WILLIAM J. HUGHES TECHNICAL CENTER

MODELING FOR VERIFICATION AND VALIDATION: Tapping into the Perspectives and Challenges of Government, Industry, and Academia

White Paper

September 22, 2015

Peter D'Amico
Verification and Validation Strategies and Practices Branch (ANG-E5A)

Clifton Baldwin, PhD
NAS Systems Engineering Integration, Strategic Initiatives (ANG-B6)

FAA WILLIAM J. HUGHES TECHNICAL CENTER
ATLANTIC CITY INTERNATIONAL AIRPORT, NEW JERSEY 08405

TABLE OF CONTENTS

LIST OF FIGURES

1. INTRODUCTION

1.1. BACKGROUND

On September 22, 2015 the first workshop on Model Based Systems Engineering (MBSE) was held in conjunction with the Verification and Validation (V&V) Summit at the William J. Hughes Technical Center (WJHTC). This paper is based on information presented and discussions held during the "Modeling for Verification and Validation" workshop in which subject matter expert presenters from organizations including NASA, Boeing, Carnegie-Melon, INCOSE, UK-NATS, and Noblis were in attendance. This year also marked the 10th anniversary for the V&V Summit, which is held every year to gather speakers from a wide range of industry and academia backgrounds to address innovative methods and strategies that embrace V&V philosophies and principles critical to moving the Next Generation Air Transportation System (NextGen) and FAA Enterprise Architecture (EA) initiatives forward.

The workshop was organized by John Frederick, Manager of the Verification and Validation Strategies and Practices Branch (ANG-E5A), and Natesh Manikoth, ANG Chief Scientist for Software (ANG-4). The primary goals of the Modeling for V&V workshop were as follows:

- Discuss the theories and uses of modeling to support the verification and validation of concepts, requirements, designs, systems, and operations.
- Identify practical techniques, practices, and model based systems engineering methodologies that employ various types of modeling in a product life cycle (especially early in the life cycle).
- Address the challenges of modeling complex systems and concepts that have emergent behaviors.

The exchange of concepts, ideas, and philosophies applied throughout the industry is a valuable tool, and while there may not be any certain answers to the issues presented in this paper the primary emphasis here is to set the wheels in motion by exposing the common challenges faced in the real world and to work towards realizing a positive change within the FAA. This workshop should mark the beginning of an iterative process that builds upon itself and improves every time so that we may eventually solve these issues.

Section 2 of this paper provides an overview of each speaker along with their main points of discussion. Section 3 documents the common challenges encountered among the presenters. Finally, the summary and conclusion comprise Section 4.

This paper was prepared by engineers within the NextGen organization [an Engineer in the V&V Strategies and Practices branch] with limited consultation with managers or other staff of that organization. Accordingly, this document does NOT represent official FAA policy or proposals for policy change. The purpose of this document is to stimulate responsible discussion within the

community regarding the need for improved approaches to Verification & Validation as well as MBSE.

2. SPEAKERS

William D. Miller – INCOSE and Stevens Institute of Technology:

Bill Miller is the executive principal analyst with Innovative Decisions, Inc. and an adjunct professor of systems engineering at the Stevens Institute of Technology. He is the editor of Insight, a publication of the International Council on Systems Engineering (INCOSE), and has previously served on the Board of Directors as Technical Director.

Bill opened the presentations by asking "Why Model" and proceeded to provide some definitions for a modeling vocabulary including the differences between physical models and abstract models (Figure 1). He specified that modeling is capable of providing cost avoidance and the ability to validate requirements, architecture, systems, and performance as well as the ability to verify against requirements. His presentation concluded by identifying some success stories, such as the Manhattan Project, the development of the Boeing 777, and the use of modeling for semiconductors and lithographic machines.

