predictive model for powertrain health monitoring system

Uncertainty affecting battery voltage is accounted for in the battery model, Eq. (UM.1). The switch matrix can be modeled through reliability analysis and failure rates λ defining how often switches fail. The PWM input $\mathbf{F} = [F_1, F_2, F_3]^T$ depends on a sine wave carrier frequency f , which decreases when the MOSFET degrades [C7]. An approach could be to model the carrier frequency as a slowly, monotonically-decreasing process, Eq. (UM.3).

$$f_k = f_{k-1} - \left. \frac{df}{dt} \right|_{k-1} e^\eta \quad (\text{UM.3})$$

The random process $e^\eta, \eta \sim N(-\sigma^2/2, \sigma^2)$ ensures the degradation process is monotonic. The DC motor first-order equation well-describe its dynamic behavior, but inertia and especially friction coefficient may be known with certain confidence. They can be modeled using bounded probability distributions (e.g., log-Normal, Weibull, Rayleigh), so that uncertainty during transient periods and varying rotational speed can be accounted for [C3]. Figure C-4 shows some results from the application of the UQ approach to a synthetic powertrain.

Case study 2 – Uncertainty quantification of times of arrival during autonomous flight

This case study shows the application of the uncertainty quantification framework to trajectory prediction of small UAVs. The approach enables the estimation of the uncertainty in the times of arrival (TAs) at the predefined waypoints and over the entire trajectory [C7][C8]. It is an example where operational variables are deterministic (i.e., deterministic flight plan), but uncertainty of environmental conditions and internal states, controller performance, etc. can affecting the actual time of arrivals at the desired locations. This case study needs a limited number of elements of the predictive estimation process; namely the input space (operational variables, external variables), the input model, and the computing space containing the algorithm to estimate the TAs. Future stage of the research will include vehicle models and the capability to update the confidence intervals on the TA based on vehicle performance.

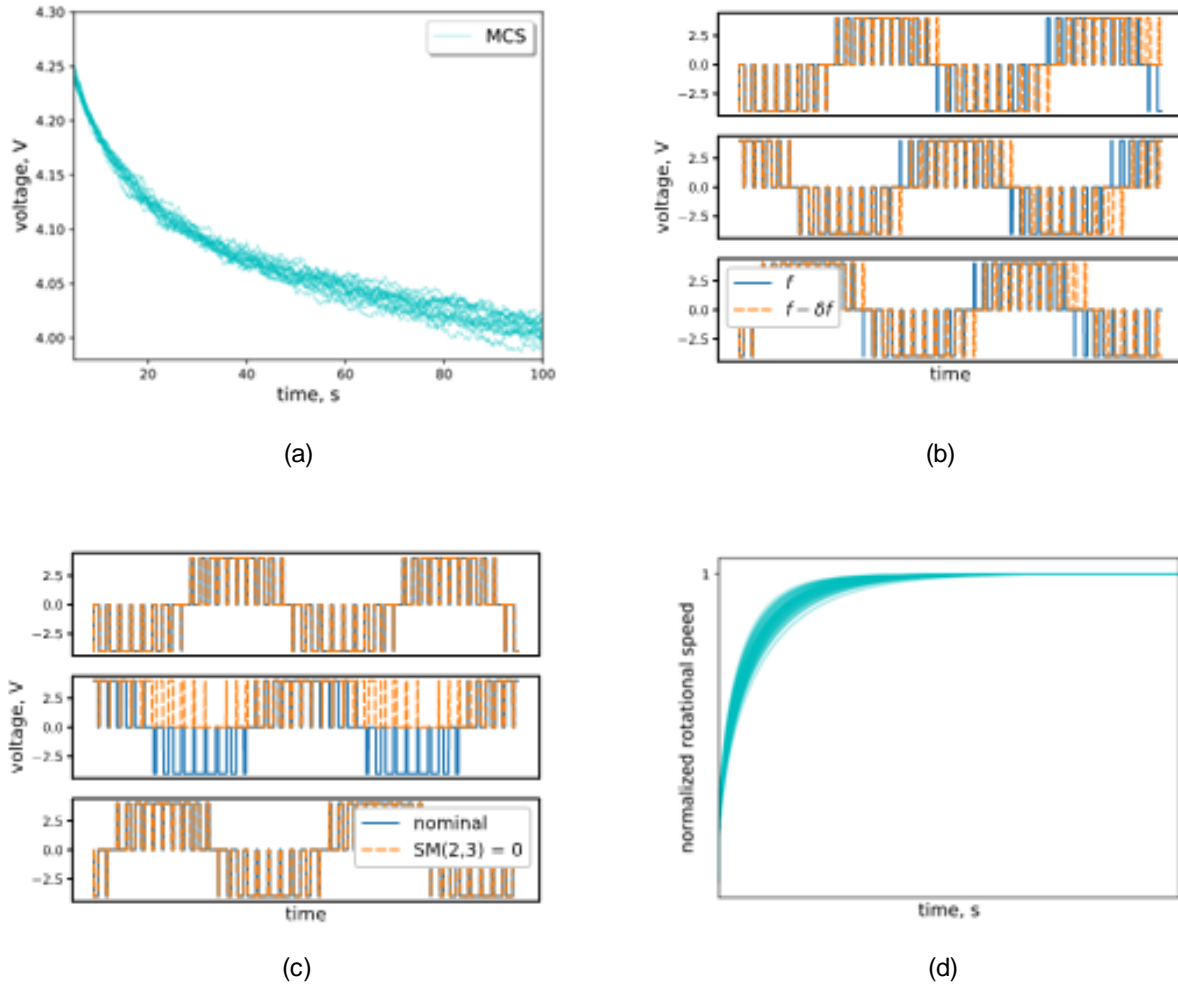


Figure C-4. Example of effects of uncertainty modeling on powertrain dynamics. Battery discharge (a), degrading PWM (b), switch failure (c), and effects of uncertain DC motor model parameters on motor speed profile (d).

The methodology assumes that both internal and external disturbances produces variations in the vehicle speed during flight. Such variations can be represented by uncertainty of such vehicle speed in the form of intervals or variance according to Uniform or Gaussian distributions, respectively. Uncertainty is then propagated via error intervals. The result is a 4D trajectory (space and time) enhanced by uncertainty in the TAs along the flight route.

Using the uncertainty on the vehicle speed as input variable, TA at waypoint k , $t_{a,k}$, can be defined as in Eq. (UM.4) assuming Uniformly-distributed velocity or Eq. (UM.5), in case of Normally-distributed velocity.

$$t_{a,k} \sim U[t_{a,k} - \delta t_{a,k}, t_{a,k} + \delta t_{a,k}] \quad (\text{UM.4})$$

$$t_{a,k} \sim N(\bar{t}_{a,k}, \sigma_{t_{a,k}}^2) \quad (\text{UM.5})$$

The term \bar{t} indicates the expected value or average of t , $\delta t_{a,k}$ is the error on the expected TA, while $\sigma_{t_{a,k}}^2$ is its variance. Estimation of error interval and variance of TAs is reported in [C8]. Figure C-5 shows an example of small UAV trajectory enhanced by the estimation of its uncertainty on the TAs, for a short flight carried out by an Octocopter at NASA Langley Research Center. Figure C-5(a) shows the nominal trajectory in thick, dashed blue line, and the confidence intervals computed using Normal (black dot-dashed) and Uniform (dashed red) distributions. The nominal trajectory prediction was generated using a NURBS (Non-Uniform Rational B-Spline) algorithm proposed in [C7]. Figure C-5(b) compares the confidence intervals from the proposed approach with the actual path recorded during flight, obtained from the filtered position estimation from the vehicle autopilot. The confidence intervals enables the estimation of the times of arrival of the vehicle at all waypoint, which can be computed during flight. Figure C-5(c) shows the uniform distributions (blue rectangles) of the TA of each waypoint computed 90 seconds after take-off (the prediction time is represented by the upside-down black triangle). The smaller, red upside-down triangles shows the observed (true) arrival time. More details on trajectory generation, uncertainty quantification and prediction are available in [C7][C8].

