2022

Major General Harold J. "Harry" Greene Awards *for* Acquisition Writing

A Tremendous Influence within the Army Acquisition Community

by Lt. Gen. Robert L. Marion

"Harry was a Soldier, a husband, a father, a son, a friend, a leader and a great patriot. He left an indelible mark on everyone he came in contact with, and when I think about Harry, I think of a scholar, an inspirational leader, one who was humble and a passionate Soldier, always committed to whatever mission he was given."

—then-Army Chief of Staff Gen. Ray Odierno, Aug. 14, 2014

Each year, through the Maj. Gen. Harold J. "Harry" Greene Awards for Acquisition Writing, we remember a highly decorated Soldier, an Army leader, a mentor and a friend who had tremendous influence within the Army acquisition community. An engineer by training, he held six academic degrees—a Ph.D., three masters of science degrees, a bachelor of science and a master of strategic studies from the U.S. Army War College—but his true strength was in his ability to communicate with Soldiers and civilians at all levels. It is those instant connections that we treasure.

Through these awards, we solemnly remember Maj. Gen. Greene's 34 years of distinguished Army service, not for how his life ended, but for what it achieved. Harry was passionate about providing our men and women in uniform with the most technologically advanced equipment available anywhere on Earth. He was equally passionate about mentoring his team to ascend the ladder of leadership or achieve whatever dreams they held. I know firsthand because when he served as the deputy for acquisition and systems management in the Office of the Assistant Secretary of the Army for Acquisition, Logistics and Technology in the Pentagon, I had the privilege of serving as his deputy.

I spoke recently at a rededication ceremony of a plaque featuring his likeness that had been transferred from Kabul, Afghanistan, to the C5ISR campus at Aberdeen Proving Ground, Maryland. I told the hundreds of people assembled that I consider myself very, very lucky to have served with Maj. Gen. Greene. I learned so much personally and professionally about what it means to be an Army leader by watching him. His keen intellect, acquisition expertise and quick wit were legend, but what I remember most about him is that he was a person who truly cared for and respected others.

Maj. Gen. Greene has been honored in many ways by the individuals he touched and the communities he served. He was the inspiration for the Fallen Star Memorial at Aberdeen that honors all fallen service members and their families. A lounge for traveling military members at Augusta Regional Airport in Georgia is named for him, as is a street, General Greene Avenue, that leads to the U.S. Army Natick Soldier Systems Center in Natick, Massachusetts.

Countless other remembrances carry on his legacy to the next generation of engineers, innovators and leaders. These include a chapter of the Association of the United States Army (AUSA) at Aberdeen, an AUSA Science, Technology, Engineering and Math scholarship, the U.S. Army Futures Command Innovation Award and, of course, the Maj. Gen. Harold J. "Harry" Greene Awards for Acquisition Writing. A replica of the same plaque now at Aberdeen is showcased in our Pentagon headquarters office with the names of all those who have won or received honorable mention since the awards began in 2014.

This special supplement of Army AL&T magazine includes the 2022 winning authors and those who received honorable mention in the categories of Acquisition Reform; Future Operations; Innovation; and Lessons Learned. My sincere thanks to all who participated in this ninth annual competition, and to their teammates and families who supported them in their writing. I also want to express my appreciation to our dedicated judges for their time and expertise in making this annual competition another success. My congratulations to all.

The winners and honorable mentions are:

Category: Acquisition Reform

Winner: Overcoming our Complexity Complex: Emerging Insights from Model Based Design

Authors: **Joseph Novick** is the product manager for the Chemical, Biological, Radiological and Nuclear (CBRN) Covers, Coatings and Protective Overlays program as well as other programs in the Joint Program Executive Office for Chemical, Biological, Radiological and Nuclear Defense (JPEO-CBRND) portfolio. Novick is matrixed to JPEO-CBRND from the Naval Surface Warfare Center in Indian Head, Maryland. He has an M.S. in systems engineering management from the Naval Postgraduate School and a B.S. in biochemistry from the University of Virginia. His DAWIA certifications include Practitioner in engineering and technical management and Advanced in program management.

