Verification and Validation of Complex Systems: A Holistic, Model-Based Approach

William D. Miller
Executive Principal Analyst, Innovative Decisions
Adjunct Professor, Stevens Institute of Technology
Editor-in-Chief, INCOSE INSIGHT Systems Engineering Practitioners Magazine
Lead, Systems Engineering of the Future Initiative
INCOSE Technical Director (2013-2014)
Bell Telephone Laboratories (Network Planning 1973-1979, Federal Systems 1983-1995)

Mr. Miller has more than forty years of experience in the conceptualization and engineering application of communications and information technologies, products and services. This experience has addressed both commercial and government sectors. These applications have fallen in the areas of resource allocation, R&D priorities, strategic planning, requirements definition, system modeling, system design, system acquisition, system development, system integration and system test. Mr. Miller has managed projects including positions as chief systems engineer and program manager funded by Bell Laboratories, AT&T, Army and Navy development commands, and elements of the Intelligence Community. Mr. Miller is an adjunct professor in the School of Systems and Enterprises, Stevens Institute of Technology, where he teaches graduate courses in systems engineering fundamentals, system architecture and design, and systems integration. He has also served as a senior researcher for the Systems Engineering Research Center (SERC) University Affiliated Research Center (UARC) focused on mission engineering. He is a Life member of the IEEE and a 28-year member of the International Council on Systems Engineering where he currently serves as the editor-in-chief of INSIGHT practitioners' magazine and lead of the Future of Systems Engineering systems community initiative. He received the INCOSE Founders Award in 2017. He previously served as INCOSE Technical Director (2013-2014) and Deputy Technical Director (2011-2013), responsible for shepherding over 40 working groups and major initiatives in systems engineering standards,

model-based systems engineering, the systems engineering body of knowledge, and the systems engineering handbook based on ISO/IEC/IEEE 15288 Life Cycle Systems. He previously served as Assistant Director – (Systems Engineering) Knowledge Enabler. He was elected secretary of INCOSE for three terms (1996-1997, 2003-2004 and 2005-2006). He has also served as secretary and president of the INCOSE Liberty Chapter.

Education
M.S., Electrical Engineering, Pennsylvania State University, 1973
B.S., Electrical Engineering, Pennsylvania State University, 1971

Selected publications
- Dennis M. Buede and William D. Miller, *The Engineering Design of Systems: Models and Methods, 3rd edition*, Wiley, 2016.
- Gregory S. Parnell, editor, *Trade-off Analytics*, (co-author) Wiley, 2016.
- B. R. LaCava, W. D. Miller and B. Yaged, *Last Trunk Usage Measurements in Step-by-Step Switching Systems*, BSTJ, Vol. 55, No, 10, 1553-1572, December 1976.
- J.C. Lawson, W. D. Miller, G. P. McNamara, K. G. Oza and G. J. Ryva, *The Impact of Potential New Telecommunications Services on the Structure of the Local Network*, Proceedings of the International Symposium on Subscriber Loops and Services, Georgia Institute of Technology, Atlanta, March 1978.
- Pamela J. Hurst and William D. Miller, *Trends in Undersea Fiber Optic Systems*, MTS/IEEE Oceans 2000, Providence, RI, September 2000.
- William D. Miller, Gay McCarter and Craig O. Hayenga, Ph.D., *Modeling Organizational Dynamics*, IEEE International Conference on Systems of Systems Engineering, SMC, Los Angeles, CA, April 2006.
- L. Keith Robinett and William D. Miller, *Adaptation of Commercial and Defense Systems Requirements Engineering Processes for Streamlined Acquisition Programs*, INCOSE Middle Atlantic Regional Conference, April 2009.
- William D. Miller, *Systems Thinking for a Secure Digital World,* CrossTalk, The Journal of Defense Software Engineering, September/October 2012.
- William Miller, Nicole Hutchison, Hoong Yan See Tao, Dinesh Verma, and Gregg Vesonder, *Framework for Mission Engineering Competencies*, 28th Annual INCOSE International Symposium, Washington, DC, 7-12 July 2018.

Abstract

The future of systems engineering initiative within the systems community has the mission to realize the INCOSE Systems Engineering Vision 2025 published in 2014 and the forthcoming SEV2035 now in draft form to be published in 2022. The *mold* for systems engineering processes, methods, and tools has its roots in the era from the 1930s to the 1970s. That *mold* embraced both disparate models and documents that were not integrated and relied on verification and validation towards the tail end of the development process to catch defects often attributable to mismatched interfaces and hidden interactions.

