Integration of Unmanned Aircraft Systems into Complex Airspace Environments

Robert R. Lutz, Paul S. Frederick, Patricia M. Walsh, Kimberly S. Wasson, and Norm L. Fenlason

ABSTRACT

The MQ-4C Triton is a high-altitude, long-endurance unmanned aircraft system suitable for conducting several Navy missions, such as maritime surveillance, battle damage assessment, and port surveillance. These missions are frequently conducted in airspace populated by both civilian and military manned aircraft, necessitating defensive strategies supported by specialized sense and avoid systems to self-separate from other aircraft and avoid potential collisions. This article describes the activities being sponsored by the Navy's Persistent Maritime Unmanned Aircraft System Program Office (PMA-262) to demonstrate the Triton's ability to operate safely in both offshore and oceanic environments. These activities include development of operational architectures, specification of airspace characteristics in defined mission areas, detailed analysis of potential hazards, and development of a safety case that integrates decomposed airspace integration claims and evidence into a compelling argument that Triton will safely operate in its intended environments. This article also describes the modeling and simulation tools and techniques that support many of these activities and highlights how this modeling and simulation infrastructure is being employed across a range of safety-related studies.

BACKGROUND

Advances in technology have facilitated the rapid fielding of unmanned systems into operations that were long assumed to require manned assets. Many of these operations are civil in nature and include such disparate applications as search and rescue, law enforcement, emergency management, border patrol, firefighting, and even mail delivery. However, it is the U.S. military that is increasingly turning to unmanned systems to perform the "dull, dirty, and dangerous" missions required to effectively counter modern threat systems. For instance, the Army regularly employs robotic unmanned ground vehicles to counter the threat to manned forces introduced by improvised explosive devices. Similarly, the Navy uses unmanned undersea vehicles for minesweeping operations and long-duration anti-submarine warfare missions.[1] However, unmanned aircraft systems (UASs) have traditionally drawn the most attention across the military community because of the wide range of missions they can support, the reductions in the number (and thus cost) of the people needed to operate them, and their ability to keep pilots and other mission-critical personnel out of harm's way.

Recognition of the benefits that UASs provide in military operations has resulted in a rapid escalation in flight hours. For instance, while it took the Army 20 years to reach the first million UAS flight hours in 2010, it has taken less than 4 years from that date to reach the 2-million flight-hour mark.[2] While UASs are transforming operational effectiveness and efficiency across a wide range of missions, the policy, technologies, and procedures necessary to routinely access airspace have not kept pace. In manned aircraft, safety systems and procedures have been designed under the assumption that the pilot is able to sense the environment and respond to potentially dangerous situations in real time. However, when the pilot is moved from the air vehicle to the ground station, the new paradigm of pilot reliance on data link technology and human–computer interfaces largely invalidates that assumption. The absence of harmonized UAS procedures and safety standards poses a significant challenge to civil regulators who are responsible for ensuring the safety of all users of the airspace yet also for balancing the needs of the military in conducting operations essential to national defense. For continental U.S. operations, federal aviation regulations, procedures, and technologies do not permit routine UAS access to the national airspace. Today, all military UAS operations in civil-controlled airspace must be approved using complex, time-consuming procedures by the country in which the operations will occur. The procedures and information needed to support national approvals are themselves not standardized, resulting in a long logistics tail, and in many instances years of advance coordination depending on the UAS and mission type. The Federal Aviation Administration (FAA) and DoD are well aware of the need for new policies, regulations, capabilities, and procedures for UAS operations in the national airspace, and they are collaborating with a broad range of stakeholders (e.g., manufacturers, standards organizations, universities, and research and development centers) to develop the needed guidance and infrastructure.[3]

Since many UAS operations are conducted in areas outside of the national airspace, the International Civil Aviation Organization (ICAO) is developing similar guidance for civil UAS operations in international airspace.[4] However, there is still much work to do. While organizations like the Radio Technical Commission for Aeronautics are actively working on UAS policy issues with ICAO and the FAA, DoD UAS programs currently have little in the way of established tools and techniques for demonstrating that a UAS can achieve an equivalent level of safety as compared to manned aircraft systems. Thus, the challenge from a system acquisition perspective is how to develop a convincing set of evidence that will demonstrate not only that a UAS can comply with existing airspace safety regulations but also that the UAS design will satisfy safety acceptability and performance requirements. Development of integrated safety systems and procedures capable of achieving the intent of these regulations will require the production of various classes of safety-related evidence, supported by innovative analysis approaches, new testing methodologies, and robust and credible modeling and simulation (M&S) infrastructure. These supporting capabilities will be a critical need for any future DoD UAS program with airspace integration requirements. The U.S. Navy's MQ-4C Triton program is actively pioneering these core capabilities, as discussed in the following sections.

TRITON OVERVIEW

The Triton is the U.S. Navy's high-altitude, long-endurance UAS (see Fig. 1). A maritime variant of the U.S. Air Force's Global Hawk system, the Triton is suitable for conducting continuous sustained operations over an area of interest at long ranges. It relays maritime intelligence, surveillance, and reconnaissance information directly to the maritime commander. Triton is capable of providing persistent maritime surveillance and reconnaissance coverage of wide oceanographic and littoral zones at a mission radius of 2000 nmi. The UAS is designed to fly 24 h a day, 7 days a week with 80% effective time on station.[5]

Triton can be deployed in a range of missions such as maritime surveillance, battle damage assessment, port surveillance, and communication relay. It will also have the capability to support other units of naval aviation to conduct maritime interdiction, anti-surface warfare, battlespace management, and targeting missions. These missions can be performed worldwide, including in areas that are potentially populated with other air traffic. To conduct these missions safely and effectively in the vicinity of other air traffic, Triton must include a sense and avoid (SAA) system that mitigates collision risk to an acceptable level, and in so doing, provides an alternative means of compliance with international and national "safe separation or collision avoidance" regulations, such as Title 14 of the U.S. Code of Federal Regulations, Part 91.113, which reads:

> When weather conditions permit, regardless of whether an operation is conducted under instrument flight rules or visual flight rules, vigilance shall be maintained by each person operating an aircraft so as to see and avoid other aircraft.

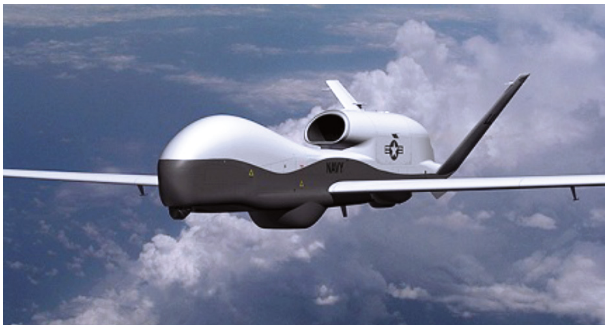


Figure 1. MQ-4C Triton.

