

# NASA's 2014 International IV&V Workshop Agenda

**Dates:** September 9-11, 2014

**Location:** 5000 NASA Blvd, Fairmont, WV

**For more information:** <http://www.nasa.gov/centers/ivv/workshops/index.html>

**All times are Eastern Daylight Time (EDT)**

| Day 1 (September 9, 2014) |   |   |
|---------------------------|---|---|
| Time                      | Title   | Speaker(s)  |
| 8:00                      | Opening Remarks   |   |
| 8:15                      | The Art & Science of Managing Command File Errors   | Leila Meshkat   |
| 8:45                      | Analysis of the Effects of Auto Generated Code on IV&V of Mission Critical Software   | Noble Nkwocha<br>Andrew Sung  |
| 9:15                      | Introduction to DMA and AMF   | Don Kranz<br>Steve Husty  |
| 9:45                      | BREAK   |   |
| 9:55                      | Plug and Play with DMA Components   | Neal Saito<br>Tom Gullion<br>Don Kranz  |
| 10:25                     | Using Combinatorial Methods to Determine Test Set Size  | Rick Kuhn   |
| 10:55                     | IRSim: A Web-Based Tool for Establishing Traceability Links Among Software Artifacts  | Dharma Ganesan  |
| 11:25                     | LUNCH   |   |
| 12:55                     | Safety and Assurance Cases for Complex System Products [Panel Session]  | Sam Brown (NASA IV&V)<br>Travis Dawson (NASA IV&V)<br>Dr. Martin Feather (NASA JPL)<br>Bob Youngblood (INL) |
| 1:55                      | Application of Goal Structure Notation (GSN) in IV&V Activities   | Taisuke Kanbe   |
| 2:25                      | Comparison of IV&V's Use of Non Verification Environments and Program Use of Verification Environments                                      | Ricky Beamer  |
| 2:55                      | BREAK   |   |
| 3:05                      | Risk Based Assessment and Information Assurance   | Joelle Loretta<br>Richard Brockway<br>Craig Burget  |
| 3:35                      | IV&V Lessons Learned From a Memory-Scrub Anomaly  | Dan Painter   |
| 4:05                      | There and Back Again – Connecting Assurance Statements to Analysis Spreadsheets in Support of Evidence Based Assurance for the GSDO Project | Pat Olguin  |
| 4:35                      | Global Precipitation Measurement (GPM) Safety Inhibit Timeline Tool   | Shirley Dion  |
| 5:35                      | END OF DAY 1  |   |

# NASA's 2014 International IV&V Workshop Agenda

| Day 2 (September 10, 2014) |  |   |
|----------------------------|--|---|
| Time                       | Title  | Speaker(s)  |
| 8:00                       | Automating Evidence Collection for Software Assurance from Existing Status Reports                                       | Bob Inscoe  |
| 8:30                       | Use of XSLT to Transform the Output of Multiple Static Code Analysis Tools Into a Consistent Analysis Spreadsheet Format | Ben Markle  |
| 9:00                       | Automated Visual GUI Testing for the Space Network   | Charles Song  |
| 9:30                       | Cost-Effectiveness of IV&V by Life Cycle Phase   | Ken Haught  |
| 10:00                      | BREAK  |   |
| 10:10                      | What IV&V Can Learn from River Guides  | Lorelei Lohrli-Kirk<br>Neal Saito   |
| 10:40                      | NASA Software Assurance Challenges for Commercial Crew Program   | Kathy Malnick<br>Chad Schaeffer   |
| 11:25                      | LUNCH  |   |
| 12:55                      | IV&V of Model-Based Systems  | Don Kranz<br>Marcus Fisher  |
| 1:40                       | Static Code Analysis for Information Assurance: Current Practice and Future Directions [Panel Session]                   | Katerina Goseva-Popstojanova (WVURC)<br>Brandon Bailey (NASA IV&V)<br>Rich Brockway (NASA IV&V)<br>Van Casdorff (NASA IV&V)<br>Marcus Fisher (NASA IV&V)<br>Rick Hess (NASA IV&V) |
| 2:40                       | BREAK  |   |
| 2:50                       | Metrics for V&V of Cyberdefenses   | Martin Feather  |
| 3:50                       | IV&V and the Heartbleed Vulnerability  | Gerald Hess   |
| 4:20                       | Get Confidence in Mission Security with IV&V Information Assurance   | Rich Brockway<br>Brandon Bailey   |
| 5:05                       | Optional Special Topic   |   |
| 5:35                       | END OF DAY 2   |   |