Daniel O'Neill is the lead digital engineer for the Combat Capabilities Development Command (DEVCOM) Chemical Biological Center (CBC) and provides matrix support to the analytical framework within JPEO-CBRND. With a B.S. in mechanical engineering from Pennsylvania State University, O'Neill has supported DEVCOM CBC for 12 years in both testing and systems engineering. He currently focuses on mission analytics and the application of digital engineering across the product life cycle.

Abstract: To address increasing complexity within system and system-of-systems design, JPEO-CBRND has embraced employing model based systems engineering (MBSE) to shape and plan early user demonstrations. Utilizing a digital approach combined with integration events leads to the exposure of emergent behaviors, allowing program managers to better plan and mitigate risk. The CBRN Covers, Coatings and Protective Overlays program used this MBSE approach in the Desert Tempest user demonstration at Dugway Proving Grounds in Dugway, Utah, to understand how the employment of covers impact Soldiers' tactics, techniques and procedures in order to improve design and development decision-making.

Honorable Mention: Square Pegs in Round Holes – Drug Development Doesn't Fit into the Adaptive Acquisition Framework Pathway

Authors: **Lt. Col. Edwin LaVell Kolen** is a joint product manager for the BIO 2 program at the Joint Project Manager for Chemical, Biological, Radiological and Nuclear (JPM CBRN) Medical, a component of the Joint Program Executive Office for Chemical, Biological, Radiological and Nuclear Defense (JPEO-CBRND), headquartered at Aberdeen Proving Ground, Maryland, which is responsible for development and fielding biological defense pharmaceuticals. In this role, he is accountable for providing research, development, acquisition management and joint service integration for products transitioning from the technology base through full life cycle management of U.S. Food and Drug Administration approved medical countermeasure pharmaceuticals against chemical, radiological and nuclear threats.

Lt. Col. Amanda Love is a joint product manager for the BIO 1 program at JPM CBRN Medical, within JPEO-CBRND. In this role, she is responsible for providing research, development, acquisition management and

joint service integration for products transitioning from the technology base through full life cycle management of U.S. Food and Drug Administration approved medical countermeasure pharmaceuticals against chemical, radiological and nuclear threats. Love was commissioned as an Army Nurse Corps officer and has held a myriad of clinical and acquisition assignments.

Abstract: This article contends that the Department of Defense (DOD) should adopt a drug development Adaptive Acquisition Framework (AAF) pathway. The authors provide evidence that supports the assertion by highlighting statutory requirements, authorities outside of the DOD, process requirements and other challenges that support an additional AAF pathway for drug development. The authors also define what the pathway should be composed of, and why. Finally, the authors provide a diagram of the proposed AAF pathway.

Category: Future Operations

Winner: Acquisition Cyber Resilience

Author: **Carlos A. Natividad** is a computer scientist who holds an MBA from New Mexico State University and a B.S. in computer science from the University of Texas at El Paso. He has 16 years of service in the civilian sector of the Army, of which 8 years have been supporting cyber experimentation and analysis. He is now a team lead for the Combat Capabilities Development Command (DEVCOM) Analysis Center's Cyber Experimentation and Analysis Division, under the Cyberspace Methodology and Mission Assurance Branch. He continues to serve the Army by providing cyber resilience subject matter expertise, analysis, research and experimentation in emerging technologies in the effort to support the current needs of the Army and contribute to building the Army of 2040.

Abstract: The essay titled "Acquisition Cyber Resilience," uses the experience of a seasoned cybersecurity analyst and team lead (Natividad) to discuss future Army operations in a multidomain cyber contested environment. The essay starts in a scenario where cyberattacks are used to cause mission failure, then moves on to discussing mitigation solutions from an operational standpoint. It concludes by revisiting the scenario but with the discussed operational mitigations to give the reader an idea of how cyber resilience can result in mission success.

Honorable Mention: Future Operations: Acquisitions for Light Formations

Author: **Capt. Zachary Matson** is an infantry company commander currently assigned to the 1st Brigade Combat Team, 10th Mountain Division (Light Infantry) at Fort Drum, New York. He commissioned from the United States Military Academy in 2016.

