Proceedings of NASA's 2014 International Independent Verification and Validation (IV&V) Workshop

September 9-11, 2014

NASA's IV&V Facility
Fairmont, W. Va.

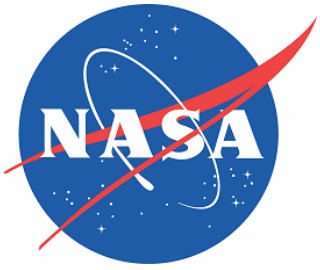

Table of Contents

The Art and Science of Managing Command File Errors

Leila Meshkat, Ph.D., NASA JPL

ABSTRACT

A command file is a piece of software code that is sent to the spacecraft for the purpose of command and control during operations. Command File Errors (CFEs) occur when (a) there is an error in a command file that was sent to the spacecraft, (b) an error in the approval, processing or up-linking of a command file that was sent to the spacecraft or (c) an omission of a command file that should have been sent to the spacecraft. CFE's account for an alarming fraction of spacecraft anomalies and near misses – hence the significance of our research.

We describe our research, and related tools and techniques developed for systematically managing CFEs. During the early phases of the research, our hypothesis was that it's possible to build analytical, probabilistic models to assess, predict and manage the CFE rates based on the attributes of the system. We then built several different classes of models and populated them with a combination of expert opinions as well as existing information. More recently, we have been testing our hypothesis by analyzing the details of the existing data in the JPL Anomaly database systems and using these results to validate the models previously built. Our empirical results are encouraging although they have led us to make adjustments to our existing models.

The various techniques we present include:

1. Bayesian Belief Network models, which provide a causal graphical depiction of the various causes of CFEs and a probabilistic model of CFEs as a function of the various causes. These are used for the purpose of sensitivity and root cause analyses.
2. Sigma Tool, which provides a distribution for the likelihood of CFEs based on the number of files (commands, blocks) and the novelty of the mission. This provides a visual understanding of how a project is doing as compared to other similar projects and helps anticipate the number of CFEs based on the expected upcoming activities.
3. Empirical Analysis techniques such as correlation and regression analysis and principal component and factor analyses. These techniques help validate the models used in (1) and (2).

Analysis of the Effects of Auto Generated Code on IV&V of Mission Critical Software

Noble N. Nkwocha, NASA IV&V
Andrew Sung, Ph.D., The University of Southern Mississippi

ABSTRACT

At NASA' IV&V Program, there is a question of whether or not there are effects to IV&V analysis if the analysis is performed on code that is auto generated from models. Observational data, indeed, suggests that there are. In a recent investigation of prior NASA IV&V projects with auto generated code, three very important facts were revealed. The first was that several, rather than fewer, IV&V projects had auto generated code. This fact will increasingly grow given the trend towards auto code generation in flight software. The second was the common theme that ran across all of the projects with auto generated code. That theme was the question of "What or where IV&V focus ought to be when it comes to auto generated software." Should IV&V focus on the inputs to the code generators, analyze the code generators themselves, analyze the output of the code generators, or, perhaps, assess all three? The third fact, and perhaps the most crucial considering the safety requirements of flight software in real-time, was the observed higher SLOC count of auto generated software when compared to their equivalently handwritten code. In this paper, we describe our study of these facts and their relationships and also report our findings. One immediate benefit of our study is an understanding of the effects when they exist in order that NASA's IV&V Program may consider them when:

1. Planning for the work to be accomplished
2. Identifying the technical rigor to be applied
3. Configuring and identifying the tools to be used in the analytical work

Added to this is an elicitation of the dominating fault types in auto generated software. Are these fault types, or any specific fault types, differently distributed for auto generated code? Our paper explores this question as well. There is a dearth of published empirical data on the application of IV&V on automatically generated code. It is our hope that our paper, especially the results, provides new insights into the effects of auto generated software and contributes to research on a topic for which not much empirical evidence exists and thus advances the state-of-the-art and practice.

Introduction to Data Management Architecture (DMA) and Analysis and Management Framework (AMF)

Don Kranz, NASA IV&V / TASC
Steve Husty, NASA IV&V

ABSTRACT

Data within NASA's IV&V Program are stored in a variety of forms by a variety of stakeholders with a variety of intents. Using data from another stakeholder and getting a program-wide, 360° view is possible, but is inefficient. Knowing what data is available is haphazard and finding it requires fore-knowledge of its existence and location. Historical data is not leveraged efficiently or effectively. Various solutions comprise the set of data management architectures available. In other words, Data Management Architecture is the term for the set of solutions available – not the name of a particular solution. The Analysis & Management Framework is a NASA IV&V Program solution based on a meta-model of NASA IV&V processes and data. The DMA is focused on defining the necessary components to support the principle activities of performing IV&V and managing an IV&V project. In some cases, that's translating documented processes into business logic (e.g., AMF business layer). In other cases, it means defining/documenting those processes (e.g. assurance strategy)

The AMF team is working closely with the Operational Data Source team to reduce duplication of efforts, standardize analysis data and improve utilization of resources. The efficiencies available go far beyond the efficiencies to be gained in handling data more efficiently – they include the efficiencies to be gained within the program from the transformative portrayals of the program that will emerge, with DMA being an enabler. By exposing data relationships and discovering new relationships, the DMA will allow data to be used as a driving input versus a post-facto outcome.

