APPENDIX B: Aviation Safety Program

B.1 Program Overview

The current U.S. air transportation system is widely recognized as among the safest in the world. Over the past ten years, the commercial accident rate has continued to drop, a credit to industry and government working together to solve problems and proactively identify new risks. However, the demand for air traffic is expected to continue to increase substantially in the next 15 to 20 years, and while NextGen will meet this demand by making passage through the increasingly crowded skies efficient and speedy, it will come with increased reliance on automation and increased operating complexity. Therefore, the vigilance of the aviation community must continue in order for the U.S. to meet the public expectations for safety in this complex, dynamic domain.

To meet the challenge, the Aviation Safety Program (AvSP) develops cutting-edge technologies to improve the intrinsic safety of current and future aircraft that will operate in NextGen. AvSP's contributions range from providing fundamental research and technologies on known or emerging safety concerns, to identifying emerging issues and to working with partners in developing new capabilities for NextGen. AvSP transfers knowledge and technology to the aviation community for both hardware and software systems.

The objectives of the AvSP are to proactively identify, research, develop, and mature tools, methods, and technologies for improving overall safety of new and legacy vehicles and systems operating in NextGen. The resulting capabilities will enable design solutions and operating concepts for present and future vehicles and systems.

The AvSP increases capabilities to predict and prevent safety issues by developing technologies to monitor for safety issues and minimize them should they occur; designing safety issues out of complex systems and system behaviors; and analyzing designs and operational data for potential hazards.

For more information, see http://www.aeronautics.nasa.gov/programs_avsafe.htm

B.2 System-Wide Safety Assurance Technologies Project (SSAT)

Amended July 30, 2013. This Amendment delays the proposal due date for Appendix B.2, System-Wide Safety Assurance Technologies Project, to allow proposers to respond to a change in Subtopic (6) extending the duration of awards from 2 years to 3 years. Proposals are now due September 5, 2013.

B.2.1 Project Overview

Public benefits derived from continued growth in the transport of passengers and cargo are dependent on the improvement of the intrinsic safety attributes of current and future air vehicles that will operate in the Next Generation Air Transportation System (NextGen). The System-Wide Safety and Assurance Technologies Project (SSAT) project will identify risks and provide knowledge required to safely manage increasing complexity in the design and operation of vehicles and the air transportation systems, including advanced approaches to enable improved and cost-effective verification and validation of flight-critical systems. SSAT is focused on methods to assess and ensure system-wide safety of complex aviation systems. The project will emphasize proactive methods and technologies, and utilize a systems analysis approach to identify key issues and maintain a portfolio of research leading to potential solutions. A proactive approach to managing system safety requires (1) the ability to monitor the system continuously and to extract and fuse information from diverse data sources to identify emergent anomalous behaviors after new technologies, procedures, and training are introduced; and (2) the ability to reliably predict probabilities of the occurrence of hazardous events and of their safety risks.

The goal of the System-Wide Safety and Assurance Technologies (SSAT) project is to develop validated multidisciplinary tools and techniques to ensure system safety in NextGen and enable proactive management of safety risk through predictive methods. The project consists of four key technical challenges: Assurance of Flight Critical Systems, Discovery of Safety Incidents, Automation Design Tools, and Prognostic Algorithm Design for Safety Assurance. Each of these areas supports the project goal and its focus on ensuring system safety and developing proactive technologies to enable a successful transition to NextGen. Each technical challenge is designed to address key issues related to NextGen.

The SSAT technical challenges were identified based on a number of key criteria, including the priorities defined in the National Aeronautics Research and Development Plan, the National Research Council (NRC) Decadal Survey of Civil Aeronautics, and the Joint Program and Development Office (JPDO) Integrated Work Plan. The NASA Aviation Safety program also conducted a Systems Analysis study, published in 2010, that gives a prioritization of key challenges facing the aviation safety community. The report identifies the types of accidents with the greatest impact to overall safety risk in US civil aviation. The report also presents an analysis of the Future Safety Risk---so-called "Tall Poles" in Aviation Safety. The Technical Challenges in the SSAT Project directly address the following key Future Safety Risks:

1. Loss of Control – In Flight
2. Approach and Landing Accident Reduction
3. Human Fatigue
4. Increasing Complexity and Reliance on Automation
5. Inadequate Protection, Analysis, and Dissemination of Safety Data

Research on each of these technical challenges delivers results to key stake holders including the Federal Aviation Administration (FAA), JPDO, Airline Carriers, the Aeronautics industry, and the General Aviation Community. These technical challenges also fully support the goal of the SSAT project.

1. Assurance of Flight Critical Systems: This technical challenge involves research in verification and validation for flight critical systems in support of system-wide safety in NextGen.

2. Discovery of Precursors to Safety Incidents: This technical challenge focuses on the development of advanced tools and techniques to discover precursors to aviation safety incidents in NextGen.

3. Assuring Safe Human-Systems Integration: This technical challenge focuses on the development of robust human-automation systems by incorporating known limits of human performance in support of NextGen.

4. Prognostic Algorithm Design for Safety Assurance: This technical challenge focuses on the development of advanced tools and techniques to estimate the remaining useful life of a complex system and make decisions under uncertainties that are related to faults and failures.

B.2.2 Description of Solicited Research

The goal of the Assurance of Flight-Critical Systems (AFCS) technical challenge is to develop multidisciplinary verification and validation tools and techniques that advance safety assurance and certification of complex, networked, distributed flight critical systems. Here flight critical systems are defined to be any system that directly controls the safe conduct of an aircraft's flight. This includes air and ground systems, concepts of operation as well as technology, and recognizes that human performance is a key factor in flight-critical systems and must be accounted for.

The increasing complexity of flight critical systems proposed for the NextGen will require new paradigms and real-time distributed system infrastructures providing high levels of confidence and safety assurances. The cost of proving a flight-critical system is safe is often expected to far surpass the costs for other aspects of design and implementation.

Research is solicited on new verification and validation (V&V) concepts for advancing safety assurance methods for flight critical systems over their life cycle to foster innovation within the NextGen air transportation system. The AFCS technical challenge focuses on five research areas: (1) argument-based safety assurance, (2) integrated distributed systems (3) authority and autonomy, (4) software intensive systems and (5) an assessment environment. With this solicitation, NASA is seeking proposals that address challenges in three of the five research areas by:

- Documenting safety assurance challenges and potential safety issues introduced by technological advances within the National Airspace System (NAS),
- Developing new V&V methods for predicting, assuring and proving the safety levels demanded of future air transportation systems,
- Developing new V&V methods to enable rigorous analysis of functionally integrated distributed systems, and
- Developing new software V&V technologies that help automate current techniques and apply V&V techniques earlier in the development process.

Approximately $2.5-4.8M of ARMD (Aviation Safety Program) funding investment is anticipated in the first year. The actual number and value of the first year awards will depend on the quality and content of the proposals received with 8-11 awards anticipated.

