The Use of M&S VV&A as a Risk Mitigation Strategy in Defense Acquisition

Michelle Kilikauskas
Joint Accreditation Support Activity
NAVAIR Weapons Division
China Lake, CA 93555
michelle.kilikauskas@navy.mil

David H. Hall
SURVICE Engineering Company
Ridgecrest Area Operation
Ridgecrest, CA 93555
dave.hall@survice.com

We describe verification, validation, and accreditation (VV&A) activities as components of risk assessment and risk mitigation in the defense systems acquisition process. We review risk assessment methodologies, application of those methodologies to models and simulations (M&S), and how this application relates to the overall risk mitigation process for the systems acquisition process.

Keywords: VV&A, verification, validation, accreditation, M&S, risk mitigation, risk assessment, defense acquisition

1. Introduction

Risk is the potential realization of undesirable consequences from hazards arising from a possible event. Risk is present in decision making because only imperfect knowledge is available to make the decision. Models and simulations (M&S) have become an integral part of the systems acquisition process, being employed in every phase of system development such as requirements development, design, production, and test. As M&S are increasingly used, it becomes increasingly important to accumulate evidence that these tools are performing correctly. Verification, validation, and accreditation (VV&A) of models and simulations are required to reduce the risk of incorrect decisions based on erroneous M&S outputs. The goal, then, of VV&A is to mitigate the risk of poor decisions based on incorrect models and simulations.

2. Overview of Relevant U.S. Defense Acquisition Policy

In 2003, the U.S. Department of Defense (DoD) issued new directives and instructions covering nearly every aspect of system acquisition including modeling and simulation. DoD Directive 5000.59, *DoD Modeling and Simulation Management,* states that M&S used to support major DoD decision-making organizations and processes shall be accredited for that purpose [1].[i] DoD Instruction 5000.2, *Operation of the Defense Acquisition System*, states that program managers must plan for modeling and simulation activities throughout the life cycle [2]. The Instruction goes on to say that the "T&E strategy shall provide information about risk and risk mitigation, provide empirical data to validate models and simulations, evaluate technical performance and system maturity, and determine whether systems are operationally effective, suitable, and survivable against the threat detailed in the System Threat Assessment." [ii] Furthermore, "appropriate use of accredited models and simulation shall support (T&E)" [2],[iii] with accreditation being defined as the official certification that a model or simulation is acceptable for use for a specific purpose [1].[iv]

DoD Instruction 5000.61, *DoD Modeling and Simulation (M&S) Verification, Validation and Accreditation (VV&A)*[3], states that it is DoD policy that "verification and validation (V&V) shall be incorporated into the development and life-cycle management processes of all M&S… commensurate with the relative

JDMS, Volume 2, Issue 4, October 2005 Pages 209–216
© 2005 The Society for Modeling and Simulation International

importance, risk, and life-cycle management phase of the model, simulation, or federation to which they are applied." [v] Furthermore, it says that the "M&S Application Sponsor shall document accreditation results, to include… the accreditation methodology, including V&V activities, that support accreditation; data verification and validation; risk assessments; and acceptability criteria"[1].[vi]

The DoD directives and instructions offer guidance on use of VV&A activities to identify and mitigate risk, but no details; these are left to service implementation instructions shown in Table 1. Documents implementing DoD Instruction 5000.61 and DoD Directive 5000.59 repeat the requirement that the acquisition process is one means of mitigating risk in planning, developing, testing, and fielding military systems. There are variations in the service-policy documentation required for a risk analysis, some being part of the VV&A plan and reports, others the accreditation plan and report. But they all call for a risk analysis and documentation of the results and how the risk analysis results affect planned uses of the M&S.