DMA and AMF are being produced in incremental integrations with measurement of the interim benefits. This work progresses on several fronts: workflow gap analysis, AMF and Analyst Workbench enhancements, roll out to production projects and definition of an operational data source.

Plug and Play with Data Management Architecture (DMA) Components

Tom Gullion, NASA IV&V / TASC
Don Kranz, NASA IV&V / TASC
Neal Saito, NASA IV&V / TASC

ABSTRACT

The IV&V community is currently unfamiliar with the wealth of analysis components being made available via the DMA effort, which includes Data Warehouse and Analysis and Management Framework.

Component-based architectures are a widely accepted industry practice. The DMA effort attempts to make existing and new capabilities available via the following components:

- User Interfaces: Analyst Workbench, Project Workbench, COMPASS, Risk Manager, organizational services, ORBIT, and reporting and scheduling tools (Microsoft Word and Excel)
- Business Objects: The building blocks are the projects, participants, actions, assessments, artifacts and tracing information
- Data Sources: SQL Server (e.g. AWB, PWB, COMPASS, Risk Manager, organizational services), DOORS, JIRA, Excel, Access, Integrity, and artifact documentation.

Implementation platforms to be discussed include Eclipse, Microsoft Office, and web services

After attending this workshop, analysts and managers will better understand the range of analysis components being rolled out to all NASA IV&V Projects by FY 2016, and their potential project applications.

Using Combinatorial Methods to Determine Test Set Size

Rick Kuhn, National Institute of Standards and Technology
Raghu Kacker, National Institute of Standards and Technology
Yu Lei, University of Texas Arlington

ABSTRACT

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. For example, tests may be run until a desired level of statement or branch coverage is achieved. Combinatorial methods present an opportunity for a different approach to estimating required test set size.

The objective of this work was to build on previous results [1] to develop a relationship between the (static) distribution of combinations in input data and (dynamic) executable code coverage. Results can be used in scoping the number of tests and level of effort, and estimating residual risk from complex combinations not tested.

Combinatorial testing is based on the observation that most failures are triggered by a single parameter value or interactions between a small number of parameters. For example, a fault that occurs when x > 10 && y < 300 is a 2-way interaction, because two variables are involved. Empirical data show that faults triggered by four or more variables interacting are rare and failures involving more than six variables have not been observed. Therefore arrays covering t-way combinations, t = 2..6, can be used to generate thorough tests. Any test array for n variables covers some level of 2-way through n-way combinations, and this coverage can be measured [2]. For example, an array covering 100% of 3-way combinations will also cover some 4-way, 5-way, etc.

This work has produced the following results:

- Catalog of t+1 and t+2 way coverage for test configurations of n = 10 to 100 input variables, and v = 2 to 10 values per variable – for initial estimation of test set size.
- Tool for computing t+1 and t+2 way coverage for typical cases where input variables do not all have the same number of values – to determine test set size more exactly.
- Expressions for the minimum level of (static) combination coverage to ensure 100% (dynamic) branch coverage (and therefore statement coverage also) of executable code, where all variables in decision predicates have values from test inputs.

[1] C. Price, R. Kuhn, R. Forquer, A. Lagoy, R. Kacker, "Evaluating the t-way Combinatorial Technique for Determining the Thoroughness of a Test Suite", NASA IV&V Workshop, 2013.

[2] D.R. Kuhn, R.N. Kacker "Measuring Combinatorial Coverage of System State-space for IV&V", NASA IV&V Workshop, 2012.

Safety and Assurance Cases for Complex System Products
PANEL SESSION

Sam Brown, NASA IV&V / TASC
Travis Dawson, NASA IV&V / TASC
Martin Feather, Ph.D., NASA JPL
Robert Youngblood, Idaho National Laboratories

ABSTRACT

Highly experienced panelists from industries meet to discuss perspectives and approaches to assurance case and safety case design for complex systems. Our 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. IV&V practitioners and planners should plan to attend this very relevant and dynamic event.

Application of Goal Structure Notation (GSN) in the IV&V activities

Taisuke Kanbe, Japan Aerospace Exploration Agency
Ikunao Tada, Japan Aerospace Exploration Agency
Naoko Okubo, Japan Aerospace Exploration Agency
Hiroki Umeda, Japan Aerospace Exploration Agency
Masa Katahira, Japan Aerospace Exploration Agency

ABSTRACT

Recently, JAXA has regularly applied IV&V activities on satellites and rockets.

On the other hand, space craft projects request ways of making IV&V activities more effective and different from verification performed by software development companies.

JAXA's IV&V activities focus on the concept of risk-based verification within their mid-term plan, from 2013 to 2017.

We introduced an IVV case for the purpose of improving stakeholder satisfaction, differentiating verification of software from development companies, and ensuring the IV&V activities' quality does not depend on the ability of the engineer.

We explain our IVV case concept and introduce examples in this presentation.

For the purpose of taking advantage of JAXA's IV&V standard process, the IVV case is defined based on the Goal Structure Notation. The IVV case does not only explain to the development project how to use the IV&V engineers to create a verification and validation strategy, but also includes how to analyze anomaly problems.

The IVV case is used in many IV&V standard processes and we have increased the reusability and improved the accuracy of the IVV case.

In addition to the purpose of the original plan, we have achieved the following three points.