# NASA's 2014 International IV&V Workshop Agenda

| Day 3 (September 11, 2014) |  |  |
|----------------------------|--|--|
| Time                       | Title  | Speaker(s)   |
| 8:00                       | Capturing Autonomy Features for Unmanned Spacecraft with ARE, the Autonomy Requirements Engineering Approach | Emil Vassev  |
| 8:45                       | The Challenges of Assuring Vision Systems for Space Missions   | Charley Price<br>Vincent Howard  |
| 9:45                       | BREAK  |  |
| 9:55                       | Robotic Systems for Asteroid Redirect and Satellite Servicing Missions Q&A [Panel Session]                   | Charley Price (NASA IV&V)<br>Dr. Thomas Evans (WVRTC)<br>Vincent Howard (NASA IV&V)<br>Dr. Brian Roberts (NASA GSFC)<br>Andre Sylvester (NASA JSC) |
| 10:55                      | Sketch Theory as a Framework for Knowledge Management  | Ralph Wojtowicz  |
| 11:25                      | LUNCH  |  |
| 12:55                      | End-to-End Fault Management Analysis Method, Results, and Future Improvements                                | Ryan Starn   |
| 1:25                       | NASA IV&V Software Emulator Technology Portfolio   | Matt Grubb   |
| 2:10                       | Space Hardware   | Steve Yokum  |
| 2:55                       | BREAK  |  |
| 3:05                       | Assessment of Fault Management in Network Resource-Intensive and Protocol-Rich Environments                  | Tom Hempler  |
| 3:35                       | Scoping and Analysis of FPGAs from an IV&V Perspective   | Pradip Maitra<br>John Ryan   |
| 4:05                       | Optional Special Topic   |  |
| 4:35                       | Closing Remarks  |  |
| 4:50                       | END OF DAY 3   |  |

# NASA's 2014 International IV&V Workshop Agenda

## Presentation Summaries

**Analysis of the Effects of Auto Generated Code on IV&V of Mission Critical Software** – With the use of auto generated code on the rise, it is critical to understand the effects to IV&V analysis if the analysis is performed on code that is auto generated from models. In a recent investigation of completed NASA IV&V projects with auto generated code, three very important facts were revealed. This presentation will describe our study of these facts and their relationships and also report our findings.

**Application of Goal Structure Notation (GSN) in IV&V Activities** – JAXA has introduced the IV&V case for the purpose of improving stakeholder satisfaction, differentiating IV&V from verification by software development companies, and to ensure the quality of IV&V activities does not solely depend on the abilities of the engineer conducting the analysis. For the purpose of taking advantage of JAXA's IV&V standard process, IV&V cases are defined based on the Goal Structure Notation. This presentation describes the IVV case concept and includes examples.

**The Art & Science of Managing Command File Errors** – A command file is a piece of software code that is sent to the spacecraft for the purpose of command and control during operations and command file errors (CFEs) account for an alarming fraction of spacecraft anomalies and near misses. This presentation discusses research conducted on building analytical, probabilistic models to assess, predict and manage the CFE rates based on the attributes of the system. Tools and techniques developed for systematically managing command file errors, including Bayesian Belief Network models, Sigma Tool, and Empirical Analysis techniques, will be discussed.

**Assessment of Fault Management in Network Resource-Intensive and Protocol-Rich Environments** – Challenges faced for IV&V of the Space Network Ground Segment Sustainment (SGSS) Ground Station implementation include the magnitude and maturity of the artifacts, the complexity and volume of code being delivered and the diverse protocols in use by ground stations to provide data/command services in support of Space Network users. Alternative analysis techniques and tools to meet the stated challenges are the focus of this presentation. The techniques presented are intended for use as new method(s) to assess and verify fault management implementation of requirements at the network and application layer; and are specified for SGSS managed network resources and messaging among them.

