



Projected Impact of Compositional Verification on Current and Future Aviation Safety Risk

*Mary S. Reveley and Colleen A. Withrow
Glenn Research Center, Cleveland, Ohio*

*Karen M. Leone
Vantage Partners, LLC, Brook Park, Ohio*

*Sharon M. Jones
Langley Research Center, Hampton, Virginia*

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 Reports Server, thus providing one of the largest collections of aeronautical and space science STI in the world. Results are published in both non-NASA channels and by NASA in the NASA STI Report Series, which includes the following report types:

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

- **CONFERENCE PUBLICATION.** Collected papers from scientific and technical conferences, symposia, seminars, or other meetings sponsored or cosponsored 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, 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 to help@sti.nasa.gov
- Fax your question to the NASA STI Information Desk at 443-757-5803
- Phone the NASA STI Information Desk at 443-757-5802
- Write to:
STI Information Desk
NASA Center for AeroSpace Information
7115 Standard Drive
Hanover, MD 21076-1320



Projected Impact of Compositional Verification on Current and Future Aviation Safety Risk

*Mary S. Reveley and Colleen A. Withrow
Glenn Research Center, Cleveland, Ohio*

*Karen M. Leone
Vantage Partners, LLC, Brook Park, Ohio*

*Sharon M. Jones
Langley Research Center, Hampton, Virginia*

National Aeronautics and
Space Administration

Glenn Research Center
Cleveland, Ohio 44135

Acknowledgments

Thanks are extended to the managers and researchers of the National Aeronautics and Space Administration's Systems-Wide Safety and Assurance Technologies Project and the Federal Aviation Administration's Joint Planning and Development Office for providing information key to this study.

Trade names and trademarks are used in this report for identification only. Their usage does not constitute an official endorsement, either expressed or implied, by the National Aeronautics and Space Administration.

Level of Review: This material has been technically reviewed by technical management.

Available from

NASA Center for Aerospace Information
7115 Standard Drive
Hanover, MD 21076-1320

National Technical Information Service
5301 Shawnee Road
Alexandria, VA 22312

Available electronically at <http://www.sti.nasa.gov>

Projected Impact of Compositional Verification on Current and Future Aviation Safety Risk

Mary S. Reveley and Colleen A. Withrow
National Aeronautics and Space Administration
Glenn Research Center
Cleveland, Ohio 44135

Karen M. Leone
Vantage Partners, LLC
Brook Park, Ohio 44142

Sharon M. Jones
National Aeronautics and Space Administration
Langley Research Center
Hampton, Virginia 23681

Summary

The projected impact of compositional verification research conducted by the National Aeronautic and Space Administration System-Wide Safety and Assurance Technologies on aviation safety risk was assessed. Software and compositional verification was described. Traditional verification techniques have two major problems: testing at the prototype stage where error discovery can be quite costly and the inability to test for all potential interactions leaving some errors undetected until used by the end user. Increasingly complex and nondeterministic aviation systems are becoming too large for these tools to check and verify. Compositional verification is a “divide and conquer” solution to addressing increasingly larger and more complex systems. A review of compositional verification research being conducted by academia, industry, and Government agencies is provided. Forty-four aviation safety risks in the Biennial NextGen Safety Issues Survey were identified that could be impacted by compositional verification and grouped into five categories: automation design; system complexity; software, flight control, or equipment failure or malfunction; new technology or operations; and verification and validation. One capability, 1 research action, 5 operational improvements, and 13 enablers within the Federal Aviation Administration Joint Planning and Development Office Integrated Work Plan that could be addressed by compositional verification were identified.

1.0 Introduction

1.1 Background

Public benefits resulting from continued growth in the air transport of passengers and cargo depend on improvements in the inherent safety features of current and future aircraft that will operate in the Next Generation Air Transportation System (NextGen). The NASA Aviation Safety Program (AvSP) is addressing this challenge by conducting foundational research and developing innovative tools, concepts, and technologies to overcome the growing demands and problems that will be created by the nation’s transition to NextGen.

The System-Wide Safety and Assurance Technologies (SSAT) project, part of the AvSP, will identify risks and provide knowledge required to safely manage increasingly complex aircraft design and operation, and the air transportation system. The SSAT project is focused on methods to assess and

ensure complex aviation system-wide safety for the NextGen by addressing the following four technical challenges (TCs):

TC1: Assurance of flight critical systems: Fill a critical gap in life-cycle development of complex systems for NextGen by developing verification and validation (V&V) techniques that prove that new technologies envisioned for NextGen are as safe, or safer than, the current system and by providing a cost-effective basis for assurance and certification of complex civil aviation systems by fiscal year (FY) 2025.

TC2: Discovery of safety incidents: Discover the precursors to aviation safety incidents through automated mining of massive heterogeneous data sets to enable proactive risk management by FY 2019.

TC3: Automation design tools: Enable development of robust human-automation systems by incorporating known human performance limitations into analysis tools by FY 2020.

TC4: Prognostic algorithm design of safety assurance: Explore processes (including algorithm design) for verifiability of system health management algorithms, thus removing obstacles to certification while enabling their deployment by industry to take advantage of their safety benefits by FY 2025.

This study is focused on a portion of the research being conducted under TC1, specifically, compositional verification. The research goal is to demonstrate that V&V of complex systems can be derived through decomposition from V&V results on system components. This will have an impact on scalability, reuse, and system evolution (Ref. 1).

1.2 Objectives

The primary objective of systems analysis is to provide information to the SSAT management team regarding the projected impact of the SSAT research portfolio on its aviation safety goals with particular attention paid to the system-wide analyses of the air transportation system. This objective is achieved through: (1) statistical analyses, (2) qualitative portfolio analyses, (3) high-level systems analyses, and (4) external collaboration. All of these analyses will assist the SSAT project team in prioritizing and adjusting the SSAT portfolio throughout the life of the project (Ref. 1).

To assist the management in achieving this objective, several systems analysis milestones have been specified in the SSAT project plan (Ref. 1). The systems analysis milestone addressed in this study is focused on compositional verification research contained within TC1. Specifically, this study will assess the projected impact of the implementation of compositional verification on current and future aviation safety risk using a combination of high-level and qualitative systems analyses.

The study has four components:

- (1) Summarized software verification and more specifically compositional verification
- (2) Reviewed compositional verification research being conducted by academia, industry, and Government agencies
- (3) Identified current and future safety risks compiled in the Biennial NextGen Safety Issues Survey (BNSIS) Database (Ref. 2) that could be impacted by the implementation of compositional verification

(4) Identified Joint Planning and Development Office (JPDO) operational improvements (OIs), enablers, research actions (RAs), development plans, and policy issues that are directly related to compositional verification

2.0 Compositional Verification Research

2.1 Verification of Flight-Critical Systems

Software verification assures that the software fully satisfies expected requirements. Various software verification methods include:

Testing using different scenarios—may be enough for conventional software, but falls short for complex systems software (Ref. 3).

Run-time monitoring—typically requires little computing resources, but can produce uncertain results and false negatives.

Theorem proving—occurs during the requirements phase and involves a lot of analyst effort and skill, and is mostly limited to a few academic studies (Ref. 4).

Model checking—used during the software development requirements and design phases. This approach advocates automatically checking software for specific design flaws. The biggest problem with model checking today is the state explosion problem (the number of states of even a relatively small system is often far greater than can be handled in a realistic computer).

Static analysis—explores the structure of the source code without execution.

Compositional verification—refer to the descriptions below.

2.2 Compositional Verification

Traditional verification techniques of testing and simulation have two major problems: testing at the prototype stage where error discovery can be quite costly, and the inability to test for all potential interactions leaves some errors undetected until use by the end user (flight crew) (Ref. 5). Formal software verification techniques such as model checking are useful in detecting errors, however, increasingly complex and nondeterministic aviation systems are becoming too large for these tools to verify (Ref. 6). One solution is the “divide and conquer” strategy used by compositional verification (Ref. 7). Larger and more complex systems are divided into smaller components (models) and are verified separately. The smaller components are then recombined and verified by checking the assumptions about the environment, guarantees provided by the components, and facts provided by design patterns (Ref. 8).

Compositional verification research is being conducted by academia, industry, research laboratories, and Government agencies. Table 1 to Table 4 show some of the recent research published (1997 to 2012) by research institutes, academia, industry, and Government agencies. The majority was performed by a wide range of academic institutions, NASA, and the Research Institute for Advanced Computer Science (RIACS), a close collaborator with NASA.