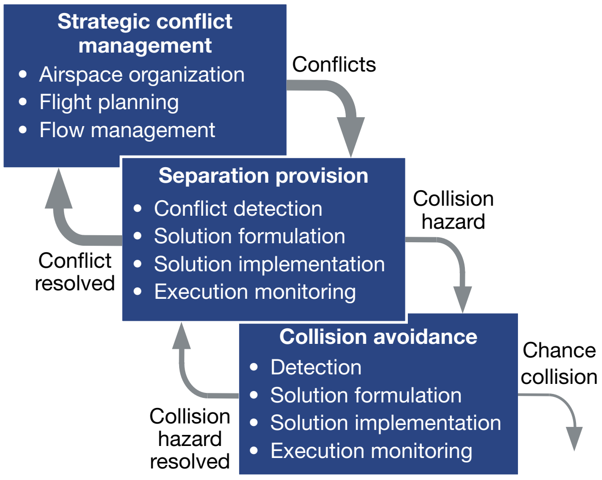


Figure 2. Layered approach to avoiding collisions.

Mission effectiveness and regulatory compliance will depend on a layered defense strategy similar to that shown in Fig. 2. The outermost defense (strategic conflict management) consists of a set of procedures, rules, and equipment, as defined by the ICAO and the FAA, for safe operation in the national and international airspace. Simply adhering to these rules substantially reduces the chance of midair collisions. The middle ring of defense (separation provision) leverages a combination of air traffic control services and onboard systems, such as the airborne/traffic collision avoidance system, the automatic dependent surveillance-broadcast system, and SAA air-to-air radar, to monitor the airspace and de-conflict potential separation minima violations.

The innermost ring (collision avoidance) comprises the same onboard sensors, but it provides for additional performance functionality such as automated collision avoidance algorithms should the first two layers fail to maintain safe separation.[6] The last two layers make up the SAA system, sometimes referred to as the tactical conflict management system.

Used in combination, the objective of the strategic conflict management system and the SAA system is to achieve a defined target level of safety, expressed in terms of X collisions per flight hour. The ability of the Triton system to attain desired target levels of safety depends on three key factors: (*i*) the complexity of the air-traffic and natural environment in which the UAS will operate over its life cycle; (*ii*) the technology and performance of the SAA system required for the operating environment; and (*iii*) the procedures used to mitigate encounters with other aircraft based on knowledge of the airspace. Addressing the full range of such factors, along with the various interrelationships and dependencies among these factors, is a highly challenging endeavor that dictates the need to solve the problem in stages. The goal is to deliver enhanced capability incrementally over the life cycle and, in so doing, to strike a balance among safety, mission effectiveness, and budgetary constraints.

TRITON AIRSPACE CERTIFICATION

The U.S. Naval Air Systems Command (NAVAIR) is the technical authority responsible for the total life cycle acquisition and technical management for all U.S. Navy aircraft. In this role, NAVAIR is responsible for ensuring that all aircraft, including UASs, are airworthy and in compliance with civil and military procedures and technical standards for equipment necessary to operate

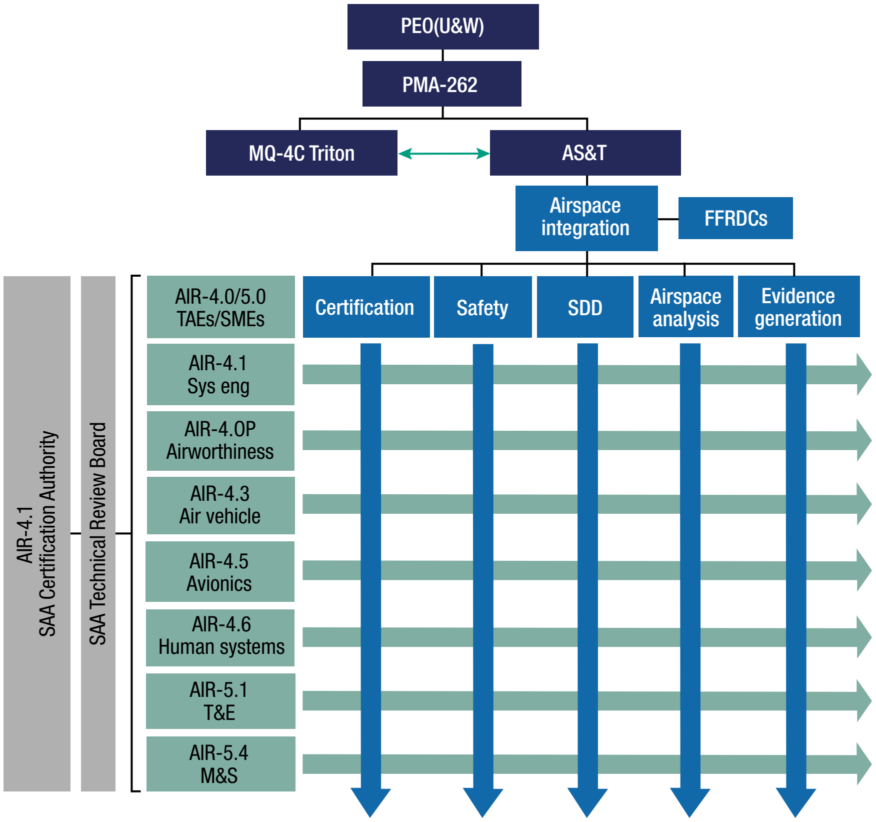


Figure 3. Organization of Triton airspace integration team. FFRDC, federally funded research and development center; PEO(U&W), Program Executive Officer, Unmanned Aviation and Strike Weapons; SDD, system development and demonstration; SMEs, subject-matter experts; T&E, test and evaluation.

safely in the airspace. When technical standards exist, systems are developed in accordance with the standards. When technical standards do not exist, it is necessary to establish the policy guidance and processes by which technical standards will be developed and approved. Since neither civil nor military technical standards exist for SAA systems, the MQ-4C Triton program has taken on the de facto role as the "path finder" for identifying the end-to-end processes for certifying such a system. To that end, the first step was to establish an airspace integration team to explore and identify the scope of work, the resources required, and the tools necessary to deliver a certified SAA system. The airspace integration team comprises NAVAIR functional subject-matter experts and technical area experts (TAEs), and when unique expertise or capability is not resident within NAVAIR, the team relies on expertise from federally funded research and development centers and university-affiliated research centers. The team is organized across product/functional areas deemed critical to SAA system development and certification (see Fig. 3).

A major milestone was achieved when NAVAIR issued NAVAIRINST 13034.4,[7] which established policy on the certification of SAA systems for use on UASs. This was a critical first step in ensuring U.S. Navy compliance with civil collision avoidance regulations. In addition to defining organizational roles and responsibilities, the policy established enterprise-level requirements that (*i*) SAA systems be certified, thus acknowledging the safety-critical nature of the capability; (*ii*) SAA systems be certified within a defined process framework; and (*iii*) SAA system certification and airworthiness certification be separate certifications using similar processes (see Fig. 4). The instruction also established the requirement for program-specific certification plans.