(1) Subtopic Number: AFCS – 1.1

(1.1) Subtopic Name: Software Intensive Systems: Verification and Validation of Model-based and Adaptive Systems

(1.2) Description

In the past fifteen years, there have been many advances in research on autonomy and model-based control. They often result in a generation of flight control systems that are very different from traditional control systems. Instead of having control rules embedded in the logic of the software, they rely on the principle that the control logic should be captured in "models" (in a loose sense) separated from the code logic in charge of applying, or executing, commands. Examples of such flight control systems can often be found in Unmanned Aircraft Systems (UAS), especially to implement non-linear control [1,5]. These model-based, or adaptive, control techniques are also being applied to air traffic control and to some vehicle systems such as Airborne Collision Avoidance System-X (ACAS-X), the new generation of collision avoidance systems [2].

Design methods of autonomous and model-based flight control systems are described with different adjectives such as "intelligent" and "adaptive" and rely on a variety of different technical fields such as neural network, machine learning, model-based programming, various Markov processes, and many others. While quite different, these fields share the characteristics that the control logic is not explicitly represented in the code and the behavioral space they cover is larger than traditional control software. These characteristics make these various technical fields hard to verify and validate. When applying testing, the traditional notions of coverage do not apply anymore. The use of formal methods, such as theorem proving or abstract interpretation, is also not obvious since the control logic does not necessarily appear explicitly in the code anymore. The control logic is often captured implicitly in input data, e.g., a table summarizing the results of the resolution of a Markov Decision Process model mapping state estimates with possible collisions for ACAS-X. Therefore the application of static analysis at the code level is not very meaningful. The application of model checking is also problematic since the states visited and stored by the model checker are likely to be very large thus increasing scalability problems. Therefore, the use of formal methods for these model-based, or adaptive, systems needs to be adapted and shown to be practical.

(1.3) Objectives

The objective of this particular topic is to develop advanced techniques (other than just traditional testing) for the V&V of model-based or adaptive systems used in aviation, be it on the ground or on board. NASA is seeking proposals that go beyond existing research for the V&V of model-based, or agent-based, or adaptive systems such as [21, 23, 31, 32], create new approaches, and, characterize how they fit within the current certification process (namely, DO-178-B/C and DO-278-A [24, 25]).

(1.4) Approach

This topic focuses on verification and validation methods for flight critical systems (both ground and airborne) that rely on software techniques such as:

- Model-based control
- Agent-based programming
- Neural networks
- Fuzzy logic
- Machine learning
- Table-driven control based on Markov models

The research proposals should identify what it means to verify and validate such systems, what guarantees can be derived (e.g., functional correctness, control stability, and others), and how the V&V can be performed. Proposals for verification techniques should make an effort to identify to what part of system specifications or requirements they apply and how traceability is provided throughout the verification process. More generally, the proposals should describe how the proposed techniques fit with the current software certification standards (DO-178-B/C and DO-278-A) and suggest how they can be modified to accommodate these new V&V techniques.

The research should be grounded in real systems, i.e., the proposed V&V techniques should be demonstrated on realistic systems, which are, or will be, in use in civil aviation in the next ten years. Demonstration of the research on notional examples is not sufficient. To the contrary, all proposed research plans should include studies of the precision (in terms of false positives and negatives) and the scalability of the approach.

(1.5) Relevant Milestones Supported

The proposed work will partially support completion of SSAT milestone, “Document an approach for creating a safety-case framework for representative adaptive (autonomous) functionality.”

(1.6) Expected Outcome

The expected outcome is new verification and validation methods for flight-critical software-intensive systems, as described in 2.1.3. Proposals that include cutting-edge high-risk investigations are encouraged; however, the balance of risk versus potential gains should be discussed. A high value will be placed on making available open source methods and tools applicable to the objectives of this sub-topic. Outcomes should generally be at a readiness level ranging from that of analytic and experimental studies of proofs of concept through validation in a relevant environment of the specific method developed, although more fundamental research outcomes are acceptable where required by limitations of the current state of the art.

(1.7) Deliverables

Proposals shall identify any and all tangible research products such as all models, methods and procedures, case studies and supporting evidence developed during this effort that shall be delivered. In addition, the award recipients shall deliver the following:

- Documentation of repeatable test and experimental validation capabilities
- Interim Report to NASA as a published report or presentation that contains a description of the specific research topic addressed, a review of relevant literature, and description of research approach, including suggested improvements to research approach as identified in the course of the research to date.
- Final Report, to be published as a NASA CR (Contractor Report), that contains a description of the specific research topic addressed, a review of relevant literature, repeatable description of the research approach, and detailing of the results, methods and tools developed, and insights into V & V approaches.
- A paper suitable for journal submission assessing the research contributions to the objectives of the software-intensive systems research given in (1.3) and identification of relevant open issues
- Written assessment of open issues relevant to the research topic and further research required to address them

(1.8) Duration And Estimated Funding

NASA anticipates awarding a single contract or cooperative research agreement for this topic that address the objectives and specific approaches described in (1.3) and (1.4) The award, in the $350k to $400k per year range, will be made for a three-year proposal. An annual review will be conducted each year. The decision whether to continue at the end of each year will be based on:

- NASA's judgment of the progress made during the year relative to quantifiable metrics defined in the proposal and agreed to by the NASA Technical Monitor at the onset of the agreement.
- NASA's judgment of the impact the findings will have on the goals of the AFCS effort.
- The availability of resources to support the proposed work for the following years.

Proposals shall include a schedule with milestones that support the evaluation of progress and highlight the achievement of goals. Decision points are acceptable as milestones.

(1.9) Potential NASA Resources

NASA will make available the case studies it develops under the AFCS effort. However, proposers should not rely on those and should therefore provide their own case studies. Proposers that make their case studies available, free of charge, to the rest of the AFCS participants (NASA, as well as previous, current, and future awardees) will be given priority.

(2) Subtopic Number: AFCS – 1.2

(2.1) Subtopic Name: Software Intensive Systems: Support for Verification of Black-box Flight Critical Software

(2.2) Description

More and more, design and implementation of software systems used in aviation is contracted out to external companies. For example, the FAA rarely develops its air traffic software systems internally; it usually acquires them from contractors who develop new systems in accordance with the FAA's requirements. The delivered products usually do not include intermediate products (e.g., design models or source code), which would allow the FAA to take advantage of advanced verification techniques (e.g., formal methods or abstract interpretation); it thus leaves black-box testing as the only means of verification. Similarly, most of the aviation industry has shifted from developing software systems entirely in house to integrating sub-systems developed in house with Commercial Off-The-Shelf (COTS) developed by sub-contractors and delivered as black boxes. Again testing, despite its shortcomings, is the only solution left for verifying the entire system.

Many of these systems have first been prototyped in the form of prototyped code or executable design models by the system integrator. For example, many FAA systems have first been prototyped by research centers external to the FAA, such as NASA or MIT Lincoln Labs (e.g., Traffic Collision Avoidance System (TCAS), ACAS-X, or Tactical Separation Assisted Flight Environment (TSAFE)). Even though such early prototypes are usually completely re-coded, they can be used to gain insights into what verification is needed for the system that will be deployed. Design models can also be used for the same purpose. By the same token, prototypes and design models can also be mined to define "V&V-related" requirements so that the final deliverable fits a pre-defined verification strategy. Compositional verification may substantially contribute to this approach.

(2.3) Objectives

The objective of this topic is to develop, demonstrate, and deliver V&V methods and tools that can take advantage of a priori knowledge obtained from early design models or prototype code to elaborate V&V requirements and efficient V&V strategies (taking advantage of formal methods) for software systems assembled from COTS or delivered as black-box software (no visibility into source code or design models). Ease of verification of critical data and scalability should be used as criteria to optimize the strategy.

