The ITEA Journal of Test and Evaluation 2016; 37: 10-16
Copyright © 2016 by the International Test and Evaluation Association

Defense System Complexity: Engineering Challenges and Opportunities

Kristen J. Baldwin
Acting Deputy Assistant Secretary of Defense for Systems Engineering,
US Department of Defense

D. Scott Lucero, Deputy Director, Strategic Initiatives
Office of the Deputy Assistant Secretary of Defense for Systems Engineering,
US Department of Defense

The mission of the US Department of Defense (DoD) is to protect national security and to generate, equip, and sustain military forces to deter war and prevail in combat. To accomplish this complex and challenging mission, the size and scale of the national security enterprise is vast: 2.5 million men and women in uniform, including 1.3 million on active duty and 862,000 in the reserves, supported by a civilian workforce of more than 742,000. Within this workforce are more than 100,000 engineering professionals, including more than 39,000 acquisition-certified engineers directly supporting the design, development, and delivery of military systems. These engineers—and their peers who carry out critical program management, test, logistics, and other acquisition functions—are engaged daily to innovate, develop, produce, and maintain superior capabilities for the nation's defense.

Kristen J. Baldwin

D. Scott Lucero

Several compounding factors drive complexity in the engineering, testing, and evaluation of defense systems. DoD engineers and testers must deliver technologically superior military capabilities, most of which involve complex, integrated, and networked systems. The capabilities must serve a diverse range of mission areas, including mounted and dismounted infantry operations; undersea navigation and protection; long-range precision strike; homeland defense; cyber operations; search, rescue, and medical treatment operations; disaster relief and humanitarian operations; sustainment and logistics support; and tactical and national situational awareness.

Although systems engineering and testing are among the DoD's strengths, the traditional practice of engineering is challenged not only by the scale and operational tempo of the national security enterprise, but by additional factors that include fiscal and budgetary constraints, the evolution and globalization of advanced technology and software, the necessary integration of complementary systems to achieve mission effects, and the responsibility to provide a safe, secure military capability that is ensured to perform as expected.

These factors translate into design and performance demands for defense engineers in terms of resilience, affordability, interoperability, reliability, safety, and security. In an ongoing effort, the DoD is taking steps to sustain and strengthen critical organic workforce capabilities; to improve engineering, test, and evaluation methods and tools; and to broaden its partnerships with commercial and defense industry, universities, and federally funded research and development centers that augment organic capabilities with critical talent.

Challenges

The nation's military must be resilient to the volatile changes in today's operational environment. The practice of engineering is most straightforward with a known set of stable boundaries and requirements for which optimal solutions can be generated, along with

clearly defined expectations for contracts and parameters for verification and validation. In the defense environment, however, the threat continues to evolve, challenging engineers to develop architectures and design margins that allow for uncertainty and the inevitable changes in operational requirements. With the democratization of advanced technology, creative adversaries can exploit emerging opportunities. Our operational forces are also creative and employ systems in unanticipated ways.

The practice of systems engineering in the DoD has shifted from the design of exquisite systems against a static set of requirements to a practice informed by war gaming and intelligence. Systems engineering involves advanced analytics to evaluate trade space at multiple levels (mission to materials), allows for margin in design decisions when uncertainty is high and stakeholder confidence is low, and crafts adaptability into architectures and business approaches to insert new technologies and keep pace with evolving requirements.

Adding to these challenges, given today's fiscal constraints, is the demand that systems engineers consider affordability as part of the trade space. With a shrinking military and increased budgetary pressure on research, development, and procurement accounts, systems engineers must understand the relationship between cost and other performance constraints. When does the value of a key performance parameter drive the design toward the use of exotic materials or unique manufacturing processes? How do short-term cost savings during development affect the overall life cycle costs? Engineers must perform robust trade space analysis that considers not only performance but also materials, manufacturing, and sustainability, and they must assess cost as a performance parameter throughout the planning and design processes to ensure that plans are affordable, with reduced life cycle costs.

Today's defense systems are critically dependent on software, which provides a flexible mechanism to rapidly improve or correct performance. The sheer quantity of software that enables defense systems today drives complexity in engineering, test, and evaluation. Defense systems use hundreds of millions of lines of code generated by defense teams, reused from known government or commercial-off-the-shelf systems, and incorporated from open sources. Software dependencies within and among systems are complex. Along with software-controlled systems has come an explosion of data and opportunities for networking and information exchange across countless combinations of system interfaces.