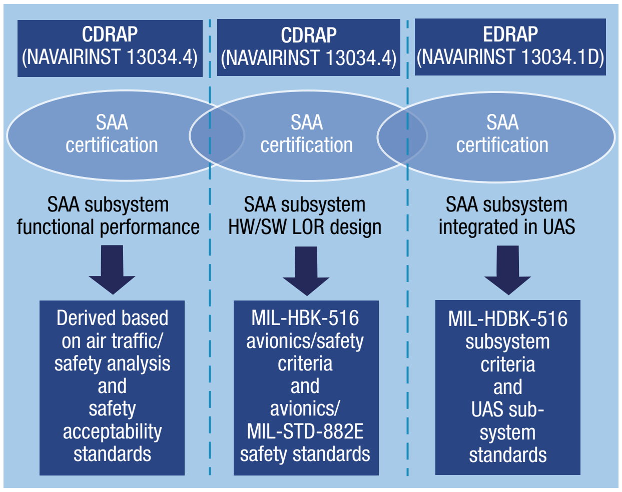

CDRAP
(NAVAIRINST 13034.4)
CDRAP
(NAVAIRINST 13034.4)
EDRAP
(NAVAIRINST 13034.1D)
SAA
certification
SAA
certification
SAA
certification
SAA subsystem
functional performance
SAA subsystem
HW/SW LOR design
SAA subsystem
integrated in UAS
Derived based on air traffic/ safety analysis and safety acceptability standards
MIL-HBK-516 avionics/safety criteria and avionics/ MIL-STD-882E safety standards
MIL-HDBK-516 subsystem criteria and UAS sub-system standards

Figure 4. SAA and airworthiness certifications relationship. EDRAP; engineering data requirements agreement plan; HW, hardware; LOR, level of rigor; SW, software.

In keeping with the NAVAIRINST 13034.4 requirement to develop a certification plan, the airspace integration team subsequently developed a framework of activities and processes leading to SAA certification, as shown in Fig. 5. This process ensures a comprehensive and defensible set of safety-related evidence to inform certification decisions.

TRITON CERTIFICATION ENABLERS

DoD Architecture Framework

Triton is one of the first UASs whose capability development document includes a requirement that the system be certified for the airspace in which it will operate. To this end, the goal of the Triton airspace integration integrated architecture is to provide a means for conducting top-down, end-to-end regulatory, safety, and performance requirements decomposition from the operational to the system and subsystem levels. The architecture defines the operational requirements to satisfy the overarching Triton requirement (per the capability development document) to safely integrate into the intended operational environment.

As part of this integrated architecture effort, the team is developing the airspace integration operational architecture (AIOA) applicable to high-altitude, long-endurance and medium-altitude, long-endurance UASs. The focus of the AIOA is to capture and define the operational context for integrating UAS operations into the airspace for the intended operational environment. The AIOA establishes a baseline from which UAS programs may tailor and decompose their airspace operating requirements and further develop systems views and standards views. In addition, it can be leveraged as a reference architecture for similar or overarching activities required by similar high-altitude, long-endurance and medium-altitude, long-endurance programs.

The Triton airspace integration integrated architecture is being developed in accordance with the DoD Architecture Framework (DoDAF), version 2.02. To ensure conformance with the DoDAF Meta Model (DM2), the development environment for the architecture model is the IBM Rational Software Architect model-based systems engineering tool with the UML Profile-Based Integrated Architecture (UPIA) add-on.

In addition to the views outlined in the DoDAF, two fit-for-purpose viewpoints are being developed to meet the objectives of the architecture: the human viewpoint and the hazard analysis viewpoint. Using a tailored version of the data-centric DoDAF six-step process (Fig. 6), the team ensured consistency between all views in the architecture and that all essential data relationships were captured in support of the desired analysis.

Using the Triton UAS Concept of Operations for Worldwide Airspace Access as a starting point, the

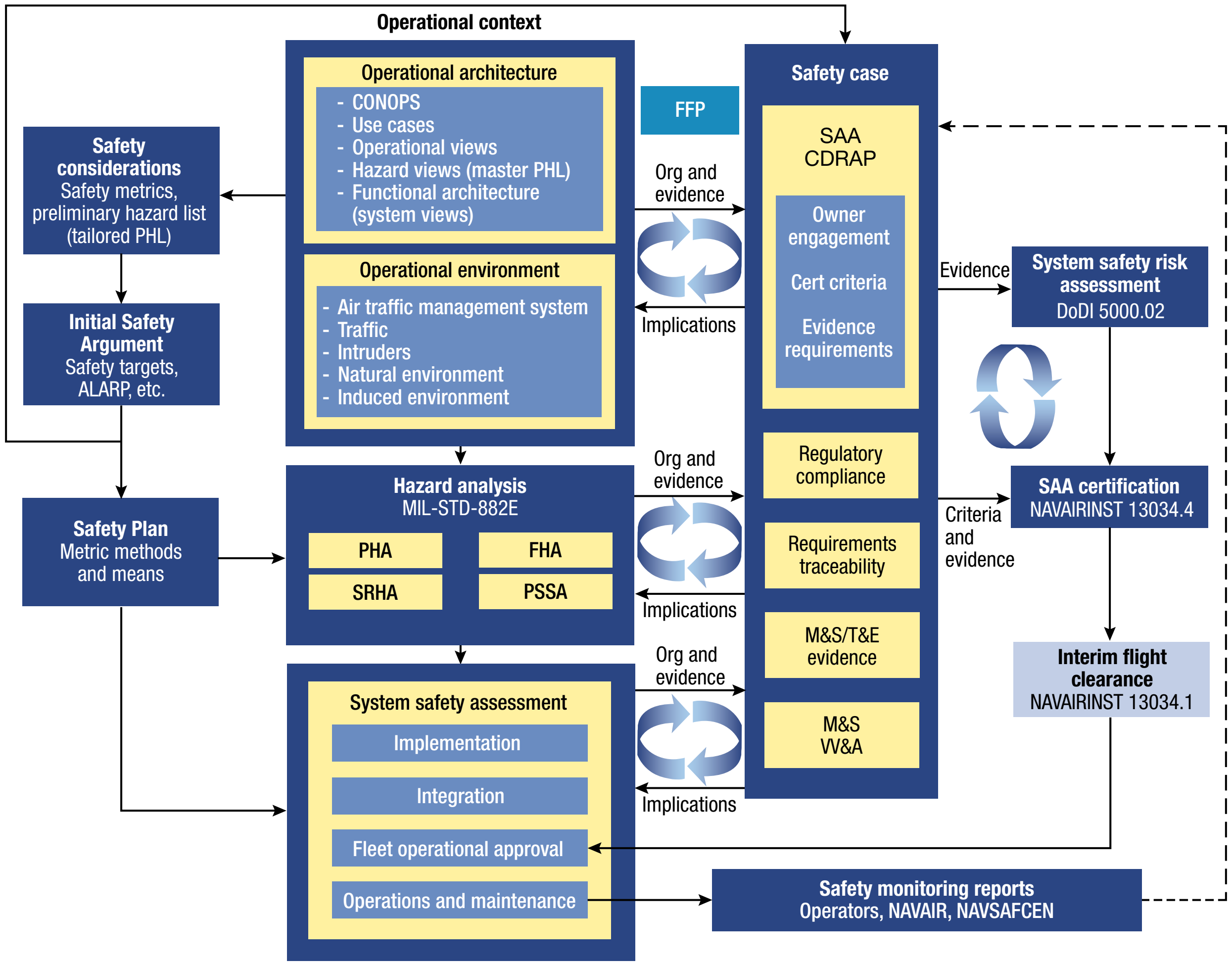


Figure 5. Triton SAA certification process. ALARP, as low as reasonably practicable; CONOPS, concept of operations; DoDI, DoD instruction; FFP, fit for purpose; FHA, functional hazard analysis; NAVSAFCEN, Naval Safety Center; Org, organization; PHA, preliminary hazard analysis; PHL, preliminary hazard list; PSSA, preliminary system safety analysis; SRHA, software requirements hazard analysis; T&E, test and evaluation; VV&A; verification, validation, and accreditation.