(2.4) Approach

Compositional verification [10, 11, 12, 13, 14, 15] is anticipated to play a central role in implementing this vision. The learning aspect of compositional verification can be used to derive the verification strategy and its associated architectural requirements. Given that this is accomplished to derive requirements, compositional verification can then be used as the underlying framework for the verification of the final product.

The proposed solution should define and demonstrate a post-delivery verification strategy that can learn from early design models or prototyped code knowing that the implemented code in the final black-box product might be quite different from the prototyped code. To simplify the problem, proposers may assume that both the prototype and the final product follow the same programming paradigm and use the same basic architecture. For example, if a prototype is messy C procedural code, the final product can be assumed to be a clean, modular, C software and not code based on a very different paradigm such as a neural network or a set of constraints with a constraint solving engine.

The information learned should include architectural constraints that can be folded into the requirements given to a sub-contractor. An instance of such architectural constraint requirements can be to impose that the delivered product can be integrated in a modular system architecture, in which interfaces between system components are defined as precise contracts (as in the programming-by-contract paradigm) or assumptions (as in the assume-guarantee framework for compositional verification). It is quite important that the learning identifies both the final verification strategy and the requirements necessary to implement the strategy.

The proposed research should also demonstrate that the final verification strategy, given the imposed architectural requirements, is likely to yield a better coverage of the final software behavior than traditional testing (as mandated in DO-178 B/C) and thus promote safety. Characterizing the scalability of the approach is also very important.

The work should be developed and demonstrated with realistic examples and not notional examples. The research can be demonstrated on air traffic systems (e.g., TCAS, ACAS-X, TSAFE, Terminal TSAFE (TTSAFE)) or modular flight software systems similar to the Integrated Modular Avionic (IMA) platforms used in current generation aircraft.

(2.5) Relevant Milestones Supported

The proposed work will partially support completion of SSAT milestone, "Document a case study on the use of advanced virtual integration technologies in a representative flight-critical system."

(2.6) Expected Outcome

The expected outcome is new verification and validation methods for flight-critical software-intensive systems, as described in 2.2.3. Proposals that include cutting-edge high-risk investigations are encouraged; however, the balance of risk versus potential gains should be discussed. A high value will be placed on making available open source methods and tools applicable to the objectives of this sub-topic. Outcomes should generally be at a readiness level ranging from that of analytic and experimental studies of proofs of concept through validation in a relevant environment of the specific method developed, although more fundamental research outcomes are acceptable where required by limitations of the current state of the art.

(2.7) Deliverables

Proposals shall identify any and all tangible research products such as all models, methods and procedures, case studies and supporting evidence developed during this effort that shall be delivered. In addition, the award recipients shall deliver the following:

- Documentation of repeatable test and experimental validation capabilities
- Interim Report to NASA as a published report or presentation that contains a description of the specific research topic addressed, a review of relevant literature, and description of research approach, including suggested improvements to research approach as identified in the course of the research to date.
- Final Report, to be published as a NASA CR (Contractor Report), that contains a description of the specific research topic addressed, a review of relevant literature,

repeatable description of the research approach, and detailing of the results, methods and tools developed, and insights into V & V approaches.

- A paper suitable for journal submission assessing the research contributions to the objectives of the software-intensive systems research given in (2.3) and identification of relevant open issues
- Written assessment of open issues relevant to the research topic and further research required to address them

(2.8) Duration And Estimated Funding

NASA anticipates awarding a single contract or cooperative research agreement for this topic that address the objectives and specific approaches described in (2.3) and (2.4). The award(s), in the $400k to $500k per year range, will be made for a three-year proposal. An annual review will be conducted each year. The decision whether to continue at the end of each year will be based on:

- NASA's judgment of the progress made during the year relative to quantifiable metrics defined in the proposal and agreed to by the NASA Technical Monitor at the onset of the agreement.
- NASA's judgment of the impact the findings will have on the goals of the AFCS effort.
- The availability of resources to support the proposed work for the following years.

Proposals shall include a schedule with milestones that support the evaluation of progress and highlight the achievement of goals. Decision points are acceptable as milestones.

(2.9) Potential NASA Resources

NASA will make available the case studies it develops under the AFCS effort. However, proposers should not rely on those and should therefore provide their own case studies. Proposers that make their case studies available, free of charge, to the rest of the AFCS participants (NASA, as well as previous, current, and future awardees) will be given priority.

(3) Subtopic Number: AFCS – 1.3

(3.1) Subtopic Name: Software Intensive Systems: Qualification of Formal Methods Tools

(3.2) Description

Formal methods tools are expected to play a larger role in implementing and certifying safety-critical systems over the next decade. Updated certification guidance for civil aviation software was published by Radio Technical Commission for Aeronautics

(RTCA) in January 2012[1]. The long-awaited DO-178C and DO-278A [24, 25] emerged after years of committee work. Four companion supplements were simultaneously published. DO-333 [27], the formal methods supplement, allows applicants to receive certification credit for verification conducted using formal methods. For the first time, avionics developers will have this technology available to help satisfy certification objectives without needing to present special justification for "alternative methods."

As a result, NASA expects formal methods tools to be inserted in the workflows for creating future avionic systems and creating evidence in support of their certification. An important question, therefore, is how to ensure that such tools and their underlying methods are themselves robust enough to be used in the analysis of critical systems? What type of assurance is needed for tools that provide assurance via mathematical analysis? This second-order problem has received little attention. Given that formal methods tools will be used in coming years to support future certifications, the question is no longer academic.

Another supplement to DO-178C and DO-278A was provided to address the topic of tool dependability. DO-330 [26], Software Tool Qualification Considerations, provides guidance for developers and users of software tools for high-consequence domains. DO-330-based qualification of formal methods tools, and more generally, the larger question of formal methods tool dependability, forms a largely unexplored area of study. Given the emergence of DO-333 and its anticipated impact, the qualification of formal methods tools under the companion DO-330 now looms as an important unaddressed topic.

(3.3) Objectives

The goal of this NRA research topic is to investigate the general problem of what sorts of assurances are necessary and appropriate to justify the application of formal methods tools throughout all phases of design in real safety-critical settings. It is a given that standard software engineering practices should be used to achieve high quality tools, just as they are with other products. What this solicitation seeks, however, is insight that looks beyond standard practice to try to identify aspects of formal methods tools that make confidence in their results either easier or harder to ascertain. With such insight in hand, the proposed research should examine how existing and upcoming formal methods tools could be qualified within the DO-330 framework.

(3.4) Approach

The approach to proposed research will include investigating both the general problem of achieving confidence in formal methods tools as well as the more specific problem of how to meet the qualification objectives of a particular framework, namely, RTCA's DO-330. This framework stipulates five Tool Qualification Levels, TQL-1 through TQL-5, in decreasing order of rigor. Given a target TQL, DO-330 lists the objectives that need to be met to earn that level of qualification. In accordance with DO-178C, verification tools

[1] www.rtca.org

need to meet only TQL-4 or TQL-5, the least rigorous levels. If they also participate in code generation for the target system, then they would require a higher TQL.