3.0 Compositional Verification Impact on Aviation Safety

Events that impact safety caused by unintended or unforeseen software failures and unanticipated behaviors have already occurred. In a final report regarding Qantas Flight 72 in 2008 where 110 people were injured, Australian Transport Safety Bureau investigators found that a programming error was partly to blame after a computer component failed. The airplane software was not written to handle a specific event in which an air data inertial reference unit produced erroneous data at regular intervals (Ref. 9). “Because the behavior of complex systems is increasingly controlled by software, software can have a significant impact on safety and reliability” (Ref. 10). For a qualitative look at the possible impacts that compositional verification might have on current and future aviation safety risk, the SSAT Systems Analysis Team identified any relevant safety issues in the recently published BNSIS (Ref. 2).

3.1 Biennial NextGen Safety Issues Survey

The JPDO Safety Working Group conducted the BNSIS (Ref. 2) to identify current and future safety issues for updating the National Aviation Safety Strategic Plan (Ref. 11). Stakeholders were asked what their five most current and future safety concerns were. These stakeholders included more than 330 subject matter experts in the global aviation community senior managers, operators, maintenance personnel, researchers, designers, manufacturers, service providers, regulators, as well as members of standard setting organizations, government-industry groups, and industry and labor associations.

The survey was completed by 102 subject matter experts. The SSAT Systems Analysis Team reviewed the survey database to identify those safety concerns that could be related to compositional verification and those that could be positively impacted by compositional verification. Of the 816 safety concerns cited, 44 were identified as possibly being impacted by the implementation of compositional verification.

A variety of safety issues, 22 current and 27 future, that could be impacted by compositional verification, were cited and organized into the following five categories:

- Automation design
- System complexity
- Software, flight control, or equipment failure or malfunction
- New technology or operations
- Verification and validation

Table 5 to Table 13 provide details about the respondents’ current and future safety issues and descriptions. Table 14 shows the number of current and future NextGen safety issues by category that could be impacted by compositional verification.

3.1.1 Automation Design

Table 5 and Table 6 show the five current and future safety issues associated with automation design. Automation is the allocation of functions to machines that would otherwise be allocated to humans. The term is also used to refer to the machines that perform those functions. Flight deck automation, therefore, consists of machines on the commercial transport aircraft flight deck which perform functions otherwise performed by pilots. Current flight deck automation includes autopilots, flight management systems, electronic flight instrument systems, and warning and alerting systems” (Ref. 12). Automation may work well under normal conditions but, due to design limitations, may not have the desired behavior under unusual conditions, such as those close to the operating margins of its operating envelope (Ref. 13).

Subject matter experts' concern for the future include inadequate software tools, systems not failing “eloquently,” the increasing reliance on software to operate properly, the need for increased analytic capabilities, and the vulnerability to hacking.

3.1.2 System Complexity

Table 7 shows the eight current safety issues and Table 8 shows the six future safety issues associated with system complexity. Virtually all software on aircraft today is growing in size and complexity. This rapid growth poses a serious challenge in the ability to verify the reliability of these complex safety-critical software systems (Ref. 14).

Compositional verification is a method for assuring the safety of these flight critical systems. The issues cited in the BNSIS include inadequate design assurance and risks associated with increasingly complex systems where errors have not always been identified before use of the software on aircraft in an operational environment. An example is seen in a 2006 incident involving an Airbus 340–642. A data bus failure to monitor fuel levels and flow caused one engine to lose power and another to fluctuate. Faulty software logic prevented a working backup computer from being selected (Ref. 15).

3.1.3 Software, Flight Control, or Equipment Failure or Malfunction

Table 9 shows the seven current safety issues and Table 10 shows the two future safety issues associated with software, flight control, or equipment failure or malfunction. While Table 5 to Table 8 cite automation design and system complexity as underlying causes, Table 9 and Table 10 cite failures without causes. These failures and malfunctions may have been related to software errors that were not detected during the verification process. Compositional verification could find these errors more cost effectively before pilots are confronted by potential failures.

3.1.4 New Technology or Operations

Table 11 shows the six future safety issues associated with the introduction of new technology or operations. Like software, flight control, or equipment failure or malfunction, this new technology or operations category does not cite specific causes. Only the difficulty of conducting adequate safety assurance process and the lack of knowledge regarding possible impacts of new technology or operations implementation are mentioned.

3.1.5 Verification and Validation

Finally, Table 12 shows the six current safety issues and Table 13 shows the eight future safety issues related to V&V. Verification in general and also as a part of the software safety assurance process is a key portion of the design and development of safe aircraft operations. Development of new V&V capabilities will provide new safety assurance capabilities for current generation aviation software, which has been implicated in anomalous in-flight behavior (Ref. 7). The current and future safety issues identified stress the importance of large complex systems.

3.1.6 Biennial NextGen Safety Issues Survey Summary

The 44 BNSIS safety issues that could be impacted by the implementation of compositional verification are grouped together in categories and include those shown in Table 14. The most frequently cited safety issues that could be impacted by compositional verification were in the system complexity, and the V&V categories.

3.2 Joint Planning and Development Office Integrated Work Plan

The FAA JPDO released its latest Integrated Work Plan (IWP) in 2011. “The IWP supports the collaborative planning and deliberation required among partners and stakeholders to prioritize needs, establish commitments, coordinate efforts, and focus resources on the work needed to achieve NextGen.” (Ref. 16). Capabilities, OIs, RAs, and enablers needed to achieve the FY2025 NextGen vision as defined in the Concept of Operations listed in the IWP (Ref. 17). Systems analysts reviewed the capabilities, OIs, RAs, and enablers and identified those that could be addressed by compositional verification.

3.2.1 Capabilities

The JPDO “Improved safety operations” capability directly relates to compositional verification specifically in the area of safety assurance techniques that are consistent and compatible with national and international regulations, standards, and procedures. This capability ensures safety considerations are fully integrated throughout the air transportation system by increasing collaboration and sharing information, improving automation (e.g., decision support systems), performing prognostic safety risk analysis, and promoting enhanced safety and assurance techniques that are consistent and compatible with national and international regulations, standards, and procedures.

3.2.2 Research Actions

The JPDO RA R-1440, “Applied Research on Complex Systems Validation and Verification,” directly relates to the need for compositional verification methods and algorithms that go beyond those for less complex systems. Complex systems provide multiple functions that support many different operating models, environments, and technologies and therefore, require more advanced and integrated methods. Research will support development of complex systems, their risk assessment, and eventual certification decisions.

3.2.3 Operational Improvements

OIs describe either an operational transformation or the improved level of performance needed to achieve the FY2025 NextGen vision, defined in the JPDO concept of operations (Ref. 17). Compositional verification directly relates to the five JPDO OIs shown in Table 15.

OI-3004, “Improved operational processes using safety management systems (SMS),” addresses equipment certification. Certifying increasingly complex, integrated modular avionics architectures will require new verification techniques such as compositional verification (Ref. 18). OI-3102, improved safety for NextGen evolution, addresses the need for improved V&V techniques that directly support certification of new complex systems. OI-3104, “Enhanced safety of airborne systems,” addresses aircraft reliability, an area directly addressed by compositional verification. OI-3105, “Enhanced safety of ground-based systems,” addresses the reliability of ground-based systems, and OI-3018, “Improved SMS standards and effectiveness,” applies to safety assurance practices. Compositional verification addresses both OI-3105 and EN-3108.

3.2.4 Enablers

Enablers are material or nonmaterial solutions that support an improved level of performance in an OI or another enabler (Ref. 17). The 12 JPDO enablers presented in Table 16 address a variety of safety assurance methods, improved fault management, advances in V&V, increased reliability, and system health management in both vehicle and groundbased systems. Compositional verification addresses these 12 enablers. Enablers related to OIs are also presented in Table 14.

3.2.5 Joint Planning and Development Office Summary

The JPDO IWP was reviewed to identify elements that could be impacted by the implementation of compositional verification. Of these, one capability, one research action, five operational improvements, and thirteen enablers were identified that could be impacted by the compositional verification. A summary of these elements is presented in Table 17.