1. Technology transfer to the skilled person from beginner
2. Establishment of a system in accordance with the degree of difficulty of the assessed work
3. Engineers get the customer's perspective

Comparison of IV&V's Use of Non Verification Environments and Program Use of Verification Environments

Ricky Beamer, NASA IV&V / New-Bold Enterprises, Inc.
Katie Warner, NASA IV&V Intern

ABSTRACT

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 within IEEE Standard 1012-2012, "IEEE Standard for System and Software Verification and Validation," Annex C Definition of independent V&V (IV&V). In these situations, Annex C states "For shared tools, IV&V conducts qualification tests on tools to assure that the common tools do not contain errors that may mask errors in the system being analyzed and tested."

NASA's Multi-Purpose Crew Vehicle (MPCV) Program has provided NASA's IV&V Program with several development test environments for the un-crewed EFT-1 mission. NASA's IV&V Program has used these environments as part of code verification and validation activities for this un-crewed mission following a basic comparison of results between a test performed by NASA's IV&V Program and the same test performed by the MPCV Program. Other NASA IV&V projects, such as ISS, have utilized program-provided assets and performed similar confidence testing. This level of confidence testing was suitable for the un-crewed EFT-1 mission as all significant test results were planned for verification in certified test environments. Results comparisons were not performed or essential.

The approach selected is adequate but does not meet the full intentions of IEEE 1012 Annex C. The approach of confirming negative results with retests in higher fidelity environments omits a class of "issues" where the results show no defects. The approach is neither technically independent nor fully effective.

NASA's MPCV Program has now completed multiple tests for the un-crewed EFT-1 mission in certified testing environments. With this data, it is possible to perform comparison tests that recreate the NASA IV&V Program's tests from certified and developmental testing environments.

This presentation will provide details of the approach utilized for NASA's IV&V Program un-crewed 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.

Risk Based Assessment and Information Assurance

Joelle Spagnuolo-Loretta, NASA IV&V / TASC
Rich Brockway, NASA IV&V / TASC
Craig Burget, NASA IV&V / TASC

ABSTRACT

NASA's IV&V Program services are expanding to projects of varying domains (e.g. ground systems, integrated networks, etc.) that are somewhat different than the typical flight software projects supported in years past. Hence it is crucial that the NASA IV&V Program's processes mature such that they maintain applicability. The current Risk Based Assessment (RBA) process defined in NASA's IV&V Program supporting document S3106 Portfolio Based Risk Assessment (PBRA) and the RBA Process "is used to create a mission-specific view to support planning and scoping of NASA IV&V Project work on each individual IV&V Project." The process results in a risk score for each system/software entity for a particular mission, and the score is based on impact categories of performance, personnel safety, operational software control and likelihood categories of complexity, testability, degree of innovation and developer characteristics. However, these criteria do not explicitly allow for a thorough assessment of the system entities and their potential risk as it relates to maintaining system security/information assurance. Although some aspects of security (e.g. integrity and availability) could be assessed per the existing impact criteria for performance, it may be more relevant to separately rate the entities based on their overall contribution to the system security to include confidentiality, integrity and availability. This presentation will introduce proposed modifications to the RBA assessment criteria to include the information assurance perspective as well as provide an example of applying the process to entities of a specific system. The proposed modifications discussed herein are products of the current IV&V SMA Support Office (SSO) Initiative: Information Assurance Analysis Techniques.

IV&V Lessons Learned from a Memory-Scrub Anomaly

Koorosh Mirfakhraie, NASA IV&V / QinetiQ
Joseph D. Painter, NASA IV&V / TMC Technologies
Lawrence C. Ullom, NASA IV&V / TMC Technologies

ABSTRACT

In this presentation, an anomaly experienced multiple times in the course of routine memory scrubbing performed on a space science mission will be discussed. The anomaly entails a double-bit error in the random-access memory (RAM) of the spacecraft's flight computer. 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. Of particular interest in investigating this anomaly is the component of software responsible for error detection and correction (EDAC). An overview of the EDAC Hamming algorithm utilized on this spacecraft to detect and correct single-bit errors, as well as to detect double-bit errors, is provided. Based on the information learned about the role of the software in this anomaly, recommendations are made to be applied to the future IV&V analysis of space mission software. The resulting improvements in performing IV&V during the development of software should help with identifying issues, whose satisfactory resolution may avert similar anomalies in the future, or will otherwise increase the quality of software and reduce the number of faults introduced during its development.

There and Back Again – Connecting Assurance Statements to Analysis Spreadsheets in Support of Evidence Based Assurance for the Ground Systems Development and Operations (GSDO) Project

Pat Olguin, NASA IV&V / KeyLogic

ABSTRACT

Evidence Based Assurance demands the results of IV&V analyses 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. If direct connections between assurance claims, and current IV&V analyses/results can be established, and integrated directly into the analysts' spreadsheets, a quantifiable measure of assurance/risk for those claims can be derived from the analysts' spreadsheet-based analysis, directly supporting evidence based assurance.

Our objective was to create a useful, low-impact tool that will dovetail into analysts' current methods, enabling them to develop consistent assurance statements, integrate assurance statements directly into their everyday work, provide two-way traceability from high-level assurance statements down to analysis spreadsheets/issues, roll-up results into high-level assurance statement summaries to quantify the level of assurance provided, and to characterize the current/residual risk stemming from missing/delayed artifacts, schedule delays, and the scope of IV&V analysis.