**Automated Visual GUI Testing for the Space Network** – The Space Network is a challenging environment for automated GUI testing. To improve the situation, a visual GUI testing approach was developed that leverages computer vision technologies to perform GUI testing via screenshots. This presentation will present the visual GUI testing approach and our visual GUI testing tool PiGuiT (Platform-independent GUI Testing).

**Automating Evidence Collection for Software Assurance from Existing Status Reports** – The International Space Station (ISS) IV&V team had a need to provide evidence-based assurance metric data, but system analysis and development of a traditional management system would have a noticeable impact on the team's analysis efforts. The ISS team developed a software utility that collects software assurance evidence from existing periodic project status reports. This presentation will describe the internal data structures and algorithms that work together to extract data from the monthly status report inputs.

# NASA's 2014 International IV&V Workshop Agenda

**Capturing Autonomy Features for Unmanned Spacecraft with ARE, the Autonomy Requirements Engineering Approach** – Along with traditional system requirements, requirements engineering for autonomous and self-adaptive systems needs to address requirements related to adaptation - when a system needs to cope with changes to ensure realization of the system's objectives. In particular, adaptation issues include: 1) what adaptations are possible; 2) under what constraints; and 3) how those adaptations are realized. This presentation discusses an approach to handling these issues called Autonomy Requirements Engineering (ARE).

**The Challenges of Assuring Vision Systems for Space Missions** – NASA is developing advanced robotics missions for the redirection of asteroids, for the servicing of satellites at geosynchronous earth orbits, and for the expanded exploration of Mars. A common capability in these missions will be robotic vision-driven closed loop control in dynamic and uncertain environments. This presentation will discuss the challenges faced by IV&V for assuring such vision systems and will describe recently developed assets to support IV&V of vision systems.

**Comparison of IV&V's Use of Non Verification Environments and Program Use of Verification Environments** – One challenge in performing IV&V analysis utilizing dynamic testing and simulation environments is providing sufficient assessment of the software while not having resources to develop an independent test bed and simulation system to meet the full intentions of technical independence. This presentation will provide details of the approach utilized for NASA's IV&V Program's uncrewed Exploration Flight Test 1 (EFT-1) mission's qualification testing on the supplied development environments, outline initial results from this method, and discuss future qualification testing strategies utilizing actual mission data. The results of the current and future tests will also support the independent evaluation of NASA's Multi-Purpose Crew Vehicle (MPCV) Program's own uses of these tools.

**Cost-Effectiveness of IV&V by Life Cycle Phase** – For IV&V to be cost effective, its ROI must exceed the ROIs of other risk-reduction alternatives. Using data from four 2012 IV&V Workshop presentations dealing with ROI, this paper provides three recommendations for modeling the cost effectiveness of IV&V by life cycle phase.

**End-to-End Fault Management Analysis Method, Results, and Future Improvements** – A system's Fault Management (FM) behavior is emergent and subject to resource starvation. Conflict analysis is necessary but assurance is difficult to maintain given the numerous developers, life cycles, and expected modifications to the system behavior up to and past launch. In this presentation, participants will learn about ongoing research to establish a method to provide robust assurance for software's role in FM in a distributed and tiered FM architecture where multiple development cycles and developer organizations are encountered over several years of development.

**Get Confidence in Mission Security with IV&V Information Assurance** – In this presentation, participants will learn about how NASA's IV&V Program provides mission security assurance throughout the design, development, implementation, operation, maintenance and disposition of information systems. Surveying the threat landscape, exploring the regulatory framework for security assessment and learning how IV&V's objective role and processes equip mission stakeholders are among the main points that will be covered in this discussion.