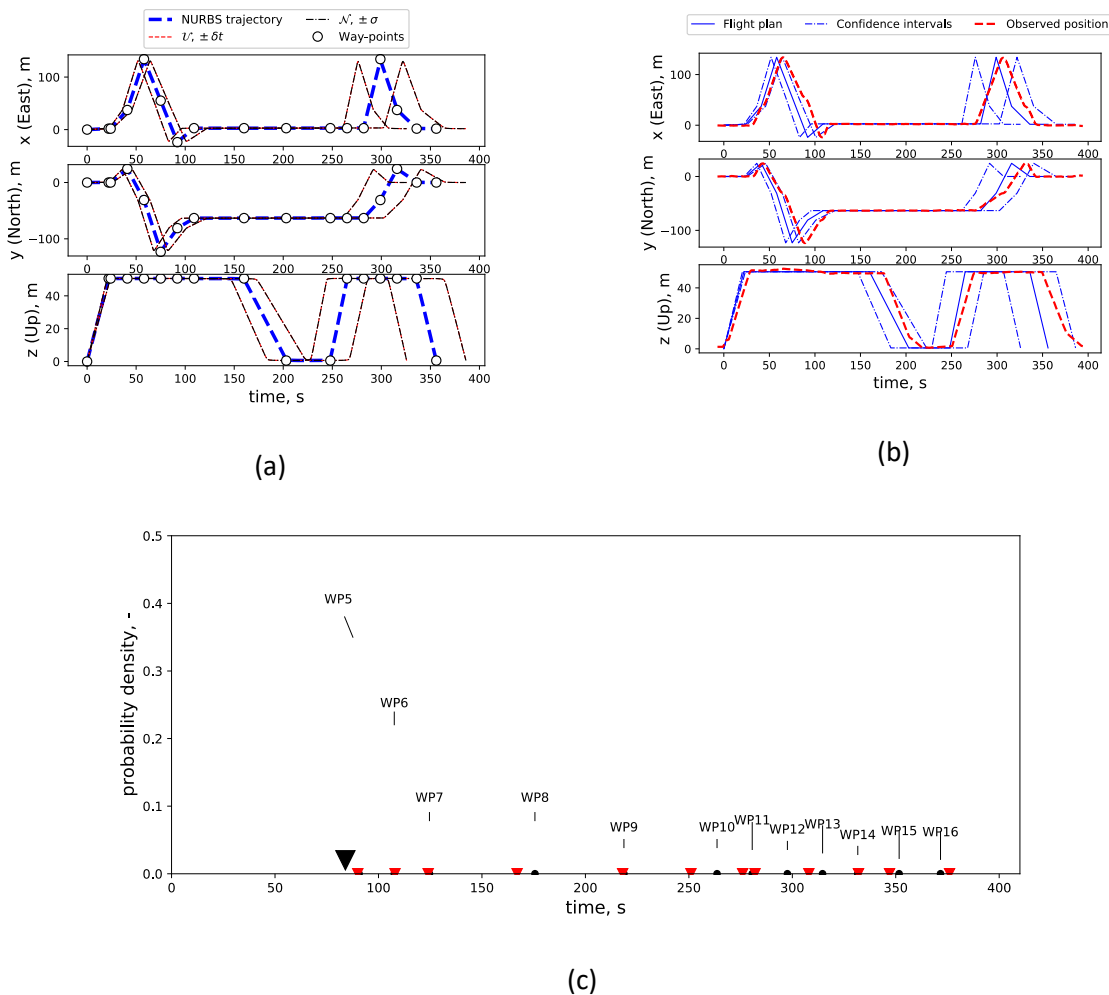


Figure C-5. Example of trajectory with TA Uniform and Gaussian confidence intervals (a), comparing the trajectory prediction enhanced by confidence interval with the executed flight path (b), predicted probability distributions of the time of arrival at each waypoint 90 seconds after take-off (c).

References

- [C1] Smith, R. C. Uncertainty quantification: theory, implementation, and applications (Vol. 12). Society for Industrial and Applied Mathematics (SIAM) 2013.
- [C2] Goebel, K. Prognostics, the Science of Making Predictions. CreateSpace Independent Publishing Platform, 2017.
- [C3] Corbetta, M. Kulkarni, C. S. An Approach for uncertainty quantification and management of unmanned aerial vehicle health. Annual Conference of the Prognostics and Health Management Society Scottsdale, AZ, 2019.
- [C4] Corbetta, M. Banerjee, P. Kulkarni, C. S. Define Framework for uncertainty representation, handling, and management. SWS Technical Report, March 31, 2019.
- [C5] Daigle, M. Kulkarni, C. S. Electrochemistry-based battery modeling for prognostics. Annual Conference of the Prognostics and Health Management Society, October 2013.
- [C6] Gorospe, G. E. J. Kulkarni, C. S. Hogge, E. Hsu, A. Ownby, N. A study of the degradation of electronic speed controllers for brushless DC motors. Asia-Pacific Conference of the Prognostics and Health Management Society, 2017.
- [C7] Corbetta, M. Banerjee, P. Okolo, W. A. Gorospe, G. E. Luchinsky, D. G. Real-time UAV Trajectory Prediction for Safety Monitoring in Low-Altitude Airspace. AIAA Aviation Forum 2019.
- [C8] Banerjee, P. Corbetta, M. Uncertainty Quantification of Flight Trajectory for Small Unmanned Aerial Vehicles. *Submitted to AIAA Journal of Guidance, Control and Dynamics*, 2019.

Appendix D. Aerodynamic Modeling

As part of the concept of model-based in-time safety assurance, aerodynamic modeling enables the prediction of vehicle states, flight behaviors, and performance which in turn can be applied to various forms of risk monitoring. Examples of this include range/endurance prediction, flight envelope and maneuvering limits, and trajectory prediction during off-nominal events such as failures or loss-of-control. NASA research has been in progress to develop concepts and methods for implementation of aerodynamic modeling and state prediction as a Supplemental Data Service (SDS). This effort has included defining modeling requirements, identifying data sources, and development of algorithms for rapid state prediction.

Current aerodynamic modeling research under System Wide Safety (SWS) builds on risk assessment research initiated under the UAS Traffic Management (UTM) project. This effort focused on trajectory prediction of small multirotor vehicles during off-nominal events including propulsion failures and control system anomalies. A Commercial Off-The-Shelf (COTS) quadcopter was used as a proof-of-concept vehicle to develop an all-attitude aerodynamic database which was subsequently implemented into a six-degree-of-freedom (6-DOF) flight dynamics simulation [D1]. The aerodynamic database was developed from experimental wind tunnel measurements for static and dynamic conditions (Figures D-1 and D-2), and was implemented as modular aerodynamic models for the rotor propulsion system, fuselage, and rotor/fuselage interaction effects. Key findings in this effort were that a properly designed aerodynamic database can predict highly non-linear flight dynamics for off-nominal events and important characteristics specific to rotors, such as vortex ring state, should be considered for off-nominal trajectory prediction. Additionally, the aerodynamic measurements enabled accurate prediction of performance parameters, such as range and endurance that may not be adequately predicted by simplified or low-order models. While efforts so far relied on experimental aerodynamic measurements, a key recommendation was to consider computational methods as a source of simulation data depending on the accuracy requirements.