Abstract: The lethality of the modern battlefield will require maximum decentralization, not just for maneuver units but also for sustainment forces. Prioritizing dispersed sustainment with swarms of unmanned aircraft systems will ensure maneuver units maintain tempo in large-scale combat operations.

Disclaimer: *The views expressed in this article are those of the author and not necessarily those of the Department of Defense or any of its components. This paper has been approved for public release.*

Category: Innovation

Winner: Leveraging Innovation to Modernize Decontamination

Author: **Lt. Col. (Ret.) James M. "Mike" Cress Sr.** is a technical liaison officer and innovation advocate assigned to the Combat Capabilities Development Command (DEVCOM) Chemical Biological Center and positioned with the maneuver support community at Fort Leonard Wood, Missouri. A retired Reserve Army officer, he is a graduate of the Command and General Staff College and the Air War College (non-resident) as well as a score of other professional education courses during his 47-year combined career.

Abstract: This article discusses novel, cross-disciplinary development of a capability set addressing a future chemical, biological, radiological and nuclear capability. Close coordination between the Army Chemical and Biological Laboratory, concept and requirements writers, academia, program management office and industry launched an innovative approach to a difficult problem.

Honorable Mention: Predicting Medical Countermeasure Product Acquisition Success: Developing Highly Reliable Medical Products

Authors: **David Booth** is an expert in medical device product development with 30 years of experience and over 25 medical device patents, patent applications and trade secrets. As a senior consultant, he is currently advising the U.S. Department of Defense in the development and manufacturing of parenteral drug delivery systems while completing his Ph.D. in biomedical science. He is a registered professional engineer and a veteran who retired as a major after 23 years of service with the U.S. Army.

Renae L. Malek, Ph.D., is the deputy joint product manager for the Joint Project Manager for Chemical, Biological, Radiological and Nuclear (JPM CBRN) Medical, headquartered at Fort Detrick, Maryland. She earned a Ph.D. in biomedical pharmacology from the University at Buffalo and a B.S. in microbiology from the State University of New York at Plattsburgh, and is a Project Management Professional. She guides the daily operational activities for managing research, development, acquisition and joint integration of U.S. Food and Drug Administration approved medical countermeasures against chemical, radiological and nuclear threats.

Abstract: The U.S. Department of Defense (DOD) relies on the medical countermeasures (MCMs) that treat chemical warfare agent (CWA) exposure, delivered through autoinjectors (AIs), to be highly reliable. Product design frameworks and methods play a large part in helping product design teams achieve their product performance and reliability goals for these autoinjectors.

Design-outcome predictive frameworks and methods are more effective for "designing in" product quality and reliability than reactive design frameworks, like the build-test-fix method typically used in the DOD's acquisition processes. Design problems are eliminated before they appear at the system level using design-outcome predictive frameworks.

The Joint Program Executive Office for Chemical, Biological, Radiological and Nuclear Defense's (JPEO-CBRND) Joint Project Manager for Chemical, Biological, Radiological and Nuclear Medical researched and created a novel design-outcome predictive framework called the Improved Product Reliability Development Framework (IPRDF) and associated methods. This framework is being used to help manufacturer design teams meet stringent reliability requirements set by the U.S. Food and Drug Administration (FDA).

Design-outcome predictive frameworks and methods used for designing AI MCMs are demonstratively effective in producing reliable products, more so than reactive design methods. Three AI development projects using IPRDF reached and exceeded the FDA 99.999 percent device reliability target, with a 95 percent confidence level in less than a year and a half. By comparison, AIs designed only using reactive design frameworks achieved at most 99.7 percent reliability.

Category: Lessons Learned

Winner: Fielding Military Health Status Wearables

Authors: **William J. Tharion** is a human factors research psychologist in the Military Performance Division at U.S. Army Research Institute of Environmental Medicine, with over 20 years of experience directing research on physiological monitoring and in transitioning technology from the lab to the end user. He has published close to 150 journal articles, book chapters and Army technical reports and is a Lean Six Sigma Green Belt. He has DAWIA certifications of Practitioner in both engineering and technical management, and test and evaluation, and holds an MBA from Northeastern University and an M.S. in exercise science from the University of Massachusetts.