Triton airspace integration integrated architecture further decomposes the high-level operational requirements within the context of Triton's mission. Mapping these capability requirements to activities provides the first level of traceability from the activities to the capabilities they support. The architecture also captures the guidance (rules/standards/policies) under which these operational activities must be performed, ensuring regulatory compliance traceability. As the systems views are developed, the model is analyzed to show traceability from the operational level to the system and subsystem levels. This analysis identifies any existing functional gaps, assisting in development of a system that will meet the necessary operational requirements and capabilities.

The addition of the human views allows for the linkage of human-related design considerations to data already captured and represented in the architecture model. The human viewpoint is defined as part of the North Atlantic Treaty Organization (NATO) Architecture Framework and contains eight defined views. Integration of these views is critical to maintaining a comprehensive systems perspective and assists in evaluation of overall system performance.

The integration of the hazard analysis viewpoint into the architecture provides an opportunity

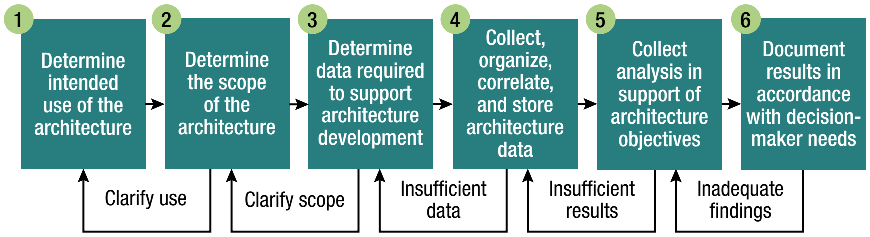

1
Determine intended use of the architecture
2
Determine the scope of the architecture
3
Determine data required to support architecture development
4
Collect, organize, correlate, and store architecture data
5
Collect analysis in support of architecture objectives
6
Document results in accordance with decision-maker needs
Clarify use
Clarify scope
Insufficient data
Insufficient results
Inadequate findings

Figure 6. Tailored DoDAF six-step process.

to assess the critical safety features currently in place and identify existing gaps between a safety event and an unsafe outcome. This viewpoint is based primarily on a barrier risk model, the bowtie hazard analysis methodology, currently used by the Civil Aviation Authority (see http://www.caa.co.uk/Safety-initiatives-and-resources/Working-with-industry/Bowtie/About-Bowtie/Introduction-to-bowtie/). The bowtie is a safety risk management tool that defines the full set of operational hazards that must be mitigated through all phases of flight for safe operations in the intended environment. The top-level bowtie establishes the hazardous condition and event for airspace integration collision risk. The analysis of the operational hazards within the bowtie identifies consequences if the controls fail or are not implemented, threats causing the hazardous event that require controls, and top-level controls for those threats. The identified controls are then traced to functions in the architecture, allowing for the derivation of system-specific requirements based on the functional decomposition addressing both lower-level threats and controls.

By capturing and integrating information from operational, system, human, and hazard/safety perspectives, the Triton airspace integration architecture model enables system safety practitioners to conduct an early operational safety assessment and establish high-level safety requirements to be addressed in system development.

Airspace Integration Safety Risk Assessment

Classic manned aviation safety concerns itself with the safety risk to passengers and crew, other operators, and persons and materiel on the ground. For Triton's initial operations in international airspace, there is little risk to persons and materiel at sea. Triton carries no passengers or crew; therefore, the principal safety risk when integrated into the airspace is from collisions with other aircraft, specifically other traffic in international airspace. This risk is quantified as collision risk, although other operational risks can use a similar methodology. Estimation of collision risk includes the reduction of risk from both strategic rules and constraints and by the tactical capability provided by the onboard SAA system. By evaluating these two coupled capabilities together with airworthiness considerations, an overall estimate of collision risk can be derived.

Triton's primary method for quantifying collision risk is a probabilistic risk assessment (PRA). The PRA consists of a binary graph, referred to as an event sequence diagram, which defines a process of binary events and describes those key events and occurrences that either happen or fail to happen. They in turn lead to a final end state or condition called an outcome. Event sequence diagrams include only those events relevant to the system of interest and that lead to other end states of concern. Nodes in the binary graph are formulated as events that occur or not (yes/no) and have associated probabilities for the event occurring. End states are calculated by treating all events independently, finding the path from an initiating event to the end state, multiplying together all event probabilities in the path, and then summing the end-state values. Note that the tree calculates a probability that, when summed over all of the end states, totals 1. Nodes include the unmitigated collision risk expressed as a probability per flight hour, hazardous events (including failure conditions and operator actions), and the risk reduction from tactical SAA system performance. Tactical system performance is evaluated using Monte Carlo analysis (a method for exploring the sensitivity of a complex system by varying parameters within statistical constraints), which leads to a determination of the fraction of encounters successfully mitigated. These results are conditionally dependent and so apply to different event node chains, analogous to cut sets used in fault tree analysis.

Airspace Analysis

Analysis of the Triton operational airspace (offshore and oceanic airspace) provides (*i*) air traffic data to determine the native, unmitigated, probability of collision in all types of airspace in which the unmanned aircraft might fly; and (*ii*) 4-D routes and flight profiles through that airspace to ensure that defined safety thresholds are satisfied. The first provision of airspace analysis yields an unmitigated collision risk (UCR) with other aircraft, while the second provides a UCR given how Triton will fly in that airspace (i.e., with strategic rules applied). The factors that affect the overall UCR for a given volume of airspace are shown in Fig. 7.

The UCR calculations, as shown in Fig. 7, are assessed over volumes of airspace with similar characteristics and, hence, similar risk. A risk volume is a volume of airspace in which other aircraft's flight trajectories, as influenced by such things as airspace structures, operating rules, and geographical or environmental factors, are largely consistent throughout its volume. Using the risk volume concept allows estimation of encounter risk in a volume of airspace, versus along a single, fixed, repeated path. This allows assessment using not only "occupancy" or density but also behavior as captured by the other aircraft's trajectories within that risk volume. The final factor affecting collision risk for a risk volume is how the unmanned aircraft will operate within it—that is, Triton's expected flight profile through that risk volume or type of airspace.