Figure D-1. Static wind tunnel testing of a small quadcopter for aerodynamic database development (NASA LaRC 12-Foot Tunnel)



Figure D-2. Free-flight wind tunnel testing of a small quadcopter for aerodynamic database development (NASA LaRC 20-Foot Vertical Spin Tunnel)

Research by Ancel, et al [D2] presented the preliminary concepts toward use of trajectory prediction for real-time risk assessment. The high-fidelity simulation reported in [D1] was used to calibrate low-order point mass trajectory prediction methods where the vehicle was in a high drag, tumbling mode due to a loss of control event. The motivation for a low-order model was due to onboard computing considerations and unknown computing requirements to run a complex 6-DOF simulation in near real time. The results of this research demonstrated the feasibility of integrating probabilistic impact areas with population densities to allow an estimate of casualty areas.

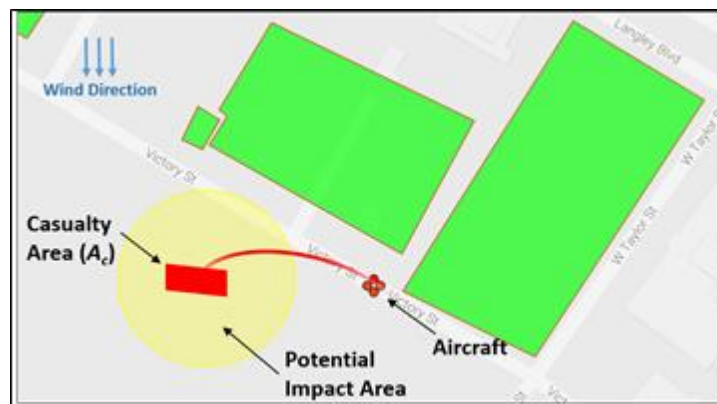


Figure D-3. Illustration of ground impact area prediction for casualty estimation [D2]

Follow-on work presented in [D3], investigated the implementation and computing requirements for a more complex onboard non-linear trajectory prediction for real-time risk assessment. A full 6-DOF simulation was installed in an onboard computer on a multirotor vehicle and used to provide real-time estimates of ground impact areas in the event of an off-nominal (loss of control) event. This testing demonstrated the feasibility of running onboard high-order flight dynamics simulations to provide critical information for risk assessment. While this effort was limited to propulsion failures, the

feasibility of predicting trajectories due to other failures or off-nominal events was demonstrated and the modeling of various failures (e.g., sensor anomaly) remains a topic for future research.

Research presented in [D4] addressed the use of a high-fidelity multirotor flight dynamics simulation [D1] for flight envelope assessment and prediction of stability boundaries. This study addressed the important influence of rotor aerodynamics on flight envelope limits and highlighted key differences between flight envelopes for multirotor vehicles and conventional fixed-wing vehicles. For example, Figure D-4 illustrates various estimated boundaries that may define the safe envelope for trajectory planning. Additionally, various optimal performance conditions may be estimated such as those for maximum range and airspeed for minimum power usage.

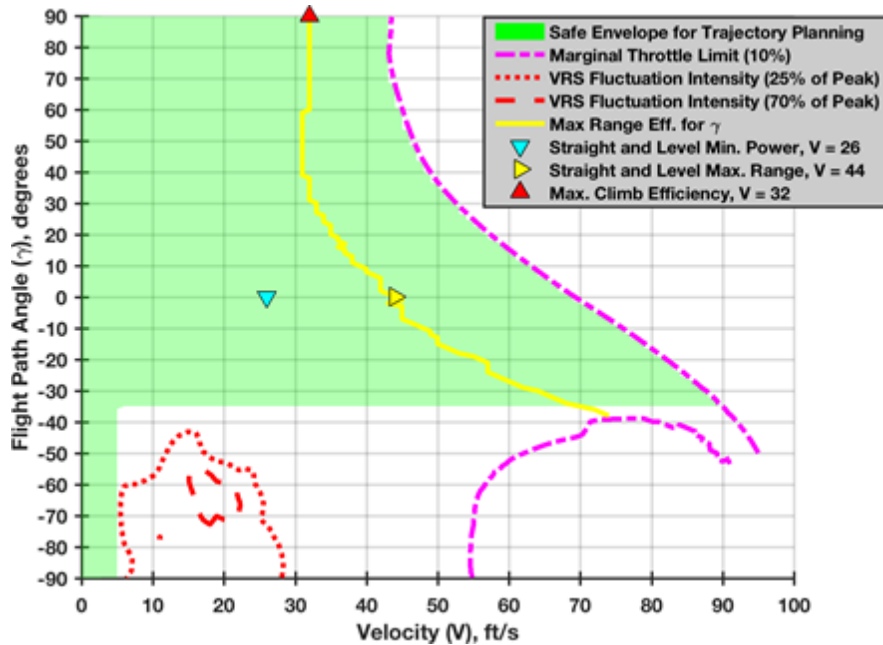


Figure D-4. Safe envelope estimation from a high-fidelity quadcopter simulation [D4]

Due to the known limitations of battery systems, the ability to predict endurance, time aloft and range will be a critical requirement for flight planning and aerodynamic modeling will likely be an important tool for safety assurance. In the context of model-based safety assurance, future research includes investigating the use of vehicle aerodynamic and state prediction models for applications to pre-flight planning, flight envelopes limits, and look-ahead or in-time calculations of performance parameters.

Information requirements – to create an initial model:

1. Propulsion effects
 - a. Rotor aerodynamic forces and moments (at least thrust, drag, and torque) as a function of flow inclination angle and rotor advance ratio

- b. Propeller and/or turbine propulsion aerodynamic forces and moments as a function of flow inclination angle, advance ratio (for a propeller) or flight condition (for a turbine engine)
2. Fuselage aerodynamic forces and moments as a function of total flow inclination angle (typically angle of attack and angle of sideslip) and control surface deflections; interference effects from the propulsion system such as rotor downwash
3. Mass properties including vehicle gross weight and moments of inertia
4. Performance metrics based on above such as flight conditions for maximum endurance, maximum range and best climb performance
5. Maneuvering limitations including maximum normal load factor, maximum turn rate and maximum body-axis angular rates
6. Envelope limits such as stall angle of attack, stall airspeed, maximum velocity and maximum normal load factor and relevant stability boundaries

Information requirements – to validate or otherwise improve the quality of the model over time

1. Flight data for steady 1g trim conditions and control response during maneuvering
2. Rotor performance data (computational, flight measurements, empirical)
3. Fuselage/airframe performance (computational, flight measurements, empirical)

References:

- D1. Foster, J. V, and Hartman, D. C.; “High-Fidelity Multirotor Unmanned Aircraft System Simulation Development for Trajectory Prediction under Off-Nominal Flight Dynamics,” AIAA-2017-3271, AIAA Aviation Technology, Integration, and Operations Conference, June 2017.
- D2. Ancel, E., Capristan, F. M., Foster, J. V., and Condotta, R.; “Real-time Risk Assessment Framework for Unmanned Aircraft System (UAS) Traffic Management (UTM),” AIAA-2017-3273, AIAA Aviation Technology, Integration, and Operations Conference, June 2017.
- D3. Ancel, E., Capristan, F. M., Foster, J. V., and Condotta, R. C.; “In-Time Non-Participant Casualty Risk Assessment to Support Onboard Decision Making for Autonomous Unmanned Aircraft”; AIAA-2019-3053, AIAA Aviation Forum, June 2019.
- D4. Hartman, D. C.; “Identification of Hazardous Flight Conditions to Establish Safe Flight Envelope for Autonomous Multirotor Aircraft”, AIAA-2019-1292, AIAA SciTech Forum, January, 2019.