Swati Maeder is an assistant program manager in the Joint Product Director for Chemical Detectors and Mobile Analytics (CDMA) Chemical, Biological, Radiological, Nuclear and Explosives (CBRNE) Rapid Acquisition Division at the Joint Program Executive Office for Chemical, Biological, Radiological and Nuclear Defense (JPEO-CBRND). She has worked for 15 years in the areas of CBRNE commercial off-the-shelf (COTS) Rapid Acquisition and Modernization (COTS MOD) process and other traditional programs of record. She has DAWIA certification as Practitioner in program

management and she holds an M.S. in systems engineering from Johns Hopkins University and a B.S. in chemical engineering from Rensselaer Polytechnic Institute.

Maj. (Ret.) Robert Jones is a retired U.S. Army officer, with over 35 years combined knowledge and experience in chemical, biological, radiological, nuclear and explosives (CBRNE). He is currently the systems engineer contractor lead of the Joint Product Manager Chemical Detectors and Mobile Analytics (CDMA), Chemical, Biological, Radiological, Nuclear (CBRN) Rapid Acquisition Division (CRAD), COTS MOD Process. He has worked the COTS MOD Process for the past 16 years, providing more than $250 million of CBRNE equipment and capability to DOD customers. He holds an MBA from Jacksonville State University and a B.A. in economics from Kings College.

Abstract: The National Guard Bureau's Weapons of Mass Destruction – Civil Support Team (WMD-CST) formally identified a need for real-time monitoring since they are at significant risk of heat injuries. A wearable system to provide physiological status to medical and leadership was provided to all WMD-CSTs across the U.S. and its key territories. This is the first deployment of this kind within the military. Key lessons learned included: 1) It took multiple organizations to make this acquisition a reality. 2) Process and product improvement are continuous. 3) Flexibility combined with good working relationships across all relevant organizations is important. 4) Continuous engagement with the customer to address problems as they arise is critical. Success of this first of its kind acquisition was based on these lessons learned that are likely to apply to others as well.

Honorable Mention: Early Cyber Technical Assessment (Quantifying Cyber Metrics and Maturity Early in a Software Development Cycle)

Authors: **Angel Pomales-Crespo** currently serves as the product lead for Network Systems Security and Experimentation within the Product Manager (PdM) Tactical Cyber Network Operations (TCNO), at the Program Executive Office for Command, Control, Communications – Tactical (PEO C3T). He holds an MBA from Monmouth University, an M.S. in technology management from Stevens Institute of Technology and a B.S. in industrial engineering from the University of Puerto Rico. He is a DAWIA certified Practitioner in engineering, testing and program management. He has over 27 years of work experience and has supported the telecommunications industry in both the private sector and the U.S. government. He has supported the Army Joint Tactical Radio System program and the Army Future Combat System program in testing and systems engineering, and integration areas. He is currently responsible for the execution of TCNO's cybersecurity mission including development of cybersecurity strategy, program protection plans, cyber requirements development, risk management framework and cyber testing at the National Cyber Range to ensure a cyber hardened Network Operations Softwarebaseline. He also currently leads the cybersecurity planning and strategy for the forthcoming Unified Network Operations program of record within PdM TCNO.

Deryk Gannon currently is an ASRC Federal senior principal cybersecurity engineer supporting PdM TCNO within PEO C3T. He holds a B.S. in computer science from Rowan University and an A.S. in business from Middlesex County College. He has over 28 years' experience as a cybersecurity engineer subject matter expert with focus in U.S. government systems and networks. He is responsible for developing cyber engineering plans and strategies for TCNO's cybersecurity mission including development of cyber technical system requirements, cyber system life cycle, program classification guides, cybersecurity technology integrations, risk management framework and cyber assessments at the DOD National Cyber Range to ensure a cyber hardened system and demonstrate systems ability to operate in a contested cyber domain. His current focus is leading the technical development of Network Operations cyber requirements for the forthcoming Unified Network Operations program of record in support of PdM TCNO.