We decomposed high-level claims into supporting assurance statements that were compatible with the level of detail of analysis spreadsheets, incorporated Adverse Conditions into the low-level assurance statements, created mappings between assurance statements and project's software requirements, created a user's guide with examples to help analysts develop assurance statements from reference material, and populated the spreadsheets. Incomplete/delayed analysis was easily identified by empty cells in spreadsheets.

The intent was to provide direct evidence using existing methods/tools to characterize the level of assurance provided to the project, to accurately quantify existing and residual risk, and to incorporate an assurance perspective into our everyday analysis, instead of something to be checked off and left as an appendix to our work.

Our initial results were encouraging. Two-way linkages were created in one easily-understood, familiar-looking sheet. The work required to establish linkages from top-level claims, through supporting assurance statements, and into our spreadsheets was time-intensive. In other words, there is no halfway method to creating this kind of traceability. As for retrofitting previously completed work, it required adding one column to existing master worksheet. That is a very low impact.

Global Precipitation Measurement (GPM) Safety Inhibit Timeline Tool

Shirley Dion, NASA GSFC

ABSTRACT

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. Global Precipitation Measurement (GPM) Mission, which launched from Japan in March 2014, was a joint mission under a partnership between the National Aeronautics and Space Administration (NASA) and the Japan Aerospace Exploration Agency (JAXA). GPM was one of the first NASA Goddard in-house programs that extensively used software controls. Using this tool during the GPM buildup allowed a thorough review of inhibit and safety critical software design for hazardous subsystems such as the high gain antenna boom, solar array and instrument deployments, transmitter turn-on, propulsion system release and instrument radar turn-on. The GPM safety team developed a methodology to document software safety as part of the standard hazard report. As a result of this process, a new tool "safety inhibit timeline" was created for management of inhibits and their controls during spacecraft buildup and testing during I&T at Goddard Spaceflight Center and at the launch range in Japan. The Safety Inhibit Timeline Tool was a "pathfinder" approach for reviewing software that controls the electrical inhibits.

The Safety Inhibit Timeline Tool strengthens the safety analyst's understanding of the removal of inhibits during the I&T process with safety critical software. With this tool, the safety analyst can confirm proper safe configuration of a spacecraft during each I&T test, track inhibit and software configuration changes, and assess software criticality. In addition to understanding inhibits and controls during I&T, the tool allows the safety analyst to better communicate to engineers and management the changes in inhibit states with each phase of hardware and software testing and the impact of safety risks. Lessons learned from participating in the GPM campaign at NASA and JAXA will be discussed during this session.

Automating Evidence Collection for Software Assurance from Existing Status Reports

Robert Inscoe, NASA IV&V / TASC

ABSTRACT

The International Space Station (ISS) team had a need to provide accessible Evidence Based Assurance (EBA) metric data, but system analysis and development of a traditional management system would have a noticeable impact on the team's analysis efforts. Also, the team already records the needed data in a monthly status report, so using a traditional data entry system would duplicate work for each analyst and could introduce inconsistencies between the report and the metrics database. To limit the impact of obtaining the EBA metric data, a software utility was developed that collects software assurance evidence from the existing periodic project status reports. The utility adapts to various writing styles using configuration files that define text constructs that are known to point at embedded data. The presentation will describe the internal data structures and algorithms that work together to extract data from the report inputs. It will describe the data collected, and discuss potential uses of the data by different users in the "IV&V food chain," from NASA management to individual analysts. It will also describe an idea to reverse the concept of the utility, and produce text reports from a database, which could assist teams that already have metric collection systems and need to generate reports to go along with that data.

Use of XSLT to Transform the Output of Multiple Static Code Analysis Tools into a Consistent Analysis Spreadsheet Format

Ben Markle, NASA IV&V / WVHTC Foundation

ABSTRACT

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. Performing analysis of the combined output of multiple tools at once can achieve greater efficiency than separate analysis of each tool's output, because it allows the analyst to quickly identify duplicate findings of multiple tools and to consider distinct findings by multiple tools against a single piece of source code. However, each tool generates output in a unique format that is not consistent with the output of other tools. Tool output can also be represented in a format that requires modification in order to cleanly translate it into a two dimensional spreadsheet.

XSLT (EXtensible Stylesheet Language Transformations), a common web technology, can be used to transform the output of multiple static code analysis tools into a consistent spreadsheet table format that IV&V analysts can use to investigate and disposition the findings. This presentation demonstrates a method using XSLT to automate the process of transforming 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. While the goal is to make dissimilar data look similar, the method is flexible in that the output can be tailored to the needs of an individual analyst or team.

Using the Klocwork and CodeSonar tools as an example, raw XML output of each tool is examined and compared. Relevant information is chosen and organized into a consistent format for output. An XSLT stylesheet is constructed to organize and transform the tool output. The stylesheet is associated with the XML output and then imported into Microsoft Excel. The result is a spreadsheet containing the output from both tools in a consistent format, ready for an analyst to investigate and disposition the findings.

Automated Visual GUI Testing for the Space Network

Charles Song, Ph.D., Fraunhofer Center for Experimental Software Engineering

ABSTRACT

The Space Network is a challenging environment for automated GUI testing. This large software system consists of thousands of individual screens, leverages proprietary GUI libraries and runs on the legacy OpenVMS platform. GUI testing for the Space Network has been completely manual because no existing tools can work in such an environment; this was not only labor intensive but also error prone.