Table 1. Service and joint implementing instructions

Service	Regulation
Air Force	Air Force Instruction AFI 16-1001, June 1, 1996 [4]
Army	Department of the Army Regulation AR 5-11, February 1, 2005 [5]
	Department of the Army Pamphlet PAM 5-11, September 30, 1999 [6]
Navy	Secretary of the Navy Instruction SECNAVINST 5200.40, April 19, 1999 [7]
	Department of Navy *Modeling and Simulation VV&A Implementation Handbook, Volume I: VV&A Framework*, March 30, 2004 [8]
	Draft Secretary of the Navy Instruction SECNAVINST 5200.40A, January 20, 2005, intended to replace 5200.40 [9]
Joint	Joint Staff Instruction, *VV&A of Joint M&S*, JSI 8104.01A, January 26, 2004 [10]

The Defense Modeling and Simulation Office (DMSO) *VV&A Recommended Practices Guide* (RPG), available from the DMSO website, contains detailed guidance for VV&A practitioners [11]. The guide provides information on risk assessment; this information is discussed in the section following. A detailed discussion of risk analysis and its impact on VV&A is provided in a special topic paper in the RPG on the DMSO website [12].

2.1 Summary

The DoD, service, and joint service policies relating to M&S and use of M&S in acquisition all mandate that M&S be used appropriately throughout the acquisition cycle. In order to assure the credibility of decisions that are made based on M&S outputs, the M&S used to support those decisions must be accredited. These directives require that the evidence required to support an accreditation decision be driven by the risk associated with the intended use. Surprisingly little specific guidance is given on how to conduct risk assessments and how to apply those principles to developing and implementing a VV&A program. The result is that the individual service M&S communities have developed individualized approaches. We survey some of these approaches below.

3. Risk-Related Principles and Terms

The DMSO VV&A RPG Special Topic Paper entitled *Risk and Its Impact on VV&A,* considers two types of risks associated with simulation development and use:

> Risks associated with simulation development and use can be categorized as either *development risk* or *operational risk*. *Development risks* are related to the simulation development itself and typically relate to potential problems in meeting technical, schedule, or cost aspects of the simulation development or modification program. *Operational risks* are those arising from using the incorrect outputs of a simulation that are believed to be correct [12].

Verification and validation activities mitigate development risk because these activities are intended to discover defects; accreditation activities mitigate operational risk. Consumers of M&S results must decide if the operational risk is at an acceptable level for their application. The M&S program manager and developer must reduce development risk, which is related to development time and budget. The verification and validation agents must reduce development risk by minimizing potential failures and producing the evidence to demonstrate the capability and credibility of the M&S. And the accreditation agent must manage operational risk for the user, doing so by assessing the impact potential failures may have on the intended use.

Operational risks are related to credibility. Whereas M&S requirements establish needed functional capabilities, the level of credibility required determines the information needed to produce a justified accreditation decision. The users must believe that the simulation results are "good enough" for their purpose; this belief depends entirely on how much risk the user is willing tolerate when using results of the M&S to make a decision. Once the level of risk tolerance is established, risk assessment techniques guide V&V and related activities to arrive at an appropriate (acceptable) risk to the user. Risk assessment also directs VV&A resources toward the most effective risk mitigation program possible with the available resources.

In practice, how much risk tolerance is acceptable is often difficult to quantify because users often cannot explicitly describe risks or their tolerance to those risks, and they almost never can express either risks or tolerance in objective terms. We must develop workable methods for identifying and quantifying risk, and we can look to the risk assessment, risk management, and system safety communities for guidance.

Risk is comprised of three components: events, the likelihood that the event occurs, and the consequences of the occurrence of events [13].[vii]

$$\text{Risk} = (\text{Impact Level}) \times (\text{Probability of Occurrence})$$

Objective values for these factors are not always available, but subjective estimates are possible using techniques from the safety community as described in Appendix A of the Military Standard on *Standard Practice for Systems Safety,* MIL-STD-882D [14]. These techniques require developing subjective rankings for impact and likelihood, and assigning risk values to the various rankings. Those risk values (called mishap risk assessment values in MIL-STD-882D) are used to categorize risks into categories such as high, serious, medium, and low. From this subjective information, a ranking can be determined, from which we can derive mitigating actions.

3.1 Risk Assessment Techniques

The two most widely used risk assessment techniques in the DoD are the following:

- *Failure Modes and Effects Criticality Analysis* (FMECA) – This process is widely used in the aerospace industry for analyzing system reliability and ballistic vulnerability. This technique examines possible component failures and the effect of those failures on the component, which are then combined into a criticality value. The criticality measures the importance of a failure of that kind.
- *Failure Modes and Impacts Criticality Analysis* (FMICA) – This extends the FMECA analysis from the *effect* to the *impact* of a failure on the system. FMICA proceeds in two phases: impact assessment (IA) and failure mode identification (FMI).