Christel Petrizzo is a JANUS Research Group senior system engineer supporting PdM TCNO. She is a Project Management Professional who holds a B.A. in applied physics from Stockton College (now Stockton University) and an A.S. in engineering sciences from Ocean County College. She has over 32 years of experience supporting the Army and over three years supporting private industry. She is a subject matter expert in areas such as: requirements (defining, writing and management, reporting), verification and valida-

tion of software and accompanying documents, test and evaluation—all stages, from writing test documents, test witnessing, step-by-step testing (software and system) and organizing Soldier excursions/touch points. In addition, she has served as a project manager, a system engineering lead, a capability set reference architecture lead, Joint Capabilities Integration and Development System and DOD Architecture Framework trained for the Office of the Assistant Secretary of the Army for Acquisition, Logistics and Technology, and a test manager. Her current focus is leading the engineering oversight and serving as the day-to-day point of contact for Small Business Innovation and Research contracts, creating DD Form 254s and Anti-Terrorism/Operations Security pages for all contracts within PdM TCNO, supporting the TCNO cybersecurity team as needed, configuration management and serving as an Integrated Product Team member for the forthcoming Unified Network Operations program of record.

Abstract: Most Army software development today is performed using the Agile methodology of the development-operations-security (DevOpsSec) process where cybersecurity is introduced at the end of the development process (or in Agile, at the hardening sprint, sprint H), usually only aligned with risk management framework. In addition, most software is not penetrated assessed until a "red team" is paid for (normally during formal test and evaluation events). This late cyber testing and the necessary late fixes have led to increases in costs, schedule and possibly non-secure applications in warfighter hands during deployment.

Product Manager (PdM) Tactical Cyber and Network Operations (TCNO) has changed our process to one that embraces building cybersecurity early in the system or application development (one could say a "DevSecOps" process). Software cybersecurity is not always seen by the user, and so it is not quantified or measured fully, even at late stages of software development. The introduction of Early Cyber Technical Assessment (ECTA) provides programs the ability to start quantifying applications' cyber maturity early in the development process. ECTA provides meaningful cyber metrics and cyber maturity findings that track against penetration risk, vulnerabilities exposure, cyberattacks and potential system or mission performance degradation. Some of the key cyber metrics assessed are cybersecurity hardening of the software, implementation of least privileged access, protection level against cross scripting, ensuring reduced attack surface, access control mechanisms and validating software supply change integrity. Cyber metrics provided and evaluated by ECTA in applications' development enable program managers to discover and address negative findings (vulnerabilities, design flaws, lack of code quality, increased attack surface, reduced mission availability, etc.) and/or adjust the software application architecture early to correct those findings. Also, ECTA enables applications' cyber architecture to keep pace with attack surface and mitigate threat vectors. In essence, programs leveraging ECTA's methodology within a DevOpsSec environment ensure applications are delivered within cost, performance and schedule, while also delivering a cyber-hardened product to function correctly in today's cyber-challenged world.

Major General Harold J. "Harry" Greene Awards for Acquisition Writing Distinguished Judges

Vincent E. Boles, Maj. Gen. USA (Ret.), Defense Acquisition University (DAU) professor of life cycle logistics

Charles A. Cartwright, Maj. Gen. USA (Ret.), DAU faculty member and former program manager, Future Combat Systems

Professor John T. Dillard, former senior lecturer, Graduate School of Engineering and Applied Sciences, Naval Postgraduate School

Professor Raymond D. Jones, chair, Department of Defense Management and Professor of Practice, Naval Postgraduate School

Roger A. Nadeau, Maj. Gen. USA (Ret.), senior vice president, American Business Development Group and former commanding general, U.S. Army Test and Evaluation Command

Gary Martin, president of GPM Consulting LLC and former program executive officer for Command, Control and Communications – Tactical

Kris Osborn, president and editor-in-chief, Warrior Maven - Center for Military Modernization and Defense Editor, The Center for the National Interest

Ken Rodgers, Col. USA (Ret.), director, Strategic Defense Systems and C4I, Cypress International

Chérie Smith, managing director of Chérie Smith Consulting LLC and former program executive officer for Enterprise Information Systems