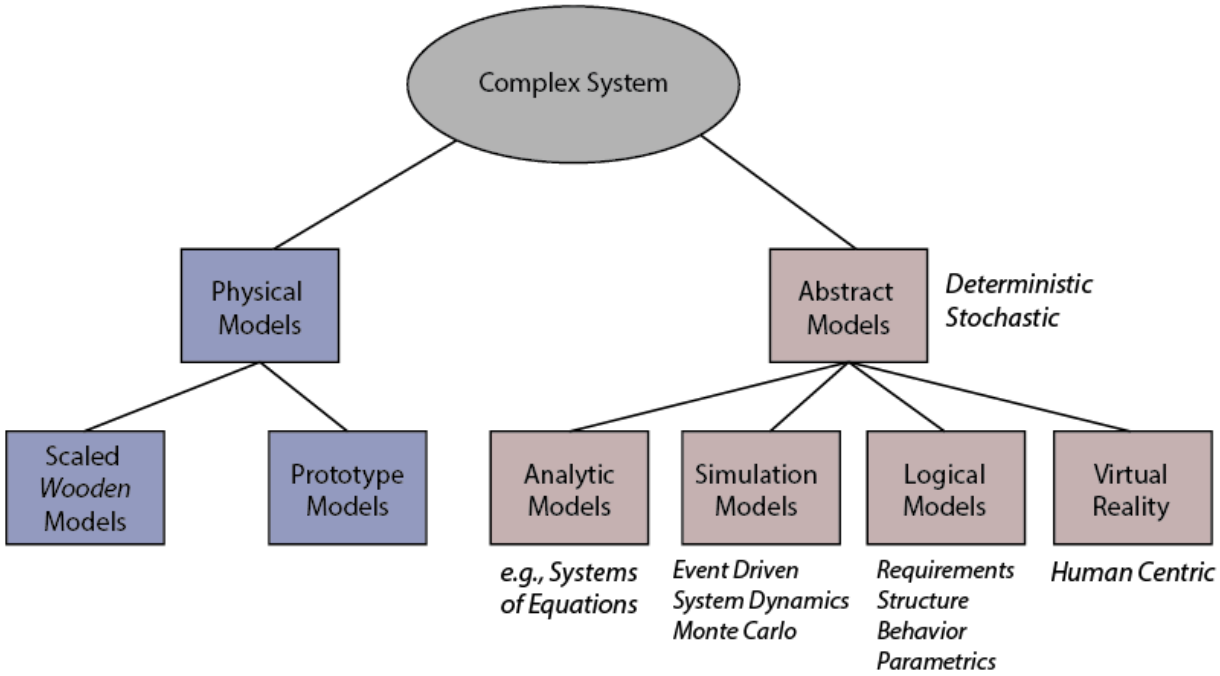

Figure 1. Models used to describe a complex system presented by Bill Miller

There were a few key lessons indicated in the presentation. Bill stressed the importance of including performance as well as structure. The models need to be useful and illuminating. Despite the pressure to cut costs, cheap models do not usually perform well. Finally, the modeler needs to be aware of emergent behaviors that may be present in the system to be

modeled. Therefore stochastic models are as important as deterministic models. Often stochastic models are forgotten or just avoided.

Mark Flanigan and Simon Daykin - National Air Traffic Services United Kingdom (NATS UK):

NATS UK is the main air navigation service provider in the United Kingdom. It provides En Route air traffic control services to 2.2 million flights within the UK Flight Information Regions and the Shanwick Oceanic Control Area, and provides air traffic control services to fourteen UK airports, including Heathrow and Gatwick. Mark Flanigan's current role is General Manager Customer Solutions, which leads Innovation, R&D, Analytics and Commercial Solutions Development in NATS for its United Kingdom and global customers.

Simon Daykin is responsible for the overall design of the NATS operational systems, ensuring that current and future systems developments are aligned with business and operational strategy. Simon discussed the importance of creating a model that everyone can understand when working with different organizations, technologies, platforms, systems and promoting a common view of capabilities. An advantage of models is that they can be used to capture emergent behavior. However, there are challenges associated with modeling safety and security. There are also significant challenges when using commercial off-the-shelf (COTS) technology.