This power comes at a cost. Software and data integration, management, test, and assurance lead to unprecedented challenges for defense engineers and testers to evaluate the totality of these exchanges and functions, as well as the safety and security of code from known and unknown sources. Complexity increases as functions are embedded into smaller microsystem components, and as systems integrate greater manned and unmanned functionality. Defense engineering and test methods are evolving to ensure systems can be verified to behave as expected and contain no unwanted behaviors. The defense research community is investigating approaches that could prove useful for certifying performance. Software opportunities and challenges will continue to be pervasive and persistent, and engineers and testers will need to be creative in addressing these challenges.

US technological superiority relies on protection of enabling technologies, as well as protection of the unique integration, adaptation, and production of technology that creates defense system capabilities. We can no longer rely solely upon network and information security specialists, layers of encryption, and perimeter-based information assurance and operational security around systems and networks. Traditional security segregation and boundary approaches leave adversaries few impediments once perimeters are breached. Complex supply chains, with software and internal components obtained from the global marketplace, make perimeter protection untenable. Systems engineers must bring security into the design trade space and seek design patterns and system architectures with inherent resilience. Rather than just conducting red team exercises during verification, engineers and testers should incorporate "red teaming" practices during the design process to ensure critical technologies and functionality can withstand adversaries' tactics. Engineers need to consider protection of data, security, anti-tamper, and exportability requirements during early development. Failure to do so can be a costly oversight.

Systems engineering traditionally has relied on monitoring the execution of defined and repeatable processes to ensure predictable development. Decisions are made at subcomponent and system levels at successive reviews to meet carefully chosen exit criteria and technical performance measures. This traditional practice is challenged by growing complexity. The DoD has initiated collaborations to advance the state of practice for current and future environments. Following are a few of these initiatives.

Partnerships

Complex engineering challenges are not unique to the DoD. US Government agencies and international

defense partners wrestle with complexity given the nature of their missions, for which there is little analogue in the commercial arena. NASA routinely introduces complex, resilient systems into unknown, adverse environments. The Federal Aviation Administration is in the midst of a major upgrade to the National Airspace System – transforming operations while maintaining expected levels of safety, security, and performance. The Department of Transportation is developing intelligent transportation systems with the potential to reduce thousands of traffic fatalities. The public depends on the safety, security, and reliability of these systems, similar to the warfighter reliance upon defense systems.

Inter-Agency Working Group for Engineering Complex Systems. In 2012, the chief engineers of several federal agencies began to meet to discuss challenges and ideas. The group formalized into the Inter-Agency Working Group (IAWG) for Engineering Complex Systems (Figure 1) and now meets several times a year to develop a common understanding of the problems associated with engineering complex systems and to collaborate, share expertise, and consider resources to make progress against these challenges. The group has developed a position paper (IAWG 2013) outlining the issues and advocating for needed research into the core principles of engineering and science to lay the foundation for significant, next-generation advances in the cross-discipline practices of engineering and the education of future engineers. The engineering leaders of each agency find great value in understanding and participating in other agencies' initiatives. The IAWG reviewed the National Institute of Standards and Technology and the Department of Homeland Security initiatives in disaster resilience, and compared them with DoD initiatives for resilient defense systems.

Figure 1: Inter-Agency Working Group for Engineering Complex Systems: Mission and Participants

Figure 2: SERC Network of Collaborators

IAWG agencies have participated in the National Science Foundation (NSF)-led program exploring fundamental science and theories of engineering, and agency experts have gathered in workshops on systems engineering education. The agencies have jointly sponsored workshops on topics of mutual interest, such as the NASA and NSF exploration of integrating decision sciences into engineering practice. After identifying a federal-level interest and common efforts in digital, model-centric engineering, the IAWG established its first IAWG task team to define common federal agency needs and expectations, as well as strategies and methods for infusing model-based engineering into organizations. The number of federal agencies participating in the IAWG has grown steadily over the years, indicative of the real challenges facing the engineering community and the opportunity for collaboration.

