NASA/TM–2010-216715

Verification and Validation for Flight-Critical Systems (VVFCS)

Summary of Responses to Solicitation Number NNH09ZEA001L, April 2009

Sharon S. Graves
Langley Research Center, Hampton, Virginia

Robert A. Jacobsen
Sierra Aviation Consulting, Inc., Reno, Nevada

June 2010

NASA STI Program . . . in Profile

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

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

- TECHNICAL PUBLICATION. Reports of completed research or a major significant phase of research that present the results of NASA programs and include extensive data or theoretical analysis. Includes compilations of significant scientific and technical data and information deemed to be of continuing reference value. NASA counterpart of peer-reviewed formal professional papers, but having less stringent limitations on manuscript length and extent of graphic presentations.

- TECHNICAL MEMORANDUM. Scientific and technical findings that are preliminary or of specialized interest, e.g., quick release reports, working papers, and bibliographies that contain minimal annotation. Does not contain extensive analysis.

- CONTRACTOR REPORT. Scientific and technical findings by NASA-sponsored contractors and grantees.

- CONFERENCE PUBLICATION. Collected papers from scientific and technical conferences, symposia, seminars, or other meetings sponsored or co-sponsored by NASA.

- SPECIAL PUBLICATION. Scientific, technical, or historical information from NASA programs, projects, and missions, often concerned with subjects having substantial public interest.

- TECHNICAL TRANSLATION. English-language translations of foreign scientific and technical material pertinent to NASA's mission.

Specialized services also include creating custom thesauri, building customized databases, and organizing and publishing research results.

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

- Access the NASA STI program home page at *http://www.sti.nasa.gov*

- E-mail your question via the Internet to help@sti.nasa.gov

- Fax your question to the NASA STI Help Desk at 443-757-5803

- Phone the NASA STI Help Desk at 443-757-5802

- Write to:
  NASA STI Help Desk
  NASA Center for AeroSpace Information
  7115 Standard Drive
  Hanover, MD 21076-1320

NASA/TM–2010-216715

Verification and Validation for Flight-Critical Systems (VVFCS)

Summary of Responses to Solicitation Number NNH09ZEA001L, April 2009

Sharon S. Graves
Langley Research Center, Hampton, Virginia

Robert A. Jacobsen
Sierra Aviation Consulting, Inc., Reno, Nevada

National Aeronautics and
Space Administration

Langley Research Center
Hampton, Virginia 23681-2199

June 2010

Available from:

NASA Center for AeroSpace Information
7115 Standard Drive
Hanover, MD 21076-1320
443-757-5802

Table of Contents

Executive Summary

On March 31, 2009 a Request for Information (RFI) was issued by the National Aeronautics and Space Administration (NASA) Aviation Safety Program to gather input on the subject of Verification and Validation (V & V) of Flight-Critical Systems. The responses were provided to NASA on or before April 24, 2009. The RFI asked for comments in three topic areas: Modeling and Validation of New Concepts for Vehicles and Operations; Verification of Complex Integrated and Distributed Systems; and Software Safety Assurance. There was a strong response with a total of 34 responses to the RFI, representing a cross-section of academic (26%), small & large industry (50%) and government agency (24%). The organizations that replied are listed below:

Organization
Adventium Enterprises, LLC
BAE Systems
Concordia University, Montreal, Canada - Department of Computer Science and Software Engineering
DornerWorks, Ltd.
Draper Laboratory
E L I AUS, LAMPS and University of Manchester, United Kingdom et al
Federal Aviation Administration (FAA) - Software and Digital Systems (SDS) Program
Florida Institute for Human and Machine Cognition (IHMC)
Honeywell International Inc.
Lockheed Martin
NASA Ames Research Center
NASA Glenn Research Center
NASA Langley Research Center
National Aerospace Laboratory (NLR) – Air Transport Safety Institute
National Transportation Safety Board
Ohio University - School of Electrical Engineering and Computer Science
Oregon State University - School of Mechanical, Industrial, and Manufacturing Engineering
Rockwell Collins, Inc.
Scientific Monitoring, Inc.
Software and Digital Systems
Software Intensive Systems, Inc.
SRI International Computer Science Laboratory
Stinger-Ghaffarian Technologies
The MITRE Corporation - Center for Advanced Aviation System Development
The University of Iowa -The Virtual Soldier Research Program, Center for Computer-Aided Design
United Space Alliance
United Technologies Research Center
University of Virginia, Department of Systems and Information Engineering
United Technologies Corporation - Pratt & Whitney
Vanderbilt