Table 2. Criteria for determining impact severity*

Impact Categories	Impact Levels			
	CATASTROPHIC	CRITICAL	MARGINAL	NEGLIGIBLE
Personnel Safety	Death	Permanent partial disability	Injury resulting in one or more lost work days	Minor injury with no lost work days
Equipment Safety	Major equipment loss; broad-scale major damage	Small-scale major damage	Broad-scale minor damage	Small-scale minor damage
Environmental Damage	Irreversible and severe damage	Reversible damage $200K< loss < $1M	Damage $10K< loss < $200K	Damage <$10K not violating laws or regulations
Occupational Illness	Severe and broad scale	Severe or broad scale	Minor and small scale	Minor or small scale
Cost	Loss of program funds; 100% cost growth	Funds reductions; 50–100% cost growth	20–50% cost growth	< 20% cost growth
Performance	Design does not meet critical thresholds	Severe design deficiencies but thresholds met	Minor design flaws but fixable	Some trivial "out of spec" design elements
Schedule	Slip reduces overall DoD capabilities	Slip has major cost impacts	Slip causes internal turmoil	Slip causes schedules to be republished
Political or Public Impact	Widespread (Watergate)	Significant (Tailhook '91)	Embarrassing ($200 hammer)	Local

* Extracted from the DMSO RPG special topic paper on risk assessment [12].

DMSO RPG authors argue that FMICA is more applicable than the FMECA [11]: "The FMICA process is based on the premise that an impact is associated with the failure of the simulation to meet a requirement. For some requirements (e.g., requirements defining fidelity or data quality), the severity of the impact may be a function of the quality or degree of the failure." Anecdotal evidence from the aerospace industry seems to indicate that FMICA is usually employed, but is misnamed FMECA. The results of the impact analysis are often displayed as a fault tree diagram, showing the impact of damage to various components on the operation of the overall system.

FMICA is usually too difficult to formally apply to risk assessments in M&S. MIL-STD-882D describes a subjective approach usually taken for estimating risks associated with systems safety analyses [14]. MIL-STD-882C [15], the previous edition, provides extensive detail not present in MIL-STD-882D.

The RPG details the FMICA as it could be applied to M&S use. Impact categories (risk factors) are developed and ordered by severity; see Table 2. Probability bands are identified for each risk factor, based either on the a priori likelihood of an event or subjective considerations.

Finally, the risk factor probabilities and impact levels are combined in a risk assessment matrix that categorizes the risk; for example, MIL-STD-882D uses high, serious, medium, and low as risk categories.

Identifying risk categories focuses VV&A planning on important issues. A low-risk application may only require assessment of M&S documentation and M&S management practices, and an evaluation of prior usage history, along with an unbiased expert opinion of M&S suitability to the specific application to make an accreditation decision. A high-risk application may require detailed VV&A results including comparison of M&S results with field test data. The benefit of risk assessment to the accreditation process is that the cost of VV&A activities can be tailored to the application's risk.

3.2 Summary of Risk Assessment Principles as Applied to VV&A

Operational risk is the risk associated with using the M&S over the life cycle of a particular acquisition program by providing wrong answers at various

Table 3. Probability levels for likelihood and frequency of occurrence*

Probability Continuum	Likelihood of Occurrence over Lifetime of an Item	Likelihood of Occurrence per Number of Items**
Frequent	Likely to occur frequently	Continuously experienced
Probable	Will occur several times in life of item	Will occur frequently
Occasional	Likely to occur sometime in life of item	Will occur, several items
Remote	Unlikely but possible to occur in life of item	Unlikely but can reasonably be expected to occur
Improbable	So unlikely that it can be assumed occurrence may not be experienced	Unlikely to occur but possible

* Extracted from MIL-STD-882D [14]. ** Number of items should be specified.