1. To address the general problem, the investigation should consider theoretical soundness issues for the various classes of formal methods, the impact of design and implementation defects in tool implementations, and the limitations of analyses produced by various formal methods. The study should address all practical sources of errors in the use of these tools, including erroneous analysis outputs, failure to detect flaws in analyzed artifacts (false negatives), user errors in operating a tool or interpreting its output, and interface problems when interacting with other tools or interpreting their data products. Particular emphasis should be placed on trying to identify problems that are either unique to formal methods tools, or are shared with other verification tools but have important distinguishing characteristics.
2. In light of the resulting findings, the study would then proceed to examine how formal methods tools might be qualified under DO-330 using its detailed guidance for tool developers. The study should investigate what aspects of formal methods tools might cause difficulties in meeting the qualification objectives, what types of testing would be most effective in meeting the verification objectives, and what impacts on the tool life cycle could be expected. Focus should be placed on a small number of actual tools or tool classes to help make the study more concrete and useful. For each tool candidate, a sketch should be provided that shows how each required qualification objective is either satisfied already or needs additional work. Where feasible, estimates of the work required would be valuable.
3. Given the results of the first two tasks, consideration should be given to possible mitigation strategies. If the impact of unknown tool flaws can be compensated for using additional analyses, plausible approaches should be proposed. The study should also examine the impact of tool weaknesses and limitations on safety case development. For example, if an analysis tool with a known limitation is used, that information should be an input to a safety case so developers can apply additional analyses as needed to reduce the risk associated with that limitation.

Other approaches that address the general problem of verification tool dependability and its impact on system safety are also invited as a part of this solicitation.

(3.5) Relevant Milestones Supported

The proposed work will partially support completion of two SSAT milestones, “Formal techniques for code level verification of numerical software”, and “Advance safety assurance to enable deployment of NextGen Flight Critical Systems”.

(3.6) Expected Outcome

The expected outcome is a study that identifies qualification considerations for formal methods tools under DO-333 along with possible mitigation strategies if applicable.

(3.7) Deliverables

Proposals shall identify any and all tangible research products such as all models, methods and procedures, case studies and supporting evidence developed during this effort that shall be delivered. In addition, the award recipients shall deliver the following:

- Interim Report(s) to NASA as a published report or presentation that contains a description of the specific research topic addressed, a review of relevant literature, and description of research approach, including suggested improvements to research approach as identified in the course of the research to date.
- Final Report, to be published as a NASA CR (Contractor Report), that contains a description of the specific research topic addressed, a review of relevant literature, and detailing of the results, methods and tools developed, and insights into tool qualification approaches.
- A paper suitable for journal submission assessing the research contributions to the objectives of the software-intensive systems research given in (2.3) and identification of relevant open issues
- Written assessment of open issues relevant to the research topic and further research required to address them

(3.8) Duration And Estimated Funding

NASA anticipates awarding a single contract or cooperative research agreement for this topic that addresses the objectives and specific approaches described in (3.3) and (3.4) The award, in the $500K per year range, will be made for a two-year proposal. An annual review will be conducted each year. The decision whether to continue at the end of each year will be based on:

- NASA's judgment of the progress made during the year relative to quantifiable metrics defined in the proposal and agreed to by the NASA Technical Monitor at the onset of the agreement.
- NASA's judgment of the impact the findings will have on the goals of the AFCS effort.
- The availability of resources to support the proposed work for the second year.

Proposals shall include a schedule with milestones that support the evaluation of progress and highlight the achievement of goals. Decision points are acceptable as milestones.

(3.9) Potential NASA Resources

See section 6, NASA Facilities, below.

(4) Subtopic Number: AFCS-1.4

(4.1) Subtopic Name: Distributed Systems: Onboard Integrated Distributed Systems

(4.2) Description

The ongoing trend of integrating functions across traditional boundaries has resulted in increasingly complex and tightly coupled systems that require new methods for assuring safety at the levels demanded of NextGen. The goal of the Onboard Integrated Distributed Systems research area is to develop assurance methods that meet the challenges of future aircraft systems that must operate safely as an integrated network of distributed systems.

The complexity of interactions and tight coupling brought on by large-scale functional integration and distributed processing can expose a system to many subtle and intricate failure mechanisms with a potential for severe safety-relevant effects. The design and assurance problems are compounded by having multiple vendors supplying different functions that must share resources on the same distributed platform. This necessitates platform-level services that ensure non-interference between functions and provide the means for safe and coordinated interaction with no undesired emergent properties. The integration of different function-level architectures further complicates the safety assurance argument. The predictability and robustness of the integrated system in the face of uncertainty in interactions and health status of components is of major importance in the certifiability of the system.

This research will develop advanced capabilities for the safety assurance of onboard integrated distributed systems, including identifying potential safety issues introduced by technological advances in distributed systems. There is a need to ensure the resilience of the overall system-level functionality in the presence of subsystem perturbations stemming from physical defects or logical systemic impairments. This includes identifying protection mechanisms against unintended interactions through unprotected shared computation or communication resources, or through physical processes. It is also important to identify protection mechanisms against cascading failures across system elements that could potentially affect multiple functions.

(4.3) Objectives

The principal focus is to generate evidence to support defensible and explicit assurance claims concerning safety implications introduced by technological advances in distributed systems. The objective is to provide advanced analysis and test capabilities to effectively evaluate the safety aspects of functionally integrated distributed systems onboard aircraft. For this, NASA is developing a collection of assurance technologies that enable comprehensive and rigorous safety assessments. Successful proposals will add to this collection of design and assurance capabilities as called out in items 1-3 in section 2.4.4.

(4.4) Approach

Functional safety assessments (such as described in SAE ARP 4761 [29]) generate system requirements in terms of functional availability (i.e., probability of loss of function) and integrity (i.e., probability of malfunction). The safety assessment also identifies threats to the operation of the system, both physical (e.g., shrapnel from an engine burst, supply voltage surges, high intensity radiated field, lightning, etc.) and systemic (e.g., functional design errors and unintended interactions). The design problem consists of satisfying the safety requirements for the space of expected threats, and the solution usually takes the form of high-level redundant architectures and corresponding lower design layers developed to meet the design objectives. The overall logical design of an integrated distributed system consists of the top-level functions with a range of criticalities supported by a structure of sub-functions that can be either dedicated or shared. The foundation for safe and dependable system operation is the property of failure independence of physical and logical architectural components achieved through isolation, separation, partitioning, dissimilarity, and error containment. From a robustness perspective, it is desirable for a system to meet its safety properties for a large set of threat scenarios beyond those anticipated or required based on regulation or previous in-service experience.

There is a need for better modeling capabilities to understand and predict both the likelihood and system effects of disturbances and degradations that can adversely affect the safety and behavior of flight critical systems. There is also a need for advanced, reusable assurance capabilities to ensure safe management of both redundancy and shared resources in functionally integrated distributed systems. In addition, the proposed research must identify credible approaches to transition results into practical application.

This topic is interested in proposals that provide substantial advancement through model development and validation in the following areas:

1. Logical and stochastic representations of physical and/or logical failures, disturbances and degradation for integrated distributed systems representative of current and anticipated designs. These models must include consideration of events that have the potential to violate assumptions of failure independence for functions and components. The models should be suitable for the analysis of system response to both expected and rare events. The

suitability of the models may be established by examination of regulation documents, in-service events and existing research literature.

