

Combined A5-T5 Session
Use of Formal Methods in V&V/ Formal Systems and Their V&V Utility

Session A5-T5 leaders:

Co-Chairs:

Dan Craigen (ORA, Canada)

Dirk Brade (Universität der Bundeswehr München, Germany)

Session Recorder: **Brad Martin** (NSA)

A5 Materials in Foundations '02 Proceedings:

Papers

Cost Effective Use of Formal Methods in Verification and Validation (38 pp)

[A5T5_kuhn]

Richard Kuhn (NIST)

Ramaswamy Chandramouli (NIST)

Ricky W. Butler (NASA/Langley Research Center)

Infusing and Selecting V&V Activities (15 pp) [A5T5_feather]

Martin Feather (NASA Jet Propulsion Laboratory (JPL) at Cal Tech)

Slides (may contain back-up materials and notes)

Cost Effective Use of Formal Methods in Verification and Validation (18 slides)

[A5T5B_kuhn in both pdf & ppt formats]

Richard Kuhn (NIST)

Ricky W. Butler (NASA/Langley Research Center)

Security Functional Testing Using Model-based Test Automation Approach (22 slides)

[A5T5B_Chandramouli in both pdf & ppt formats]

Ramaswamy Chandramouli (NIST)

Infusing and Selecting V&V Activities (29 slides) [A5T5B_feather in both pdf & ppt formats]

Martin Feather (NASA Jet Propulsion Laboratory (JPL) at Cal Tech)

A5T5 Participants are identified at the end of this document

Discussion Synopsis (this material is to provide perspective on papers and briefings mentioned above – it should not be used without that context)

Paper Abstracts:

Cost effective use of formal methods in verification and validation authored by Richard Kuhn, Ramaswamy Chandramouli and Ricky W. Butler.

Formal methods offer the promise of significant improvements in verification and validation, and may be the only approach capable of demonstrating the absence of undesirable system behavior. But it is widely recognized that these methods are expensive, and their use has been limited largely to high-risk areas such as security and safety. This paper focuses on cost-effective applications of formal techniques in V&V, particularly recent developments such as automatic test generation and use of formal methods for analyzing requirements and conceptual models without a full-blown formal verification. We also discuss experience with requiring the use formal techniques in standards for commercial software.

Infusing and selecting V&V activities authored by Martin Feather.

The evolving nature of software development poses a continuing series of challenges for V&V. In response, the V&V community selectively adapts the use of existing V&V activities, and introduces new and improved ones.

These responses are instances of the more general issues of technology selection and technology infusion. These are recurring challenges at JPL where novel spacecraft applications demand novel adaptations of existing technologies, and infusion of new ones. JPL has been developing and applying a process specifically to assist in the planning for these. This paper shows how this same process has the capacity to aid in planning the selection and infusion of V&V activities.

Session Report

1. The session started with presentations from Rick Kuhn, Ramaswamy Chandramouli and Martin Feather. Amongst the points discussed by Rick Kuhn were:
 - Formal techniques can serve as the foundation for the V&V techniques (DMSO 2001).
 - Kuhn discussed where to apply formal methods in the lifecycle.
 - Advocated new approaches using lightweight verification and test case generation in addition to traditional approaches. Kuhn discussed when and where these methods make sense.
 - Formalizing the specification may be the most valuable part of a formal verification. The main benefit is through the improvement of the precision of specifications.
 - Regarding the analysis of formal artifacts, Kuhn described two main flavors of tools: theorem-proving and model checking
 - It was noted that verification can be viewed as “are we building the system right” whereas validation relates to “are we building the right system.” In the context of modeling and simulation, lightweight formal methods could be applied to conceptual model validity and computer model verification.

- Through examples derived from FIPS 140-1 experiences, Kuhn reported on the successful application of formal methods in certification standards. He also discussed the history of formal methods as it related to the US DoD Trusted Computer Security Evaluation Criteria (TCSEC). Dorothy Denning was cited as having argued that formal methods were prohibitively expensive in the context of TCSEC. Further problems related to the long evaluation process vis-a-vis market timing, and the need for a large market. Kuhn discussed some of the lessons learned from using TCSEC resulting in a changed perspective with regards to the requirements for formal methods in FIPS 140-1. These included giving developers the option of using either formal (machine aided) or informal proofs. Furthermore, instead of having a single accrediting government agency, FIPS 140-1 has a set of accredited commercial laboratories. As a result, formal methods have been successfully used within FIPS 140-1.
- It was claimed that there is an additional requirements and design phase costs of around 10-15% through the use of formal methods. Kuhn discussed a table that suggested anecdotal evidence of overall cost savings through the use of formal methods.
- Finally, Kuhn reported that his view on the formal methods implications for M&S are certified components, requirements validation, and automated test generation for one-of-a-kind systems.
- In the ensuing question and answer session we had the following interactions:

Q: How do tools/techniques become accepted by non-software engineering cadre?