Table 1: List of Organizations that Responded to V&V RFI

The respondents universally acknowledged the importance of developing more effective methods and techniques for the verification and validation of flight critical systems. Implicit in their comments was the encouragement for NASA to take the lead in developing improved methods and techniques for V & V of critical systems. Indeed, many mentioned that other safety critical systems shared the need for improved V & V methods. It was clear from the responses that the difficulty of verifying and assuring the validity of increasingly complex systems is universally acknowledged.

It should be noted that the respondents generally acknowledged a need for research and development in all three of the topics listed in the RFI, and many then addressed one or more of the specific topics. There was considerable variation in the subject matter and in the technical depth of the respondent's comments, with more consistency among the responses by type of organization than by the topics listed in the RFI. Consequently, summary comments of the responses are provided in a structure which reflects the organizational breakdown of the respondents.

The need for consideration of the human in the definition of the system was acknowledged in several of the responses. More adequate modeling of human cognition and performance as well as human-machine interactions were of particular interest. Additional mention of modeling was common, especially the need for validation of the models used in simulations.

Considerable emphasis was placed on design phase analysis and verification. The continued need for formal methods in verification was noted and it was acknowledged that a provably correct code generation capability needs to be developed. However, it was also proposed that a fundamental departure from current technology is necessary for software construction, and that it must be more holistic was a consistent theme.

A particularly noteworthy suggestion made was that a team of world-class technical experts be engaged to help guide the research effort through a series of workshops.

Judging by the interest shown in the RFI, the Verification and Validation of Flight-Critical Systems is a subject which many members of the aviation community view as a necessary and timely subject for research and development of new methods, technologies, and policies.

Introduction

This Report provides a synopsis of the responses to the Request for Information (RFI) issued by NASA's Aviation Safety Program entitled "REQUEST FOR INFORMATION IN 'VERIFICATION AND VALIDATION OF FLIGHT-CRITICAL SYSTEMS'", Solicitation Number NNH09ZEA001L. This RFI solicited information on Verification and Validation (V&V) challenges for the next generation of flight-critical systems. The RFI was issued on March 31, 2009 and responses were submitted to NASA by noon on April 24, 2009.

A summary of the RFI is presented with identification of the goals and objectives of the effort. The topic area structure that the RFI requested the respondents use is also described. However, comments outside of the provided structure were explicitly identified as welcome within the RFI. Responses were submitted by organizations broadly representing Industry, Academia, and Government.

The responses were tabulated and statistical information which categorizes the responses in terms of the respondent and the topic area is provided.

An aggregated summary of the technical content of the responses is also provided.

Summary of Request for Information

The current aviation system has an enviable safety record; however, advances in technology are placing an increasing strain on our ability to assure the integrity of new and anticipated systems. Additionally, there is a perception that current approaches for the assurance of complex flight-critical systems impose a barrier to innovation.