To improve the situation, we developed the Visual GUI Testing approach that leverages computer vision technologies to perform GUI testing via screenshots. Our visual GUI testing tool, PiGuiT (platform-independent GUI testing), can work on any system implemented using any GUI technologies running on any platform

For this ongoing project, we successfully deployed the PiGuiT tool and a set of automated GUI test cases for the Space Network at the White Sands Complex. The deployed set of test cases automates 4-6 hours of testing effort without tester intervention. In this talk, we will present the Visual GUI Testing approach and the PiGuiT tool. We will also share the experiences of implementing automated GUI testing for the Space Network and the challenges that we had to be overcome during the project.

IV&V and the Heartbleed Vulnerability

Rick Hess, NASA IV&V / TASC

ABSTRACT

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 vulnerability was found in the "Heartbeat" section of OpenSSL, which is used to test and keep alive secure communication links without the need to renegotiate the connection continuously. Although there was a patch developed to fix the vulnerability, when the vulnerability was made public, the issue had been in place since December of 2011. Concerns were raised that vulnerabilities like the "Heartbleed" may still be out in the public domain, and could directly affect Software being used in NASA. Since the vulnerability had been out in the public domain for some time, would NASA IV&V have been able to find this particular type of issue if it existed?

IV&V expected that a vulnerability would be detected if a similar problem existed in one of the current pieces of software that was analyzed at IV&V._Based upon the concern mentioned above, SCAWG and SWAT were given an RFA by OOD to determine what static code analysis tools could be used to determine if such a problem existed. This was a quick turnaround activity, since there was a great need to provide assurance that we could detect similar issues within IV&V.

The method used to find this particular vulnerability was part of the "Verify Software Code Quality using Static Analysis Tools" method from the IV&V Catalog of Methods. The intended results were that the vulnerability would be found by one or more tools at IV&V, without extensive effort.

SCAWG and SWAT found that there was at least one tool that successfully identified the Heartbleed vulnerability in OpenSSL. Although it is great to be able to provide the assurance that we could find the vulnerability in question, this brings other questions to light. What kind of testing was performed before OpenSSL released the Heartbeat functionality? Should we be concerned with other Open Source/Third Party applications that are generally accepted?

What IV&V Can Learn from River Guides

Lorelei Lohrli-Kirk, NASA IV&V / TASC
Neal Saito, NASA IV&V / TASC

ABSTRACT

Software independent verification and validation (IV&V) deals with flows of information moving towards a series of gates (e.g., critical design reviews, launch approvals). As developers increasingly employ agile processes to generate system products, IV&V is challenged with managing larger amounts of seemingly chaotic information streams. In the whitewater rafting industry, raft guides have the primary responsibility for the safety of customers wanting to experience the thrill of shooting the rapids on wild rivers. Their jobs involve analyzing hazards, assessing risks and managing teams to safely and successfully perform series of difficult tasks. Techniques used to navigate the fluid dynamics of whitewater have analogies in the fluid information environment of complex projects. 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 Software Assurance Challenges for Commercial Crew Program

Kathy Malnick, NASA IV&V / WVHTC Foundation
Chad Schaeffer, NASA IV&V / TASC

ABSTRACT

This presentation will provide a description of some of the challenges NASA is facing in providing software assurance to the Commercial Crew Program (CCP). The CCP Program is an acquisition. The Program will establish safe, reliable, and affordable access to the International Space Station. The CCP providers have varying experience with software development in safety-critical space systems. NASAs role in providing effective software assurance support to the CCP providers is critical to the success of 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. It is expected that these challenges will exist in future programs, especially if the CCP paradigm proves successful.

The proposed CCP approach to address these challenges includes a risk-based assessment with varying degrees of engagement and a distributed assurance model. This presentation will describe local responses to several of the challenges, but not all.

Static Code Analysis for Information Assurance: Current Practice and Future Directions
PANEL SESSION

Katerina Goseva-Popstojanova, Ph.D., WVU Research Center
Richard Brockway, NASA IV&V / TASC
Van Casdorph, NASA IV&V / TASC
Marcus Fisher, NASA IV&V
Rick Hess, NASA IV&V / TASC

ABSTRACT

NASA develops, runs, and maintains many systems for which software security is of vital importance. Static code analysis provides a scalable method for security code review. Over the years, NASA's IV&V Program has developed expertise in using static code analysis for verification and validation focused on identification of software bugs that affect the correctness and performance of software systems. Since some software bugs are actually security vulnerabilities that can be exploited to launch cyberattacks on NASA systems, it is becoming an imperative to leverage the current IV&V practices with information assurance capabilities.

This panel is focused on using static code analysis for detection of security vulnerabilities. The panelists will address both theoretical and practical advantages and limitation 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.

The objectives of the panel are to address the current state-of-art and state-of-practice in using static code analysis for information assurance and to promote open discussion on NASA projects' needs and challenges, and potential future directions.