Appendix E. More on In-Time Safety Assurance Functions

As described previously, in-time safety assurance systems comprise three high-level functions: Monitor, Assess, and Mitigate. These functions are described in Section 1 and in more detail below. Additional information can be found in [1], [2], and [6].

- Monitor – A collection of functions and information services that provide awareness and predictive capability regarding relevant information types. These capabilities should be designed such that uncertainty can reduce over time based on evolving on-line model validation (e.g., initial models and databases are updated over time based on operational data to improve quality of the monitoring services). Information produced by these functions are recorded and/or shared during operations with on-line assessment functions and services.
- Assess – One or more function or service that can span hazard types, contexts, and/or cascades to look for precursors, anomalies, and trends (PATs) with respect to overarching risk tolerance, aggregate safety metrics, and desired margins. Outputs from this function may be fed to auto-mitigate functions, operators for human intervention, and/or designers for off-line product improvements.
- Mitigate – Automated or multi-agent planning and execution of timely responses when necessary to maintain a desired safety margin (e.g., selecting and executing fail-safe auto-mitigations under certain safety-critical circumstances).

The scope of each function can be tailored to specific operational requirements of a given domain (e.g., hazard types, assurance levels, mitigation actions and agents). For example:

- Functions may reside at a remote service provider location (e.g., an SDSP or USS or SWIM), within the Ground Control Station (GCS), and/or onboard the vehicle.
- Functions may be employed pre-flight, in-flight, and/or post-flight.
- A human role may exist within functions, or as oversight to configure, supervise, or intervene.

Earlier in this document we describe a set of sub-functions and enabling technologies we are developing and testing that fall from the scope and assumptions given in Section 1 with respect to these high-level functions. These address apparent gaps between state-of-the-practice and the larger concept. Per the ConOps, a hazard assessment should be done for each unique domain or use-case (considering the vehicle, mission, and environment); then the appropriate set of sub-functions and enabling technologies can be applied to help mitigate any risks that are judged as too high without such mitigation. In other words, these can become tools to help make a safety case.

As described in Appendix B, two types of Assessment functions are initially developed. The first estimates the likelihood and consequence of a catastrophic event. Wherein the catastrophic event initially considered is a non-participant casualty. This function considers several hazard types that can contribute to the likelihood and consequence estimates, while also considering uncertainty propagation. The second uses proximity to high-risk areas as an aggregate measure. This approach is analogous to the Terrain Awareness and Warning System (TAWS) and the Traffic Alerting and Collision Avoidance System (TCAS). However, it allows for mapping several hazard types into a common geo-spatial reference frame. In other words, several types of areas or volumes can be hazardous for different reasons (i.e., not just terrain and traffic).

Ground-based services are in most cases, data-driven model-based predictive services that may provide or support aspects of all three functions: monitoring, assessment, and/or mitigation. An aircraft 'connection' to these services between flights versus during flights must carefully consider several factors including link bandwidth limits, information security and integrity, and risk exposure.

On-board services may also be model-based but are predicting (including making assessments) to much shorter time horizons and at higher rates and with more fidelity. For UAS, because there is no pilot onboard, some assessment and mitigation sub-functions will be automated/autonomous. We call these 'auto-assess' and 'auto-mitigate' functions. These functions may coordinate with relevant ground-based services in-flight; but this would primarily be done pre-flight (e.g., updating to latest model or information set) or post-flight (sending observations/data recorded during the flight to help with validation/update processes). It is recommended that link reliance be avoided during flight for such autonomous functions (i.e., flight-critical functions that may re-direct the flight).

Operator station functions would support the operator to manage/mitigate safety risks in different ways depending on the trained role of the operator and the phase of the operation: pre-flight, in-flight, and post-flight. Here, the human-system interface must provide for effective situation awareness and supervision given the automation functions that have been applied.

Appendix F. Test Summaries

Several tests were conducted during 2018-2019 to expose and validate requirements; evaluate the efficacy and feasibility of the envisioned information system; demonstrate interoperability within a UTM ecosystem; collect data to support R&D of on-line analytics tools regarding PATs; verify and advance technology maturity for selected elements; and inform decisions regarding R&D priorities and plans. These tests are summarized below.

Flight Testing at CERTAIN

Over 200 flights were conducted at NASA Langley's CERTAIN test range using the architecture described in Figures 4-6. Flight scenarios were designed to facilitate system checkout as well as to mimic two urban use-cases. The first was single-vehicle (and occasional multi-hop) transit flights such as would be performed for surveillance monitoring or small package delivery. The second was multi-vehicle flights executing coordinated merging-and-spacing maneuvers as may be required when sequencing for sharing of flight path segments near verti-ports in urban areas. Both included some roof top takeoffs and landings as well as flight near building structures and over people, surface traffic, and streets. Images of the flight test operational areas and flight plans are shown in Figures F-1 and F-2.

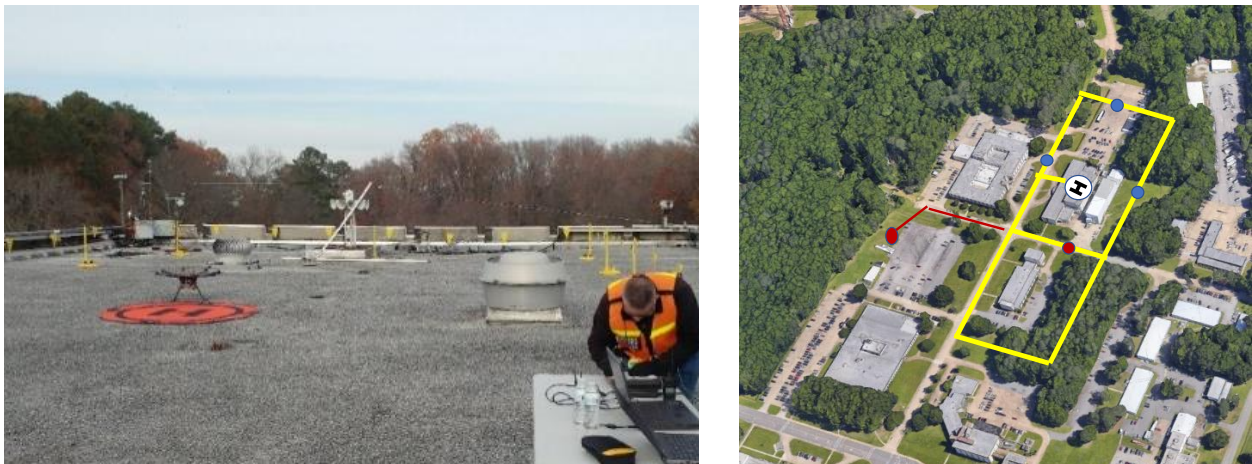


Figure F-1. Flight test location on CERTAIN (B1202 Rooftop as Takeoff/Landing Location)

During the flights, many of the 'apps' described in Section 2.3 (and shown in Figure 6) were operational on the test aircraft; as were the ground-based functions shown in Figure 5 and described further in Appendix B. As shown in Figure 6, onboard avionics consisted of COTS systems operating in parallel with the cFS-based research system. The COTS-based avionics were Arducopter/Pixhawk-based. cFS and research 'apps' were hosted on a NUC single-board computer. The research system accessed Arducopter/Pixhawk information via a serial telemetry port. CANbus communication is used to pass data gathered by the research data system to the NUC single-board computer. To test auto-mitigations, the ICAROUS technology was used in a manner similar to previous testing [31]. Namely, ICAROUS commanded a switch of the COTS autopilot (Arducopter) from 'auto' mode to 'guided' mode. Then, after the mitigation was complete (e.g., desired spacing and flight path conformance was achieved), ICAROUS commanded a switch back to 'auto' mode.