Verification is the matching of *configuration items*, components, subsystems, and the system to their corresponding requirements to ensure that each has been *built right*. Validation is the determination by the stakeholders that the *right system* has been produced based upon their needs. Early validation is the determination that the right problem is being defined at the current level of abstraction, given the validity of the problem definition at a higher level of abstraction. Verification and validation methods include inspection, analysis (and simulation), test, and demonstration. Specific to test are functional testing, structural testing, performance testing, recovery testing, interface testing, and stress testing (Buede and Miller 2016).

Verification and validation (V&V) need to consider the political, economic, social, technological, environmental, legal, and ethical (PESTELE) factors that contextually influence systems. V&V is challenged to cope with the exponential increase in scale and complexity of systems that are inherently nondeterministic with tightly coupled unintended, unanticipated, and possibly unanticipatible internal and external interactions. V&V is further challenged by autonomous systems, AI and machine learning technologies in assuring the observability, identifiability, controllability, stability, and verifiability of systems.

Michael Griffin makes a compelling case that systems engineering is broken and envisions a path forward in his 2010 paper "How do we fix system engineering?" presented at the 61st Aeronautical Congress in Prague, Czech Republic. Systems engineering is fundamentally concerned with *elegant design* having four attributes posed as questions relevant to both verification and validation:

1. Does the system produce the anticipated behavior, the expected output, over the expected range of input conditions, control variations, and so forth?
2. Is the system resilient?
3. Is the system efficient in the consumption of resources over the course of its lifecycle?
4. Does the system accomplish its intended purposes while minimizing unintended side actions, side effects, and consequences?

Model-based systems engineering (MBSE), model-based engineering (MBE), and digital engineering with its digital threads and digital twins are intended to assure the goodness of design earlier in development with structural model checks and simulation. MBSE is centered on the Object Management Group (OMG) Systems Modeling Language (SysML). The current methods and tooling have systems engineers, or modelers supporting the systems engineers, manually building diagram viewpoints with the system structure, behavior, and parametrics captured in a database supporting structural checks and simulation. Given the scale, rich interconnectedness, non-determinism, and complicatedness/complexity of today's systems, how many diagram viewpoints are needed? How much energy and time is required to generate these model artifacts and assess their goodness? What is the balance between upfront modeling and back-end verification and validation?

The fitness for purpose of our legacy and current *molds* is suspect in engineering the complex systems of our current era and onwards into the future. The legacy *mold* was hardware centric

whereas today's systems are computer/software centric with resultant mismatches in the interface between systems engineering and software engineering. We must find a new *mold* for systems engineering, including V&V, that is fit for purpose. We can look to the systems engineering and software engineering practiced by the big five tech giants collectively known as GAFAM or FAAMG: Alphabet (Google's parent), Amazon, Apple, Facebook, and Microsoft; as well as the semiconductor industry and SpaceX. Google's site reliability engineering, described both online and in print, covers both systems and software engineering. Many of these organizations use formal requirements and formal methods for verification as well as a SecDevOps workflow.

V&V pain points include a) the basics such as inputs/outputs and artifacts, b) perceived value, c) roles and responsibilities of the V&V lead and team, d) resourcing, e) prioritizing activities given resource constraints, f) symbiotic relationships with other systems engineering activities and artifacts to achieve early validation and build confidence towards verification, g) collectively fighting the problems rather than fighting people, and h) using a measured, graded approach to V&V.

V&V is inherently integral to risk and opportunity management and is therefore a consideration in the concepting, requirements engineering, architecture, and integration of systems and the development or revision of the enabling systems around the system of interest. These enabling systems include C4ISR systems, acquisition systems, development systems, production systems including the supply chains, training systems, deployment (transition) systems, operations & maintenance systems, and disposal systems.

V&V applies as well to models in engineering, the modeling of the system context, phenomenology, the system of interest, and the enabling systems. The V&V of these models assesses both their fidelity and the stakeholder confidence in the models critical to the imperatives for digital engineering, digital threads, and digital twins. The V&V of the integration of these models is assessed by constraint theory as defined by INCOSE past president George Friedman in his PhD research and is different from the theory of constraints.

The fundamental approach to the V&V of engineering models, systems of interest, and enabling systems performs the following activities leveraged from model-based systems engineering:

1. Develop operational concept including use cases
2. Define ecosystem with system (or model) boundary and external interfaces
3. Develop, assess, and refine value model of objectives
4. Develop, relate, analyze, and refine inputs, outputs, functions, performance constraints, interfaces, system-wide/technology constraints, trade-offs, and qualification constraints
5. Develop, relate, analyze, and refine architecture with relevant contextual, functional, logical, physical, allocated, and interface views
6. Ensure feasibility
7. Obtain approvals.

Case studies, example models, and exercises illuminate the tutorial material from a V&V perspective including test coverage and how much testing to achieve a given confidence level. Also, what level of fidelity in analysis to be acceptable for V&V.