Metrics for V&V of Cyberdefenses

Martin Feather, NASA JPL / California Institute of Technology
Joel Wilf, , NASA JPL / California Institute of Technology
Joseph Priest, , NASA JPL / California Institute of Technology

ABSTRACT

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. Our hypothesis is that our adaptation of a traditional V&V workflow, coupled with collection and presentation of the appropriate metrics for each stage of that workflow, will serve this evaluation need. We aim to develop and demonstrate this approach on representative cyberdefenses executed in a cybertesting laboratory.

The steps of our adapted workflow are:

1. Setup – Identify key aspects of the flight project environment, its vulnerabilities (motiving the defense), and the defense itself, all of which form the basis for configuring the test environment.
2. Attack – Conduct the attack(s) in an undefended test environment and capture metrics of the attack
3. Defend – Deploy the defense in the test environment and measure its characteristics under both attacked and un-attacked conditions.
4. Verify – Gather metrics of the flight project environment to assess the fidelity of the test environment; extrapolate from the metrics in the test environment to predict their equivalent in the project environment, and on that basis determine whether to proceed with, revise, or abandon the defense.
5. Validate – Carefully field the defense in the project environment to decide on its permanent deployment, and, if necessary, to improve the fidelity metrics.

We have preliminary results from developing and testing alternative defenses from a plausible (believed to have occurred elsewhere) reconnaissance cyberattack. Our work includes elaboration and gathering of the cost, benefit and fidelity metrics that guide progress through the workflow. Our elaborated metrics cover computational resource and budgetary costs, effectiveness of the defense, inconveniences and risks (if any) introduced by the defense and fidelity measures necessary to characterize the test versus flight project environments. We are working towards presenting the metrics through visualizations (e.g., a time chart visualization of the CPU etc. costs of the defense; a radar chart to summarize each defense's characteristics in terms of project-relevant metrics).

Get Confidence in Mission Security with IV&V Information Assurance (IA)

Rich Brockway, NASA IV&V / TASC
Brandon Bailey, NASA IV&V

ABSTRACT

Systems must operate securely in order to operate safely and reliably. How does NASA's IV&V Program provide mission security assurance throughout the design, development, implementation, operation, maintenance, and disposition of information systems?

NASA's IV&V Program has a role for assessing and monitoring security controls as highlighted in NIST 800-37, Guide for Applying the Risk Management Framework to Federal Information Systems – A Security Life Cycle Approach. V&V security analyses are specified throughout the development life-cycle in IEEE-1012, Standard for System and Software Verification and Validation. What techniques should NASA's IV&V Program use to fulfill its role to ensure appropriate security controls are selected, implemented, tested, and maintained to sufficiently protect the confidentiality, integrity and availability of mission systems and information?

Participants will discover how to "Get Confidence in Mission Security with IV&V IA" by: surveying the threat landscape and the ever-increasing risks of disruption to mission operations, exploring the regulatory framework for security assessment and authorization, examining the IA methods, practices, and techniques that NASA's IV&V Program is integrating into its analyses, and learning how the NASA IV&V Program's objective role and disciplined processes equip mission stakeholders with the basis for making informed, risk-based decisions throughout all phases of the system life-cycle.

IRSim: A Web-Based Tool for Establishing Traceability Links among Software Artifacts

Dharmalingam Ganesan, Ph.D., Fraunhofer Center for Experimental Software Engineering
Mikael Lindval, Fraunhofer Center for Experimental Software Engineering

ABSTRACT

During software V&V, analysts often face the challenge of establishing traceability links among artifacts such as requirements, source code, test cases, etc. To help analysts in this non-trivial task, we developed a web-based tool that suggests traceability links among the exported software artifacts. The tool, which is based on information retrieval technologies, is used to automatically index, search, and match texts from the different artifacts. The tool computes token-based similarity scores for each of the artifacts and links, e.g., each requirement to the corresponding source code functions where the requirement is implemented. Since the tool is web-based, the analyst can then use the traceability links to navigate between artifacts, e.g., requirements and code. In this presentation, we will give an overview of the different features of IRSim.

We will also present an empirical study in which we evaluated IRSim by applying it to NASA's Core Flight Software (CFS). We first manually established a golden model that shows exactly where each requirement is implemented in the code. We then let the tool automatically conduct the same tracing and compared the outcome to the golden model. The results from the study show that IRSim is able to successfully trace 85% of the requirements to source code functions.

Capturing Autonomy Features for Unmanned Spacecraft with ARE, the Autonomy Requirements Engineering Approach

Emil Vassev, University of Limerick
Mike Hinchey, University of Limerick

ABSTRACT

Along with the traditional requirements, requirements engineering for autonomous and self-adaptive systems needs to address requirements related to adaptation issues, in particular: 1) what adaptations are possible; 2) under what constrains; and 3) how those adaptations are realized. Note that adaptations arise when a system needs to cope with changes to ensure realization of the system's objectives. To handle these and other issues, Lero - the Irish Software Engineering Research Center has developed the Autonomy Requirements Engineering (ARE). Basically, ARE converts adaptation issues into autonomy features where goal-oriented requirements engineering (GORE) is used along with a model for generic autonomy requirements (GAR). The approach is intended to help engineers develop missions for unmanned exploration, often with limited or no human control. Such robotics space missions rely on the most recent advances in automation and robotic technologies where autonomy and autonomic computing principles drive the design and implementation of unmanned spacecraft.