**Global Precipitation Measurement (GPM) Safety Inhibit Timeline Tool** – NASA has placed more emphasis on assessing safety hazards for spacecraft operations at the launch range rather than at the integration and testing (I&T) site. The Safety Inhibit Timeline Tool was created as one approach to capturing and understanding inhibits and controls from I&T through launch. With this tool, the Safety Analyst can confirm proper safe configuration

# NASA's 2014 International IV&V Workshop Agenda

of a spacecraft during each I&T test, track inhibit and software configuration changes, and assess software criticality.

**Introduction to DMA and AMF** – Data within IV&V are stored in a variety of forms by a variety of stakeholders with a variety of intents. Data management solutions that reduce duplications of efforts, standardize analysis data, and improve utilization of resources are needed. The Analysis & Management Framework (AMF) is an IV&V solution providing a meta-model of IV&V processes and data. The Data Management Architecture (DMA) project attempts to migrate the activities of performing IV&V and managing an IV&V project to a more data-driven process.

**IRSim: A Web-Based Tool for Establishing Traceability Links Among Software Artifacts** – During software V&V, analysts often face the challenge of establishing traceability links among artifacts such as requirements, source code, test cases, etc. This presentation will discuss IIRSim, a web-based tool that suggests traceability links among exported software artifacts. An overview of the different features of IIRSim will be presented, as well as the results of empirical study performed by applying it to NASA's Core Flight Software.

**IV&V and the Heartbleed Vulnerability** – In April of 2014, an estimated two-thirds of the world's web servers were susceptible to what has been called the "Heartbleed" vulnerability. This presentation explores whether NASA's IV&V Program would have been able to find this particular type of issue utilizing our standard set of tools.

**IV&V Lessons Learned From a Memory-Scrub Anomaly** – In this presentation, an anomaly experienced multiple times in the course of routine memory scrubbing performed on a space science mission will be discussed. A description of the anomaly will be provided, along with the potential factors leading to the anomaly and the impact of the anomaly on the mission.

**IV&V of Model Based Systems** – Mission and safety critical development efforts utilizing agile-based development processes and model-based engineering approaches present unique assurance challenges. Model based system engineering produces documentation, code, and sometimes of models as outputs of the modeling process. Reviewing process outputs is not the most effective means of performing IV&V and this presentation discusses concentrating IV&V more on the input information, i.e. models, transformation, configuration and control processes.

**Metrics for V&V of Cyberdefenses** – There is a need for a disciplined approach to evaluation of a cyberdefense prior to its introduction into a flight project environment (development or operations) to assure that the benefits of the defense will be worth its costs. This presentation will describe research focused on using the adaptation of a traditional V&V workflow, coupled with collection and presentation of the appropriate metrics for each stage of that workflow to meet this need.

**NASA IV&V Software Emulator Technology Portfolio** – Software-Only-Simulations have been an emerging but quickly developing field of study throughout NASA. This presentation overviews the technologies and processes that have been utilized to design, implement and deploy end-to-end simulation environments for various NASA missions. The presenter will describe how these technologies are utilized within NASA's IV&V Program and how they have benefited other organizations.

# NASA's 2014 International IV&V Workshop Agenda

**NASA Software Assurance Challenges for Commercial Crew Program** – This presentation will provide a description of some of the challenges NASA is facing in providing software assurance to the Commercial Crew Program (CCP). These challenges include multiple funding vehicles that execute in parallel and have different rules of engagement, multiple providers with unique proprietary concerns, providing equivalent guidance to all providers, permitting alternates to NASA standards, and a large number of diverse stakeholders. The proposed CCP approach to address these challenges includes a risk-based assessment with varying degrees of engagement and a distributed assurance model.

**Plug and Play with DMA Components** – Component based architectures are a widely accepted industry practice. The NASA IV&V Data Management Architecture (DMA) effort is focused on defining the necessary components to support the principle activities of performing IV&V and managing an IV&V project. The Analysis & Management Framework (AMF) attempts to make existing and new capabilities available to user interfaces, business objects, and data sources, which includes the Data Warehouse. This presentation will inform the IV&V community of the wealth of analysis components being made available via the DMA effort.

**RBA Challenges (IA)** – This presentation addresses the risk based assessment (RBA) and scoping of IV&V work as it pertains to Information Assurance (IA).