Under this RFI, the NASA Aviation Safety Program solicited insight into V & V obstacles to timely and cost-effective implementation of flight-critical systems, i.e., systems comprising hardware, software and physical systems, used to execute pre-defined concepts of operation or operating procedures, and interacting with human operators including pilots and controllers, that will directly control some aspect of flight and thus must be demonstrated to the highest levels of safety. Additionally, the RFI solicited insight into innovative theories, methods and tools for V & V of Flight-Critical Systems at all levels of development. Articulation of all obstacles to their implementation was encouraged, including further technical developments required, changes they imply in current processes for design, test and evaluation, regulatory compliance and other implementation considerations, and other implications such as policy concerns. This focus was identified in the RFI as supporting the Next Generation Air Transportation System (NextGen), targeting NextGen safety activities and interests encompassing vehicles, vehicle systems, airspace, airspace concept of operations, and air traffic technologies such as communication, guidance and navigation.

Within the RFI, three broad categories were identified for the purposes of organizing possible research and objectives. Suggestions for alternate organizations of the research areas, and descriptions of V & V issues not noted in the three topics below, were encouraged. The following topic descriptions are excerpted from the RFI.

Topic 1. Modeling and Validation of New Concepts for Vehicles and Operations: Current safety assessments of new concepts for vehicles and operations need to be extended to better address transformative changes that are not covered by extending current V & V methods. In addition, there is a need to predict key blocks to human performance and to provide rigorous design guidance early-and-throughout development of these concepts. The objective is to develop safety-case methods and

supporting technologies, such as methods for modeling concepts of operation to identify safety issues, capable of analyzing the system-wide safety properties suitable for civil aviation vehicles and for complex concepts of operation involving airborne systems, ground systems, human operators and controllers.

Topic 2. Verification of Complex Integrated and Distributed Systems: The integration of functions across traditional boundaries (e.g., integration of discrete and continuous behaviors, integration of distributed vehicle (and ground-vehicle) functions, novel distributions of functions between air and ground and between human and automation) demands new methods for predicting, assuring and proving the safety levels demanded of NextGen. The objective is to develop a collection of technologies and mathematical models that enable rigorous, comprehensive analysis of new integrated (and distributed) systems interacting through various structures such as communication networks and human-automation and human-human interaction.

Topic 3. Software Safety Assurance: Establishing sufficient confidence in the safety of complex software-intensive systems, such as those envisioned for NextGen, is a significant challenge. While this problem has been widely recognized, it is generally viewed as incremental changes to a current process that is cost-prohibitive and automatically precludes a wide range of functions and capabilities; thus, a transformative view of software safety assurance is needed. The objective is to develop a collection of techniques, tools, and policies which will enable efficient and accurate analysis of safety aspects of software-intensive systems; ultimately reducing the cost of software V & V to the point where it no longer obstructs many safety innovations and NextGen developments, and ultimately enable in-the-field assurance of composed software-intensive systems.

Summary of Responses

Respondent and Response Topic Statistics

There were 34 responses to the RFI, representing a reasonable cross-section of academic (26%), small & large industry (50%) and government agency (24%).

There were 17 responses to the RFI from Industry [Adventium, Florida Institute for Human and Machine Cognition, BAE Systems, Boeing Enterprises, Dorner Works (2), Draper Laboratories, Honeywell, Lockheed Martin, NLR/ASTI , Rockwell Collins, SMI, Software Intensive Systems, Inc., SRI International, USA LLC, UTC Pratt Whitney, and UTRC].

There was one response to the RFI jointly authored by Industry and Academia [UVA-NIA].

There were five responses to the RFI from Academic Institutions [Concordia University, Ohio University, University of Iowa, University of Manchester, and Vanderbilt].

There were three responses to the RFI jointly authored by NASA and Academia [NASA Ames-University of California, NASA Ames-UCLA, and NASA Ames-Oregon State-Ohio State].

There were four responses to the RFI from within NASA [Ames (2), Glenn (1), and Langley (1)].

There were two responses to the RFI from Non-NASA Government Agencies [FAA, and NTSB] and two responses from Federally Funded Research and Development Centers [JPL Laboratory of Reliable Software, and MITRE CAASD].

There were 13 responses addressing Topic 1 of the RFI.

There were 10 responses addressing Topic 2 of the RFI.

There were 13 responses addressing Topic 3 of the RFI.