Table 4. Sample risk assessment matrix*

Frequency	Level of Impact			
	CATASTROPHIC	CRITICAL	MARGINAL	NEGLIGIBLE
Frequent	High	High	Medium	Low
Probable	High	High	Medium	Low
Occasional	High	Medium	Low	Low
Remote	Medium	Medium	Low	Low
Improbable	Medium	Low	Low	Low

* Based on a sample in MIL-STD-882D [14].

stages of the program. Risk is relative to a single use, so a single accreditation may not satisfy all M&S uses, and the risk assessment may have to be redone for each accreditation point in the life of the program. Risk assessment determines the effort required to support accreditation of the M&S for that application, prioritizing VV&A tasks.

Development risk is associated with meeting the cost, schedule, and technical constraints of the M&S development program. While VV&A tasks can help to minimize the development risk, there is a risk associated with the VV&A program itself. Program managers often view VV&A as contributing to M&S development risk. However, from the standpoint of the M&S user, minimizing operational risk is worth a perceived small increase in development risk.

4. Examples of Risk Based VV&A Approaches within the U.S.

4.1 Joint Accreditation Support Activity Approach

The Joint Accreditation Support Activity (JASA) supports the VV&A of M&S used by acquisition programs across the services. The fundamental goal of the JASA team is to decrease risk in acquisition by applying proven VV&A principles in a cost-effective way to establish and document the credibility of M&S used in the acquisition process.

The JASA approach to risk assessment [16] begins by quantifying risk, using impact and likelihood tables as described in MIL-STD-882D to develop overall risk categories (high, medium, low) for each risk factor (cost, schedule, loss of life), and can be tailored to the specifics of individual problems for each of the ways in which the M&S output could be wrong. If weapon effectiveness as measured by probability of kill (Pk) is the question under consideration, for example, we would consider the impact and likelihood of the candidate M&S both over-predicting and under-predicting Pk. The highest level of risk associated with any risk factor is selected as the level that drives the simulation credibility requirement. The criteria used in each step of the risk assessment process are subjective, subject to expert review and consensus.

Once the risk factors have been evaluated, the user has some assessment of the risks associated with using simulation outputs. Risk assessment elucidates what unfavorable events can happen if the simulation outputs are wrong by quantifying impact severity and probability of occurrence. For a detailed example, the reader is directed to [17]. Based on that risk level, the information-gathering effort required to make an adequate assessment of simulation credibility is determined.

There are two distinct questions in identifying the information necessary to adequately assess the credibility of an M&S. The first consideration is specific simulation credibility requirements issued by the accreditation authority, either by policy or by special instructions. The second consideration is information necessary to address the three key elements of simulation credibility: capability, accuracy, and usability. *Capability* concerns the functional representations in the M&S; that is, what the M&S does. *Accuracy* is comprised of three elements: *software accuracy,* which addresses whether there are errors in the software, as determined by verification tasks; *data accuracy,* which measures the completeness and confidence in M&S data; and *results accuracy,* which measures correlation between M&S results and real-world observations. Lastly, *usability* describes those features that ensure the user does not misuse the M&S (documentation, user groups, etc.).

JASA personnel use a series of tables that identify the major questions associated with each of the three credibility components, the types of information required to answer each of those questions, and specific potential sources for each information type. This defines the information space that establishes simulation credibility. The tables provide suggestions as to information required to mitigate each level of risk. Greater risk levels require more detailed information to establish simulation credibility [16].

The assignment of specific information requirements to specific levels of risk is subjective, based on our experience supporting a wide range of M&S VV&A efforts within the DoD over the past thirteen years. This tabular approach is described in the DMSO VV&A RPG [11].

4.2 U.S. Army Approach

The army uses the principles of risk assessment extensively throughout the acquisition process to identify, manage, and mitigate risk in many areas, including software. The Army Materiel Systems Analysis Activity (AMSAA) risk assessment process is described in Special Publication 71, a primer on conducting risk assessments for army systems [18]. AMSAA historically has provided risk assessments for many acquisition programs, but AMSAA also provides independent risk assessments to organizations requesting such service. AMSAA actively reviews risk assessment documents throughout the acquisition program's life cycle, fitting within the framework of army risk management [19].