By using ARE, software engineers can determine what autonomic features to develop for a particular unmanned spacecraft. The inputs required by this approach are the system goals and domain-specific GAR reflecting the specifics of the domain of the system-to-be. Note that ARE has been developed as part of a contract with ESA, the European Space Agency, where ARE was applied to a proof-of-concept case study, to capture autonomy features of the ESA's BepiColombo Mission.

The ARE approach starts with the creation of a goals model that represents system objectives and their interrelationships for the mission in question. Goals models might be organized in different ways copying with the mission specifics and engineers' understanding about the mission goals.

The next step in the ARE approach is to work on each one of the system goals along with the elicited environmental constraints to come up with the self-objectives providing the autonomy requirements for this particular system's behavior. In this phase, we apply our GAR model to a mission goal to derive autonomy requirements in the form of goal's supportive and alternative self-objectives along with the necessary capabilities and quality characteristics.

The Challenges of Assuring Vision Systems for Space Missions

Charley Price, NASA IV&V / TASC
Vincent Howard, NASA IV&V / TASC
Jeremy Yagle, NASA LaRC

ABSTRACT

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. Vision systems consist of cameras and software processing of the camera images to extract key geometric information of a workspace for input to a spacecraft/rover/manipulator actuation system to operate in that workspace.

The challenges for NASA's IV&V Program for assuring such vision systems include characterization of the risks associated with vision system requirements, design, and testing methods; determining the stability of the vision algorithms under changing environments; and developing methods of identifying these risks during IV&V. This paper will expand on these risks, and will describe recently developed assets to support IV&V of vision systems, including a vision system information base, a space mission vision system technical reference, and a hands-on vision workstation for training IV&V analysts with limited experience with computer vision theories and applications—which also provides them with a method to independently test and verify developer's solutions.

The vision system information base consists of case studies, literature review, and tutorials developed that support identifying risks involved with such systems. Applications other than space are included, such as self-driving cars, UAV's, AUV's and medical technology for comparison. The technical reference for expected vision system characteristics for the asteroid redirect and satellite servicing missions includes operational, configuration, and environmental considerations. The laboratory vision system workstation enables assessing vision algorithms against various targets and imaging streams for different lighting conditions, background composition, and target characteristics to establish a reference of algorithm performance for use by IV&V analysts.

Robotic Systems for OSIRIS-REx, Asteroid Redirect and Mars 2020 Missions Q&A PANEL SESSION

Charley Price, NASA IV&V
Dr. Thomas Evans, WV Robotic Technology Center
Andre Sylvester, NASA JSC
David Turner, NASA IV&V
Vincent Howard, NASA IV&V

ABSTRACT

Future NASA missions for asteroid redirect (ARM) and satellite servicing (SS) will have robotic systems with associated levels of autonomy. This panel, all active in the development of these missions, will discuss the elements of ARM and SS, and provide insight into how NASA is preparing for the technological advances required for mission success. The panelists will be provided with orientation information from the NASA IV&V Program's charter and practices and a list of thought-provoking question about the panel objectives. In an effort to stimulate vigorous audience participation and discussion, questions will be solicited from the audience and on-line participants at the beginning of the session. All audience questions will be addressed, either during the panel or in an immediate follow-on session.

Sketch Theory as a Framework for Knowledge Management

Ralph Wojtowicz, Baker Mountain Research Corporation

ABSTRACT

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. Knowledge management involves many challenges including storing and retrieving data; representing types, relationships and constraints; aligning overlapping or inconsistent information; uncertainty; extracting context-relevant views of data and meta-data; dynamics; reasoning; and decision-making. Established frameworks include mathematical logic, relational databases and the semantic web. Each has particular strengths but also limitations.

Sketch theory was introduced in abstract algebra in 1968. Applications to information modeling emerged in the 1980s. Our research objectives are to develop and demonstrate sketch theory as a complementary knowledge management technology capable of solving the challenges of knowledge alignment, context, and uncertainty. In this talk we will give an introduction to the theory and examples of it in action.

Distinct knowledge models can represent common concepts differently (e.g., 'uncle' vs 'brother of parent'). This is the source of the knowledge alignment problem. In sketch theory we solve this problem via the Carmody-Walters algorithm. In logic, the analogous construction is an infinite and abstract syntactic category. In the semantic web, derived concepts are built manually via ontology rules.

Modularity is a key paradigm for enabling humans to develop reliable, complex systems. A strength of sketch theory is its support for modular development: meta-data, instance data and uncertainty are specified independently. This contrasts with the semantic web, for example, in which ontologies integrate all these components into a monolithic document. Sketch maps, moreover, are a precise tool for modeling knowledge dynamics.

Effective use of context can greatly reduce the complexity of information system problems. Sketch theory provides a rich notion of view of meta-data and instance data. We will demonstrate this construction and describe a program for adapting new context-sensitive Internet search techniques to this richer problem domain.

Mathematical logic and the semantic web have components for rational inference based on available data. Lack of a reasoning engine has been missing from sketch theory. We will demonstrate a novel approach to sketch-based reasoning using the notion of Q-trees.

End-to-End Fault Management Analysis Method, Results and Future Improvements

Ryan Starn, NASA IV&V / TASC

ABSTRACT

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.

Methods 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 are required for IV&V.

A two-phased approach for establishing a method to provide assurance efficiently and effectively up to and beyond the launch of the project has been identified.