2. Generic, platform-level distributed services (e.g., communication, synchronization, diagnosis, reconfiguration, etc.) for various representative communication topologies. The resilience to physical and/or logical failures, disturbances and degradations should be examined. The models should be suitable for verification of continued service for a bounded number of persistent failures, disturbances and degradations, and for verification of recovery strategies for local and global transient events. The quality and utility of the models may be established through credible demonstrations of system design verification.
3. Functionally integrated distributed systems. The resilience to failures, disturbances and degradations due to physical and systemic defects should be examined. The modeled systems should be representative examples of current and anticipated configurations, including complex systems with a large number of integrated functions of various criticalities. Consideration should be given to systems concurrently supporting combinations of redundant configurations with various degrees of similar and/or dissimilar redundancy, as well as different resource management strategies, including static and dynamic, and synchronous and asynchronous configurations. The models should be suitable for verification of system safety for a bounded number of persistent impairments, and for verification of recovery strategies for local and global transient events. Realistic demonstrations of system verification may be used to assess the usefulness of the models.

(4.5) Relevant Milestones Supported

The proposed work will partially support completion of three SSAT milestones, "Publish design/evaluation guide for safe distributed systems," "Verify and document that design/evaluation guide provides safety assessment," and "Advance safety assurance to enable deployment of NextGen Flight Critical Systems".

(4.6) Expected Outcome

The expected outcome is technologies and mathematical models that enable rigorous, comprehensive analysis of functionally integrated distributed systems interacting through various structures such as communication networks and human-automation and human-human interaction, as described in (4.3).

Proposals that include cutting-edge high-risk investigations are encouraged; however, the balance of risk versus potential gains should be discussed. A high value will be placed on openly available and re-usable models and verification approaches applicable to a broad spectrum of distributed flight-critical systems V&V challenges related to integrated distributed systems. Also of interest are publically available design artifacts illustrating particularly difficult aviation V&V problems suitable for demonstrating and validating novel V&V techniques

(4.7) Deliverables

Proposals shall identify any and all tangible research products such as all models, methods and procedures, case studies and supporting evidence developed during this effort that shall be delivered. In addition, the award recipients shall deliver the following:

- Documentation of repeatable test and experimental validation capabilities
- Interim Report(s) to NASA as a published report or presentation that contains a description of the specific research topic addressed, a review of relevant literature, and description of research approach, including suggested improvements to research approach as identified in the course of the research to date.
- Final Report, to be published as a NASA CR (Contractor Report), that contains a description of the specific research topic addressed, a review of relevant literature, repeatable description of the research approach, and detailing of the results, methods and tools developed, and insights into V & V approaches.
- A paper suitable for journal submission assessing the research contributions to rigorous, comprehensive analysis of functionally integrated distributed systems as described in (4.3) and identification of relevant open issues.
- Written assessment of open issues relevant to the research topic and further research required to address them

(4.8) Duration And Estimated Funding

NASA anticipates awarding two or three contracts or cooperative research agreements for this topic that address the objectives and specific approaches described in (4.3) and (4.4). The awards, in the $250-300K per year range, will be made for a three-year proposal. An annual review will be conducted each year. The decision whether to continue at the end of each year will be based on:

- NASA's judgment of the progress made during the year relative to quantifiable metrics defined in the proposal and agreed to by the NASA Technical Monitor at the onset of the agreement.
- NASA's judgment of the impact the findings will have on the goals of the AFCS effort.
- The availability of resources to support the proposed work for the second and third years.

Proposals shall include a schedule with milestones that support the evaluation of progress and highlight the achievement of goals. Decision points are acceptable as milestones.

(4.9) Potential NASA Resources

See section 6, NASA Facilities, below.

(5) Subtopic Number: AFCS-1.5

(5.1) Subtopic Name**:** Distributed Systems: Distributed Airspace Systems

(5.2) Description

A central goal of NextGen is to improve the efficiency and capacity of our nation's airports and airspace through the strategic use of existing and emerging technologies [4]. NASA envisions that automation will play a vital role in the realization of this goal through a broad range of applications such as automating low-level background activities to free human operators to focus on higher-complexity tasks, providing automated advisories to a human operator to support decision-making, or completely replacing some instances of human decision-making.

In addition to automation, NextGen will require coordination and cooperation between unprecedented numbers of disparate system elements using a wide range of communication protocols. System functions that historically have been provided locally using dedicated resources may be distributed among a network of ground, airborne and space-based resources.

(5.3) Objectives

The introduction of automation and the realization of system functions through distributed, rather than localized, resources are two significant challenges to NextGen safety assurance. Disruptions to distributed system elements that support automated functions must not adversely impact safety under any realizable conditions, and a wide arsenal of approaches will need to be available to provide conclusive evidence towards this end. The objective of the research is to develop initial capabilities to analyze and assess safety of NextGen capabilities from a distributed systems perspective.

(5.4) Approach

In view of this objective, NASA is soliciting research that specifically assesses how credible faults, disturbances, and degradations might impact NextGen automation in a manner that adversely impacts safety. NASA has selected as an initial focus area automated aircraft separation using the existing communication channels defined for NextGen.

NASA is currently researching a variety of automated separation strategies, such as:

Improved ground-based tactical conflict detection provided as advisory to human controller [2] [3].
Autonomous Flight Rules (AFR) integrated with traditional instrument and visual rules [1] [6] [7].

These, as well as other NextGen separation assurance strategies will depend on data provided through a defined set of communication platforms, such as Traffic Information Service-Broadcast (TIS-B), Automatic Dependent Surveillance-Broadcast (ADS-B) (in/out), Global Positioning System (GPS), and Controller–Pilot Data Link Communications (CPDLC) [5]. Accordingly, the approach envisioned for this research is to:

- Develop a comprehensive view of the individual and integrated failure space of NextGen communication technologies that support automated aircraft separation.
- Understand the fault detection and mitigation strategies for these communication technologies.
- Understand the dependencies of various proposed separation strategies on these communication technologies – in particular: dependencies related to safety.
- Identify the mechanisms by which communication disruptions and associated detection and mitigation may adversely affect separation assurance.

Proposals should produce an overarching framework for assessing the adverse impact of communication disruptions on separation assurance. Proposals should also address detailed analysis of one or more communication technologies. It is understood that Year One resource limitations may preclude an extensive assessment of all technologies; however, sufficient analysis should be proposed as part of Year One to demonstrate the efficacy of the proposed assessment framework.

(5.5) Relevant Milestones Supported

The proposed work will partially support completion of three SSAT milestones, “Publish design/evaluation guide for safe distributed systems”, “Verify and document that design/evaluation guide provides safety assessment” and “Advance safety assurance to enable deployment of NextGen Flight Critical Systems”.

(5.6) Expected Outcome

The expected outcome is technologies and mathematical models that enable rigorous, comprehensive safety analysis and assessment of functionally integrated distributed systems interacting through various structures such as communication networks and human-automation and human-human interaction, as described in (5.3).

Proposals that include cutting-edge high-risk investigations are encouraged; however, the balance of risk versus potential gains should be discussed. A high value will be placed on openly available and re-usable models and verification approaches applicable to a broad spectrum of distributed flight-critical systems V&V challenges related to integrated distributed systems. Also of interest are publically available design artifacts illustrating particularly difficult aviation V&V problems suitable for demonstrating and validating novel V&V techniques.