Systems Engineering Research Center. In 2008, the DoD established the Systems Engineering Research Center (SERC), a university-affiliated research center, today a network of 22 universities led by the Stevens Institute of Technology (Figure 2). The SERC and DoD partner to conduct systems engineering research – developing improved methods, processes, and tools in four areas (Figure 3):

- Systems Engineering and Systems Management Transformation
- Trusted Systems
- Enterprises and Systems of Systems
- Human Capital Development

The SERC's research strategy directly addresses the challenges of complexity in defense systems. The SERC

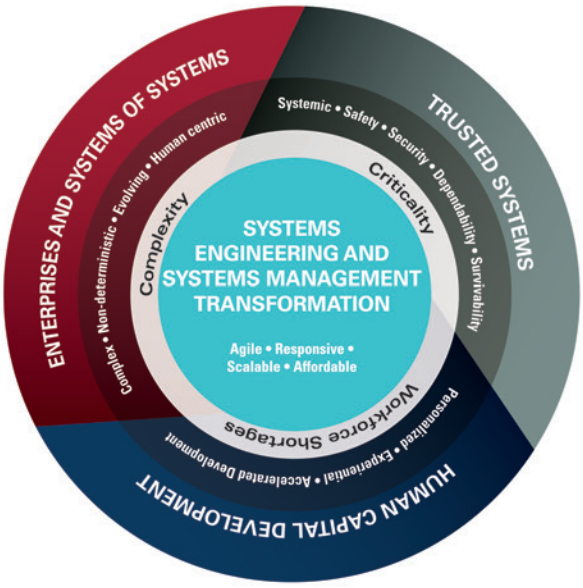

Figure 3: SERC Research Focus Areas

has made several notable contributions since its inception, such as the development of the Systems Engineering Body of Knowledge (SEBoK). SERC led the SEBoK development but sought participation from renowned experts worldwide. The product, a wiki-based, living, authoritative guide to systems engineering practice, is now maintained by the International Council on Systems Engineering (INCOSE) and the Institute of Electrical and Electronics Engineers Computer Society (IEEE-CS).

Another transition activity under way is the SERC's system-of-systems (SoS) analytic workbench. This capability is undergoing pilot efforts at DoD laboratories, helping SoS engineers assess the impact of development disruptions and critical dependencies, and develop architectures that are resilient to a variety of missions and threats. The SERC is working with the Army to pilot system security engineering methods into selected integrated fire control systems. These new methods embed system-aware design patterns that can monitor the system for unintended behaviors or other attack symptoms. The SERC also has been a key participant in the Department's Engineered Resilient Systems (ERS) program.

Initiatives and Opportunities

Engineered Resilient Systems. In 2011, the DoD established a science and technology priority for ERS, identifying a need for research into engineering methods that would improve the resilience of DoD's systems to changes in threats and missions. The ERS team is developing a suite of products that will provide improved processes and tools for existing acquisition activities. The ultimate goal of ERS is DoD-wide use of these processes and tools for analyzing new concepts and systems, or adapting existing systems to changing mission requirements. ERS capabilities will provide engineering, warfighting, and acquisition decision makers with an advanced capability to manage a multidimensional trade space with full and consistent information throughout the life cycle of a materiel system. The result will be better-informed decisions that are made effectively and quickly.

ERS research and development efforts focus on implementing a suite of computational engineering tools, models, simulations, and related capabilities, as well as tools for trade space assessment and visualization within an architecture aligned with acquisition and operational business processes. These integrated tools operate within a framework that supports data-driven decision making; provides advanced knowledge management, including data retention and lessons learned; and enables multicommunity collaboration. ERS uses multifidelity physics-based models developed by DoD's science and technology community to inform the acquisition decision process, for example, increased and easier use of high-performance computing, web-based analysis of large data sets, and life cycle cost sensitivity analysis. These new computational and model-based frameworks will adapt advanced design and modeling approaches from government, industry, and academia to deliver an affordable and effective warfighting capability.

Modular, Open Systems Approaches. The desire for systems to be agile, flexible, and technologically advanced is consistent with the philosophy of modular, open systems. Defense acquisition has long recognized the benefits of open systems and has established best practices and tools to support program implementation. Driven by defense challenges, there has been a renewed focus on the enablers of modular, open systems, including data rights, intellectual property, contracting and business practices, and technical approaches. These approaches offer opportunities to encourage subsystem-level competition to "future-proof" systems, provide pathways for innovation, and potentially reduce long-term cost.

DoD programs are required to implement open systems approaches where feasible and cost-effective. To support these goals, engineers must adopt these approaches and tailor them to program characteristics and desired outcomes. One key enabler is the system architecture itself. DoD system development efforts should be accompanied by an architecture definition that provides flexibility in the design, with subsystem boundaries that are

defined, coherent, and loosely coupled to enable the agility called for in defense strategy. Technical standards are also important enablers. Implementation of modular design approaches requires the prudent use of standards across system development, acquisition, and sustainment. In 2015, the Defense Standardization Council chartered an exploratory technical standards working group to identify standards, determine gaps, and define the role for defense standardization in supporting modular and open systems approaches.