There were seven responses that did not address a specific topic but provided general input on the subject of the RFI. Additionally, several of the responses which addressed specific topics also provided more general input to the subject of V&V of Flight-Critical Systems.

Aggregated Technical Response

All of the responses acknowledged the importance of developing more effective methods and techniques for the verification and validation of flight critical systems. Implicit in their comments was encouragement for NASA to take the lead in developing improved methods and techniques for V & V of critical systems. Indeed, many mentioned that other safety critical systems, beyond aviation, shared the need for improved V & V methods. It was clear from the responses that the difficulty of verifying and assuring the validity of increasingly complex systems is universally acknowledged.

Respondents generally acknowledged a need for research and development in all three of the topics listed in the RFI, however there was considerable variation in the subject matter and in the technical depth of the respondent's comments, with more consistency among the responses by type of organization than by the topics listed in the RFI. Consequently, summary comments of the responses are provided in a structure which reflects the organizational breakdown of the respondents.

Appendix A provides a summary of responses listing needed V&V methodologies, targeted application, problems addressed and suggestions for types of V&V products that might fill technological gap.

Emerging V&V Challenges

Noted emerging V&V challenges include: increasing system complexity; an exponential increase in software requirements; an increase in tests required using current V&V methods; safety, cost and schedule impacts associated with V&V; emergence of distributed architectures & trends in microprocessor technologies; emergence of multi-Vehicle and cooperative control Requirements.

Collaboration

Many of the respondents saw the need for collaboration between technical experts across NASA, industry, academia, FAA, and other government agencies. Safety assurance approaches for Air Traffic Management and Aircraft should have clear engagement of certification authorities as well as aerospace industries with domain experts in aircraft, ground, and space flight critical systems.

Responses from Industry

Virtually all of the Industry responses endorsed the effort by NASA to consider the need for research in V & V. One respondent expressed the need for the results of any research program to be made publicly available so that the entire community can benefit. Several suggested formation of a cross-functional team including NASA, industry (Airframe, Engine, and Subsystem Manufacturers), academia, and the FAA to help guide the research effort.

Considerable variation existed in the responses from Industry in both the breadth and depth of the information provided. Several of the responses offered the use of tools which had been developed to assist in the V & V of safety-critical systems.

The response from the Air Transport Safety Institute of National Aerospace Laboratory (NLR) in The Netherlands was motivated by the similarities between NextGen needs and those of (Single European Sky ATM Research (SESAR). Both air traffic system modernization projects seek to implement large, complex, distributed systems which have to contend with internal and external stochastic influences for which traditional safety analysis tools are inadequate. From this response, it is clear that the European community is also making an effort to address the myriad issues facing the introduction of complex flight critical systems. The need for data collection processes that focus on ensuring new complex systems work as intended when they become operational.

Common subjects addressed in the Industry responses included:

The need for consideration of the human in the definition of the system was acknowledged in several of the responses. More adequate modeling of human cognition and performance as well as human-machine interactions were of particular interest. The use of human-in-the-loop simulations was suggested to be of considerable value. The need for techniques for validating Air Traffic Controller Human Agent Models was noted as well as decision protocols for V&V of human-automation interfaces on aircraft.

Respondents placed considerable emphasis on design-phase analysis and verification. Included was the need to develop sound design processes, structural principles, and associated philosophies supporting the development of flight critical systems. Several responses addressed the need for an optimized V&V structure to be used early in the design process based on formal methods and dependability cases.

Many responses recommended utilization of a unified approach such as dependability cases or safety cases as a means to improve requirement definition and provide systematic and rigorous analytical methods for validating safety requirements. Responses specified the need for new and improved ways to represent system and software requirements and one response suggested the creation of an ontology that could be queried throughout the product lifecycle about inferences or potential ramifications of a requirement or specification. Another respondent recommended a fully functional approach to safety assessment according to guidance contained in industry safety standards and FARs: Society of Automotive Engineers (SAE) 4761 " *Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment*", ARP 4754 *"Certification Considerations for Highly-Integrated Or Complex Aircraft Systems", ARP* 5150 "*Safety Assessment of Transport Airplanes in Commercial Service*" , Federal Aviation Regulations (FAR) 25.1309.