Donald Firesmith – Software Engineering Institute (SEI) Carnegie Mellon:

Don Firesmith is a Principal Engineer at the Software Engineering Institute, where he helps the US Government acquire large, complex, software-reliant systems. With over 35 years of experience working as a software and system engineer, he is internationally recognized as an expert in requirements engineering, system and software architecture, object-oriented development, testing, and process engineering.

Mr. Firesmith began by expressing some challenges which drive model testing. He mentions that requirements defects are very common and that many of these requirements, architecture, and design defects are not exposed and fixed until after significant effort has been wasted on implementing them. Factors like the delay of testing until the software exists causes problems such as increased difficulty in debugging. He also stressed the importance of modeling for moving test earlier in the system lifecycle, which he called the "V model" (Figure 2). The term "V" refers to the systems engineering V model. The V model is a graphical depiction of the system life cycle, and although it is often confused as a linear model, it represents an iterative life cycle. In any case, the point was modeling helps the systems engineer test executable requirements, architectural models, and design models prior to system development. However the models are as important for analysis. Therefore they are useful for more than test.

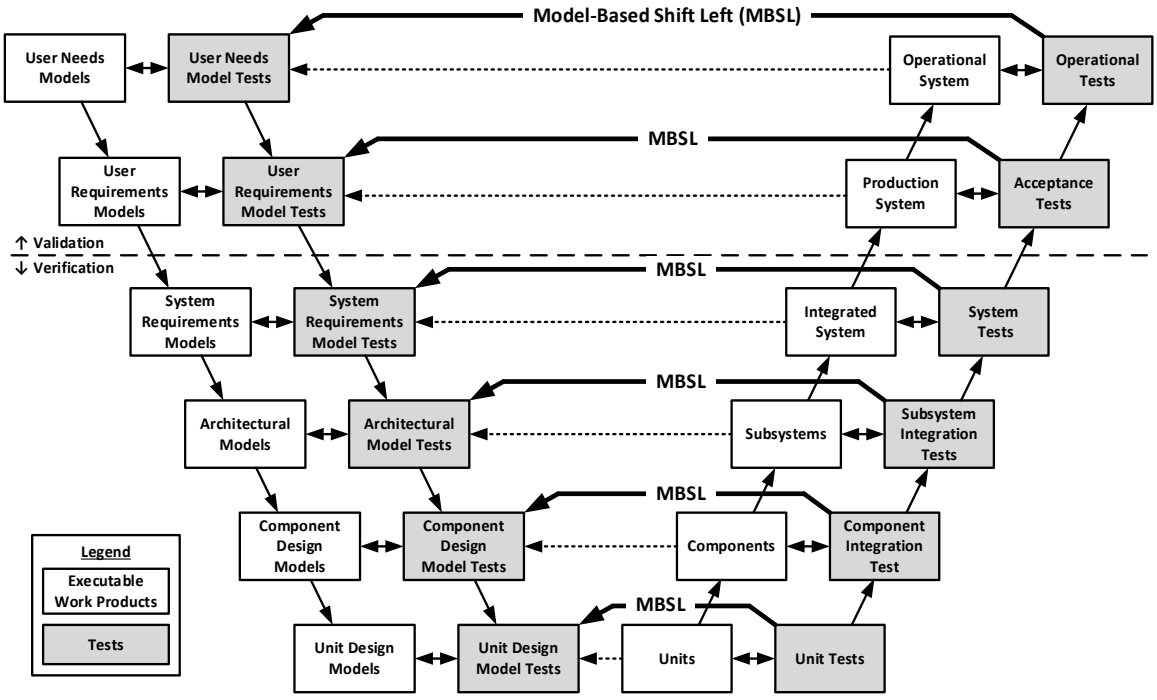

Figure 2. Model Based Shift Left Testing presented by Donald Firesmith

For completeness, Mr. Firesmith presented three other ways to test earlier in the lifecycle. Traditionally one can move emphasis from system-level testing to GUI testing as an early means of component integration and unit testing. Incremental development allows early testing by focusing on each deliverable or release (large increments) of a system under development. Lastly, agile development is similar to incremental development except there are more releases and therefore more chances to test (small increments). One item to note is model testing is not the same as model-based testing, which is another topic.