**Scoping and Analysis of FPGAs from an IV&V Perspective** – Recent years have seen an explosion of FPGA-based systems in day-to-day activities including automobiles, household appliances, intelligent systems and finally the space program itself. The presenter will propose a number of criteria for scoping FPGAs and then detail some procedures on how to perform IV&V analysis on them.

**Sketch Theory as a Framework for Knowledge Management** – To build autonomous systems with revolutionary capabilities to transform data into knowledge, understand their environments, coordinate activities and communicate, we must advance our technologies for representing and managing knowledge. This presentation will discuss research aimed at developing and demonstrating sketch theory as a complementary knowledge management technology capable of solving the challenges of knowledge alignment, context and uncertainty.

**Space Hardware** – The NASA IV&V Program is challenged with the task of performing IV&V on complicated systems that have complex hardware/software interactions that cannot be fully investigated using static analysis or software emulation alone. This presentation will describe a specific mission anomaly and how the NASA IV&V Program's JSTAR hardware test environment was utilized to perform independent testing.

**There and Back Again – Connecting Assurance Statements to Analysis Spreadsheets in Support of Evidence Based Assurance for the GSDO Project** – Evidence Based Assurance demands that the results of IV&V analysis are quantifiable, in order to accurately characterize the assurance provided, and to quantify residual risk. Current spreadsheet-driven, issue-based results do not directly support this. This presentation discusses an approach to create direct connections between assurance claims and current IV&V analyses and results and integrate them directly into the analysts' spreadsheets.

**Use of XSLT to Transform the Output of Multiple Static Code Analysis Tools Into a Consistent Analysis Spreadsheet Format** – IV&V analysts often wish to use multiple Static Code Analysis tools to examine a software build. The use of multiple tools enables the analyst to achieve broader coverage of code checkers than a single tool can provide on its own. In this presentation, the audience will learn about EXtensible Stylesheet Language

# NASA's 2014 International IV&V Workshop Agenda

Transformations (XSLT) that can be used to transform the output of multiple Static Code Analysis tools into a spreadsheet table format that can be used to investigate the findings of the tools and track the disposition of the findings.

**Using Combinatorial Methods to Determine Test Set Size** – A key issue in testing is how many tests are needed for a required level of coverage or fault detection, with estimates often based on error rates in initial testing, or on code coverage. Combinatorial methods present an opportunity for a different approach to estimating required test set size. This presentation discusses developing a relationship between the (static) distribution of combinations in input data and (dynamic) executable code coverage.

**What IV&V Can Learn from River Guides** – In the whitewater rafting industry, raft guides have the primary responsibility for the safety of customers - analyzing hazards, assessing risks and managing teams to safely and successfully perform series of difficult tasks. This presentation will explore some of the techniques river guides use to enhance their customers' experience, the value they add, and how IV&V can apply these techniques to add value to the analysis performed. The lessons learned from this examination will enlighten the work of both IV&V managers and analysts.

# NASA's 2014 International IV&V Workshop Agenda

## Panel Session Summaries

**Robotic Systems for Asteroid Redirect and Satellite Servicing Missions Q&A** – Future NASA missions for asteroid redirect (ARM) and satellite servicing (SS) will have robotic systems with associated levels of autonomy. This panel will discuss the elements of ARM and SS, and provide insight into how NASA is preparing for the technological advances required for mission success.

**Safety and Assurance Cases for Complex System Products** – Highly experienced panelists from industries will meet to discuss perspectives and approaches to assurance case and safety case design for complex systems. Their topics include applications of assurance cases to planning and reporting safety/assurance status, developing and maintaining assurance cases, and a comparative discussion of approaches taken in multiple applications.

**Static Code Analysis for Information Assurance: Current Practice and Future Directions** – This panel is focused on using static code analysis for detection of security vulnerabilities. The panelists will address both theoretical and practical advantages and limitations of static code analysis, its integration with other IV&V techniques focused on cybersecurity, challenges imposed by large scale NASA projects, and recent efforts to develop and implement tool support for selection and prioritization of messages produced by static code analysis tools.