4.0 Discussion and Conclusions

This analysis presented an overview of the variety of methods available for software verification: testing, run-time monitoring, theorem proving, model checking, static analysis, and compositional verification. Traditional verification techniques have two major problems: testing at the prototype stage where error discovery can be quite costly and the inability to test for all potential interactions leaving some errors undetected until use by the end user (flight crew). Increasingly complex and nondeterministic aviation systems being checked are becoming too large for these tools to verify. Compositional verification is a “divide and conquer” solution to addressing increasingly larger and more complex systems by dividing systems into smaller components and verifying them separately. The components are then recombined and verified by checking the environmental assumptions.

Compositional verification research has been conducted by academia, research institutes, industry, and Government agencies across the world. The majority of this research today has been conducted by a wide range of academic institutions and the collaboration between the Research Institute for Advanced Computer Science (RIACS) and NASA.

Because the behavior of complex systems is increasingly controlled by software, software could have a more significant impact on safety and reliability. The Biennial NextGen Safety Issues Survey was reviewed to identify current and future safety issues that could be impacted by the successful implementation of compositional verification. The survey was completed by 102 subject matter experts resulting in 816 distinct current and future aviation safety issues. Of these, 44 were identified as having the possibility of being impacted by the implementation of compositional verification. These safety issues were grouped together in categories:

- Automation design
- System complexity
- Software, flight control or equipment failure or malfunction
- New technology or operations
- Verification and validation

The most frequently cited safety issues were in the system complexity and the V&V categories.

The Joint Planning and Development Office (JPDO) Integrated Work Plan (IWP) capabilities, operational improvements (OIs), research actions (RAs), and enablers were reviewed to identify those that could be impacted by the implementation of compositional verification. Of these, 1 capability, 1 RA, 5 OIs, and 13 enablers were identified that could be impacted by the implementation of compositional verification.

If compositional verification can be successfully implemented, it could help verify and validate large complex systems. Compositional verification has also been found to address a wide variety of identified current and potential future safety issues, as well as JPDO IWP elements.

TABLE 1.—RESEARCH PUBLICATIONS BY RESEARCH INSTITUTE

| Institute | Title | Author | Forum |
|---------------------------------|---|---|---|
| RIAC ^a | Automated Assume-Guarantee Reasoning by Abstraction Refinement | Mihaela Gheorghiu Bobaru, Corina Pasareanu, Dimitra Giannakopoulou | 20 th International Conference on Computer-Aided Verification, July 2008, Princeton, New Jersey |
| RIAC | Composing Safety Systems | John Rushby | 8 th International Symposium on Formal Aspects of Component Software, September 2011, Oslo, Norway |
| RIAC | Modular Certification | John Rushby | CSL Technical Report, funded by NASA, DARPA, and Honeywell, June 2002 |
| RIAC | Component Verification with Automatically Generated Assumptions | Dimitra Giannakopoulou | Journal of Software Engineering, July 2005 |
| RIAC | A Robust Compositional Architecture for Autonomous Systems | Guillaume Brat, Ewen Denney, Kimberley Farrell, Dimitra Giannakopoulou, Ari Jonsson, Jeremy Frank, Mark Boddy, Todd Carpenter, Tara Estlin, Mihail Pivtoraiko | Aerospace Conference, IEEE 2006, March 2006, Big Sky, Montana |
| RIAC | Learning Assumptions for Compositional Verification | Jamieson Cobleigh, Dimitra Giannakopoulou, Corina Pasareanu | TACAS'03 Proceedings of the 9th international conference on Tools and algorithms for the construction and analysis of systems, April 2003, Warsaw, Poland |
| National Institute of Aerospace | Compositional Verification of a Communication Protocol for a Remotely Operating Vehicle | Cesar Munoz, Alwyn Goodloe | 14 th International Workshop of Formal Methods for Industrial Critical Systems, November 2009, Eindhoven, The Netherlands |

^aResearch Institute for Advanced Computer Science

TABLE 2.—RESEARCH PUBLICATIONS BY ACADEMIA

| University or college | Title | Author | Forum |
|---|---|--|--|
| Georgia Institute of Technology | A complete compositional reasoning framework for the efficient verification of pipelined machines | Panagiotis Manolios | ICCAD-2005, International Conference on Computer-Aided Design, November 2005, San Jose, California |
| University of Illinois | Compositional Verification of Architectural Models, presentation | Lui Sha | Safe & Secure Systems & Software Symposium AFRL, June 2012, Fairborn, Ohio |
| University of Minnesota | Compositional Verification of Architectural Models, presentation | Michael Whalen | Safe & Secure Systems & Software Symposium AFRL, June 2012, Fairborn, Ohio |
| West Virginia University | A Component-based Approach to Verification and Validation of Formal Software Models | Dejan Desovski | Dissertation, 2006 |
| Oxford University, Oxford, England | Compositional Verification of Probabilistic Systems Using Learning | Lu Feng, Marta Kwiatkowska, David Parker | 7th International Conference on Quantitative Evaluation of Systems, September 2010, Williamsburg, Virginia |
| University of Manchester, Manchester, England | Component Verification with Automatically Generated Assumptions | Howard Barringer | Journal of Software Engineering, July 2005 |

TABLE 2.—RESEARCH PUBLICATIONS BY ACADEMIA

| University or college | Title | Author | Forum |
|---|---|---|--|
| University of Toronto, Toronto, Canada | Automated Assume-Guarantee Reasoning by Abstraction Refinement | Mihaela G. Bobara | 20th International Conference on Computer-Aided Verification, July 2008, Princeton, New Jersey |
| University of Kaiserslautern, Kaiserslautern, Germany | Compositional Reasoning I Model-Based Verification of Adaptive Embedded Systems | Ina Schaefer, Arnd Poetzsch-Heffter | 6th IEEE Conference on Software Engineering and Formal Methods, November 2008, Cape Town, South Africa |
| Univ. des Saarlandes, Saarbrücken, Germany | Synthesizing certificates in networks of timed automata | H. Peter, B. Finkbeiner | 2008 Real-Time Systems Symposium, Nov. 30 to Dec. 3, 2008, Barcelona, Spain |
| Vrije Universiteit, Amsterdam, Netherlands | Compositional Verification of Knowledge-Based Systems: a case study in Diagnostic Reasoning | Frank Cornelissen, Catholijn Jonker | 10th European Workshop on Knowledge Acquisition, Modeling and Management, October 1997, Catalonia, Spain |
| Verimag Academic Research Center, Grenoble, France | Compositional Verification for Component Based Systems and Application | S. Bensalem, M. Bozga, T.-H. Nguyen, J. Sifakis | IET Software, Volume 4, Issue 3, June 2010, p. 181-183 |
| Charles University, Prague, Czech Republic | Assume-Guarantee Verification of Software Components in SOFA 2 Framework | P. Parizek | IET software, Volume 4, Issue 3, June 2010, p. 210-221. |
| University of Lugano, Lugano, Switzerland | Interface Decomposition for Service Compositions | Domenico Bianculli; Dimitra Giannakopoulou, Corina S. Pasareanu | Software Engineering (ICSE), 2011 33rd International Conference on IEEE, 2011, Waikiki, Honolulu |

TABLE 3.—RESEARCH PUBLICATIONS BY INDUSTRY

| Company | Title | Author | Forum |
|--|--|---|---|
| WW Technology Group, Ellicott City, Maryland | Compositional Verification of Architectural Models, presentation | Chris Walter, Brian LaValley | Safe & Secure Systems and Software Symposium, AFRL, June 2012, Fairborn, Ohio |
| Fujitsu Labs, Sunnyvale, California | Environment Generation for Validating Event-Driven Software Using Model Checking | O. Tkachuk | IET Software, Volume 4, Issue 3, June 2010, p. 194-2009 |
| Rockwell Collins, Minneapolis-St Paul, Minnesota | Compositional Verification of Architectural Models [presentation] | Darren Cofer, Steven Miller, Andrew Gacek | Safe & Secure Systems and Software Symposium, AFRL, June 2012, Fairborn, Ohio |
| Smart Information Flow Technologies, Minneapolis, Minnesota | Prismatic: Unified Hierarchical Probabilistic Verification tool | David Musliner, Eric Engstrom | Final Report to DARPA and AFRL, September 2011, Report number AFRL-RZ-WP-TR-2011-2097 |
| Adventum Enterprises, Minneapolis, Minnesota | A Robust Compositional Architecture for Autonomous Systems | Guillaume Brat, Ewen Denney, Kimberley Farrell, Dimitra Giannakopoulou, Ari Jonsson, Jeremy Frank, Mark Boddy, Todd Carpenter, Tara Estlin, Mihail Pivtoraiko | Aerospace Conference, IEEE 2006, March 2006, Big Sky, Montana |