This analytical approach requires sufficient geospatial and temporal granularity so that locally high and unacceptable UCRs will not be masked by the averaging that occurs over longer time frames or wider nonhomogenous geographical areas. A typical unmanned aircraft

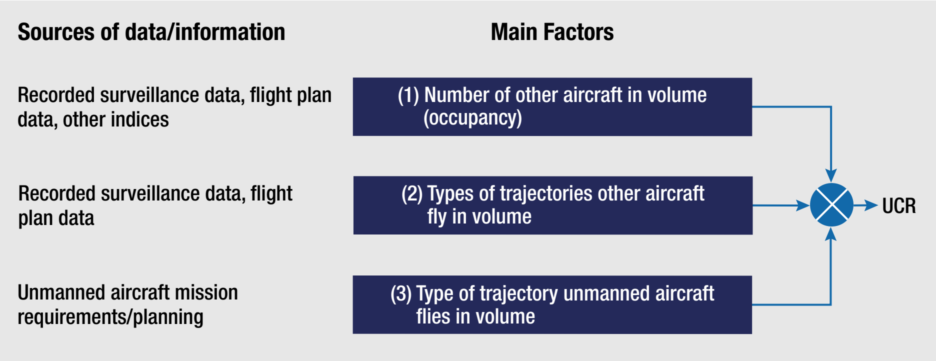

Sources of data/information
Main Factors
Recorded surveillance data, flight plan data, other indices
(1) Number of other aircraft in volume (occupancy)
Recorded surveillance data, flight plan data
(2) Types of trajectories other aircraft fly in volume
Unmanned aircraft mission requirements/planning
(3) Type of trajectory unmanned aircraft flies in volume
UCR

Figure 7. Main factors influencing the UCR.

profile, for example, might transit a variety of types of airspace with varying levels of occupancy by other aircraft. Having sufficient resolution in the results highlights how the UCR varies over the course of a mission.

The risk volume is discretized into calculation units where other aircraft are observed. These discrete calculation volumes provide the environment for a Monte Carlo calculation of collision probability when Triton is virtually flown through them. Statistics on collisions and other proximity hazard conditions are accumulated in the analysis. Discretizing the airspace also allows a granular view into the risk volume. This view highlights how Triton behavior affects the collision risk—for example, altitudes and routes that yield higher collision rates. This insight is then used to define operational bounds where risk may be too high. It also provides insight into alternative strategies and tactics from which operational best practices can be proposed to reduce UCRs when transiting a given airspace volume. Analysis of the airspace also yields distributions on the types of other aircraft, equipage, their speeds, routes, climbs/descents, etc. These distributions are used in the PRA to map risk volume-dependent UCR values to corresponding SAA system performance measures.

Safety Case

Motivation and Overview

NAVAIR will provide the approval for Triton to operate in its intended environments, and NAVAIR will also certify the SAA subsystem for installation on Triton to support the due regard capability. To achieve these approvals, the Triton program must both build the Triton system to meet its performance goals under safety and regulatory constraints and also show the certification authority that these goals and constraints are comprehensively understood and satisfied.

The engineering life cycle drives the Triton build. Like any system, Triton must progress through a process of requirements development, design, implementation, and test in order come into existence. The novelty and safety criticality of Triton make this process particularly complex, but it is still an engineering life cycle. The demonstration requirement, however, is not fully addressed by existing frameworks of regulation or performance standards. Absent community-agreed standards for SAA, or certification and approval processes for Navy UASs intended for due regard missions, NAVAIR is using a safety case approach to direct the collection, organization, analysis, and presentation of the Triton SAA certification rationale to the certification authority. The Triton airspace integration operational safety case supports the identification of SAA certification criteria through stakeholder-modulated decomposition of certification claims. It then integrates those decomposed claims with supporting evidence and situating context into a compelling argument that Triton will safely operate in its intended environments.

Definition and Basic Organization

Definitions of safety cases vary through the research and practice community, although all concern the identification, analysis, and evidence-based support of system properties through a traceable chain of reasoning. NAVAIRINST 13034.4,[7] the SAA certification instruction applicable to this effort, defines a safety case as:

> The process by which a formally documented body of evidence is created that provides a convincing and valid argument that a system is safe for a given application in a given environment. The safety case documents the safety requirements for a system, provides evidence that the requirements have been met, and documents the argument linking the evidence to the requirements. Elements of the safety case include safety claims, evidence, arguments, and inferences.

The linking argument, or traceable chain of reasoning, arises from the decomposition of top-level safety claims to sub-claims, to the level that sub-claims can be supported directly by evidence. This results in a tree structure terminating in evidence items supporting sub-claims. If the evidence is valid and complete, and the claim decomposition sound, then the top-level claim is supported.

The certification authority is the ultimate arbiter of these evaluations, but the safety case development process leads stakeholders to decisions regarding system design and development as well as the demonstration strategy. Through this process, the development of the safety case supports definition of certification criteria where none existed previously, as the claims and the evidence items required to satisfy them are identified and refined. Analogous to an airworthiness certification based in MIL-HDBK-516,[8] TAEs discover, negotiate, and stabilize the criteria and the required evidence items, versus choosing those applicable to the instance from the set provided in the handbook. The criteria and the evidence items later populate the data elements list portion of the certification data requirements agreement plan (CDRAP), as the related entities do for an engineering data requirements agreement plan supporting and airworthiness certification.

As the safety case matures, it documents the end-to-end rationale for asserting the certification claim, integrating the claims decomposition, evidence, and all engineering and regulatory inputs over which the argument is made.

Safety Case Implementation for Triton

The safety case for the Triton acquisition effort focuses on operation using the due regard capability and on the SAA subsystem supporting that capability. It has a two-part structure including a Triton operational case, at the system level, and a nested SAA certification case dedicated to NAVAIRINST 13034.4 requirements and simultaneously supporting the Triton operational case. This modular architecture allows the appropriate sorting of system- and subsystem-level concerns, and it makes clear the boundaries of material supporting Triton operational approval versus SAA certification. It also allows for the possibility of upgrade to the SAA subsystem capability in the future (for example, to enable greater autonomy) while minimizing the scope of change required for the overall Triton safety case. Further, the nested SAA case is being designed for reuse potential for future non-Triton acquisitions. Finally, the design leverages the likely environmental and regulatory commonalities between Triton and later Navy UAS acquisitions to organize the higher-level system operational case for reuse potential.

The Triton safety case manages complexity and information flows through the definition of a series of interfaces with other Triton airspace integration sub-efforts. Examples include the following:

- The SAA certification process, with its requirements for CDRAP and data elements list entities as key inputs to the safety case, and populated versions, along with a final report, as key outputs
- The operational architecture development, with operational scenario definitions and core safety requirements as key inputs to the safety case, and implications for supportability as outputs
- The evidence generation process, including M&S, test and evaluation (T&E), and analysis, with evidence requirements as outputs from the safety case and evidence items as input from the respective sources

The safety case development also coordinates with the airspace characterization and system safety assessment efforts to align specifications for environmental context and to receive evidence and contextual inputs concerning risk measurement, respectively. All of these interfaces facilitate continual information sharing over the parallel developments such that the mutual feedback can be used in the refinement of the product associated with each effort.