Digital, Model-Based Engineering. Technological advances in capturing, managing, and analyzing data offer a game-changing opportunity for engineering. Today, model-based engineering incorporates digital modeling methods, processes, and tools to introduce analytical rigor into all acquisition processes, including engineering concept, design, development, test, manufacturing, and delivery. A digital approach to these processes, with an open framework for reusing the models and data throughout the system's life cycle, can transform the traditional waterfall approach to become predictive and highly integrated. The DoD sees value in adopting digital engineering design and model-centric practices, enabling a shift from the linear, document-centric acquisition and engineering process toward a dynamic digital, model-centric ecosystem.

By organizing information in a standard way, using model-driven approaches, and taking advantage of advances in computing, the DoD seeks to create opportunities to reduce cycle time and lower the cost required to modify designs and sustain systems over time. Using model-based processes, engineers have the tools to readily assess how changes made in requirements and design impact manufacturing and quality, minimizing potential rework. Engineers also will be able to develop a deeper understanding of the non-linear, complex relationships in today's systems to ensure that design, development, and delivery happen predictably, with fewer surprises.

A digital system model, along with simulations and test results, will help ensure that design and development efforts do not become divorced from actual performance. Engineers will be able to store and share design information, rationale, and models in a digital form, reducing the work to regenerate information from paper-based products and the potential introduction of errors. The DoD is sponsoring SERC research in interactive, model-centric systems engineering and is developing policy and guidance to encourage the use of digital system models. Many of these tools are in use today, and with policy and leadership support over time they should be commonplace across the DoD.

System Security Engineering. To address the comprehensive set of threats to defense systems, systems engineering must include system security engineering as a fundamental element.

Security specialties have emerged over time in response to new threats and risks. For example, information security protects information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction; physical and personnel security protects information and other valuable assets physically stored within facilities and installations; and communications/network security protects information transiting networks. Security now has risen to a system-level risk.

Twenty years ago, systems were relatively standalone, software was critical but not prevailing, and the supply base was known and traceable. Today's complex, software-controlled, highly networked systems are built by prime contractors who integrate hundreds of suppliers' and commercial-off-the-shelf components of opaque origin and integrity. Security vulnerabilities now present themselves not only in a manner to which information assurance controls are typically applied, but in internal systems' embedded software and hardware components, and system-of-systems architecture designs. The system security engineering discipline provides an important mechanism for the engineering team to assess and mitigate system and subsystem vulnerabilities.

For the past several years, the DoD has organized initiatives to establish the practice of system security engineering. Engineering teams now perform criticality analysis as a risk-based approach to determining allocation of security requirements. Components identified as having high consequence if attacked or exploited are engineered to be resilient to attack and are subjected to additional vulnerability reduction methods, including supply chain risk management practices.

The DoD continues to mature these practices with academia and industry partners. It is hoped that in the long run, system security engineering will be as commonplace a discipline as reliability, safety, and quality engineering practices, replete with tools and methods for assessing the adequacy of these design parameters. Security standards will become integral to engineering, along with technical and management practices, and security will be simply another design requirement. Program and technical teams will address security requirements while the largest possible trade space exists, and ensure the technical maturity and resilience of the security solution throughout the acquisition life cycle. To achieve this goal, the DoD along with its

partners must develop ways to measure and evaluate security, tools, and techniques to support design for security, architectural approaches to neutralize threats, and the means to optimize life cycle security costs.

As described, system security engineering plays an important role in ensuring our systems function as intended and are free from malicious vulnerabilities. This threat is challenging and varies from the traditional kinetic, capability overmatch, or even nontraditional threats seen in overseas contingency operations. This information-age threat challenges the engineering community to treat security as a consideration in the risk and design trade space.

Human Capital. The complexity of today's defense systems drives a demand for engineering and testing talent. The DoD has a number of ongoing and planned human capital initiatives to strengthen our workforce. The military departments are taking steps to identify critical technical competencies and to track and maintain them. To maintain the technical edge of this organic engineering workforce, the DoD seeks to provide technical training in critical technologies and specialty engineering practices, and encourages advanced education. To address gaps, the SERC is conducting efforts in human capital as well. The experience accelerator project seeks to provide an immersive experience in which engineers make decisions on an acquisition program and see the consequences of their actions. The SERC's Helix project is researching what makes systems engineers effective and identifying specific factors that enhance their proficiency.