TABLE 4.—RESEARCH PUBLICATIONS BY GOVERNMENT AGENCIES

| Agency | Title | Author | Forum |
|---|---|---|---|
| Tsinghua National Laboratory for Information Science and Technology, Beijing, China | Data Mining Based Decomposition for Assume-Guarantee Reasoning | He Zhu, Fei He, William Hung, Xiaoyu Song, Mig Gu | Formal Methods in Computer-Aided Design, 2009. FMCAD, November 2009, Austin, Texas |
| Office national d'études et de recherches aérospatiales (ONERA), the French Aerospace Lab, Meudon, France | A Framework for Heterogeneous Formal Modeling and Compositional Verification of Avionics Systems | Yamine Ait-Ameur, Remi Delmas, Virginie Weils | International Conference on Formal Methods and Models for Co-Design, June 2004, San Diego, California |
| NASA, Hampton, Virginia | Baseline Assessment and Prioritization Framework for IVHM Integrity Assurance Enabling Capabilities | Eric Cooper, Benedetto Di Vito, Stephen Jacklin, Paul Miner | June 2009, NASA/TM—2009-215764 |
| NASA, Mountain View, California | Automated Compositional Verification Editorial | Dimitra Giannakopoulou | Editorial in IET Software Journal, Volume 4, Issue 3, June 2010, p. 179-180 |
| NASA, Mountain View, California | Compositional Verification for Discovering Failures in Adaptive Flight Control Systems | Sarah Thompson, Misty Davies, Karen Gundy-Burlet | AIAA InfoTech, November 2009, Seattle, Washington |
| NASA, Mountain View, California | “Fly me to the Moon.” Verification of Aerospace Systems | Dimitra Giannakopoulou | 8 th IEEE International Conference on Software Engineering and Formal Methods, May 2010 |
| NASA, Mountain View, California | Hybrid Decompositional Verification for Discovering Failures in Adaptive Flight Control Systems | Sarah Thompson, Misty Davies, Karen Gundy-Burlet | AIAA InfoTech, April 2010, Atlanta, Georgia |
| NASA, Mountain View, California | Interface Decomposition for Service Compositions | Dimitra Giannakopoulou, Corina Pasaeanu | ICSE 2011, Waikiki, Honolulu, May 2011 |
| NASA, Mountain View, California | Towards a Compositional SPIN | Dimitra Giannakopoulou, Corina Pasaeanu | 13 th International SPIN Workshop on Model checking of Software, Vienna, Austria, March 2006 |
| NASA, Mountain View, California | A Robust Compositional Architecture for Autonomous Systems | Guillaume Brat, Ewen Denney, Kimberley Farrell, Dimitra Giannakopoulou, Ari Jonsson, Jeremy Frank, Mark Boddy, Todd Carpenter, Tara Estlin, Mihail Pivtoraiko | Aerospace Conference, IEEE 2006, March 2006, Big Sky, Montana |
| Jet Propulsion Lab, La Canada Flintridge, California | A Robust Compositional Architecture for Autonomous Systems | Guillaume Brat, Ewen Denney, Kimberley Farrell, Dimitra Giannakopoulou, Ari Jonsson, Jeremy Frank, Mark Boddy, Todd Carpenter, Tara Estlin, Mihail Pivtoraiko | Aerospace Conference, IEEE 2006, March 2006, Big Sky, Montana |

TABLE 5.—CURRENT SAFETY ISSUES ASSOCIATED WITH AUTOMATION DESIGN

| Issue | Description |
|---|--|
| Aircraft automation | “The concern is that automation may cause the aircraft to perform in ways that are not understood or [are] uncommanded by the flight crew” |
| Altitude errors | “These can be caused by communication ambiguity, automation issues, pilot monitoring, etc.” |
| Human factors–automation | “Automation can be misleading in that a compelling interface can lead the operator to believe the operator is using the interface properly when in fact they are not. Case in point: ATC [Air traffic Control] sent a data link message confirming the route of flight using the wrong format. The ground automation allowed for the use of the improper format. No error message was generated by the ground automation. The automation onboard the aircraft attempted to process the message as a valid route clearance which caused the navigation computer to skip required waypoints in the intended route clearance. Although the new route clearance did not load properly the flight crew used common procedures they use to correct similar problems. The airborne automation did not generate an error message; it only displayed to the pilots a situation they deal with every day. This would not have been an issue except the particular circumstances which led to this issue were automation interfaces that were compelling to both the pilot and air traffic controller.” |
| Lack of a principled approach in developing automated systems | “Too many band aids are placed on automation without sufficient understanding of the risks associated with application of the band aid.” |
| Overreliance on flight deck automation | “While new pilots have been exposed to and are comfortable with automation and technology, they are also potentially more prone to overdependence on these aids and potentially less resilient when emergencies arise. Increased integration and complexity means that a failure in one system may result in erroneous information propagating to seemingly unrelated systems, leading to pilot confusion or degraded performance of flight control systems. Aircraft designers need to assess the ability of the airplane to gracefully degrade to a pilot-operated configuration from more automatic modes. To prevent pilots from becoming overwhelmed and over reliant on automated systems, the hardware and software will need to be designed to keep the pilot appropriately informed using prioritization schemes or adaptive automation.” |

TABLE 6.—FUTURE SAFETY ISSUES ASSOCIATED WITH AUTOMATION DESIGN

| Issue | Description |
|---|--|
| Automation failures | “Systems still do not display the ability to fail eloquently. They generally just shut down; this is unacceptable for the systems of tomorrow.” |
| Ineffective introduction of automation and software tools | “Automation has functional logic that can be perceived as strange and unpredictable behavior by humans. Adequate design, testing and training will be needed.” |
| The Trophy-for-Every-Child generation | “There is an ever increasing trend in all industries creating a root cause for multiple safety concerns. Modern education has moved away from allowing students to suffer consequences from failure. Therefore, many workers in all industries are starting to perform "success-focused" work in the design and implementation of transportation systems. "Success-focused" work is assumed to function properly as designed or intended. Less thought is being placed on the "what if's" that may occur during the life-cycle of a product or operation. An example of such is the increasing number of failures of high energy density storage devices. No consideration was given to the effects of failures on the transportation system. Many aircraft flight control systems, which are becoming increasingly more neutral to negative in stability, rely heavily on software to operate properly. The software safety aspects of design are not sufficiently robust in their failure analysis, relying heavily on assumptions made during the design in order to successfully achieve a launch of the product by a certain date. However, increased complexity requires increased failure analysis. The limits of technology appear to be exceeding the abilities of the current industry workforce to envision potential downfalls.” |
| Identifying weak signals in large aviation data sets | “Inability to identify the weak signals of impending problems in the large data sets that will grow exponentially in the future. Analytical methods that are not robust when applied to heterogeneous database formats and content. Challenges in integration of legacy and modern data archives. Identification and filtering of erroneous sensor outputs. An effective, proactive, data analysis capability demands that erroneous sensor output must be detected and removed from the data stream or flagged prior to application of analysis software. Increased complexity and heterogeneity of data will require advance analytical capabilities within the assessment platform.” |
| Exposure to potential third-party hacking | “Many systems upgrades, as well as air-ground communications, will be performed via software or without direct human interaction. The potential exists for external agents to intervene or ‘hack into’ these systems.” |