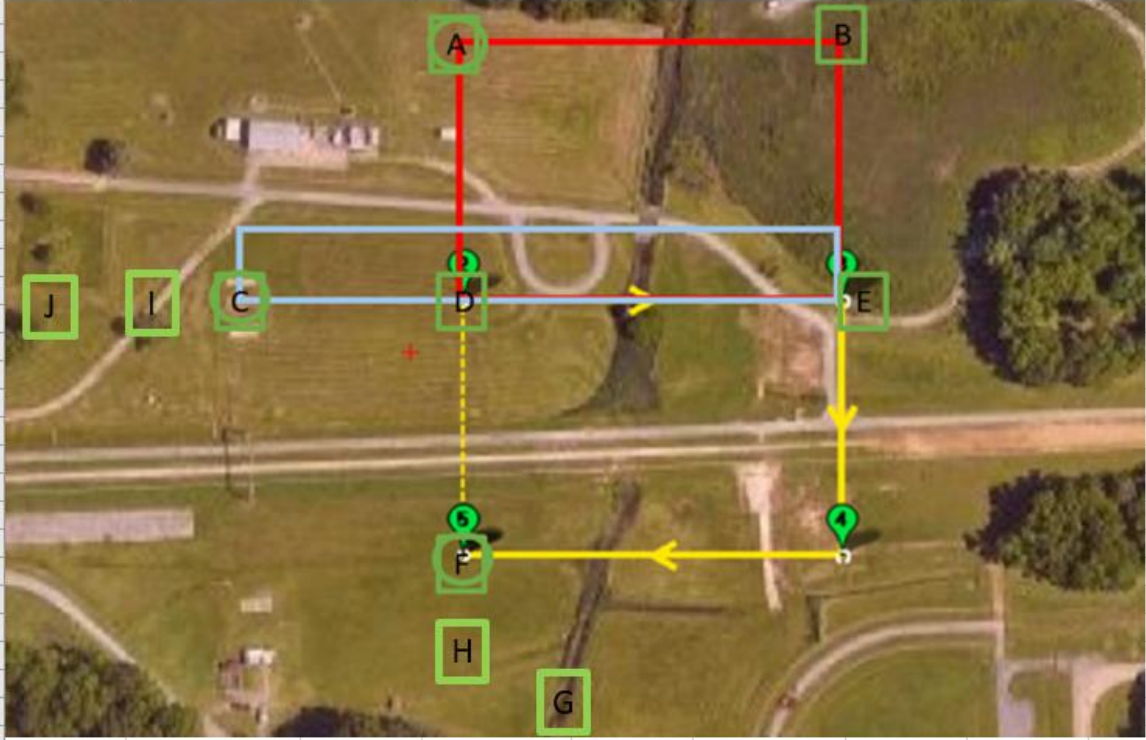


Figure F-2. Flight test location on CERTAIN (North of B1202)

In addition to continuously monitoring and reporting (e.g., back to the SDSP servers), selected ground-based infrastructure technologies were also tested per the envisioned OS&N concept for monitoring RF, wind, weather, and navigation system quality in urban areas. For this purpose, a network of stations were positioned at rooftop locations across CERTAIN. Although this network was connected and operational, the data was not part of an end-to-end in-time safety assurance service for these tests. This is a subject of future work.

Since the information system (not the aircraft) is the central focus of the research, flights used low cost, commercially available multi-rotor platforms. For these tests, COTS octo-copters were used, modified to host Arducopter/Pixhawk, the cFS-based research system, and other equipment (e.g., Safeguard for conformance monitoring [33][34], a Software Defined Radio (SDR) for monitoring received signal strength on selected RF channels, and a NextNav receiver [22]).

Flight tests began with some basic capabilities and a single vehicle, then progressed to increasingly integrated systems, functionality, and complex multi-vehicle scenarios. Some tests were tailored to evaluate or demonstrate or collect data for specific elements of the system. A breakdown of these tests is given in Table F-1. Illustrative examples of data collected are given in Figures F-3 and F-4. An example of the research GCS operator interface is shown in Figure F-5.

Table F-1 Examples of tailored testing of selected functions or system elements.

System/Function	#Flights	Data Note
RF monitoring	6	500+ GB I-Q data: 2.4 GHz and 900 MHz ISM bands
Safeguard (Tests for Class B certification)	7	Various verification logs
Battery Prognostics (BP)	64	Battery usage data (Flight plan power estimation)
APNT system (NextNAV)	7	Logs on various systems
Real-Time Risk Assessment (RTRA)	32	cFS RTRA app logs, 1 log per flight
Interfacing with SDSPs and UTM	10	Verify data marshalling between vehicle and server. Checks of receipt of "Trajectory", "Battery EOD", and "Battery SOC" info from Ames-based SDSP services
UTM M&S software integration tests	55 (38 Cerf) (17 ISSAAC)	Single and multi-vehicle test cases verifying merge and spacing algorithm using ICAROUS
		Operating in conjunction with on-board and off-board services
		Checks of RTRA interoperability on-board

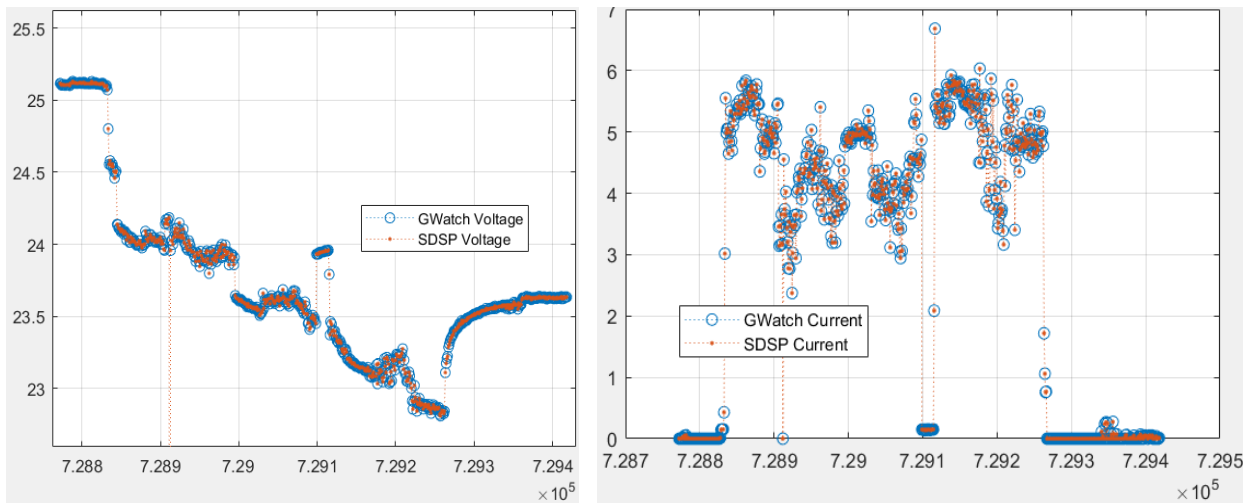


Figure F-3: Data exchange verification test. Voltage (left) and current (right) levels as sent from GCS (blue) and received by the Battery Prognostics (BP) service over the 4G LTE cell phone network. Data sent from vehicle to GCS was via a 900 MHz telemetry link. This data segment is from a landing during a multi-stop flight scenario.