Answer: Use of notations (such as state tables) that are more easily accepted by non-software engineering technical folks.

Q: Is there a practical use for formal methods in M&S?

Answer: Yes.

2. Kuhn's presentation was followed by his co-author Ramaswamy Chandramouli (Mouli). Mouli's focus was on Model-based automated security functional testing (TAF-SFT Toolkit).
 - Mouli discussed the differences between security testing and traditional software conformance testing. Hence, security functional testing versus security vulnerability testing
 - The Test Automation Framework (TAF) is aimed at improving the economics of security functional testing through end-to-end tool support. Currently, security function testing is rarely performed because of the cost and complexity.
 - TAF automatically translates SCR into T-VEC test specifications, generate test vectors and perform coverage analysis. The TAF-SFT Toolkit uses the following process:
 - Develop behavioral model – SCR tabular spec
 - Translate SCR spec to T-Vec Test spec – automatic
 - Generate test vectors to perform coverage analysis – automatic
 - Develop test driver schemas for target test environment
 - Generate test drivers, execute tests, generate test report – automatic
 - Mouli discussed the TAF-SFT Toolkit Architecture and briefly discussed SCR tabular representation notation.

- Mouli observed that the formal specification can be used to create both input stimulus and expected outputs for testing purposes.
- Mouli then discussed an example application of TAF-SFT toolkit to the Oracle DBMS security functional testing.
- Advantages are better quality of specifications and quality of test data, automated coverage analysis, generation of test code and results analysis.
- Disadvantages are detailed knowledge of security function semantics required for the modeler and development of object mapping information laborious for products with complex interfaces.
- A particular conclusion from the talk was that there is some possible reuse of SCR concepts and Object Mapping Information from project to project. Interoperable security APIs, like CDSA and some cryptographic APIs are potential candidates for this approach to reuse.
- In the ensuing question and answer session we had the following interactions:

Question: What were the savings from the use of the toolkit?

Answer: No quantitative measurement made. Future work on common-access-card spec will provide more scientific measurement.

3. After the two NIST presentations, JPL's Martin Feather presented his paper on infusing and selecting V&V activities.

- Feather observed that he had worked in the SQA group.
- With software increasing dramatically and is becoming more complex, Feather asked how can one best use one's QA resources.
- He observed that a challenge (for flight software) that was easy to say, but difficult to manage, for example,
 - How do we determine the right set of assurances?
 - What are the benefits?
 - What are the risks?
 - Are there unnecessary redundancies in assurance activities?
 - Is there a way to optimize these assurance activities?
- When and where do these methods make sense?
- Feather presented a hypothetical V&V Pyramid (analogous to the FDA nutrition pyramid), that included suggestions of optimal use of assurance methods.
- So, Feather's objectives are to improve infusion of V&V techniques and to improve development process and products.
- Feather and his colleague Steve Comford take that view that assurance activities "filter out" mission risks.
- Feather then went on to discuss his DDP tool: A quantitative model of risk and means to reduce it. Risks, should they occur, cause loss of objectives. Assurance activities, if they are applied, reduce risks by preventing, detecting or alleviating. One should analyze whether project assurance activities have been optimized to cover risks. In many instances, a collection of assurance activities may miss certain risks or may be overly redundant.
- Risk as a resource: www.hq.nasa.gov/office/codeq/risk/.

- Feather provided the discussion group with a topology perspective on DDP Risk Model.
- With the DDP risk model, it was noted that the benefit equals the sum of attainment of objectives and that cost equals the sum of mitigation and repairs.
- DDP is to be applied very early in the lifecycle, when one lacks detailed and/or well-understood designs. All approaches must scale to large problems. Feather observed that there has been initial reluctance to using DDP because of skepticism relating to the value of the process, even though there is anecdotal evidence of success.
- Feather then demonstrated the DDP tool
- V&V selection is an assurance optimization problem: <http://ddptool.jpl.nasa.gov>
- Discussion of optimizing data sets for maximizing benefit and minimizing cost, including the use of simulated annealing or Tim Menzies' optimization techniques.
- In summary, Feather was in essence discussing a Bayesian-like weighted network interconnecting objectives, risks and mitigation objects.
- In the ensuing question and answer session we had the following interactions:
Question: Where did you get quantitative numbers?
Answer: Asked experts.