TABLE 7.—CURRENT SAFETY ISSUES ASSOCIATED WITH SYSTEM COMPLEXITY

| Issue | Description |
|---|---|
| Inadequate design assurance for complex flight critical system certification | “All recently certified transport airplane models have suffered breakdowns of flight critical functions that under less benign circumstances would have resulted in a crash. Clearly, the current design assurance processes used for certification do not root out design errors and flight critical function failures that have a probability of occurrence greater than the allowable 10^{-9} /flight hour.” |
| Complexity of design | “Answering safety concerns from regulators has resulted in designs that incorporate complexity with unknown failure modes regardless of hazard analysis. Increased safety through added complexity usually only results in the illusion of added safety.” |
| Risks inherent in increasingly complex systems. | “New, complex systems may exhibit behaviors that bring up new risks.” |
| The impact of future system changes on ANS [Air Navigation System]-wide safety | “Many changes, such as NextGen and SESAR, modifications in avionics, and other trends will change the baseline risk of the ANS [Air Navigation System].” |
| Increasing integration and complexity of systems | “As system complexity increases, unrelated systems may react in a way that the pilot may not be able to properly understand or interpret. As aircraft are equipped with more complex and integrated equipment, training needs to be commensurate with the level of complexity. Heterogeneous equipment and the emergence of new, highly integrated, ground-based and aircraft-based systems are potential sources for this added complexity. There is also a concern that the complexity of a system of systems will exceed our ability to truly understand its characteristics and mitigate safety problems produced by the complexity itself. Addressing organizational considerations implicit within a complex, automated system with multiple interacting agents across highly heterogeneous levels is a current challenge. The civil aviation infrastructure is extraordinarily dependent on computer-telecommunications information systems. Some of the most prominent and widely used systems include those for ATC [Air Traffic Control], navigation, reservations, and aircraft flight control. Increasingly, these information systems have become critical to the spectrum of activities in aviation.” |
| Resilience | “In introducing automation support to ATC [Air Traffic Control] in the form of tools or procedures, further research is needed on what the system needs to remain resilient. The complexity of the system (not necessarily for the ATCo [Air Traffic Controller] or the pilot) should not be increased without modeling what is needed in terms of redundancy.” |
| The continued innovation, development, and integration of automation and safety enhancing technology into GA [general aviation] aircraft. | “[Organization] has seen marked improvements in automation in aviation applications, which has led to significant safety enhancements. However, the complexity of these automated systems has also led to difficulties in certification, human machine interface, and operational reliability in some cases. [Organization] is committed to continuously improving our [development] processes for highly complex systems and our procedures for evaluating and improving the human-machine interface to reduce crew workload and confusion. We are also working to [improve] the testing and evaluation of complex systems to improve operational reliability, availability, accuracy, and ease of use.” |
| Overreliance on flight deck automation | “While new pilots have been exposed to and are comfortable with automation and technology, they are also potentially more prone to overdependence on these aids and potentially less resilient when emergencies arise. Increased integration and complexity means that a failure in one system may result in erroneous information propagating to seemingly unrelated systems, leading to pilot confusion or degraded performance of flight control systems. Aircraft designers need to assess the ability of the airplane to gracefully degrade to a pilot-operated configuration from more automatic modes. To prevent pilots from becoming overwhelmed and over reliant on automated systems, the hardware and software will need to be designed to keep the pilot appropriately informed using prioritization schemes or adaptive automation.” |

TABLE 8.—FUTURE SAFETY ISSUES ASSOCIATED WITH SYSTEM COMPLEXITY

| Issue | Description |
|--|---|
| System will not be coherent in deployment | “It will be a patchwork of different complex systems without a proper systemic safety approach. The human (ATCo [Air Traffic Controller]) will be used to mitigate ” |
| System vulnerability | “System design appears very complex.” |
| Complex system interactions | “The existing level of complexity of aircraft systems has sometimes led to inappropriate crew actions because they do not comprehend the actions being driven by automated systems. This concern will grow as both aircraft systems and air traffic management systems become more highly automated and interactive.” |
| Inadequate attention to the human factors considerations and interactions of air-ground automation | “Various proposals are on the table to change the roles and responsibilities for airborne separation, merging, and spacing. These involve automation aids in the flight deck and at ATC [Air Traffic Control] workstations. The concern is that the perceptual, cognitive, memory, workload, and communication aspects for these software decision support systems have not been given due diligence and that the systems have been developed in isolation rather than in an integrated fashion.” |
| Integrated information systems may allow a single entry point to the entire ANS [Air Navigation System] for a hacker | “Federated systems are only vulnerable by themselves. Integrated information systems may be vulnerable throughout.” |
| System-wide or net-centric information | “Mega systems and SESAR theory” |

TABLE 9.—CURRENT SAFETY ISSUES ASSOCIATED WITH SOFTWARE, FLIGHT CONTROL, OR EQUIPMENT FAILURE OR MALFUNCTION

| Issue | Description |
|---|--|
| Component failure | “The failure of hardware or software that can lead to people being hurt or the loss of an asset.” |
| Equipment outage | “To do the job efficiently, the equipment must work. Impact on the safety of the operation varies depending on what goes out of service. As a general rule any degradation in equipment will affect safety.” |
| Adequate aircraft performance | “This includes all aircraft, structural, propulsion, and equipment failures that result in the aircraft not completing its flight safely.” |
| LOC [Loss of Control] | “The aircraft is no longer proceeding on a trajectory desired by the pilot in command. This may have been caused by exceeding the normal flight envelope into a stall or below VMC, it may be caused by aircraft or flight control system failure, or by extreme weather or turbulence.” |
| Inappropriate high altitude upset recovery techniques | “Engine/flight control malfunction or other disturbance, resulting in the aircraft departing controlled flight.” |
| Overreliance on flight deck automation | “While new pilots have been exposed to and are comfortable with automation and technology, they are also potentially more prone to overdependence on these aids and potentially less resilient when emergencies arise. Increased integration and complexity means that a failure in one system may result in erroneous information propagating to seemingly unrelated systems, leading to pilot confusion or degraded performance of flight control systems. Aircraft designers need to assess the ability of the airplane to gracefully degrade to a pilot-operated configuration from more automatic modes. To prevent pilots from becoming overwhelmed and over reliant on automated systems, the hardware and software will need to be designed to keep the pilot appropriately informed using prioritization schemes or adaptive automation.” |
| UAS [Unmanned Aircraft Systems] | “UAS [Unmanned Aircraft Systems] and their introduction to daily ANS [Air Navigation System] operations; malfunctioning of software and "hacking" of UAS [Unmanned Aircraft Systems] in mid-flight” |

TABLE 10.—FUTURE SAFETY ISSUES ASSOCIATED WITH SOFTWARE, FLIGHT CONTROL, OR EQUIPMENT FAILURE OR MALFUNCTION

| Issue | Description |
|--|---|
| Dependency on technology equipment failure | “As added levels of technology interface with aviation, the probability of failures of the automation or terrorist cyber-attacks increase. What would happen if all the CNS [Communication, Navigation, and Surveillance]/ATM [Air Traffic Management] systems went down in a planned terrorist attack? Are sufficient contingencies and security measures in place to protect us from the ever changing security threats?” |
| Highly integrated critical systems relying on redundant identical technology | “Critical inputs from sensors that are redundant but suffer from common cause environmental failures can create a complex situation for the crew to understand and manage while navigating in the new environment with possible degradation to the navigation systems.” |

TABLE 11.—FUTURE SAFETY ISSUES ASSOCIATED WITH NEW TECHNOLOGY OR OPERATIONS

| Issue | Description |
|---|---|
| New technology | “Data link, satellites, fiber optics, etc.” |
| New operations | “Precision RNAV [Area Navigation], Basic RNAV [Area Navigation], continuous descents, etc.” |
| Inability to introduce innovations | “Due to the high cost, time required, and difficulty of doing safety assurance of new technologies, potential safety solutions may not be introduced” |
| New systems | “NextGen/SESAR interface” |
| New CNS [Communication, Navigation, Surveillance]/ATM [Air Traffic Management] developments | “New operational concepts and systems introduced by NextGen/SESAR” |
| As yet unidentified factors | “With widespread changes in infrastructure, aircraft, environmental constraints, and economic pressure, changes may be implemented without sure knowledge of their impact.” |