- Phase 1 (Traceability) – Use a database to capture FM artifacts (FMEA, FTA, Fault Algorithms, etc.) and relationships between them to build a traceability matrix for assurance. Analyze the relationships and reliance on software to ensure the appropriate software requirements are established, implemented, and verified.
- Phase 2 (Conflict Analysis) – Use a Quasi-Dynamic model of the system to analyze the potential for conflict based on local, global, scripted, and automated behaviors. The model should interface with the database to establish coverage and dependency. Use these "suspect" scenarios in a fully dynamic, high-fidelity simulator to uncover actual problems.

The goals of this approach are:

- Creating a strong evidence-based case for software FM assurance through traceability.
- Uncovering gaps or conflicts in the software requirements (Validation) based on the needs of the system and the need to preserve safety of the mission assets.
- Establishing high risk independent test scenarios.

Our IV&V team has used Phase 1 of the method to analyze a project's FM design with the following results:

- Uncovered (331) issues against the developer's spacecraft element FM assurance matrix.
- Uncovered two Severity-1 and one Severity-2 TIMs identifying missing FSW requirements.

IV&V has effectively used the End-to-End database method to uncover significant findings. Work is on-going to improve the method and expand into the second phase by developing the quasi-dynamic model. The first phase (and associated processes) have been effective for the IV&V team and can be applied to other IV&V teams and projects.

NASA IV&V Software Emulator Technology Portfolio

Justin Morris, NASA IV&V
Matt Grubb, NASA IV&V / TMC Technologies

ABSTRACT

Software-only simulations have been an emerging but quickly developing field of study throughout NASA. The NASA Independent Verification & Validation (IV&V) Independent Test Capability (ITC) team has been rapidly building a collection of simulators for a wide range of NASA missions. ITC specializes in full end-to-end simulations that enable developers, V&V personnel, and operators to "test-as-you-fly." In four years, the team has delivered a wide variety of spacecraft simulations that have ranged from low complexity science missions such as the Global Precipitation Management (GPM) satellite and the Deep Space Climate Observatory (DSCOVR), to extremely complex missions such as the James Webb Space Telescope (JWST).

This paper overviews the technologies and processes that have been utilized to design, implement and deploy end-to-end simulation environments for various NASA missions. The paper describes how these technologies are utilized within our organization and how they have benefited other organizations.

Space Hardware

Justin Morris, NASA IV&V
Steve Yokum, NASA IV&V / TMC Technologies

ABSTRACT

NASA's 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. Typically, NASA's IV&V Program does not have access to the necessary hardware components to adequately V&V specific hardware/software interactions and anomalies. Although there are methods to accomplish V&V objectives in these situations; it has proven important to continue to mature the JSTAR hardware capabilities of the IV&V program. This paper will describe a specific mission anomaly and how the Jon McBride Software Testing and Research (JSTAR) hardware test environment was utilized to perform independent testing.

Assessment of Fault Management in Network Resource-Intensive and Protocol-Rich Environments

Tom Hempler, NASA IV&V / TASC

ABSTRACT

The NASA Space Network Ground Segment Sustainment (SGSS) project has delivered hundreds of engineering artifacts to NASA's IV&V Program for analysis and assurance that the SGSS system components will function correctly (Q1), handle operational anomalies sufficiently (Q2), and withstand adverse environmental conditions successfully (Q3) to provide reliable 24/7 Space Network data relay services [1]. The SGSS IV&V team used the Portfolio Based Risk Assessment process to make decisions on the mission critical and safety critical aspects of system components on which to focus our analysis. We scoped our analysis to focus on SGSS program stated priorities and keep pace with the developer's artifact and code deliveries.

Ensuring the SGSS Ground Station implementation provides sufficient coverage of Q1, Q2, and Q3 is challenging. This is due to 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 paper. 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. Fault management in high availability (24/7) systems such as SGSS Ground Stations and Tracking and Data Relay Satellite (TDRS) satellites is mission- and safety-critical.

A new perspective on fault management and analytical techniques exploiting Java's exception and error handling framework is presented. Applying fault management analysis techniques to the Java exception handling framework facilitates Q2 implementation verification and provides an assessment of fault tolerance in network resource intensive and protocol rich environments; all of which are discussed in this paper.

[1] Please visit http://www.nasa.gov/centers/ivv/services/services_index.html for more information on the NASA IV&V Program's three questions.

Scoping and Analysis of FPGAs from an IV&V Perspective

Pradip Maitra, NASA IV&V / TASC
John C. Ryan, NASA IV&V / TASC

ABSTRACT

Recent years have seen an explosion of field-programmable gate array (FPGA)-based systems in day-to-day activities, including automobiles, household appliances, intelligent systems and the space program itself. The ability to incorporate a simple CPU/memory subsystem using just one cost-effective FPGA is one of its many advantages.

The NASA IV&V Program's traditional approach to assessing FPGAs has been to categorize them in the class of pure hardware which is out of the realm of software IV&V. As the technology and customization of FPGAs has increased, the NASA IV&V Program's scoping approach is questionable as the CPU/memory subsystem created by the FPGA is able to execute downloadable code, or in other words, it offers stored program execution. The increased ability to execute downloadable code also provides the capability to provide software updates for satellites in operation.

In this paper, we propose a number of criteria for scoping FPGAs and then detail some procedures on how to perform IV&V analysis on them.