Question: How accurate are the experts?

Answer: Some analysis in this area but not very mature regarding understanding of confidence of experts.

4. Discussion

- An observation was made that in the automotive industry there is substantial simulation, but little V&V. In contradistinction, it appears that government-related efforts perform substantial V&V. It was noted that this may not be a difference between commercial and governmental efforts, but have more to do with financial resources.
- As the discussion continued, it was noted that 50% of the cost in aviation is validation. Substantial amount of Airbus code is automatically generated.
- There was some discussion on the use of formal methods within specific domains, but making sure that while the advantages of formal methods accrue, the complexity is hidden (invisible formal methods).
- The importance of V&V is directly related to the consequences of failure.
- There was a generalized discussion on the semantics of V&V and it was noted that formal methods has a role in both verification and validation.
- Formal methods can be used to increase automation. 70% of code in the airbus is automatically generated.
- Feather was asked how he developed the values for risk, etc. He asks experts on what the estimated values should be. They also perform sensitivity analysis.
- One participant suggested that almost all M&S systems are over schedule, over budget, and under-delivered. Highly suggestive that current processes are inadequate.
- A discussion ensued on rapid prototyping and executable specifications.
- Discussion then focused on the actual value added of formal methods. Some claimed that it was uncertain that formal methods added anything to the design phase. Formal

methods are better, like most mathematics, when you wish to prove some properties. Hence, a claim that formal methods is better on validation, not on design. However, some argued that there are benefits from early stage debugging.

- Discussion about the value of formal specification of models with respect to the application of formal V&V methods.
- It was noted that formal methods have been successfully used in reverse engineering commercial software, formalizing and then analyzing.
- Formal methods was viewed by some as a computing science technology while simulation is closer to information systems. It was claimed that simulation is more willing to accept internal inconsistencies.
- How does one check the fidelity of simulation, especially for future-based scenarios.
- High level validation is a bit outside the scope of formal methods.
- A question was raised on whether from a Department of Defense acquisition sense, if formal methods could play a role regarding COTS. Kuhn responded yes.
- The group started to discuss where formal methods can provide improvements in M&S and where it was appropriate? Some claimed that viability depended upon the maturity of the simulation. The greater the maturity the more likelihood that formal methods would be valuable. It was further claimed by some that the technology was not as useful in simulations of future-set scenarios.
- Participants noted that it would be useful to have a catalogue of techniques that can be used in V&V. For example, a manager's handbook (which, for example, would include predictability of cost when using formal methods). Reference was made to the SimVal'99 workshop, in which various formal methods were listed, but not assessed.
- By the end of the discussion, it seemed as though the non-formal methods participants felt that there were possibilities for formal methods, but were still not sure of actual applicability.

5. Conclusions/Themes

- It would be useful to have a catalogue of formal methods techniques with indications of what they are capable of, when they should be used, and what their cost profile is.
- The M&S experts appeared to come to the conclusion that there were possibilities in using formal methods within M&S, but were still uncertain of actual applicability.

A5 Session Participants (21)

First Name	Last Name	Organization
Richard	Bernstein	JHU/APL
William	Blackert	Johns Hopkins University/APL
Dirk	Brade	ITIS
Ranaswamy	Chandramouli	Nat'l Inst. of Standards & Technology
John	Christakos	OSEC
Dan	Craigen	ORA Canada
Martin	Feather	NASA Jet Propulsion Laboratory/Cal Tech
Richard	Hills	New Mexico State University
Scott	Hilterbrick	Johns Hopkins University
Rene	Jacquart	ONERA-DTIM

Heikki	Joonsar	SAIC
Andreas	Koester	ITIS e.V.
Kenneth	Konwin	Booz Allen Hamilton Inc.
Richard	Kuhn	NIST
Eric	Lazur	JHU/APL
Robert	Lewis	Boeing
Brad	Martin	NSA
Ann	Pollack	John Hopkins University
Sean	Price	Cranfield University
William	Stevens	NASA-LARC
William	Tucker	The Boeing Company