Great engineers require technical depth, breadth, and leadership skills to manage today's complex systems. This ability starts with education. Most engineers, however, graduate from college with depth in one discipline but with limited breadth of experience and limited leadership skills. Academic stovepipes are tough to break—there are few incentives to work across departments, leading to shortfalls in systems and design thinking, and in systems engineering. These competencies are typically addressed after graduation through industry training, mentoring, and rotational assignments. Although industry training helps address these shortfalls, there are opportunities for engineering students to gain breadth of experience and leadership skills in an academic setting.

Capstone Projects. The DoD has conducted successful research in providing undergraduate design teams with relevant DoD problems for their senior capstone projects, helping these teams gain a broad understanding and build leadership skills. For the last several years, the US Special Operations Command (USSOCOM) has placed many challenging problems requiring multidisciplinary solutions in the capstone marketplace (www.capstonemarketplace.org) and has seen a great return on their investment. Several student teams have outperformed industry by providing fresh insights, novel approaches, and innovative solutions to complex problems.

Student teams have participated in USSOCOM's tests of the capabilities and limitations of their systems. A student team from Stevens Institute has pursued patents on their water/pressure-activated floatation device. Other research at the University of Texas (UT), Austin has identified how fundamental systems engineering principles can be integrated into a capstone design course without displacing other educational content. Exposing the students to defense system challenges not only enhances their breadth of experience and increases their leadership skills, it shows young engineers the opportunities available in the DoD to make a significant contribution to the nation's defense. Many capstone students have gone on to internships in DoD labs and in the defense industrial base.

Although the research at the SERC and UT Austin has shown great promise, incentives are needed to encourage universities to work across departments and provide the competencies needed to deal with the complexity of today's systems. Government, industry, and professional organizations can benefit from engaging with academia to:

- Provide the hard problems that require technical leadership and multidisciplinary solutions
- Serve as the customer and mentor, conveying realistic experiences

Continued leadership and commitment are needed to realize the benefits of this research on a broader scale. A professional association or consortium could take on the mission to serve as a clearinghouse for multidisciplinary capstone projects. This capstone effort would not only provide sponsors with a fresh look at challenging problems, it would help build the engineering workforce of the future.

Continuing Commitment

Although there are many sources of complexity in today's defense systems, the DoD is making progress. Federal agencies are communicating, coordinating, and collaborating on initiatives to improve the engineering of complex systems. The SERC and ERS are developing improved methods and tools. Complexity is inherent in providing our warfighters with the best systems and latest cutting-edge technology to remain superior to any

potential adversary, but the DoD acknowledges this challenge and is seizing opportunities to improve its ability to engineer these complex systems. ❑

KRISTEN J. BALDWIN is the Acting Deputy Assistant Secretary of Defense for Systems Engineering, US Department of Defense. Her areas of responsibility include the engineering and technical workforce, engineering policy, and systems engineering planning for major defense acquisition programs.

DON SCOTT LUCERO is the Deputy Director for Strategic Initiatives within the Office of the Deputy Assistant Secretary of Defense for Systems Engineering. He is the government program manager for the Department of Defense Systems Engineering Research Center, a consortium of universities that work collaboratively to conduct research addressing defense systems engineering challenges.

References

National Institute of Standards and Technology (NIST) Special Publication 1190. *Community Resilience Planning Guide for Buildings and Infrastructure Systems*. Vols I and II. Washington, D.C.: NIST, U.S. Department of Commerce, October 2015. http://www.nist.gov/el/resilience/guide.cfm

Inter-Agency Working Group (IAWG) on the Engineering of Complex Systems. "Transforming the Practice of Engineering for Large Complex Systems." Position paper. Washington, D.C.: IAWG, December 2013. http://www.acq.osd.mil/se/outreach/pubs.html

Websites

Capstone Marketplace.
www.capstonemarketplace.org.

Department of Defense Systems Engineering.
http://www.acq.osd.mil/se/index.html

Systems Engineering Research Center (SERC).
http://www.sercuarc.org/

Guide to the Systems Engineering Body of Knowledge
(SEBoK).http://sebokwiki.org/wiki/Guide_to_the_Systems_Engineering_Body_of_Knowledge_(SEBoK)