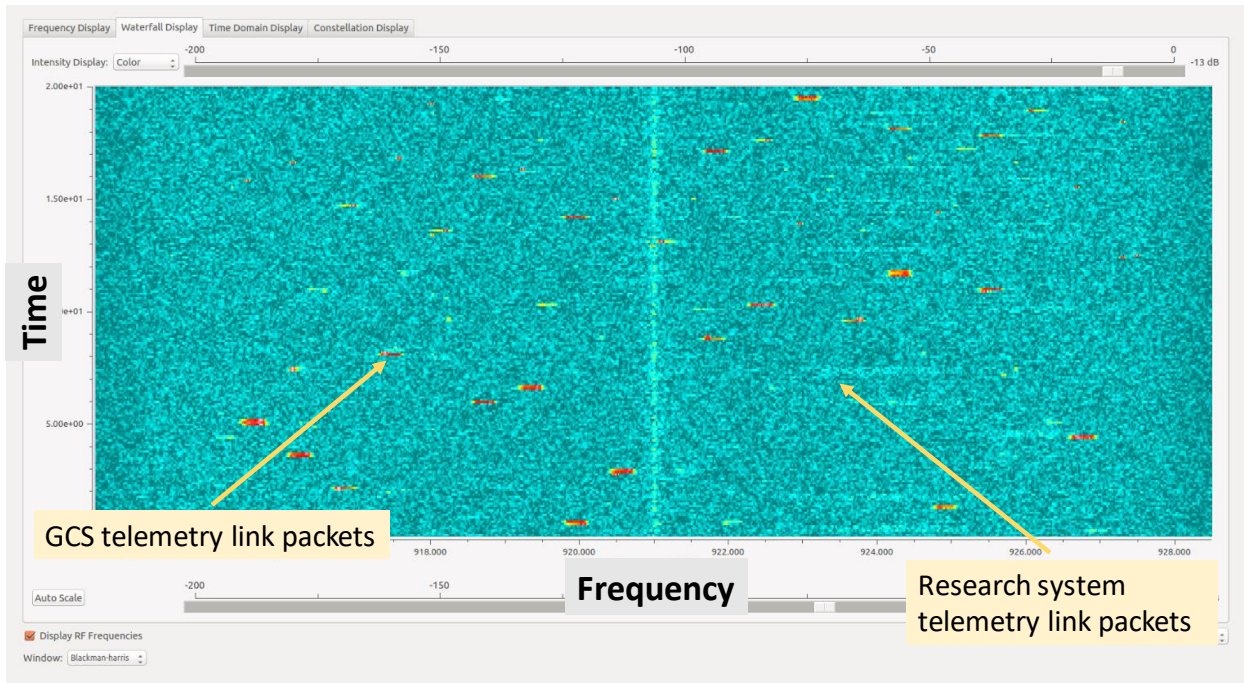


Figure F-4. GCS and research telemetry link data packets as seen by the SDR RF sensor during Flight 141 (multiple transmitting links operating)

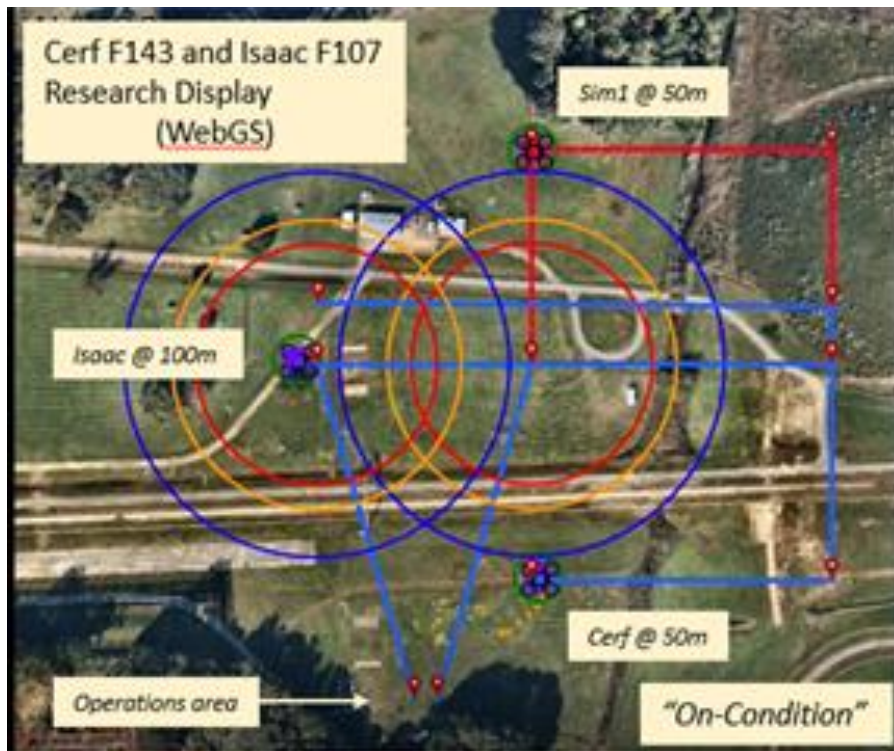


Figure F-5. Research GCS display showing vehicle geometries at beginning of merging scenario. Isaac aircraft (left); Cerf aircraft (bottom right); Sim1 is a simulated aircraft (top right). Labels are aircraft altitudes. All three aircraft are moving toward a merge point (center).

UTM TCL-4 Sprint 4 Simulation

The ‘Sprint 4’ tests were conducted in February 2019. This was an extension of the ‘Sprint 3’ exercise, in which the team demonstrated basic integration and communication with the Airspace Operations Laboratory (AOL) USS (a.k.a the ‘NASA USS’) to show interoperability within the UTM architecture. At the time of this testing, the developmental SDSP service provided two safety metrics: battery End-of-Discharge (EOD) prediction and obstacle proximity prediction. These are referred to more generally in Figure 4 and Appendix B as the ‘BP’ and ‘PtT’ services. The architecture used for the simulation is shown in Figure F-6.

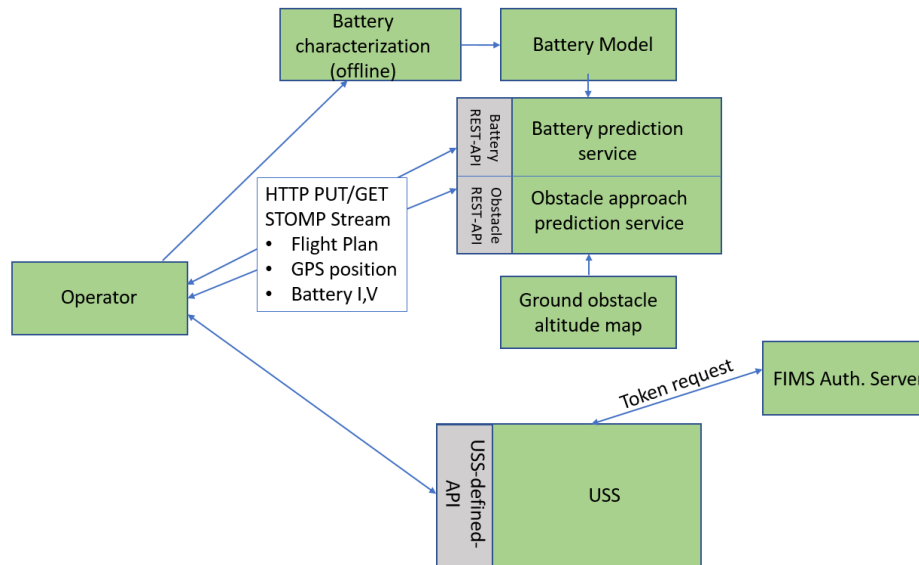


Figure F-6. SDSP Architecture for UTM Sprint 4 Simulation Testing

This testing was limited to USS implementers and did not have an “Actor Role” for SDSP participation. Nevertheless, we wanted to build upon Sprint 3 capability and show a more complete integration between the NASA Ames Airline Operations Lab (AOL) USS and the SDSP server. In addition to testing the connection with AOL USS, we wanted to demonstrate reliable transmission of the prognostic event data as calculated by SDSP back to the AOL USS for display.