TABLE 12.—CURRENT SAFETY ISSUES ASSOCIATED WITH VERIFICATION AND VALIDATION

| Issue | Description |
|--|--|
| Established safety assessment techniques fall short in safety validation of NextGen and SESAR developments | “The established safety assessment techniques are able to evaluate local functionality, but not overall functionality for a system as complex as ATM [air traffic management] is. The consequence is that [with] continued use of established safety assessment techniques, safety risks at overall functionality level do not become visible during the design phases, but only when everything is in operation. Identification and repair of the problems at such [a] late phase may be extremely costly (in economic terms and in terms of loss of lives).” |
| Overreliance on flight deck automation | “While new pilots have been exposed to and are comfortable with automation and technology, they are also potentially more prone to overdependence on these aids and potentially less resilient when emergencies arise. Increased integration and complexity means that a failure in one system may result in erroneous information propagating to seemingly unrelated systems, leading to pilot confusion or degraded performance of flight control systems. Aircraft designers need to assess the ability of the airplane to gracefully degrade to a pilot-operated configuration from more automatic modes. To prevent pilots from becoming overwhelmed and over reliant on automated systems, the hardware and software will need to be designed to keep the pilot appropriately informed using prioritization schemes or adaptive automation.” |
| Integration techniques | “Directed activity that significantly improves integration techniques for airplane impact of common cause failures needs to take place. Currently, these integration techniques are not fully coordinated, resulting in late design changes, certification difficulties, and the potential release of unmitigated common cause failures in service.” |

TABLE 12.—CURRENT SAFETY ISSUES ASSOCIATED WITH VERIFICATION AND VALIDATION

| Issue | Description |
|--|---|
| Verification and validation for large complex systems, or systems of systems | “As systems become larger and more complex the cost of verification and validation using traditional techniques becomes prohibitively expensive. There also needs to be a way to understand the safety implications of introducing a new system in to a large existing system.” |
| Lack of a principled approach in developing automated systems | “Too many band aids are placed on automation without sufficient understanding of the risks associated with application of the band aid.” |
| Potential risks from new and novel designs and design features | “Regulations developed to help ensure aircraft safety may not be adequate.” |

TABLE 13.—FUTURE SAFETY ISSUES ASSOCIATED WITH VERIFICATION AND VALIDATION

| Issue | Description |
|--|---|
| Reliability and redundancy of satellite-based navigation systems | “[Association] is concerned about vulnerability of the GPS [Global Positioning System] satellite constellation to solar flare activity, hacking/sabotage, and or nuclear threats to global security (electromagnetic wave propagation, etc.)” |
| Reliability and redundancy of satellite-based navigation systems | “Reliability and susceptibility to jamming, interference, degradation, etc.” |
| Ability to produce required functionality and reliability in new systems | “Many new systems are being put in place. These concerns are about functionality requirements and, especially, reliability requirements being integrated with acquisitions.” |
| Safe, reliable and affordable flexible separation management | “Given the occasional system-wide disruptions that impact [Air Navigation Service Provider] computers, how can we be confident of error-free traffic separation in an RVSM [Reduced Vertical Separation Minima] and RNAV [Area Navigation] RNP [Required Navigation Performance] environment? How resistant will these decision-support systems be to cyber-attack? Will this be an autonomous "smart" system or will human intervention be possible or necessary?” |
| Safe, reliable and affordable flexible separation margins. | “[Organization] is concerned about the reliability of the air traffic system and the possibility that outages will adversely impact in flight separation margins” |
| Verification and validation for large complex systems or systems of systems | “As systems become larger and more complex the cost of verification and validation using traditional techniques becomes prohibitively expensive. There also needs to be a way to understand the safety implications of introducing a new system into a large existing system.” |
| Both the ANSP [Air Navigation Service Provider] and the ANS [Air Navigation System] user will increasingly depend on automation. | “What type of validation and verification certification testing, and life cycle maintenance validation and verification will be used on both aircraft and ANSP automation system to assure continued airworthiness of total system.” |
| Requirements for off-nominal operations | “Future systems will be designed for optimum conditions. How will designs assure safety is maintained when either systems fail or there are external hazards: weather, wind gusts, sabotage, etc.” |

TABLE 14.—NUMBER OF CURRENT AND FUTURE BIENNIAL NextGen SAFETY ISSUES THAT COULD BE IMPACTED BY COMPOSITIONAL VERIFICATION IMPLEMENTATION

| Category | Current | Future | Total |
|--|---------|--------|-------|
| Automation design | 5 | 5 | 10 |
| System complexity | 8 | 6 | 14 |
| Software, flight control or equipment failure or malfunction | 7 | 2 | 9 |
| New technology or operations | 0 | 6 | 6 |
| Verification and validation | 6 | 8 | 14 |

TABLE 15.—JOINT PLANNING AND DEVELOPMENT OFFICE OPERATIONAL IMPROVEMENTS AND RELATED ENABLERS

| OI ID | OI Name | Description | Related enablers ID | Related enabler name |
|---------|---|--|---------------------|--|
| OI-3004 | Improved operational processes using the safety management system (SMS) | “The risk of incidents and accidents is reduced by the systematic application of standardized safety management processes throughout government and industry. Through a Safety Management System (SMS) construct, organizations will speak the same language regarding safety; safety management processes, tools, and information will be aligned within and among all aviation participants; and organizations will share risk mitigation solutions. This OI provides a consistent approach to achieve an acceptable level of safety risk in the operation of aircraft, certification of procedures and equipment, the conduct of maintenance, etc., and establishes the mechanisms necessary to deliver and monitor safety performance.” | EN-3018 | Safety management requirements |
| OI-3102 | Improved safety for NextGen evolution | “This OI mitigates safety risk associated with the evolution of NextGen by providing enhanced safety methods that support making changes to the air transportation system (ATS), including: advanced capabilities for integrated, predictive safety assessment; improved validation and verification (V&V) processes supporting certification; an enhanced focus on safe operational procedures; and enhanced training concepts for safe system operation. Developers discover and mitigate hazards more quickly allowing the flying public and ATS stakeholders to experience a safety benefit through more rapid and reliable implementation of NextGen systems. An advanced integrated, predictive safety assessment capability will ensure the management of safety risk associated with complex systems and interactions between these systems. It will involve the monitoring of system safety performance to accelerate the detection of unrecognized safety risks and thus contribute to overall safer operational practices. Improved V&V processes will ensure that systems are certified to be reliable enough to perform automated operations, to include recovery from critical failures, without compromising safe operations. Automated operations are necessary to achieve ATS efficiency and capacity benefits. As particular operations become more automated, newly developed operational procedures that involve human interaction must be optimized with assurance that an acceptable level of safety is maintained. Additionally, advanced training concepts will maintain levels of proficiency for humans to conduct safe operations in place of degraded or failed automation.” | EN-3107 | Advanced capabilities for integrated, predictive safety assessment |
| | | | EN-3050 | Advanced complex system validation and verification methods |

TABLE 15.—JOINT PLANNING AND DEVELOPMENT OFFICE OPERATIONAL IMPROVEMENTS AND RELATED ENABLERS

| OI ID | OI Name | Description | Related enablers ID | Related enabler name |
|---------|---|---|---------------------|--|
| OI-3104 | Enhanced safety of airborne systems | “Safety requirements are integrated into the development and implementation of NextGen advancements for aircraft, to maintain or improve safety as changes are introduced. The reliability and airworthiness of aircraft is improved at the sub-system level; vehicle systems health management is improved at the sub-system and system level. The reliability and accuracy of operational information sourced from vehicle systems is improved. Aircraft conformance to more stringent operational requirements is improved, and aircraft system contributions to crash survivability are enhanced.” | EN-3057 | Improved vehicle systems health management—Level 2 |
| | | | EN-3058 | Increased reliability and accuracy of data and information—Level 1 |
| | | | EN-3059 | Increased reliability and accuracy of data and information—Level 2 |
| | | | EN-3113 | Improve reliability and airworthiness of aircraft |
| OI-3105 | Enhanced safety of ground-based systems | “Safety requirements are integrated into the development and implementation of NextGen advancements for ground-based systems, to maintain or improve safety as changes are introduced. Ground-based systems health management is improved at the sub-system and system level. Ground-based systems support more stringent operational requirements, and contribute to enhanced crash survivability.” | EN-3066 | Improved ground-based systems health management—Level 1 |
| | | | EN-3067 | Improved ground-based systems health management—Level 2 |
| OI-3108 | Safety assurance processes and tools | “The Joint Planning and Development Office (JPDO) members and the organizations they oversee demonstrate continuous improvement in the processes, tools, and procedures associated with safety management through incorporation of lessons learned and best practices in the implementation of the national Safety Management System (SMS) Standard ensuring the continuous improvement of safety. SMS practices (e.g., safety policy, safety risk management, safety assurance, and safety promotion) are more effective as improvements are institutionalized after initial SMS implementation. Overall safety of national aviation system-wide processes is improved.” | EN-3027 | Improved fault management |
| | | | EN-3102 | Safety risk management processes and tools |
| | | | EN-3103 | Safety assurance processes and tools |