The safety case is being developed in accordance with a systematic process of staged maturity gates that engage key stakeholders in the identification, decomposition, and validation of claims and evidence requirements, as well as the audit and approval of produced evidence and integrated argument. Safety case partitions are associated with owner teams of TAEs and subject-matter experts by competency, and each partition must be signed off by the TAE owner to progress to the next stage of development. All issues by stage are tracked and worked to resolution as a condition of sign-off. The detailed basis for progression at each stage is documented.

The safety case is delivered internally in periodic incremental releases as a standalone interactive electronic artifact navigable within standard modern hypertext browsers. The completed safety case will include a final report to the certification authority summarizing the scope, strategy, content, and implications from the arguments, as well as documentation of the owner approval chain and bases leading to the certification submission. Together, these artifacts tell the integrated story to the certification authority, demonstrating the proposition of safe operation given the system definition, the environment definition, the decomposition through sub-claims, and support of the sub-claims by evidence.

TRITON M&S INFRASTRUCTURE

The previous sections describe the activities and resulting artifacts needed for Triton to obtain certification for due regard operations. All of these activities are enabled by M&S tools of various types. However, since the systems that implement each layer of Triton's defensive strategy are tightly integrated into a cohesive and unified system of systems, the M&S tools must themselves be integrated into an M&S system that faithfully replicates the airspace integration capabilities that Triton provides. This implies not only a rigorous definition of the tool interfaces but also an overarching process through which the developers and users of these tools implement a defined set of roles and responsibilities, including required interactions with other stakeholders.

The M&S strategy for Triton safety case evidence production is captured in the Triton Evidence Generation Management Plan.[9] The plan heavily leverages the IEEE 1730[10] standard as the process framework into which the set of lower-level tasks needed to develop

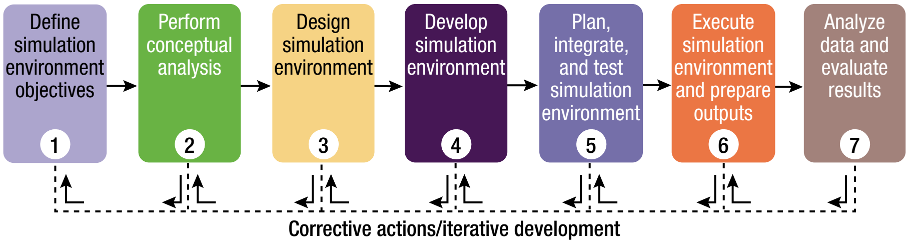

Define simulation environment objectives
1
Perform conceptual analysis
2
Design simulation environment
3
Develop simulation environment
4
Plan, integrate, and test simulation environment
5
Execute simulation environment and prepare outputs
6
Analyze data and evaluate results
7
Corrective actions/iterative development

Figure 8. IEEE 1730 (high-level view).

and employ the Triton airspace integration M&S infrastructure are mapped. This mapping ensures that (*i*) the full set of required subtasks (e.g., requirements development, scenario development, integration testing) are identified and properly planned for early in the overall process; (*ii*) all tasks and subtasks are allocated to appropriate owners with associated execution responsibility; (*iii*) interfaces among dependent tasks and subtasks are fully defined; and (*iv*) products are produced at each step of the process that satisfy documentation requirements and/or provide needed inputs to subsequent tasks. A high-level view of the IEEE 1730 process framework is provided in Fig. 8.

The M&S architecture for Triton airspace integration analysis is shown in Fig. 9. The system inputs in the box in the upper left corner collectively define the partitioning of system/airspace requirements into analysis objectives and the M&S capabilities needed to support the associated studies. This information is combined with the data inputs in the lower left corner to define the spe-