A flight scenario was chosen from the set of scenarios previously flown at NASA Langley in 2018. We specifically chose Scenario ‘4’ as it was the shortest and the sim was configured to run for only a few minutes. Simulated GPS coordinates were based on flight test data from the Langley flights of 2018. Battery calibration parameters were set to be the same as used for the flights.

Scenario 4. Simulate building proximity violations; test system connectivity performance as well as the performance of the predictive services for battery EOD and proximity to obstacles. Description: See Figure F-7. Start at rooftop launch point (A), pick up package at E, deliver to G, return to base (A). Due to time-criticality of package, fly direct to G. Plan: A @ 0m, A-E @ 10m, E @ 0m (hover, 15sec), E @ -10m (land), E-G @ 30m, G @ 0m (hover, 15sec), G @ -10m (land), G-F-B-A @ 30m, A @ 0m(land).



Figure F-7. Scenario 4 Flight Plan Waypoints (based on CERTAIN flight tests)

During the tests, both position and battery performance data were successfully received from the UTM simulation via the RESTful interface, and safety metrics were calculated with that data using the PaaS/GSAP architecture. Performance was verified via real-time server logs on the SDSP side. Safety metric events were then returned to the AOL console screen, displaying time to each event, time to end of event, and threshold percentages. Communication reliability and data integrity were established during Sprint 3, thus in test we successfully showed that the events could be successfully returned to the AOL USS and displayed to the user. Figure F-8 is a screenshot of the chart displaying proximity metrics for one of the tests.

Last update: Thu Feb 14 2019 11:54:50 GMT-0800 (Pacific Standard Time)

Hazard ID	Hazard Type	Minimum Margin	Start Time	Start Location	End Time	End Location
Bldg	342418160	78.77447645245113	-14869:06	37.09908/-76.38548	-14869:06	37.09908/-76.38548
Bldg	342418172	-81.42638200811453	-14869:06	37.09836/-76.38474	-14869:06	37.09836/-76.38474
Bldg	342418160	78.77447645245113	-14869:04	37.09908/-76.38548	-14869:04	37.09908/-76.38548
Bldg	342418172	-81.42638200811453	-14869:04	37.09836/-76.38474	-14869:04	37.09836/-76.38474
Bldg	342418160	78.77447645245113	-14869:02	37.09908/-76.38548	-14869:02	37.09908/-76.38548
Bldg	342418172	-81.42638200811453	-14869:02	37.09836/-76.38474	-14869:02	37.09836/-76.38474
Bldg	342418160	78.77447645245113	-14869:00	37.09908/-76.38548	-14869:00	37.09908/-76.38548
Bldg	342418172	-81.42638200811453	-14869:00	37.09836/-76.38474	-14869:00	37.09836/-76.38474
Bldg	342418160	78.77447645245113	-14868:58	37.09908/-76.38548	-14868:58	37.09908/-76.38548
Bldg	342418172	-81.42638200811453	-14868:58	37.09836/-76.38474	-14868:58	37.09836/-76.38474

Figure F-8. AOL Console Screenshot with Proximity Predictions from Server

UAM X2 Simulations

The X2 simulation experiment was designed to test a service-oriented ATM architecture for future UAM operations. The simulation was conducted by NASA's ATM-X project and was aimed primarily at ATM issues such as scheduling and de-conflicting UAM vehicles flying into and out of vertiports in the Dallas/Fort Worth area. Varying levels of automation were considered to assist in traffic management. X2 is part of preliminary work leading to the Grand Challenge (GC) series of events planned for coming years. The stated goals/objectives of the GC series are as follows¹:

“The Grand Challenge itself will be a full field demonstration in an urban environment that tests the readiness of companies’ vehicles and airspace operators’ systems to operate during a full range of passenger transport and cargo delivery scenarios under a variety of weather and traffic conditions.”

“Its objectives are to:

- *Accelerate technology certification and approval*
- *Develop flight procedure guidelines*
- *Evaluate communication, navigation and surveillance options*
- *Demonstrate an airspace system architecture based on NASA’s UTM construct*
- *Collect initial assessments of passenger and community perspectives on vehicle ground noise, cabin noise and on-board ride quality”*

Although the X2 simulation was initially designed without the in-time safety assurance system concept in mind, the ecosystem (based on UTM) allowed for fairly direct migration and evaluation of interoperability. This also allowed the opportunity to see if the system design was flexible enough to be applied within a different underlying simulation framework. For X2, the ‘Testbed’ sim was used for traffic simulation, rather than the AOL sim that had been used for prior UTM studies. In this environment, we were able to monitor the data stream being passed across the ActiveMQ messaging server and subscribe to messages of interest while the experiment was underway. This was done by connecting to a “broker” messaging adapter that published and subscribed to all of the UAM-specific message types. The in-time safety assurance services were able to listen and record all sim data sent from both NASA and industry participants via this connection through the use of two message types. These types are described in more detail below.

A `UssWebSocketAdapter` was chosen in particular because it was able to access both the Track data from the Traffic Publisher, the MACS simulated Track data, and the UAM-specific data being communicated to the NASA USS.

The architecture used for the simulation is shown in Figure F-9, with the in-time safety assurance services denoted as ‘Testbed PaaS’. Connections were via an Amazon Web Services (AWS) gateway using a RESTful interface. While this diagram is an over-simplification of the overall architecture, it does show the industry partner elements (in blue) and underscores the idea that services communicated via the use of TestBed adapters.

The adapter software was installed via the Testbed’s SDK package. Installation was straightforward, though some modifications were required for each test in order to connect with the correct instance of

¹ [Online] <https://www.nasa.gov/uamgc>

the publisher. During this phase of the simulation, only data subscription was tested. For future tests and during GC demonstrations, end-to-end capability would be evaluated (i.e., publish back to the data bus information about airspace safety metric tracking and predictions).