TABLE 16.—JOINT PLANNING AND DEVELOPMENT OFFICE ENABLERS

| ID Number | Name | Description |
|-----------|---|--|
| EN-3018 | Safety management requirements | “A systematic approach to safety management, which has as its cornerstones safety policy, Safety Risk Management (SRM), safety assurance, and safety promotion, provides a deliberate process for ensuring system safety. Generally referred to as a Safety Management System (SMS), the integrated elements of this systematic approach establish safety accountability at all levels within an organization, using quality management principles to identify and control safety risk. The SMS will promote the understanding, measurement, and improvement of the organization's safety culture. Providing a consistent framework for SMS throughout the government and industry will allow the creation of a system of SMS systems which will support the establishment of accountability at all levels within the Air Transportation System (ATS) and reliance on the cornerstones identified above for safety management. Requirements for safety policy with appropriate organizational support will be promulgated through the establishment of a National SMS Standard. In addition, the national SMS Standard will facilitate alignment and integration of SMSs at the national level.” |
| EN-3027 | Improved fault management | “Fault management involves both prevention of and preparation for faults and failures. Planning for successful mitigation and management of these occurrences, and creating plans for system continuity, despite failures, contributes to a safe system. Tools and processes are needed that focus on managing the systemic impact of off-nominal conditions, and on developing a greater understanding of the propagation of fault and failure effects through systems. Implementation of fault prevention, fault tolerance, and fault recovery tools and processes will increase the robustness of the NextGen system by enabling tolerance of non-ideal conditions without compromising safety. The tools and processes will include linkages to the design assumptions in the enterprise and system architectures. These architectures will be analyzed for their potential for system risk propagation and designs will be recommended that make the system less likely to propagate risk.” |
| EN-3050 | Advanced complex system validation and verification methods | “Advanced tools and processes are developed to improve the verification and validation of complex systems and software. Improvements will focus on reducing the time and resources needed to conduct validation and verification as well as improving the quality of the results. The advanced tools and processes will be created using the combined results of analysis, research and development. Advanced tools and processes such as fast time, real time, and human in the loop simulations will be used to test and evaluate complex systems and software. They will replace and substitute for exhaustive testing. The tools and processes will provide estimates of system risks associated with complex system and software deployment. They will use standards protocols for system simulation and support the creation of a standard protocol for implementation. The tools and processes will establish the minimum acceptability criteria and risk standards applied for Validation and Verification (V&V).” |
| EN-3056 | Improved vehicle systems health management—Level 1 | “As design guidelines are developed (continuous), implement technologies that reduce systems failures or impact of failures that occur. An important part of the aircraft is the vehicle health monitoring system. Advanced monitoring systems will integrate information from various sensors to not only identify and mitigate sub-system failures, but send information to dispatch and maintenance so that trends may be assessed to avert potential failures. The performance measure is reduced systems failures or reduced impact of those failures that occur. (Level 1 - less difficult improvements, component level).” |
| EN-3057 | Improved vehicle systems health management—Level 2 | “As design guidelines are developed (continuous), implement technologies that reduce systems failures or impact of failures that occur. An important part of the aircraft is the vehicle health monitoring system. Advanced monitoring systems will integrate information from various sensors to not only identify and mitigate sub-system failures, but send information to dispatch and maintenance so that trends may be assessed to avert potential failures. The performance measure is reduced systems failures or reduced impact of those failures that occur. (Level 2 - difficult improvements, total vehicle health)” |
| EN-3066 | Improved ground-based systems health management—Level 1 | “As design guidelines are developed (continuous), implement and deploy technologies that reduce systems failures or impact of failures that occur. These ground-based systems will manage information flow, aid in decision-making, and perform monitoring functions to reduced systems failures or reduced impact of failures that occur. (Level 1 - less difficult improvements, component level) |

TABLE 16.—JOINT PLANNING AND DEVELOPMENT OFFICE ENABLERS

| ID Number | Name | Description |
|-----------|--|--|
| EN-3067 | Improved ground-based systems health management—Level 2 | “As design guidelines are developed (continuous), implement and deploy technologies that reduce systems failures or impact of failures that occur. These ground-based systems will manage information flow, aid in decision-making, and perform monitoring functions to reduced systems failures or reduced impact of failures that occur. (Level 2 - difficult, system level, new design)” |
| EN-3058 | Increased reliability and accuracy of data and information—Level 1 | “As design guidelines are developed (continuous), implement and deploy technologies that reduce data acquisition, processing and display errors. These technologies will increase the reliability and accuracy of data/information, with a performance measure of reduced data acquisition, processing, and display errors. (Level 1 - less difficult improvements, component level)” |
| EN-3059 | Increased reliability and accuracy of data and information—Level 2 | “As design guidelines are developed (continuous), implement and deploy technologies that reduce data acquisition, processing and display errors. These technologies will increase the reliability and accuracy of data/information, with a performance measure of reduced data acquisition, processing, and display errors. (Level 2 - difficult, system level, new design)” |
| EN-3102 | Safety risk management processes and tools | “Improvements to Safety Risk Management (SRM) processes and tools result from research into analysis methods, risk estimation techniques, fault management, and other aspects of SRM. Routinizing SRM processes and reducing the SRM cycle time will reduce the potential for recurrence of incidents and accidents from known risks.” |
| EN-3103 | Safety assurance processes and tools | “Improvements to safety assurance processes and tools result from research into safety monitoring methods, unexposed risk surveillance techniques, comprehensive logical modeling and simulation to determine the contribution of singular actions to system-level risk outcomes, and methods to extract context from textual data, synthesize data from numerous diverse databases, and quantify causal relationships.” |
| EN-3107 | Advanced capabilities for integrated, predictive safety assessment | “Current Safety Risk Management (SRM) practices focus on ensuring the safety of individual elements of systems, but not on the aviation system as a whole. The underlying assumption in this approach is that, if each component of the system is shown to have acceptable risk, the system as a whole will have acceptable risk. This assumption is invalid, especially for complex systems where interactions between elements occur on multiple levels. Characterizing direct and indirect system interactions can help to promote a greater understanding of system of systems behaviors. New assessment techniques are needed to consider safety from a macro perspective to ensure that, as systems become more complex, our understanding of and ability to manage system safety risk is maintained or enhanced. Rapid prototyping of complex systems is a critical component of this macro-level understanding, permitting system developers to engage in full mission simulation, helping the identification of system safety considerations. Ultimately, adaptation of analytic tools used to consider system-wide interactions is needed to monitor system safety performance in real or near-real time to speed the discovery of emergent system safety risks. While these tools may provide early detection of system safety risks, they will not be able to predict them. Work is also needed to develop reliable predictions of system safety risk based on individual behaviors, both in nominal and in off-nominal conditions, within the system. Although prediction for human behavior is less reliable than for technology, reasonable estimations of human performance can be simulated to determine whether the system meets an acceptable level of risk.” |
| EN-3113 | Improve reliability and airworthiness of aircraft | “Increase the reliability of control, avionics, and Information Management Systems (IMS), as well as the long-term structural airworthiness of new materials and advanced aircraft designs. The result will be reduced systems failures and reduced diversions or incomplete missions.” |

TABLE 17.—NUMBER OF CURRENT AND FUTURE BIENNIAL NextGen SAFETY ISSUES THAT COULD BE IMPACTED BY COMPOSITIONAL VERIFICATION IMPLEMENTATION

| Category | Current | Future | Total |
|--|---------|--------|-------|
| Automation design | 5 | 5 | 10 |
| System complexity | 8 | 6 | 14 |
| Software, flight control or equipment failure or malfunction | 7 | 2 | 9 |
| New technology or operations | 0 | 6 | 6 |
| Verification and validation | 6 | 8 | 14 |