(5.7) Deliverables

Proposals shall identify any and all tangible research products such as all models, methods and procedures, case studies and supporting evidence developed during this effort that shall be delivered. In addition, the award recipients shall deliver the following:

- Documentation of repeatable test and experimental validation capabilities
- Interim Report(s) to NASA as a published report or presentation that contains a description of the specific research topic addressed, a review of relevant literature, and description of research approach, including suggested improvements to research approach as identified in the course of the research to date
- Final Report, to be published as a NASA CR (Contractor Report), that contains a description of the specific research topic addressed, a review of relevant literature, repeatable description of the research approach, and detailing of the results, methods and tools developed, and insights into V & V approaches
- A paper suitable for journal submission assessing the research contributions to rigorous, comprehensive analysis of functionally integrated distributed systems as described in 2.5.3 and identification of relevant open issues
- Written assessment of open issues relevant to the research topic and further research required to address them

(5.8) Duration And Expected Funding

NASA anticipates awarding two or three contracts or cooperative research agreements for this topic that addresses the objectives and specific approaches described in (5.3) and (5.4). The awards, in the $250-300K per year range, will be made for a three-year proposal. An annual review will be conducted each year. The decision whether to continue at the end of each year will be based on:

- NASA's judgment of the progress made during the year relative to quantifiable metrics defined in the proposal and agreed to by the NASA Technical Monitor at the onset of the agreement.
- NASA's judgment of the impact the findings will have on the goals of the AFCS effort.

- The availability of resources to support the proposed work for the second and third years.

Proposals shall include a schedule with milestones that support the evaluation of progress and highlight the achievement of goals. Decision points are acceptable as milestones.

(5.9) Potential NASA Resources

See section 6, NASA Facilities, below.

(6) Subtopic Number: AFCS-1.6

(6.1) Subtopic Name: Authority and Autonomy: Safety Analysis of Multiple Human-System Interactions in the NAS

(6.2) Description

The National Airspace System (NAS) can be viewed as a large complex system in which humans and automated systems interact to perform a safe air transport service, mostly the transportation of passengers and goods across the US. As it stands, the NAS is quite safe and we do not suffer from frequent catastrophic accidents. Yet, the air traffic density is expected to increase over the next 20 years. The NextGen program [8, 16] is seeking to address this increase in traffic while maintaining (and possibly improving) the NAS safety record by introducing more automation. The roles and responsibilities of humans and automation will change in NextGen and potentially introduce unforeseen safety issues. Moreover, soon, UAS will be sharing the NAS with the rest of commercial aviation and modifying further the interactions between human agents and automated agents. Therefore, it becomes critical to have techniques that can take into account the stochastic nature of the NAS and analyze how roles and responsibilities change in NextGen and what the impact on safety might be.

(6.3) Objectives

NASA is seeking proposals that deliver analytical capabilities to assess safety issues due to the interaction of humans and automation over large sections (at least three sectors and three major airports, multiple flight crews, multiple controllers) of the NAS. At this time, NASA is specifically seeking techniques that can handle the stochastic and complex nature of many elements (including automated systems, humans, environment conditions) in the NAS, especially the unpredictable nature of human responses and the safety aspects involved in trying to “game the system”. Current human factor studies often assume a nominal, expert human subject and are not always capable of accounting for diversity in human responses. NASA is seeking analysis techniques that complement traditional human factor studies by addressing off-nominal conditions and coping with variability.

(6.4) Approach

Given the complexity of the NAS (both in size and levels of interaction), methods should evaluate safety issues related to decision-making. The focus should be on human-human as well as human-automation interactions and the exploration of off-nominal scenarios that can emerge from these interactions. It is important to take into account the stochastic elements of the NAS. For example, the analyses of interest could include the following, non-exhaustive list of off-nominal scenarios:

- Misunderstandings due to mixed equipage
- Sudden deviations from planned trajectories due to exceptional circumstances such as unexpected pilot actions or unexpected critical hardware or software failures
- Safety issues resulting from overly competitive behaviors or from gamesmanship.

In particular this solicitation seeks techniques that can handle stochastic events and emerging behaviors. The techniques of interest include:

- Game theory: in particular for modeling human aspects involved in decision making between humans, but in the context of interaction with some automation.
- Bayesian analysis: for modeling probability propagation throughout a graph of modeling interactions between human and automated agents.
- Learning and coordination in multi-agent systems: for capturing the evolution of human behaviors over time and especially the learning of specific situations and the optimization or simplification of procedures in air traffic that can lead to confusion for other agents.
- Evolutionary algorithms for capturing the effect of evolutionary behavior in complex systems such as the NAS.

The focus is on modeling to evaluate safety and not for optimizing traffic in the NAS.

These techniques must be demonstrated in the context of realistic air traffic scenarios involving multiple humans and multiple automated systems. The focus should be on the capability to conduct safety evaluation of large parts of the NAS and, if possible, emergent behaviors emerging from unforeseen interactions in the deployment of various automated systems. For example, can the use of ADS-B affect responses to TCAS advisories? Also of great interest is the ability of seamlessly modeling the NAS at different levels of abstractions and propagating emergent, off-nominal behaviors across sectors, automation, and human hierarchies.

(6.5) Relevant Milestones Supported

The proposed work will partially support completion of SSAT milestone “Document the compositional verification of human models and automation for analyzing the safety of a NextGen air traffic system.”

(6.6) Expected Outcome

NASA expects publications, software prototypes, and demonstrations of the technique using simulations of the NAS involving at least one automated system (e.g., TCAS or ADS-B) and interactions between crews of multiple airplanes and multiple controllers.

(6.7) Deliverables

Proposals shall identify any and all tangible research products such as all models, methods and procedures, case studies and supporting evidence developed during this effort that shall be delivered. In addition, the award recipients shall deliver the following:

- Documentation of repeatable test and experimental validation capabilities
- Interim Report(s) to NASA as a published report or presentation that contains a description of the specific research topic addressed, a review of relevant literature, and description of research approach, including suggested improvements to research approach as identified in the course of the research to date
- Final Report, to be published as a NASA CR (Contractor Report), that contains a description of the specific research topic addressed, a review of relevant literature, repeatable description of the research approach, and detailing of the results, methods and tools developed, and insights into V & V approaches.
- A paper suitable for journal submission assessing the research contributions to rigorous, comprehensive analysis of functionally integrated distributed systems as described in (6.3) and identification of relevant open issues
- Written assessment of open issues relevant to the research topic and further research required to address them

(6.8) Duration And Estimated Funding

NASA anticipates awarding one or two contracts or cooperative research agreements for this topic that addresses the objectives and specific approaches described in (6.3) and (6.4). The award, in the $250-$300K per year range, will be made for a **three-year** proposal. An annual review will be conducted each year. The decision whether to continue at the end of each year will be based on:

- NASA's judgment of the progress made during the year relative to quantifiable metrics defined in the proposal and agreed to by the NASA Technical Monitor at the onset of the agreement.
- NASA's judgment of the impact the findings will have on the goals of the AFCS effort.

- The availability of resources to support the proposed work for the second and third years.

Proposals shall include a schedule with milestones that support the evaluation of progress and highlight the achievement of goals. Decision points are acceptable as milestones.

(6.9) Potential NASA Resources

See section 6, NASA Facilities, below.