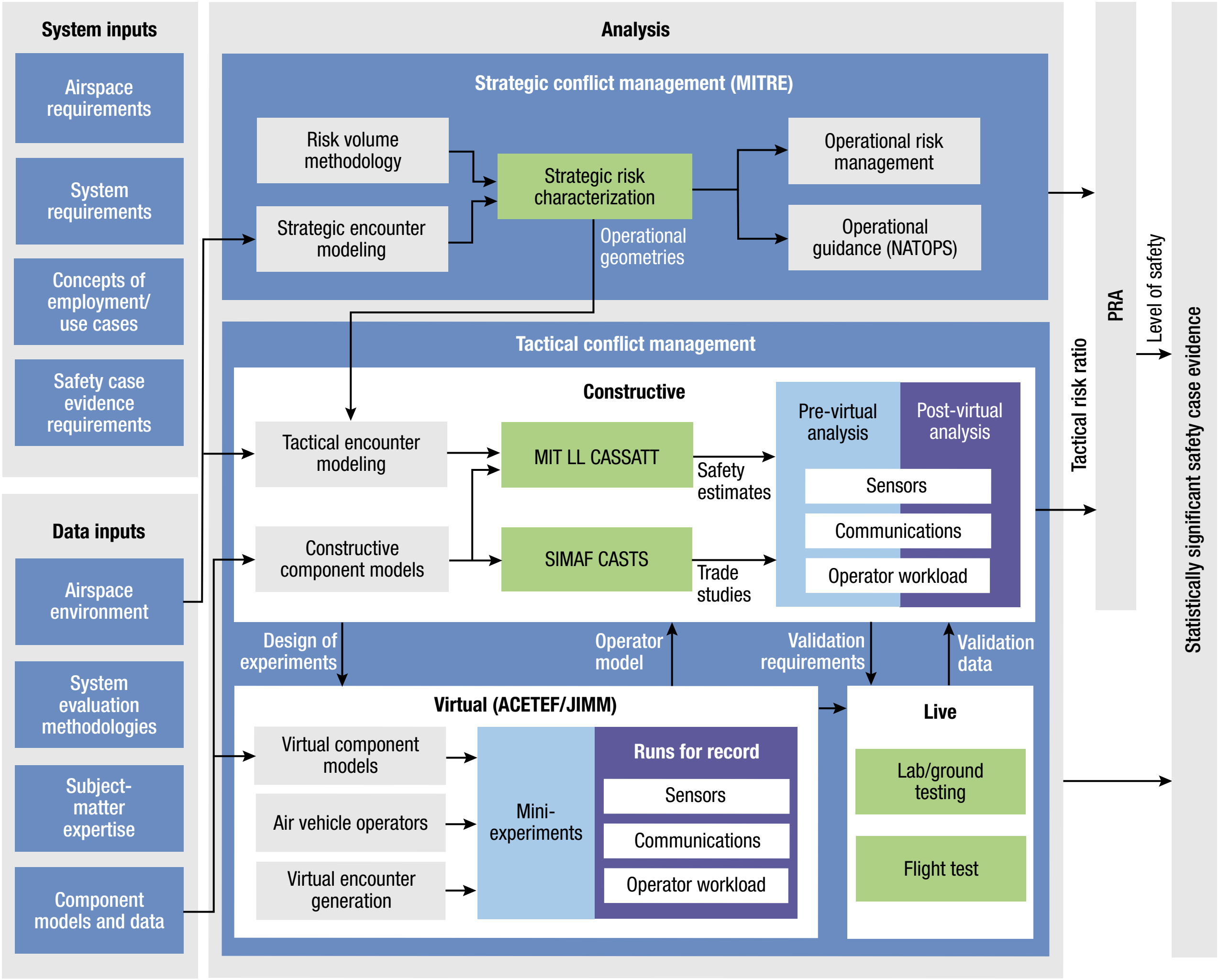


Figure 9. Triton M&S architecture for airspace integration analysis. ACETEF/JIMM, Air Combat Environment Test and Evaluation Facility/ Joint Integrated Mission Model; MIT LL CASSATT, MIT Lincoln Laboratory Collision Avoidance System Safety Assessment Tool; NATOPS, Naval Air Training and Operating Procedures Standardization; SIMAF CASTS, Simulation and Analysis Facility Collision Avoidance Sensor Trade Simulation.

cific configuration of M&S tools needed to support the study requirements along with the authoritative sources of data and supporting components (e.g., subsystem models, loggers, viewers) needed to fully implement that configuration. A subset of these data (airspace environment) is then used to develop a characterization of strategic risk (i.e., level of collision risk in different areas of the airspace). The operational geometries from this risk assessment provide an additional input to a constructive M&S-based assessment of the effectiveness of the onboard SAA sensors in maintaining desired separation distances and avoiding near midair collisions. The key M&S tools used in this assessment include the following:

- **Due Regard Encounter Model:** Describes the types of encounter situations that occur when operating due regard in an oceanic airspace for input to SAA system simulation evaluation. The model generates random aircraft trajectories that are statistically similar to those observed in the airspace.
- **Collision Avoidance System Safety Assessment Tool:** Performs faster-than-real-time (fast-time) analysis of aircraft encounters. Implemented in MATLAB/Simulink, this tool leverages aircraft positional information predicted by the Due Regard Encounter Model and simulates aircraft encounters over a period of up to 10 min near the closest point of approach.
- **Collision Avoidance Sensor Trade Simulation:** This model evaluates sensor requirements for reliably and safely conducting UAS missions in various operational environments. Intended for rapid evaluation of very large trade spaces, the model comprises modules operating within the OpenEaagles framework (Open Extensible Architecture for the Analysis and Generation of Linked Simulations).

The results of the constructive M&S assessment, along with the strategic risk characterization, provide critical inputs to the PRA as described earlier. However, the constructive M&S assessment is also a valuable source of design of experiments data for human-in-the-loop virtual M&S exploration of encounter geometries that are particularly difficult to resolve. The main components of the virtual M&S infrastructure include the following:

- **Joint Integrated Mission Model:** The main synthetic environment generator for Triton airspace integration virtual analysis, this model provides an ability to immerse external resources (e.g., hardware, software, other models, and people) in a simulated mission environment. The model is highly flexible and general-purpose in nature, allowing scenario developers to create large numbers of disparate simulation entities with tailored and varying characteristics.
- **High-Fidelity Virtual Models:** The Triton aerodynamic representation is a six-degree-of-freedom model derived from the Northrop Grumman Corporation Triton closed-loop simulator. The traffic collision avoidance system and automatic dependent surveillance-broadcast models are based on the designs of existing high-fidelity models developed by external organizations (e.g., NASA). The mission control system emulator provides air vehicle operators with the actual displays and symbology that they would see in actual Triton operations.

The human-in-the-loop experiments also provide the instrumented air vehicle operator behavior and performance data needed to build a high-fidelity constructive representation of the human operator. This operator model is used in subsequent constructive M&S analysis to produce the statistically significant evidence needed to substantiate claims in the Triton safety case.

Because the consequences of M&S error are relatively severe for airspace integration analysis, an extensive verification, validation, and accreditation process overlays the Triton IEEE 1730 implementation. As stated earlier, the Triton safety case evidence requirements are partitioned into studies. Each phase (pre-virtual constructive, virtual, post-virtual constructive) of every study introduces a new intended use for the M&S infrastructure. Each intended use requires an accreditation plan to map M&S requirements to test acceptability criteria and to identify M&S risk areas. A verification and validation (V&V) plan is then developed to specify which tests of the M&S infrastructure will be performed and how data from the testing will address the risks and satisfy the acceptability criteria. After execution of the V&V testing is complete, a V&V report is produced to summarize test results and compare them to the acceptability criteria. Finally, an accreditation report is produced to update the risk assessment and provide a final accreditation recommendation. TAEs from the Triton program then review the V&V test results and accreditation recommendations and determine whether M&S execution for that study can begin. New iterations of this process may be necessary depending on TAE feedback.

TRITON STATUS

The airspace integration team, working in coordination with federally funded research and development centers, university-affiliated research centers, Northrop Grumman Corporation, and NAVAIR TAEs, continues to conduct safety analysis and requirements validation of key SAA elements, including the SAA radar (SAAR), collision avoidance algorithms, and human–computer interfaces. The MQ-4C Triton SAA certification plan is expected to be approved and signed out by the NAVAIR technical authority in the fourth quarter of 2016. The SAAR is in the final stages of development and will enter flight test in 2017. To maximize confidence that the Triton SAA system will be interoperable with future civil standards, the program is pursuing the option to leverage elements of the Airborne Collision Avoidance System Xu system, currently in development by the FAA and industry stakeholders.[11] In addition, the Triton airspace integration team participates in Radio Technical Commission for Aeronautics SC-228 and SC-147 meetings, during which civil SAA standards are being developed.

NEXT STEPS

The SAA system is moving into a critical phase as development of the SAAR is completed and the system enters into test and evaluation. The team is developing test plans to conduct surrogate flight tests on a NASA HU-25 in the early 2017 time frame, with follow-on tests on Triton. A second surrogate test may take place in the 2019 time frame to test the Airborne Collision Avoidance System Xu with the SAAR. The Triton airspace integration concept of operations and architecture is expected to be mostly complete in the early 2017 time frame, with plans to leverage the foundational elements of this architecture to establish a similar architecture for the portfolio of NAVAIR PEO(U&W) (Program Executive Officer, Unmanned Aviation and Strike Weapons) UAS programs. In so doing, the U.S. Navy will have a more complete picture of the policies, capabilities, and resources needed to integrate the range of UAS types into the airspace. Likewise, the majority of the MITRE Center for Advanced Aviation System Development air traffic analysis is expected to be completed in 2017, which will provide the necessary information to assess Triton's expected level of safety with and without SAA capability. This analysis will inform limitations, procedures, and operational risk management tools necessary to maintain safe operations of other aircraft across the range of expected operations.