TABLE 18.—JOINT PLANNING AND DEVELOPMENT OFFICE INTEGRATED WORK PLAN ELEMENTS THAT
COULD BE IMPACTED BY COMPOSITIONAL VERIFICATION IMPLEMENTATION

| Element | ID | Element Name |
|-------------------------|---|---|
| Capability | N/A | Provide improved safety operations |
| Research action | R-1440 | Applied research on complex systems validation and verification |
| Operational improvement | OI-3004 OI-3102 OI-3104 OI-3105 OI-3108 | Improved operational processes using the safety management system (SMS) Improved safety for NextGen evolution Enhanced safety of airborne systems Enhanced safety of ground-based systems Improved SMS standards and effectiveness |
| Enabler | EN-3018 EN-3027 EN-3050 EN-3056 EN-3057 EN-3066 EN-3067 EN-3058 EN-3059 EN-3102 EN-3103 EN-3107 EN-3113 | Safety management requirements Improved fault management Advanced complex system validation and verification methods Improved Vehicle Systems Health Management–Level 1 Improved Vehicle Systems Health Management–Level 2 Improved ground-based systems health management–Level 1 Improved ground-based systems health management–Level 2 Increased reliability and accuracy of data and information–Level 1 Increased reliability and accuracy of data and information–Level 2 Safety Risk Management Processes and Tools Safety assurance processes and tools Advanced capabilities for integrated, predictive safety assessment Improve reliability and airworthiness of aircraft |

References

1. National Aeronautics and Space Administration: R&T Portfolio Project Plan, System-Wide Safety and Assurance Technologies (SSAT) Project Plan. Oct. 1, 2011 (Draft).
2. Darr, Stephen T.; Morello, Samuel A.; and Ricks, Wendell R.: Biennial NextGen Safety Issues Survey Database. Unpublished document.
3. Menzies, Tim; and Pecheur, Charles: Verification and Validation and Artificial Intelligence. *Advances in Computers*, M. Zelkowitz, ed., vol. 65, Elsevier, New York, NY, 2004.
4. Baier, Charles; Katoen, Joost-Pieter; and Larsen, Kim Guldstrand: *Principles of Model Checking*. MIT Press, Cambridge, MA, 2008.
5. Mach, Martin; Plasil, Frantisek; and Kofron, Jan: Behavior Protocols Verification: Fighting State Explosion. *Internat. J. Comput. Inform. Sci.*, vol. 6, no. 1, 2005, pp. 22–30.
<http://d3s.mff.cuni.cz/publications/download/MachPlasilKofron-Explosion.pdf>
6. Rouff, Christopher, et al.: The AdaptiV Approach to Verification of Adaptive Systems. *Proceedings of the Fifth International C* Conference on Computer Science and Software Engineering*, ACM, New York, NY, 2012, pp. 118–122.
7. Cooper, Eric G.: Baseline Assessment and Priorization Framework for IVHM Integrity Assurance Enabling Capabilities. NASA/TM—2009-215764, 2009. <http://ntrs.nasa.gov/>
8. Cofer, Darren: PSL for Assume-Guarantee Contracts in AADL Models. Rockwell Collins presentation, 2011. <https://wiki.sei.cmu.edu/aadl/images/0/0b/RC-AADL-contractsOct2011.pdf> Accessed July 31, 2014.
9. Australian Transport Safety Bureau: In-Flight Upset—Airbus A330–303, VH–QPA, 154 km West of Learmonth, WA. *Aviation Safety Investigations & Reports*, Investigation number AO–2008–070, 2008. http://www.atsb.gov.au/publications/investigation_reports/2008/aair/ao-2008-070.aspx Accessed July 31, 2014.
10. National Research Council: *Decadal Survey of Civil Aeronautics: Foundation for the Future*. The National Academies Press, Washington, DC, 2006, p. 151.
http://www.nap.edu/openbook.php?record_id=11664&page=R1 Accessed Aug. 1, 2014.
11. Joint Planning and Development Office: *National Aviation Safety Strategic Plan*. Version 1.0B, 2011.
<http://www.flightdeckautomation.com/issues.htm.intro>
12. <http://www.flightdeckautomation.com/issues.htm.intro>
13. Lyall, E.; Niemczyk, M.; and Lyall, R.: Evidence for Flightdeck Automation Problems: A Survey of Experts. 1996. <http://www.flightdeckautomation.com/resource.aspx?ID=93> Accessed Sept. 26, 2014.
14. Holzmann, Gerard J.: *Verifying Complex Software Systems: The Challenge*. The Fifth International Conference on Secure Software Integration and Reliability Improvement, Keynote Speech I, Jeju Island, Korea, 2011.
15. Hayhurst, Kelly J.: *Neglecting Achilles' Heel: Why Software Safety Research is Important*. Presented at the Aviation Safety Technical Conference, St. Louis, MO, 2007.
16. Gilligan, Margaret: *AVS Work Plan for NextGen 2011*. Federal Aviation Administration, Washington, DC, 2011.
17. Joint Planning and Development Office: *Concept of Operations for the Next Generation Air Transportation System*. Version 3.2, Next Generation Air Transportation System (NextGen), Washington, DC, 2010.
18. Rushby, John: *Modular Certification*. NASA/CR—2002-212130, 2002. <http://ntrs.nasa.gov/>

| REPORT DOCUMENTATION PAGE | | | Form Approved OMB No. 0704-0188 | | |
|---|--|--------------|---|---------------------------|---|
| <p>The public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number. PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.</p> | | | | | |
| 1. REPORT DATE (DD-MM-YYYY) 01-10-2014 | 2. REPORT TYPE Technical Memorandum | | 3. DATES COVERED (From - To) | | |
| 4. TITLE AND SUBTITLE Projected Impact of Compositional Verification on Current and Future Aviation Safety Risk | | | 5a. CONTRACT NUMBER | | |
| | | | 5b. GRANT NUMBER | | |
| | | | 5c. PROGRAM ELEMENT NUMBER | | |
| 6. AUTHOR(S) Reveley, Mary, S.; Withrow, Colleen, A.; Leone, Karen, M.; Jones, Sharon, M. | | | 5d. PROJECT NUMBER | | |
| | | | 5e. TASK NUMBER | | |
| | | | 5f. WORK UNIT NUMBER WBS 534723.02.01.03.40 | | |
| 7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) National Aeronautics and Space Administration John H. Glenn Research Center at Lewis Field Cleveland, Ohio 44135-3191 | | | 8. PERFORMING ORGANIZATION REPORT NUMBER E-18677 | | |
| 9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) National Aeronautics and Space Administration Washington, DC 20546-0001 | | | 10. SPONSORING/MONITOR'S ACRONYM(S) NASA | | |
| | | | 11. SPONSORING/MONITORING REPORT NUMBER NASA/TM-2014-217877 | | |
| 12. DISTRIBUTION/AVAILABILITY STATEMENT Unclassified-Unlimited Subject Category: 03 Available electronically at http://www.sti.nasa.gov This publication is available from the NASA Center for AeroSpace Information, 443-757-5802 | | | | | |
| 13. SUPPLEMENTARY NOTES | | | | | |
| 14. ABSTRACT The projected impact of compositional verification research conducted by the NASA System-Wide Safety and Assurance Technologies on aviation safety risk was assessed. Software and compositional verification was described. Traditional verification techniques have two major problems: testing at the prototype stage where error discovery can be quite costly and the inability to test for all potential interactions leaving some errors undetected until used by the end user. Increasingly complex and nondeterministic aviation systems are becoming too large for these tools to check and verify. Compositional verification is a "divide and conquer" solution to addressing increasingly larger and more complex systems. A review of compositional verification research being conducted by academia, industry, and Government agencies is provided. Forty-four aviation safety risks in the Biennial NextGen Safety Issues Survey were identified that could be impacted by compositional verification and grouped into five categories: automation design; system complexity; software; flight control or equipment failure or malfunction; new technology or operations; and verification and validation. One Capability, 1 research action, 5 operational improvements, and 13 enablers within the Federal Aviation Administration Joint Planning and Development Office Integrated Work Plan that could be addressed by compositional verification were identified. | | | | | |
| 15. SUBJECT TERMS Verification; Flight safety; Aircraft safety; Automation; Complex systems; Flight control; System failures | | | | | |
| 16. SECURITY CLASSIFICATION OF: | | | 17. LIMITATION OF ABSTRACT | 18. NUMBER OF PAGES | 19a. NAME OF RESPONSIBLE PERSON |
| a. REPORT | b. ABSTRACT | c. THIS PAGE | | | STI Help Desk (email:help@sti.nasa.gov) |
| U | U | U | UU | 28 | 19b. TELEPHONE NUMBER (include area code) 443-757-5802 |