B.2.3 Programmatic Considerations

The SSAT project plans to invest $2.5-4.8M per year for 3 years. We anticipate 8-11 awards depending on proposed scope of work and number of topics covered in the proposal. The actual number and value of the awards will depend on the quality of the proposals received; depending on quality NASA may choose not to make an award under a given topic. Multi-year awards are subject to funding availability in subsequent fiscal years. In some cases, a subset(s) of a proposal may be selected for a partial award.

The following describe the minimum information expected in the science-technical-management section of the proposal. It must clearly describe:

- The specific topic(s), listed in this solicitation, the proposal is addressing
- Statement of relevance to the SSAT project goals
- Background and objectives of the proposed research
- Technical approaches
- Any and all tangible research products such as all models, methods and procedures, case studies and supporting evidence proposed to be developed during this effort
- Level of effort to be employed
- Targeted/anticipated results
- Specific quantifiable metrics to be used to judge progress
- Detailed work plan - includes a schedule with milestones and measurable metrics; as well as the qualifications, capabilities, and experience of the lead organization and team members.
- Contribution of the proposed work to system-wide safety technologies
- Statement of what intellectual property is expected to be publicly available at the conclusion of the work (note that it is our intent to share knowledge developed under this solicitation, thus, any restrictions to the objective may impact the evaluation of the proposal)
- Plans for oral presentations, interim reports, and final report. There will be a kick-off meeting at the beginning of the award period, annual reviews and a final review. These meetings will be held at/near one of the NASA centers, and must be attended by at least the principal investigator for the award. A travel budget to support these reviews should be included in the proposal.
- Test facilities to be used including proposed use of NASA facilities

The science-technical-management section must not exceed 20 pages. Supporting information such as budget, resumes, and commitment letters will not be counted toward the 20 page limit. Please refer to NASA ROA-2013 section IV, “Proposal and Submission Information”, for requirements on proposal content, format, budget details, and submission procedures. Bidders should propose an appropriate level of effort (cost and duration). The estimated level of effort provided with the topic description is for general guidance.

Milestones with measurable metrics toward achieving the proposed goal must be provided. Annual and final oral presentations to be made as part of an open technical exchange meeting for purposes of technology transfer and knowledge dissemination will be expected. There will be a kick-off meeting at the beginning of the award period, annual reviews and a final review. These meetings will be held at/near one of the NASA centers, and must be attended by at least the principal investigator for the award. Quarterly reports are expected; the information in these reports will be one of the factors used to determine whether adequate progress has been made. Complete documentation of approach and results in the form of a written final report is required at the end of the complete effort.

The intent of the NRA process is to foster strategic partnerships between NASA and the awarded institutions for collaborative research and development of innovative concepts, ideas, technologies and approaches. Therefore substantial interaction with NASA researchers may be anticipated while performing work under these awards. Bidders may include as part of the proposal visits of appropriate length to a NASA Center for the purpose of coordinating the proposed work with corresponding efforts by NASA researchers. If a proposal is selected for negotiation towards a potential award, then and only then can the details of any proposed collaboration including time in residency at a NASA Center, if applicable, be discussed and finalized. Communications with NASA during the solicitation period can only occur through the designated POC (see Section B.2.7). There can be no direct or indirect communications with NASA researchers from the time this solicitation is posted to NSPIRES until proposal selections are final. See Questions 34-41 in ROA 2013 NRA Q&A’s for guidance on this issue: http://nspires.nasaprs.com/external/solicitations/summary.do?method=init&solId={0A8625E4-D356-4A03-C358-EFD0D8A5562C}&path=open

B.2.4 Evaluation Criteria And Basis For Award

The principal elements considered in evaluating a proposal are its relevance to NASA’s objectives, technical merit, and effectiveness of the proposed work plan (including cost and team qualifications). Failure of a proposal to be highly rated in any one of the following elements is sufficient cause for the proposal to not be selected.

1. Relevance (weight 30%):

- Evaluation of a proposal's relevance to NASA's objectives includes the consideration of the potential contribution of the effort to the specific objectives and goals given in the solicitation to which the proposal is submitted.

2. Technical Merit (weight 50%):

- Overall scientific or technical merit of the proposal, including unique and innovative methods, approaches, or concepts.
- Evaluation will also include: credibility of technical approach, including a clear assessment of primary risks and a means to address them.
- The selection process will also assess the proposal against the state-of-the-art.
- Evaluation will consider the value of the proposed deliverable research products

3. Effectiveness of the Proposed Work Plan (weight, 20%):

- Comprehensiveness of work plan, effective use of resources, management approach, and proposed schedule for meeting the objectives.
- Proposed team qualifications (capabilities, related experience)
- Facilities, techniques, or unique combination of these which are integral factors for achieving the proposal's objective.
- Proposed cost realism and reasonableness.
- Degree and type of cost sharing
- Objectives with measurable metrics toward achieving the proposer's goal must be provided, with a minimum of one metric per year.
- Documentation of approach and results in the form of final written technical reports is required.
- A clear statement of what intellectual property is expected to be publicly available at the conclusion of the work. It is NASA's intent that all deliverables under the contract be provided to NASA with unrestricted/unlimited rights; thus, any restrictions must demonstrate a significant net benefit to NASA and may cause a lower score.
- Collaboration with NASA researchers (including joint use of facilities, sharing of materials, development of computer code modules compatible with NASA's software, and synergistic research goals) is desirable, with the objective of enhancing knowledge transfer and the long-term value of the proposed work (applies only to cooperative agreements).

B.2.5 References

The references listed here are intended to be illustrative only; and do not represent the comprehensive set of previous research that should be considered when proposing to these topics. NASA is seeking truly novel, innovative, approaches to the objectives described and proposers should not feel compelled to use these past works as a basis for the proposed effort. However, these works are considered significant and are recommended reading materials when considering new V&V functions required for NextGen.

1. http://www.nasa.gov/centers/dryden/news/FactSheets/FS-076-DFRC.html

2. R. Butler, G. Hagen, J. Maddalon, C. Munoz & A. Narkawicz (2012). "The search for effective algorithms for recovery from loss of separation." In Digital Avionics Systems Conference (DASC), 2012 IEEE/AIAA 31st, 4–2. doi:10.1109/DASC.2012.6382343

3. T. Chandra, R. Griesemer, & J. Redstone, J. (2007) Paxos made live: an engineering perspective, In Proceedings of the 26th ACM Symposium on Principles of Distributed Computing (PODC'07)

4. K. Driscoll, B. Hall, H. Sivencrona, & P. Zumsteg. (2003) Byzantine Fault Tolerance, From Theory to Reality. Proc. 22nd International Conference on Computer Safety, Reliability and Security (SAFECOMP03), pp.235-248, Edinburgh, Scotland, UK

5. J. Eklund, J. Sprinkle & S. Sastry, "Implementing and Testing a Nonlinear Model Predictive Tracking Controller for Aerial Pursuit/Evasion Games on a Fixed Wing Aircraft", 2005 American Control Conference, June 8-10, 2005. Portland, OR, USA.

6. H. Erzberger, H. (2001). "The automated airspace concept." In 4th USA/Europe Air Traffic Management R&D Seminar.

7. H. Erzberger& K. Heere. (2010). "Algorithm and operational concept for resolving short-range conflicts." Proceedings of the Institution of Mechanical Engineers, Part G: Journal of Aerospace Engineering 224 (2): 225–243.