The AMSAA risk assessment process has four elements: planning, assessment, analysis, and handling. The planning element develops a structured approach to eliminate, minimize, or contain effects of undesirable events; the outcome is a formal risk assessment plan. The risk assessment element contains two major steps: risk identification and stratification. Risk identification determines the *real* risks associated with the program through interviews with subject-matter experts, reviews of program documents, and plans. Stratification uses a series of indicators and expert opinion to place risks into categories. The analysis element evaluates the impacts of the risks against the overall system/program completion; sensitivity analyses may be conducted as part of the analysis process. Handling involves taking action to address the risk areas identified and categorized, accomplished by risk avoidance, risk control, risk transfer, or by assuming or accepting the risk identified.

The AMSAA approach classifies risk using five aspects: technical, supportability, programmatic, cost, and schedule. Technical risk in this context is the risk that the new or existing design will not perform adequately. Supportability risk is the risk associated with fielding and maintaining systems that are in development as measured by reliability, availability, and maintainability, as well as training, packaging, and human interface. Programmatic risk is associated with obtaining and using applicable resources and activities outside of the program's control. These include new legislation and contractor personnel base stability. Finally, cost and schedule risks can include unrealistic cost/schedule estimates, technical risk issues, poor program execution, and so on. In DMSO RPG terms, these risks are classified as development risks.

The AMSAA approach to performance risk assessment is similar to that of MIL-STD 882C [15]. Risks are categorized into five bands (low, medium-low, medium, medium-high, high) based on the combination of consequence and likelihood of occurrence.

Both risk likelihood and consequence are organized into five bands to better fine-tune the approach. In order to support this many categories, impacts are broken down by specific definitions, based either on performance or schedule and cost. Likelihood is determined by the maturity of the system technologies and the extent to which testing has been conducted. Using those two matrices, the overall level of risk can be extracted from the likelihood/consequence combination matrix.

The AMSAA risk assessment primer described a number of lessons learned from applying their approach that are worth noting here.

- Complete risk assessment early in the program so that it has some beneficial effect.
- Focus on the user's requirements and the current acquisition strategy.
- Define risk category definitions and maintain those definitions throughout the program.
- AMSAA and the program manager may disagree on risk assessment, but that disagreement is likely due to their differing perspectives on the program.
- Be concise in presenting the risk assessment results: don't inundate the customer with details.

4.3 Great Britain

In a 1999 paper by Chris Mugridge [20], the U.K. Ministry of Defence Evaluation and Research Agency (DERA) described a risk-based approach to planning VV&A efforts. Mugridge describes a formal hazard/risk/benefit analysis process similar to the JASA and AMSAA approaches followed by appropriate verification and validation activities. The approach is to minimize VV&A activities based on perceived risk and a benefits analysis. The approach was derived from many of the fundamental principles of safety analysis, which transferred easily over to the VV&A context.

The U.K. approach is divided into several steps. The first produces a complete list of the functions required by the M&S to meet the specified purpose. Based on this functionality analysis, a hazard analysis is developed using a functional failure analysis. The hazard analysis table contains the complete list of functions, their failure modes, the domains in which their impact is to be assessed, the estimated most critical phase/condition, the effect of the functional failure at the system level, and the estimated maximum possible severity category in each of the impact domains.

The U.K. paper provides a refinement of the general risk-based approach using consequence analysis. Consequence analysis is a diagrammatic technique that focuses on one hazard and its interactions with events in the system. Each hazard triggers a series of events that pass through various decision points until the consequences at the system level can be determined; this produces a consequence tree for each hazard.

It may be the case that the risks involved with a particular M&S are fairly low, but the potential benefits to be realized are high; in these cases a separate benefits analysis may be deemed appropriate. Benefits can be viewed as positive hazards, making benefit analysis susceptible to risk analysis techniques.

Once the levels of risk (and benefits) have been identified, a list of development, verification, and validation activities can be selected.

4.4 A Formal Approach

A formal analysis of risk assessment is provided by Brade based on studies the author conducted in Sweden [21]. A mathematical approach to risk assessment is described with details in the Proceedings of Foundations 2004 [22].