A focus on modeling was common, especially on the need for validation of the models used in simulations. Also noted was the need to understand the uncertainty represented by the models and how that affects their results and their use. Consideration of both state- and model-based architectures was suggested. It was noted that the models need to address system level properties. Continued use of enhanced closed-loop models to analyze system performance was encouraged.

The continued need for formal methods and formal verification was noted. One respondent encouraged the development of methodologies for the analysis of complex uncertain systems. Many respondents called for improved formal verification enabling subsystem validation in the context of entire vehicle-level integrated system. Use of formal methods and formal verification was seen as a viable alternative to reducing predicted NextGen exhaustive testing requirements. In Formal Methods, the need for new V&V automatic analysis techniques combining model checking and theorem proving was noted.

One response stated that a provably correct code generation capability needs to be developed. Another proposed that a fundamental departure from current technology is necessary for software construction and that it must be more holistic.

Joint Response from Industry and Academia

The joint Industry/ Academia response suggested that a breakthrough in integration of formal methods and human factors engineering methods is required to include human behavior in the formal verification process.

Responses from Academic Institutions

One response suggested that self-forensics technology taken from the cyber-crime domain may be useful in V & V of flight critical systems. Another suggested that an error analysis of the accumulation of small (quantization, round-off) errors would be helpful in understanding its potential impact on the performance of the system.

Another respondent forwarded the proposition that new human-human interaction and human-automation interaction simulation tools will help identify safety concerns.

Another suggested that research in Automatic Flight Control Systems control algorithm V & V be conducted.

Joint Responses from NASA and Academia

One respondent suggested that recent developments from the IVHM domain could augment V & V of NextGen software systems.

Another respondent proposed building on the work done be the Air Force Office of Scientific Research into functional failure identification and propagation, suggesting that it could be helpful in the design phase of critical systems.

Another respondent suggested that traditional methods or formal methods alone are not adequate to conduct V & V of complex systems and that statistical validation tools are needed.

NASA Responses

The responses from NASA generally discussed subjects which could provide for improved V & V but needed additional research. These subjects included: the advocacy of probability analysis as a means to translate the objectives of the system into a set of required system parameters; the need to adopt recent progress in formal methods theory and software verification tool development; and development of structural principles for mission and safety critical flight software systems.

One response advocated the use of advanced V & V techniques already developed and employed to provide benefit in the future. Conversely, another response provided a discussion of the rapidly increasing complexity of aviation systems, including software, and that current V & V methods are not

sufficient. Another response presented the case for applying new developments in V & V to electronic hardware systems as well as to the air transportation system.

Responses from Non-NASA Government Agencies

A response from the FAA presented some of the improved safety techniques and tools being applied to both software and airborne electronic hardware systems. The NTSB provided a response which endorsed the efforts by NASA to increase the level of safety in flight critical systems and encouraged the use of their accident and incident databases. The NTSB's response called for specific research in the following areas: identifying, predicting, and resolving potential airspace system failure modes; determining how technological approaches may assist pilots in identifying and recovering from inflight upsets; ensuring that verification and validation processes and tools adequately consider operator abilities; and designing data collection processes for ensuring that new complex systems work as intended during their operation. The response also emphasized the difficulty of ensuring that software-intensive systems are safe, and the importance of using existing accident and incident data, reports, studies, and safety recommendations to provide insight into the limitations of current V&V processes.

Closing

Judging by the interest shown in the RFI, the Verification and Validation of Flight-Critical Systems is a subject which many members of the aviation community view as a necessary and timely subject for research and development of new methods, technologies, and policies.