8. FAA. 2012. "NextGen Implementation Plan."

9. R. Fagin, J. Halpern, Y. Moses, & M. Vardi, M. (1995) Reasoning about Knowledge, MIT Press

10. M. Gheorghiu, C. S. Pasareanu, & D. Giannakopoulou, "Automated Assume-Guarantee Reasoning by Abstraction Refinement". Proceedings of the 20th International Conference on Computer Aided Verification (CAV 2008), Princeton, USA, July 2008.

11. D. Giannakopoulou, D., Z. Rakamaric, & V. Raman, " SAS 2012, Symbolic Learning of Component Interfaces.

12. D. Giannakopoulou, D, Bushnell, D., Schumann, J., Erzberger, H., Heere, K.: Formal testing for separation assurance. Ann. Math. Artif. Intell. 63(1): 5-30 (2011).

13. D. Giannakopoulou & C. S. Pasareanu, "Interface Generation and Compositional Verification in JavaPathfinder". Proceedings of the ETAPS conference on

Fundamental Approaches to Software Engineering (FASE 2009), York, UK, March 2009.

14. D. Giannakopoulou, C. S. Pasareanu, & J. M. Cobleigh, "Assume-guarantee Verification of Source Code with Design-Level Assumptions", Proc. of the 26th International Conference on Software Engineering (ICSE'2004), Edinburgh, Scotland, May 2004.

15. D. Giannakopoulou, C. S. Pasareanu & H. Barringer, "Assumption Generation for Software Component Verification", in Proc. ofthe 17th IEEE International Conference on Automated Software Engineering (ASE 2002). September 2002, Edinburgh, UK.

16. JPDO. 2007. "Next Generation Air Transportation System (NextGen) Enterprise Architecture v2.0."

17. M. Kochenderfer, J. Holland, and J. Chryssanthacopoulos, "Next-generation airborne collision avoidance system", Lincoln Laboratory Journal, volume 19, number 1, 2012.

18. H. Kopetz, (1997) Real-Time Systems: Design Principles for Distributed Embedded Applications, Kluwer Academic Publishers

19. N. Leveson (2012) Engineering a Safer World, MIT Press

20. N. Lynch (1996) Distributed Algorithms, Morgan Kaufmann

21. T. Menzies and C. Pecheur. Verification and Validation and Artificial Intelligence. *In: M. Zelkowitz, Ed., Advances in Computers, vol. 65, 2005, Elsevier.*

22. C. Munoz, Cesar, R. Butler, A. Narkawicz, J. Maddalon, & G. Hagen (2012). A Criteria Standard for Conflict Resolution: A Vision for Guaranteeing the Safety of Self-Separation in NextGen.

23. F. Raimondi, C. Pecheur, G. Brat, *PDDL, a tool to verify PDDL planning domains*, in proceedings of VVPS 2009.

24. RTCA, Inc., Washington, DC. DO-178-B/C, Software Tool Qualification Considerations. December 2011. http://www.rtca.org`

25. RTCA, Inc., Washington, DC. DO-278-A, Software Tool Qualification Considerations. December 2011. http://www.rtca.org

26. RTCA, Inc., Washington, DC. DO-330, Software Tool Qualification Considerations. January 2012. http://www.rtca.org

27. RTCA, Inc., Washington, DC. DO-333, Formal Methods Supplement to DO-178C and DO-278A. January 2012. http://www.rtca.org

28. SAE Aerospace Recommended Practice ARP4754, Revision A, Society of Automotive Engineers, Inc., December 2010.

29. SAE Aerospace Recommended Practice ARP4761, Society of Automotive Engineers, Inc., December 1996.

30. U. Schmid (2001) How to model link failures: A perception-based fault model, In proceedings of the International Conference on Dependable Systems and Networks, (DSN'01)

31. J. Schumann and Y. Liu., "Tools and Methods for the Verification and Validation of Adaptive Aircraft Control Systems", IEEE Aerospace Conference, IEEE Press, 2007.

32. J.Schumann and W.Visser, "Autonomy Software: V&V Challenges and Characteristics," IEEE Aerospace Conference, IEEE Press, 2006.

33. R. Singh, D. Giannakopoulou, C. S. Pasareanu, "Learning Component Interfaces with May and Must Abstractions." CAV 2010.

34. D. J. Wing & W. B. Cotton (2011). "For Spacious Skies: Self-Separation with‘ Autonomous Flight Rules’ in US Domestic Airspace." In 11th AIAA Aviation Technology, Integration, and Operations (ATIO) Conference.

B.2.6 NASA Facilities

The following websites provide information on NASA aeronautics facilities capabilities, testing, and contact information. If use of NASA facilities is proposed, the facility costs associated with testing must be covered in the proposal cost. The costs of fabricating test articles, fixtures, and instrumentation required for the testing shall be incurred by the proposer and included in the proposed cost. The proposal will need to specify the test article size, requirements, facility, and approximate testing time. Specific details such as timeframe and duration of testing will be negotiated upon selection of a proposal. A non-NASA facility may be proposed, in which case the costs must also be included in the proposed cost. Information on NASA test facilities can be found at the following websites.

NASA Center	URL

Ames Research Center	http://windtunnels.arc.nasa.gov/ http://ffc.arc.nasa.gov/ (simulations facilities)
Dryden Flight Research Center	http://www.nasa.gov/centers/dryden/capabilities/index.html
Glenn Research Center	http://facilities.grc.nasa.gov/
Langley Research Center	http://gftd.larc.nasa.gov/index.html (ground facilities)

B.2.7 Summary Of Key Information

Expected annual program budget for new awards	$2.5-4.8M
Number of new awards pending adequate proposals of merit	8-11 awards
Maximum duration of awards	3 years
Due date for Notice of Intent to propose (NOI)	7/22/13
Due date for proposals	**9/5/2013**
General information and overview of this solicitation	See the *Summary of Solicitation* of this NRA.
Detailed instructions for the preparation and submission of proposals	See the *NASA Guidebook for Proposers Responding to a NASA Research Announcement – 2013* at http://www.hq.nasa.gov/office/procurement/nraguidebook/.
Page limit for the central Science-Technical-Management section of proposal	Maximum of 20 pages; see also Chapter 2 of the *Guidebook for Proposers Responding to a NASA Research Announcement-2013 at* http://www.hq.nasa.gov/office/procurement/nraguidebook/
Submission medium	Electronic proposal submission is required; no hard copy is required. See also Section IV in the Summary of Solicitation of this NRA and Chapter 3 of the *NASA Guidebook for Proposers Responding to a NASA Research Announcement-2013 at* http://www.hq.nasa.gov/office/procurement/nraguidebook/.
Web site for submission of proposal via NSPIRES	http://nspires.nasaprs.com/ Help desk available at nspires-help@nasaprs.com or (202) 479-9376

Expected award type	Contracts or Cooperative Agreements. If a contract is desired, please provide a draft Statement of Work with your proposal.
Funding opportunity number	NNH13ZEA001N-SSAT1
NASA points of contact (POC) Written responses will be posted on the solicitation website.	Email questions to: Project Scientist: Robert Mah, Ph.D., robert.w.mah@nasa.gov NRA Manager: TBD Procurement POC: TBD