The presentation included some cautionary themes. If insufficient detail is provided in the model, one cannot extract useful information out of the model. The same goes for problems with concurrency of models, in which case any information from one model is contradicted by the other model. Even if a model is useful as a static model, it does not mean it will be executable. These models may as well be considered equivalent to having no model at all.

On the other hand, if the modeling describes the system in sufficient detail, executable models can be tested the same as traditional testing of software and systems, albeit earlier in the lifecycle. Some examples of executable models, assuming sufficient detail, are Concept of Operation storyboards, use case path sequence diagrams, decision trees, finites state machines, Petri nets, executable requirements languages, and requirements prototypes.

Paul Miner – NASA:

Paul Miner is a senior research engineer in the Safety-Critical Avionics Systems Branch at NASA's Langley Research Center. His principal research interests are the development and

application of formal methods for the analysis of safety-critical systems with a particular emphasis on the design and analysis of distributed systems. He was the principal architect for the SPIDER family of fault-tolerant architectures developed at NASA Langley. Dr. Miner holds a Ph.D. in computer science from Indiana University, an M.S. in computer science from the College of William and Mary.

Paul stressed the importance of determining the validity of a model. Often there is the issue of invalid and unstated assumptions when developing a model, and these assumptions impact the validity and make it difficult to accredit the model. Once a model has been demonstrated to be valid for the intended system, it has the ability to verify properties of a system that cannot otherwise be effectively demonstrated through testing. Furthermore, the modelers need to focus on how the system may misbehave, especially things that may not be able to be captured by testing. Similar to previous speakers, Paul discussed the value of models in exploring system behavior early in the lifecycle.

Dr. Miner identified several risks in addition to the problems with assumptions. A risk attributed to the users of a model is the tendency to conflate the model with reality. The users become accustomed to thinking about the model as the complete system, they then begin thinking it fully represents the real system, when in reality it does not. As stated by Bill Miller in the earlier presentation, a model is a representation or approximation of certain attributes of a system. Basically, a model is not the same thing as the system it represents.

A risk of Model-Based Systems Engineering (MBSE) is maintaining consistency and compatibility between multiple models. Also the difficulty of capturing safety and security is a risk.

David Allsop – Boeing:

David Allsop is the senior systems engineer for the Systems Test Capability within Boeing's Test and Evaluation (BT&E) organization. Within BT&E, David is actively working the Shift the Product Validation Paradigm (shift left) initiative and actively supports cross-domain integration to validate and verify systems early. David also manages the Boeing modeling and simulation community of excellence, which is an enterprise-wide core capability to establish and promote modeling and simulation.

Mr. Allsop questioned how we can convince stakeholders of the importance of identifying risks early. The late discovery of issues drives up the program costs and schedule (Figure 3); and so Boeing has been focusing on early Integrated Validation to address these issues.