Brade draws the following qualitative conclusions:

- The lower the *acceptable* probability of erroneous simulation output, the lower the maximum acceptable residual risk.
- The maximum acceptable probability of erroneous simulation output decreases with increasing influence of simulation results on the decision.
- If the probability of erroneous simulation output cannot be reduced below a given acceptable threshold, the decision maker must reduce the influence of simulation results on the decision or change the intended use of the M&S to decrease the impact of an erroneous decision. Otherwise a higher maximum residual risk must be accepted.

Thus, if the model's accuracy cannot be demonstrated as acceptable for the intended use, then the user will need to identify work-arounds for the model in those areas where it is not acceptable or to accept a higher risk than he or she would have liked.

The dissertation concludes that a scalar measure for risk as described in MIL-STD-882D is helpful as an overall risk statement, but that it does not support the focused identification of VV&A strategies and objectives. In order to identify VV&A activities required for a given risk level, a statement of prioritized worst-case impacts is required. All planned VV&A activities are driven by the identified worst-case impacts.

5. Concluding Thoughts

We have explored the fundamentals of risk assessment and mitigation as they apply to modeling and simulation practice. We have reviewed risk assessment techniques and their use in planning and executing VV&A activities to reduce the risks.

All of the VV&A risk techniques that we reviewed are based on the systems safety approaches outlined in MIL-STD-882D, and they are largely subjective in nature. These approaches primarily emphasize qualitative judgment, although Brade's approach is quantitative. In all of these approaches, the VV&A activities required to satisfy the perceived maximum residual risk requirement are based on these perceived risk categories.

How these risk assessments for VV&A planning and execution fall into the overall risk mitigation strategy of a program is dependent on the expertise and judgment of the program manager. There is no single approach to integrating M&S VV&A activities into overall program activities addressing risk. While these activities can be integrated into a larger program, they usually are considered separately from other program risk factors such as maintainability, reliability, and technical risk. Exceptions to this are those cases where M&S are used to support mitigating those risks. The risk assessment techniques described in this paper relating accreditation information requirements to the level of acceptable risk in using M&S results—including the guidelines developed by JASA and incorporated into the DMSO VV&A RPG—have proven to be a practical help in planning and conducting a cost-effective VV&A effort.

6. Endnotes

i. U.S. Department of Defense. DoD Directive 5000.59. January 20, 1998. *DoD Modeling and Simulation (M&S) Management*. Section 4.8.

ii. U.S. Department of Defense. DoD Instruction 5000.2. May 12, 2003. *Operation of the Defense Acquisition System.* Paragraph E.5.

iii. Ibid. Paragraph E.5.4.7.

iv. U.S. Department of Defense. DoD Directive 5000.59. January 20, 1998. *DoD Modeling and Simulation (M&S) Management*. Page 11, Enclosure 2.

v. U.S. Department of Defense. DoD Instruction 5000.61. May 13, 2003. *DoD Modeling and Simulation (M&S) Verification, Validation, and Accreditation (VV&A*). Paragraph 6.1.

vi. Ibid. Page 18, Enclosure 3 Paragraph E3.1.3.

vii. See, for example, Ropeik, David, and George Gray. 2002. *Risk: A Practical Guide for Deciding What's Really Safe and What's Really Dangerous in the World Around You*. Ropeik and Gray provide a more complete definition of risk (page 4): "Risk is the probability that exposure to a hazard will lead to a negative consequence." They point out that there are four basic elements of risk: probability, consequences, hazard, and exposure.

7. References

[1] U.S. Department of Defense. *DoD Modeling and Simulation (M&S) Management*. DoD Directive 5000.59. (Administrative Change 1 to the original document dated Jan 4, 1994). January 20, 1998.

[2] U.S. Department of Defense. *Operation of the Defense Acquisition System*. DoD Instruction 5000.2. May 12, 2003.

[3] U.S. Department of Defense. *DoD Modeling and Simulation (M&S) Verification, Validation, and Accreditation (VV&A*). DoD Instruction 5000.61. May 13, 2003.

[4] U.S. Air Force. *Operations Support: Verification, Validation and Accreditation (VV&A).* Air Force Instruction AFI 16-1001. June 1, 1996.