NASA wishes to express their appreciation to all of those who responded, and encourages them to continue their contact with NASA as the results of this RFI are included in the planning of NASA's future research programs.

For further information on this subject, please contact:
Sharon S. Graves
MS 238, 4 Langley Blvd, B1230:R214
NASA Langley Research Center
Hampton, VA 23681-0001
Phone: 757.864.5018 (office), 757. 506.5388 (cell)
E-mail: Sharon.S.Graves@nasa.gov

APPENDIX A: SUMMARY OF RFI RESPONSES TO NASA SOLICITATION NUMBER NNH09ZEA001L, DATED APRIL 2009

Legend: SIS = Software Intensive Systems, DS = Distributed Systems, A&A = Authority and Autonomy, SA = Safety Assurance

Research Area	V&V Methodology	Application	Problem description	V&V Product
SIS DS, A&A, SA	Optimized V&V Structure for early software design	Flight-critical software systems; Mixed redundancy systems Adaptive control system	Increased levels of autonomy and automation requires fundamental effort to V&V using current techniques	Optimized V&V structure for early software design; include Formal Methods and safety/dependability case approach
SIS DS A&A	Optimized V&V Structure for early software design	Flight-critical software systems; Mixed redundancy systems Adaptive control system	Increased levels of autonomy and automation requires fundamental effort to V&V using current techniques	V&V early design algorithm checkers; data handlers; and system integration techniques
SA SIS	Optimized V&V Structure for early software design	Flight-critical software systems; Mixed redundancy systems Adaptive control system	Increased levels of autonomy and automation requires fundamental effort to V&V using current techniques	Formalization and standardization of dependability case methodologies
SIS SA	Optimized V&V Structure for early software design	Flight-critical software systems; Mixed redundancy systems Adaptive control system	Increased levels of autonomy and automation requires fundamental effort to V&V using current techniques	Error susceptibility & risk management
SIS SA	Optimized V&V Structure for early software design	Flight-critical software systems; Mixed redundancy systems Adaptive control system	Future aircraft trend toward multivariable and model-based controls introducing complex and intensive math into software	Formal methods to be used in early design to obtain verification credit and reduce need for exhaustive testing; Safety case approach working in concert with certification authority and industry
A&A	Techniques for Validating Air Traffic Controller Human Agent Models	Automation-supported separation management	Changing roles and responsibilities currently employed by air traffic controllers & flight crews driven by NextGen goal of safely and efficiently supporting 3 times present-day traffic levels. Calls for a substantial employment of advanced automation for separation assurance and other airspace management functions. Unconventional allocation of functions between air traffic controllers and automation have no standard and verified means of evaluation, considering the unprecedented operational	Controller agent models and V&V schemes with qualitative and quantitative aspect prediction; controller in the loop simulations; aspects should consider operational criteria, human cognitive capabilities and limitations
A&A SA	Decision Protocols for V&V of Human-Automation (Software) Interfaces on Aircraft	Task of control and management of aircraft, onboard autonomy and human operators	Future aircraft trend toward multi-agent systems - unchartered roles and responsibilities Conflicts between TCAS and ATC, inconsistent protocols, or inconsistently followed protocols	Procedures for rigorous and comprehensive analysis and inclusion of verified decision protocols V&V methods for human-centered automation and organization automation definition of human-in-the-loop simulations that are integral to V&V of systems; scenarios, principles and human factors V&V criteria and issues
SIS DS SA	Aircraft Software Configuration Verification and Management.	Aircraft configuration management	Manual process for managing aircraft configurations no longer viable Technology refresh problem as h/w, s/w ages	Simplified onboard network to receive and perform configuration verification and management Interchangeability/Compatibility Database to ensure combinations of h/w and s/w are valid and safety Ground-based data management system
SA	Validation of safety requirements for product development and continued airworthiness	Aircraft flight critical systems	Improved rationale needed for validated requirements for improved safety at reduced cost	Systematic and rigorous analytical methods of aviation safety data in support of risk analysis prescribed by SAE ARP 4761