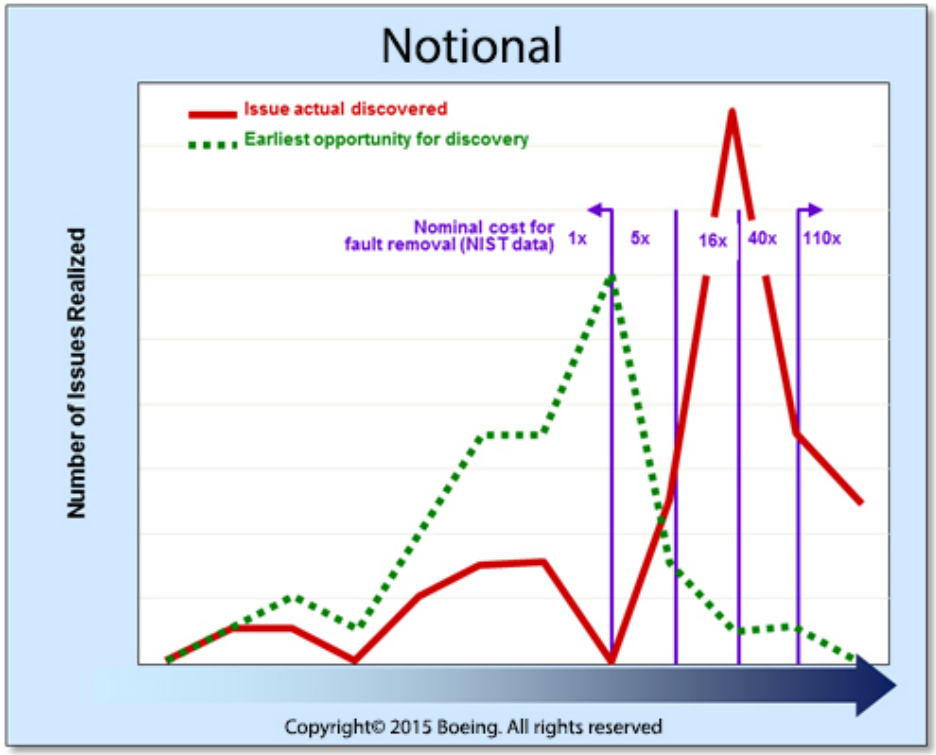

Figure 3. Number of realized issues over time presented by David Allsop (actual discovery vs. earliest opportunity for discovery)

One of the challenges faced by Boeing is integrating semantically heterogeneous models. Another challenge is to convince engineers to adopt new approaches, specifically MBSE. The culture is resistant to new mental models.

Jonathan Hammer – Noblis:

Jonathan Hammer is a Senior Advisor for Noblis. Mr. Hammer has had a 33-year career focused on aviation including research and development in radar tracking and surveillance, aircraft avionics, and air-traffic control automation systems from concept through post-operational analysis. He has been a leader in developing industry standards, and has received 3 RTCA Citations for leadership in standards development. Mr. Hammer was instrumental in developing requirements and standards for ADS-B.

Jonathan's presentation focused heavily on system complexity. By its nature, complexity leads to incomplete data; but complexity cannot be ignored if for no other reason than its impact on integration. So the modeler needs to determine what aspects must be correct in the model. Where does the modeler want to be right and where is it alright to be wrong?

In an attempt to address the complexities, Monte Carlo modeling can be used as a complimentary technique to other forms of analysis. Monte Carlo modeling is low cost and quite flexible. It can shake down the system under stress conditions and help identify problems. Overall, Monte-Carlo Methods can be a valuable tool in the "tool kit" for FAA system analysis and V&V.

3. MAJOR ISSUES AND CHALLENGES

After the conclusion of the presentations, the attendees of the workshop discussed the main issues and challenges presented. Four issues appeared to surface multiple times: culture, security and safety, accreditation, and determining the correct model for the situation (also known as "right-sizing"). Due to the fact that this entire workshop took place over the course of four short hours, it seemed unnecessary to burden the reader with more text than necessary. For the purpose of avoiding an excessively long paper, the following section is organized in a bulleted format.

3.1. CULTURE – ACCEPTANCE OF MODELS

Arguably the top challenge for the FAA, but also throughout the industry as a whole, is culture. This was the topic most emphasized during the workshop discussions. There is the common assumption that a first time analysis is substantial and that implementing models can be too costly or time consuming to provide enough benefit to be warranted. There also seems to be a perception that software does not need modeling. The following section lists the cultural dogmas that were recognized during the workshop. A key challenge here is the process of overcoming and mitigating these cultural challenges.

3.1.1. DRIVERS/ROOT CAUSES

- Users, funders, and stakeholders all have different perspectives and levels of understanding of the system to be modeled
- Engineers are generally not used to testing models and, as a result, they do not
- It takes months to figure a program out, and the scope of that project may not necessarily include modeling
- Incompatible cultures:
  - Cultural trends that make it hard to accept modeling ("we don't need documentation, it's iterative" – programmers)
- "If it is not in the contract, we're not getting paid to do that, so we are not going to do it"…Until a later point in time, where the customer requests the work product and then it is created post process, haphazardly
- The discussion about changing culture comes up often, but the problem is that we don't change our training. The idea of modeling is not rippling through into the workforce and as a result we aren't getting the workforce moving in the direction that we want or need to go