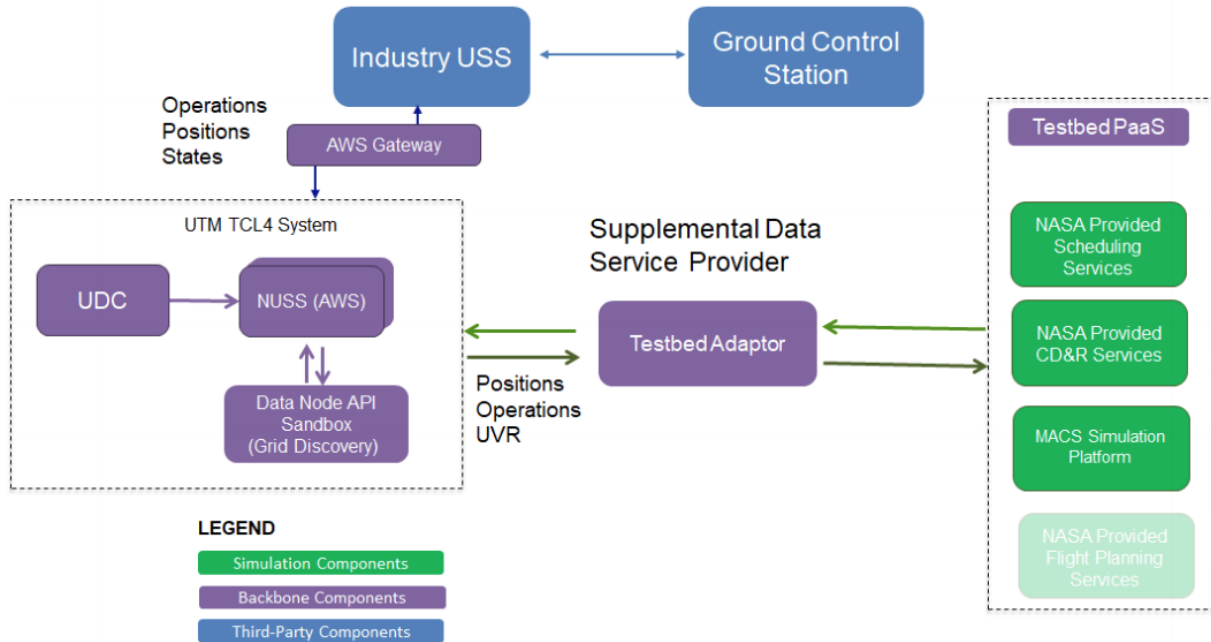


Figure F-9. X2 Simulation Architecture

Data collected from the ActiveMQ communication bus came in two distinct datatypes and one subtype: *UAMPosition*, *UAMCommonFlightProfile* and its subtype *TrajectoryChangePoint*. *UAMCommonFlightProfile* datatype includes 12 parameters, including for example aircraft ID, takeoff time, trajectory change points, cruise altitude, and cruise speed. *TrajectoryChangePoints* subtype included for each point, waypoint name, location, speed and ETA expected at the point. *UAMPosition* includes 12 parameters, including for example time, position, altitude, track, and ground speed of the simulated vehicle. Note: The reference vehicle was modeled as having four lifting rotors for vertical takeoff, and a forward propeller and wings for forward flight.

The test cards were designed to run through three use cases under two different traffic conditions and different configurations of autonomy. Overall there were three use cases, with two different traffic scenarios and three autonomy configurations for a total of 24 test cards. Details of the experiment design are to be published separately by researchers in the ATM-X project.

Data collected during the simulated flights is currently being analyzed, but it should be noted that the intent of the participation in the X2 simulation was to enable future integration across UAM-related projects, and to identify gaps or barriers regarding effective information exchange and interoperability of ATM functions with in-time safety assurance functions.

Appendix G. Acronym List

ADS-B	Automatic Dependent Surveillance - Broadcast
AIM	Aeronautical Information Management
AIS	Aeronautical Information Services
AIXM	Aeronautical Information Exchange Model
AMSL	Above Mean Sea Level
ANSP	Air Navigation Service Provider
ASAP	Aviation Safety Action Programs
ASIAS	Aviation Safety Information Analysis and Sharing
ASRS	Aviation Safety Reporting System
ATC	Air Traffic Control
ATM	Air Traffic Management
BBN	Bayesian Belief Network
BHM	Battery Health Monitoring
BP	Battery Prognostics
CANbus	Controller Area Network Bus
cFS	Core Flight System
CAS	Convergent Aeronautics Solutions
COTS	Commercial Off The Shelf
DC	Direct Current
DoF	Degrees of Freedom
DPAL	Data Processing Assurance Level
DQR	Data Quality Requirement
EOD	End Of Discharge
EPT	Engine Power Train
ESC	Electronic Speed Controller
ETA	Estimated Time of Arrival
FIMS	Flight Information Management Systems
FIXM	Flight Information Exchange Model
GBAS	Ground Based Augmentation System
GCS	Ground Control System
GPS	Global Positioning System
GRASP	Ground Risk Assessment Service Provider
GUI	Graphical User Interface
HRRR	High Resolution Rapid Refresh
ICAROUS	Independent Configurable Architecture for Reliable Operations of Unmanned Systems
IMU	Inertial Measurement Unit
IMU	Interval Management
INS	Inertial Navigation System
IASMS	In-Time Aviation Safety Management System
ISSA	In-Time System-Wide Safety Assurance

JSON	Javascript Object Notation
LAANC	Low Altitude Authorization and Notification Capability
LOCD-IN	Location Corrections through Differential Networks
MAVLink	Micro Air Vehicle Link
MOR	Mandatory Occurrence Reports
NAS	National Airspace System
NAVQ	Navigation system Quality service
NPCRA	Non-Participant Casualty Risk Assessment
NSQ	Navigation System Quality
OS&N	Observation Stations and Network
PATs	Precursors, Anomalies, and Trends
PCE	Polynomial Chaos Expansion
PIREP	Pilot Report
PtR	Proximity to Risk
PtT	Proximity to Threat
PWM	Pulse Width Modulation
QOI	Quantities of Interest
R&D	Research and Development
RC	Remote Control
RFI	Radio Frequency Interference
RTA	Run-Time Assurance
RTL	Return To Launch
RTRA	Real-Time Risk Assessment
SAIL	Specific Assurance and Integrity Level
SDSP	Supplemental Data Service Providers
SMS	Safety Management
SORA	Specific Operations Risk Assessment
sUAS	Small Unmanned Aircraft Systems
SWIM	System-Wide Information Management
SWS	System-Wide Safety
TA	Time of Arrival
UAM	Urban Air Mobility
UAS	Unmanned Aircraft Systems
UAV	Unmanned Aerial Vehicle
UM	Uncertainty Management
UQ	Uncertainty Quantification
URAF	UTM Risk Assessment Framework
USS	UAS Service Suppliers
UTM	UAS Traffic Management
WAAS	Wide Area Augmentation System
WGS84	World Geodetic System 1984
WXXM	Weather Information Exchange Model

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

The public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing the burden, to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.
PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.

1. REPORT DATE (DD-MM-YYYY) 1-01-2020		2. REPORT TYPE Technical Memorandum		3. DATES COVERED (From - To)	
4. TITLE AND SUBTITLE Architecture and Information Requirements to Assess and Predict Flight Safety Risks During Highly Autonomous Urban Flight Operations				5a. CONTRACT NUMBER	
				5b. GRANT NUMBER	
				5c. PROGRAM ELEMENT NUMBER	
6. AUTHOR(S) Young, Steve D.; Ancel, Ersin; Moore, Andrew J.; Dill, Evan T.; Quach, Cuong C.; Foster, John V.; Darafsheh, Kaveh; Smalling, Kyle M.; Vazquez, Sixto L.; Evans, Emory T.; Okolo, Wendy; Corbetta, Matteo; Ossenfort, John; Watkins, Jason; Kulkarni, Chetan S.; Spirkovska, Liljana				5d. PROJECT NUMBER	
				5e. TASK NUMBER	
				5f. WORK UNIT NUMBER 340428.02.40.07.01	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) NASA Langley Research Center Hampton, VA 23681-2199				8. PERFORMING ORGANIZATION REPORT NUMBER L-21052	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) National Aeronautics and Space Administration Washington, DC 20546-0001				10. SPONSOR/MONITOR'S ACRONYM(S) NASA	
				11. SPONSOR/MONITOR'S REPORT NUMBER(S) NASA-TM-2020-220440	
12. DISTRIBUTION/AVAILABILITY STATEMENT Unclassified- Subject Category 03 Availability: NASA STI Program (757) 864-9658					
13. SUPPLEMENTARY NOTES					
14. ABSTRACT This report comprises architecture and information requirements and considerations toward enabling such a capability within the domain of low altitude highly autonomous urban flight operations. This domain may span, for example, public-use surveillance missions flown by small unmanned aircraft (e.g., infrastructure inspection, facility management, emergency response, law enforcement, and/or security) to transportation missions flown by larger aircraft that may carry passengers or deliver products.					
15. SUBJECT TERMS Assurance; Complexity; Modeling; Unmanned Aircraft; Urban Air Mobility					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			STI Help Desk (email: help@sti.nasa.gov)
U	U	U	UU	80	19b. TELEPHONE NUMBER (Include area code) (757) 864-9658