Research Area	V&V Methodology	Application	Problem description	V&V Product
SIS DS SA	Airplane, System and Functional Analysis Methodology for Product Development and Continued Airworthiness.	Aircraft flight critical systems		System and Functional Analysis methodologies - Configuration control, including interfaces to design tools and requirements data bases. - Linkage to multi-variety performance and regulatory criteria - Simple and intuitive interfaces to allow standardized and specialized analyses, including Monte-Carlo or equivalent methods to assess a massive matrix of failure combinations. - Emphasis on airplane level safety assessment - Failure case summaries and report generation.
SA	Airplane, System and Functional Analysis Methodology for Product Development and Continued Airworthiness.	Aircraft flight critical systems		Fully functional approach to safety assessment according to guidance contained in industry safety standards and FARs: SAE ARP 4761, ARP 4754, ARP 5150, FAR 25.1309
SA	Safety Certification Process for ATM Systems	Aircraft flight critical systems	On average, it takes 18 years to introduce new system or procedure in ATM system. Established processes for ground based (SMS) and separate processes to certify safety of airborne systems.	Need safety certification process that takes entire operation into account, joining ground-based systems/procedures w/ airborne systems/procedures.
SIS DS SA	Assessment tools for necessary V&V	Flight critical systems		Methods for determining minimum V&V required for certification while ensuring safety and reliability
DS	Systems validation approaches		Propulsion system development and comprehensive checkout often precedes airframe development by several years. Vehicle control system not available to support engine software V&V	Improved methods for formal verification that enable subsystem validation in context of entire vehicle-level integrated system
SIS DS SA	V&V optimizing techniques	Flight critical systems	no effective notation for specifying system design (arch specs, interconnections bet fcn comp)	Compositional verification; Reusable certified code; Cookie cutter approaches; New methods for requirements understandability/clarification
SIS SA	Continuous validation methods	Flight critical systems	Control system V&V cost and schedule challenges have become so great that they now constrain industry's ability to introduce new and upgrade existing aerospace products;	Run-time adaptive safety assurance system monitoring and mitigation capability
SIS	Formal Methods for Software V&V cost reduction	Flight critical systems	There are still many technical challenges to be overcome to enable FM application to full range of problems found in large, complex systems Model checkers unable to analyze complex continuous geometries typical in aircraft conflict detection	New V&V analysis techniques (e.g. proof scripts to drive the automated application of theorem provers or script-based invocation of model checkers)
SIS	Formal Verification Methods for numerically intensive systems	ADS-B applications (Surface Indications & Alerts, In Trail Procedure (ITP), Closely Spaced Parallel Approaches (CSPA), Flight Deck Merging and Spacing, and Airborne Conflict Management	These applications involve non-linear trajectory computations that generally go beyond the capabilities of current formal method techniques	New V&V analysis techniques (e.g. proof scripts to drive the automated application of theorem provers or script-based invocation of model checkers) automatic analysis by combining model checking and theorem proving
SIS DS SA	Composition Techniques for Software Safety Assurance	Flight critical systems	Architectures will leverage new and existing sub-systems; Current certification approach for such systems limits the reuse of certification evidence of components from previously certified systems in new and updated systems.	Compositional development approaches