3.1.2. GENERAL COMMENTS

- Being able to create a model that everyone can understand when working with different organizations, technology, platforms, systems and promoting a common view of capabilities is important
- Model based concept development can be a useful tool for reduce effort duplication and can help with the decision making throughout the entire process
- A cultural issue within the United States Air Force is:

  - Who is responsible for creating models? …The Government?
  - Does this responsible party provide these models to the contractors?
  - Is this the 'final word'?
  - Can a model be started by the government entity and then be passed down to the contractor for them to finish/modify?
- Continuous management of the model and management in operations are necessary

3.1.3. RESOLUTION/MITIGATION

- Talk to testers and insist that this is not much different than what they are already used to; it's just not at the same coding/programming level like before
- On the right side of the V model we tend to be more committed to the discipline, but we are much less committed to discipline on the left side of the V model. People tend to surge forward and brush discipline to the side early on, which is a problem; proper discipline needs to be committed to
- Have a forum where all lessons learned are captured. The same lessons learned may apply to both a weather program and a surveillance program. Creating a community to share these lessons learned and best practices could be very beneficial. (Community of practices hosted on an easily accessible site is a good idea but the issue is that people do not utilize this community especially in NASA)
- Promote understanding and adoption among different backgrounds and perspectives (engineers vs. program managers) in order to help long term employees understand new technology and software based models
  - More effort needs to be put into recognizing and influencing the psychological change of the users and understanding their perspectives
- Emphasize the practice of good Configuration Management (CM) and documentation around your modeling in order to make sure that it lives on
- Invest in the workforce and get a training battery/regime into the agenda to provide an influential push in the direction of model based thinking
- There needs to be more outreach from Modeling & Simulation groups to raise awareness and help people understand and take advantage of resources available to them

3.2. SECURITY AND SAFETY – HOW WE APPROACH AND EXECUTE SECURITY

3.2.1. DRIVERS/ROOT CAUSES

- One of the largest issues, noted by Mr. Firesmith, was "we aren't using the security models which are available to us."
- Security engineers have many security modeling techniques (attack trees, attack surfaces, misuse/abuse). It's not that the techniques don't exist, but the special security guys aren't being brought into the conversation early enough to drive good software development behavior

- The probability of someone trying to do something malicious or attack a system with regards to security is Level 1. It's going to happen no matter what. "In fact it is higher than Level 1 if you think about it, considering multiple people are going to try and break into a system day after day"
- There is a constant attack on multiple surfaces of every complex system

3.2.2. GENERAL COMMENTS

- Safety and Security can largely be considered to be two sides to the same coin. In fact they are directly proportional to one another
- The only difference between safety and security is that security is about malicious intent and safety is about accidental things, but both try to prevent something bad from happening. A decreased security factor will result in a decrease in safety, as both are inversely proportional to risk
- Security is an active effort to provide protection from sabotage, attack, or espionage
- Safety is life, property, and the environment. Money in the bank and reputation is property in this case, and all of these things are at risk if security is compromised
- A threat tree has to be secured, because it has everything that you are worried about
- Attackers are using models themselves in order to find attack surfaces and develop their own attack systems
- In the case of Bell Labs, a Burglar's Licenses may be granted so that people may break into every computer and exploit vulnerabilities in the system, for the sake of building a more secure system

3.3. ACCREDITATION – IS THE MODEL DOING WHAT IT IS SUPPOSED TO BE DOING?

3.3.1. DRIVERS/ROOT CAUSES

- Does the model fulfill its purpose? Is it promoting understanding and communicating the product's framework, content, and scope?
- It can be difficult to determine the appropriate fidelity of a model
- Implementing the virtualization of an environment is very complex and actively changing, making is a complicated task.
- There is a lack of commitment when it comes to Verifying and Validating models themselves which causes issues since these are the models that will ultimately be used to V&V a given system