SUMMARY

The MQ-4C Triton program is a pathfinder for the policy, technology, processes, and procedures leading to certification of a critical UAS capability necessary to fully integrate UASs into the airspace. From the extensive air-traffic analysis to the airspace integration DoDAF architecture, M&S infrastructure, SAAR development, safety case, and SAA certification policy and procedures, the Triton program will provide a solid foundation for other programs going forward, mitigating unnecessary duplication of effort. When fielded, the SAA capability will provide a significant enabling capability for Triton through increased access to airspace and resultant mission effectiveness.

ACKNOWLEDGMENTS: Many individuals are responsible for the success of the Triton airspace integration effort—too many to list here. However, the authors especially thank Matthew Edwards of MIT Lincoln Laboratory, Jeremy Warren of Booz Allen Hamilton, Thomas Hanrahan and Kevin Warren of Naval Air Warfare Center Aircraft Division, and Dr. Dan Schneider of AMEWAS for their contributions to this article. The authors also thank the leadership of the Navy's PMA-262 office for their sponsorship of the technical activities described in this article.

REFERENCES

[1] *Unmanned Aircraft Systems: Perceptions & Potential*, Aerospace Industries Association, Arlington, VA (2013).

[2] Bledsoe, S., "Army Celebrates 2 Million Hours of Unmanned Aircraft Flight," U.S. Army website, 19 Mar 2014.

[3] *Integration of Civil Unmanned Aircraft Systems (UAS) in the National Airspace System (NAS) Roadmap*, U.S. Department of Transportation Federal Aviation Administration, Washington, DC (2013).

[4] *Unmanned Aircraft Systems*, International Civil Aviation Organization, Montréal, Quebec, Canada (2011).

[5] "MQ-4C Triton Broad Area Maritime Surveillance (BAMS) UAS, United States of America," *naval-technology.com*, http://www.naval-technology.com/projects/mq-4c-triton-bams-uas-us/ (accessed 3 Oct 2016).

[6] Schneider, D., Edwards, M., Gould, N., Graeff, R., Lutz, R., and Hanrahan, T., "Advanced Modeling and Simulation Techniques for Evaluating System-of-Systems Performance," in *Proc. Interservice/Industry Training, Simulation, and Education Conf.*, paper 13014 (2013).

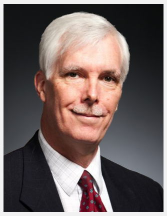
[7] *NAVAIR Instruction: Policy for Certification of Sense and Avoid Systems for Employment with Unmanned Aircraft Systems*, NAVAIRINST 13034.4, Department of the Navy, Patuxent River, MD (2014).

[8] *Department of Defense Handbook: Airworthiness Certification Criteria*, MIL-HDBK-516, Department of Defense, Washington, DC (2002).

[9] "Triton Unmanned Aircraft System Airspace Integration Safety Case Evidence Generation Management Plan," Version 1.1 (2014).

[10] *IEEE Recommended Practice for Distributed Simulation Engineering and Execution Process (DSEEP)*, IEEE Standard 1730-2010, IEEE Standards Association, Piscataway, NJ (2011).

[11] "Airborne Collision Avoidance System XU Concept and Flight Test Summary," Briefing to Royal Aeronautical Society DAA Workshop, FAA TCAS Program Office (2015).



Robert R. Lutz, Force Projection Sector, Johns Hopkins University Applied Physics Laboratory, Laurel, MD

Robert Lutz is a member of the Principal Professional Staff and a scientist at APL. His background includes 35 years of practical experience in the development, use, and management of models and simulations across all phases of the DoD systems acquisition process. He currently serves as the Navy's MQ-4C (Triton) Program M&S Lead in the airspace integration area. He also serves as the Test Lead for both the Safe Testing of Autonomy in Complex Interactive Environments Project and the Collaborative Operation in Denied Environments Program. In addition, Mr. Lutz serves as the chair of the Simulation Interoperability Standards Organization (SISO) Board of Directors and vice chair of the SISO Executive Committee; serves on the Tutorial Board and Fellows Committee at the Interservice/Industry Training, Simulation, and Education Conference; and is a guest lecturer on various M&S-related topics for the Johns Hopkins University Whiting School of Engineering. His e-mail address is robert.lutz@jhuapl.edu.

Paul S. Frederick, Naval Air Systems Command, Patuxent River, MD

Paul Frederick is a systems engineer for the Naval Air Systems Command. He currently serves as the Navy's MQ-4C Triton Program Systems Engineering Lead for airspace integration. In this role, he is responsible for ensuring that all government and contractor technical activities required in support of the airspace integration safety case are identified, planned, and executed. He is responsible for developing the policy and technical certification requirements for the sense and avoid (SAA) system currently in development by Northrop Grumman Corporation under contract to PMA-262. In addition, he serves as the U.S. Head of Delegation and Co-Chair to the NATO Flight In Non-Segregated Airspace work group. His e-mail address is paul.frederick@navy.mil.

Patricia M. Walsh, Force Projection Sector, Johns Hopkins University Applied Physics Laboratory, Laurel, MD

Patricia Walsh is a Senior Professional Staff member at APL. She graduated from the United States Military Academy in 1997 and served for 5 years as an engineer officer in the U.S. Army. Mrs. Walsh received her enterprise architecture certification from Carnegie Mellon in 2006. She has over 18 years of professional experience, including 12 years of practical experience in the development, analysis, and maintenance of DoDAF architecture models in support of all phases of the DoD systems acquisition process. She currently serves as the Lead Operational Architect for the Navy's airspace integration area, with a current focus on the Triton UAS. Her e-mail address is patricia.walsh@jhuapl.edu.

Kimberly S. Wasson, Dependable Computing, LLC, Charlottesville, VA

Kimberly S. Wasson is a principal scientist at Dependable Computing, LLC. She completed her Ph.D. in computer science at the University of Virginia in 2006, with a focus on safety-critical requirements engineering. She subsequently joined the research staff there, investigating safety assurance and certification of such systems, on applications ranging from aircraft to medical devices, and with collaborators including FDA and NASA. She has particular interest in the topics of conceptual modeling and organizational dynamics as they relate to complex system-of-systems safety assurance. Dr. Wasson joined Dependable Computing in 2010 and currently serves as the Safety Case Lead for the Navy's Triton airspace integration effort. She has delivered invited presentations at NASA and the National Institute of Aerospace, and her publications include a Best Paper Award at the International System Safety Conference. Her e-mail address is kim.wasson@dependablecomputing.com.

Norman L. Fenlason, Center for Advanced Aviation System Development, MITRE Corporation, McLean, VA

Norman Fenlason is a senior lead multidisciplinary engineer with the Center for Advanced Aviation System Development at the MITRE Corporation. He holds an M.S. and a B.S. in aeronautical engineering from the Air Force Institute of Technology and the University of Texas at Austin, respectively. Mr. Fenlason served as an aircraft analyst for the United States Air Force and principal systems engineer in industry and for the government for 30 years. He has been leading the PMA-262 Triton UAS sense and avoid safety assessment for the past 6 years. His e-mail address is nfenlason@mitre.org.