Research Area	V&V Methodology	Application	Problem description	V&V Product
SA	V&V Automated Techniques to ensure safety of complex FCS systems	Flight critical systems	New methods needed for establishing safety at lower cost and schedule	V&V automated techniques that exploit safety certification and assurance; Develop trusted suite of assessment tools that evaluate whole body of safety evidence Provably correct code generation
DS	Technologies to support V&V of Nonlinear control	Adaptive Flight control systems	Incorporation & implementation of nonlinear control designs into an integrated flight control system which is valid throughout nonlinear operating envelope of a modern transport aircraft is often problematic; Monte Carlo-based analysis and simulations often costly and require revalidation	Develop V&V techniques applicable to nonlinear control systems to expand acceptance of highly nonlinear, coupled vehicle dynamics models within the controller
DS	Common V&V processes for facilitating Integration of Aircraft Systems (to Increase Performance)	Aircraft flight critical systems	Flight performance improvement can be achieved through integrating aircraft subsystems	Develop V&V processes and structure for V&V design to facilitate efficient integration and testing
SIS	Software process for enabling rigorous, comprehensive analysis of FCS system	Flight critical systems	Advances in flight control technology outpacing software verification techniques	Formulate transformative process for enabling certifiable and cost-effective analyses of the safety aspects for adaptive flight critical system software
SA	Unified approach for specifications/requirements at system level	Flight critical systems	Lack of formal interaction semantics specification	Techniques for specifying interactive properties and automatic verification Ontology that can be queried about inferences and potential ramifications of a requirement or spec through life cycle
DS	Architectural modeling and analysis	Flight critical systems	Large systems consisting of networks of interacting components remain a challenge for V&V techniques	Fault tolerance methods; virtual machine infrastructures; mixed criticality components
DS	Architectural modeling and analysis	Flight critical systems	Large systems consisting of networks of interacting components remain a challenge for V&V techniques	Provide research to provide V&V methods for system integration that validate system is performing as desired architecture modeling reasoning methods for sync and async communications compositional reasoning methods that verify capable operation in the face of reduced or eliminated system assets.
SA DS	Unified approach for specifications/requirements at system level	Flight critical systems	Control system V&V cost and schedule challenges have become so great that they now constrain industry's ability to introduce new and upgrade existing aerospace products; innovation barriers	Safety based decomposition through dependability cases Formal Analysis tools
SIS	Model based software engineering	Flight critical systems	Although a number of tools are available, difficulties arise in producing an integrated environment that allows for seamless operation over models representing numerous aspects of analysis and synthesis	Integrated V&V environments for testing
SA DS	Unified approach for specifications/requirements at system level	Flight critical systems	Lack of design modeling techniques at the system level	Effective notation standards for specifying requirements; standardization and acceptance of modeling notations and tools; architecture specification of processing/communication resources; interconnections among the functional components;

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
01- 06 - 2010	Technical Memorandum	

4. TITLE AND SUBTITLE
Verification and Validation for Flight-Critical Systems (VVFCS) - Summary of Responses to Solicitation Number NNH09ZEA001L, April 2009

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Graves, Sharon S.; Jacobsen, Robert A.

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
NASA Langley Research Center
Hampton, VA 23681-2199

8. PERFORMING ORGANIZATION REPORT NUMBER
L-19885

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
National Aeronautics and Space Administration
Washington, DC 20546-0001

10. SPONSOR/MONITOR'S ACRONYM(S)
NASA

11. SPONSOR/MONITOR'S REPORT NUMBER(S)
NASA/TM-2010-216715

12. DISTRIBUTION/AVAILABILITY STATEMENT
Unclassified - Unlimited
Subject Category 01
Availability: NASA CASI (443) 757-5802

13. SUPPLEMENTARY NOTES

14. ABSTRACT

On March 31, 2009 a Request for Information (RFI) was issued by NASA's Aviation Safety Program to gather input on the subject of Verification and Validation (V & V) of Flight-Critical Systems. The responses were provided to NASA on or before April 24, 2009. The RFI asked for comments in three topic areas: Modeling and Validation of New Concepts for Vehicles and Operations; Verification of Complex Integrated and Distributed Systems; and Software Safety Assurance. There were a total of 34 responses to the RFI, representing a cross-section of academic (26%), small & large industry (47%) and government agency (27%).

15. SUBJECT TERMS
Flight safety; Flight-critical systems; Validation; Verification

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			STI Help Desk (email: help@sti.nasa.gov)
					19b. TELEPHONE NUMBER *(Include area code)*
U	U	U	UU	17	(443) 757-5802