3.3.2. GENERAL COMMENTS

- In the Department of Defense (DoD), when dealing with safety critical events, the testing tools and environment all need to be certified
- The DoD requires interoperability testing, or testing whether the program or work product is compatible with others, to promote seamless operation

- There is a lack of discipline with respect to going back to validate the model based on the real world deployed product, or newly implemented technology
- Multiple models can help you validate each of the models against each other, if people are aware of this goal when they are going into it. Otherwise it can lead to wasted effort and may cause confusion

3.4. RIGHT SIZING – THE RIGHT MODEL FOR THE RIGHT SITUATION

3.4.1. DRIVERS/ROOT CAUSES

- Keeping modeling alive throughout the process and lifecycle is a difficult challenge since models can become unwieldy or inconvenient to update. Once something becomes inconvenient, it dies
- Development of appropriate random models based on incomplete data is a challenge
- Determining what the right model for the right situation is vs. a static model vs. a high fidelity overdesigned model is an ongoing challenge

3.4.2. GENERAL COMMENTS

- What's the right level? Is the cost of modeling too much, or too little? Simply put, cheap models don't necessarily perform well; while over-modeling is a waste of time and money
- Quantum modeling also known as Analysis Paralysis, or the state of over-analyzing a problem to the point of prohibiting progress, is a real problem
- Choose Architectural Description Languages (ADL) over Unified Modeling Language (UML) and Systems Modeling Language (sysML) when it comes to software architecture. However, there are many circumstances where ADL is not capable of providing the results necessary
- Different models, providing different levels of fidelity, are important and useful throughout an entire product's lifecycle

4. SUMMARY AND CONCLUSIONS

The first Workshop on Model-Based Systems Engineering of NextGen, titled "Modeling for Verification and Validation," transpired within just three short hours. There was great effort demonstrated by the participants to discuss the need to implement a model-based systems engineering (MBSE) approach in V&V, with special emphasis on its impact to testing. As this was the first workshop of its type at the FAA, a majority of the discussion was on techniques involved with MBSE and the challenges that are faced in implementing any MBSE. Although few answers and no resolutions were identified, this workshop was undoubtedly a solid first step towards fully realizing MBSE within NextGen.

The need for MBSE within NextGen centers around improving the way requirements are developed and the way concepts and systems are tested, or verified and validated. A goal of MBSE

is to allow earlier testing of concepts and earlier testing of designs. The graphical and executable models should complement the existing textual requirements to more successfully the inherent complexities within the National Airspace System.

Despite the promises of MBSE, there are still risks and challenges with regards to implementing it within the FAA. First is the simple fact that many people and cultures are naturally resistant to change. Even with cultural acceptance, there will be the challenge of validating and accrediting the models. It is important to ensure that we V&V the models used to V&V complex systems. The models must be at the right "level" at the right time, and they must fulfill their purpose. It is foolish to think that money can be saved by producing a cheap model, since it has been expressed that cheap models simply do not perform their objectives, however, it is also equally as impractical to over-model a system. These objectives will not necessarily be easy to achieve and they will provide their own sets of challenges but the results are worth it. Finally, there is the problem of effectively modeling security and safety. Security is about the prevention of something malicious, and safety is the prevention of accidents but other than that they are very similar. It is difficult to model "prevention", the focal point of both. Nonetheless, attackers have started to use models, and the FAA cannot fall behind the attackers. Now, more than ever, the FAA is becoming a more net-centric organization. With programs such as System Wide Information Management (SWIM) becoming a driving force in providing users with information across the web, we now need to focus on safety and security more than ever. Modeling cyber security is difficult, but that should not be a reason to avoid it.

At the conclusion of the Workshop, there were proposals to hold follow up workshops in the near future to keep the conversation and initiative alive. Overall, the group did an extraordinary job at communicating their lessons learned with regards to verification and validation and the applications of MBSE. The event was very well received by all who attended and there was a harmonized feeling of success in demonstrating the various challenges that we see within our respective areas of work. Follow-up workshops will be critical in paving the way to the successful adoption of MBSE in V&V and will provide an opportunity to promote more unity between the government, industry, and academia.