[5] U.S. Army. *Management of Army Models and Simulations*. Department of the Army Regulation AR 5-11. February 1, 2005.

[6] U.S. Army. *Verification, Validation and Accreditation of Army Models and Simulations*. Department of the Army Pamphlet PAM 5-11. September 30, 1999.

[7] U.S. Navy. *Verification, Validation and Accreditation (VV&A) of Models and Simulations*. Secretary of the Navy Instruction SECNAVINST 5200.40. April 19, 1999.

[8] Department of Navy. *Modeling and Simulation Verification Validation and Accreditation Implementation Handbook, Volume I: VV&A Framework*. March 30, 2004.

[9] U.S. Navy. *Verification, Validation and Accreditation (VV&A) of Models and Simulations.* Secretary of the Navy Draft Instruction SECNAVINST 5200.40A (in coordination). January 20, 2005.

[10] *Verification, Validation and Accreditation of Joint Models and Simulations*. Joint Staff Instruction JSI 8104.01A, January 26, 2004.

[11] Defense Modeling and Simulation Office (DMSO). *Accreditation Agent Role in the VV&A of Legacy Simulations*. DMSO VV&A Recommended Practices Guide Core Document. August 4, 2004. (online at vva.dmso.mil)

[12] Defense Modeling and Simulation Office (DMSO). *Risk and Its Impact on VV&A.* DMSO VV&A Recommended Practices Guide Special Topic Paper, November 30, 2000. (online at vva.dmso.mil)

[13] Ropeik, David, and George Gray. *Risk: A Practical Guide for Deciding What's Really Safe and What's Really Dangerous in the World Around You*. Harvard Center for Risk Analysis, Harvard School of Public Health. Houghton Mifflin. 2002.

[14] U.S. Department of Defense. *Standard Practice for Systems Safety.* Military Standard MIL-STD-882D. February 10, 2000.

[15] U.S. Department of Defense. *System Safety Program Requirements*. Military Standard MIL-STD-882C. January 19, 1993.

[16] Kilikauskas, Michelle, and David H. Hall, et al. "Estimating V&V Resource Requirements and Schedule Impact." In *Proceedings of the Foundations for VV&A in the 21st Century Workshop* (*Foundations '02*). 2002.

[17] Joint Accreditation Support Activity. *Risk Assessment Example*. January 2004.

[18] U.S. Army. Army Materiel Systems Analysis Activity Combat Evaluation Division, Infantry Branch. *AMSAA Risk Assessment Primer*. Special Publication No. 71. May 1995.

[19] U.S. Army. *Risk Management.* Army Field Manual FM 100-14. April 23, 1998.

[20] Mugridge, Chris. *Verification, Validation and Accreditation of Models and Simulations Used for Test and Evaluation: A Risk/Benefit Based Approach*. Defence Evaluation and Research Agency, U.K. March 1999.

[21] Brade, Dirk. "A Generalized Process for the Verification and Validation of Models and Simulation Results." Ph.D. diss., Universität der Bundeswehr, München. October 2003.

[22] Kilikauskas, Michelle and David H. Hall. "The Use of M&S VV&A as a Risk Mitigation Strategy in Defense Acquisition." In *Proceedings of Foundations '04: A Workshop for VV&A in the 21st Century.* 2004.

Author Biographies

Michelle L. Kilikauskas *is the Director of the Joint Accreditation Support Activity (JASA) at the Naval Air Systems Command (NAVAIR), Weapons Division at China Lake, California in the USA. She has served as the accreditation support agent for several international missile and military aircraft acquisition programs and is a frequent writer, speaker, and teacher on the practical implementation of VV&A policy, principles, and methodology.*

David H. Hall *is the Chief Analyst for SURVICE Engineering Company and deputy manager of their Ridgecrest Operation. Prior to his retirement from the government in 2002, he served as the interim JASA Director. From 1992 through 1996 he was also the Joint Project Manager of the Susceptibility Model Assessment and Range Test (SMART) project, which developed and demonstrated Joint M&S VV&A and configuration management processes for the DoD. At SURVICE he continues to participate in JASA VV&A support services to DoD systems acquisition programs. He is a frequent speaker, author, and instructor on survivability and M&S VV&A.*