Rickey E. Smith, former deputy chief of staff, G-9, U.S. Army Training and Doctrine Command

Michael A. Zecca, chief futures officer, U.S. Army Combat Capabilities Development Command Armaments Center

Category: Acquisition Reform

WINNER

Overcoming our Complexity Complex: Emerging Insights from Model Based Design

By the following authors:

Joseph Novick

Daniel O'Neill

"How did we miss THIS?" Program managers, test engineers and many acquisition professionals have likely experienced unforeseen problems at test events that seem obvious in hindsight, particularly when combining new systems with legacy systems to create new systems of systems (SoS). These issues can wreak havoc in an acquisition program causing delays, major engineering changes and cost increases. But what if these issues are not predictable until all the constituent systems in the SoS operate together? How should acquisition professionals address problems that cannot be known until seen or understood in operational environments?

The application of SoS methodology to acquisition programs is a hot button issue in the Department of Defense (DOD) today. The DOD defines a SoS as "a set or arrangement of systems that results when independent and useful systems are integrated into a larger system that delivers unique capabilities."[1] By this definition, only when all constituent systems work together do new properties or behaviors of the SoS present themselves and cannot be deduced from the performance of the constituent systems.[2] In other words, program managers cannot test the constituent systems independently and predict all the behaviors of the system of systems. These unpredictable and irreducible patterns and properties are known as emergent behaviors. As SoS increase in complexity, emergent behavior becomes more difficult to predict.

The DOD manages risks by conducting extensive developmental and operational testing, yet unexpected behaviors of SoS still emerge. Can the DOD make changes to its acquisition and test and evaluation processes to further mitigate the risks associated with emergence? This essay will examine the Joint Project Manager for Chemical, Biological, Radiological and Nuclear (JPM CBRN) Protection's approach to addressing the risks of emergence using simple products: tarps and plastic covers.

Emergence and Emergent Behavior

Emergence presents itself in both beneficial and problematic ways. The DOD expects new behaviors from a SoS that the individual systems cannot accomplish alone, otherwise, it would not need a SoS approach. Conversely, SoS can show problematic, negative or even dangerous emergent behaviors. Penicillin changed the world by combating bacterial infections but caused serious health effects in patients who had allergic reactions, an unpredictable side effect only observed after administration of penicillin treatment on a case-by-case basis. The introduction of a new system into the DOD's arsenal may have both positive and negative second- or third-order effects that do not emerge until introduction into the force structure. It is imperative that program managers understand these emergent behaviors early in the acquisition and development processes and not wait until the end of the program when funding and time has run out.

Program managers have tools available to understand the interactions and emergent behaviors of individual systems and systems of systems through model based systems engineering (MBSE) modeling languages like the System Modeling Language (SysML). The JPM CBRN Protection used SysML to conduct a user demonstration evaluating common covering materials' ability to protect high-value assets from CBRN contamination in an event at Dugway Proving Grounds, Dugway, Utah, in April 2022 called Desert Tempest.

Desert Tempest

Historically, CBRN product development follows typical product development, beginning with material testing and building up to component, subsystem, system and finally SoS or operational testing. The CBRN Covers, Coatings and Protective Overlays (C3PO) program conducted user demonstrations throughout product development to understand the operational impacts of inserting covers into existing CBRN doctrinal processes and user tactics, techniques and procedures (TTPs) for

the Army. By understanding these impacts and potential emergent behaviors early in the acquisition process, the program management team could design and engineer better and more user-friendly systems.

The team executed the user-driven event, Desert Tempest, using chemical simulants, safe alternatives that have behaviors similar to actual chemical agents, in more operationally realistic environments. It involved the detonation of an aerial burst that included a chemical agent simulant payload. The simulant would then deposit on a series of assets such as generators, High Mobility Multipurpose Wheeled Vehicles (HMMWVs), Medium Tactical Vehicles (MTVs) and other auxiliary equipment. Some of these assets would be covered with existing cover materials such as 4- and 6-mil plastic and standard issue tarps to understand how these materials would impact user TTPs. The information gathered from the user would then provide the program office with a better understanding of the problems that the program would solve and possibly uncover unexpected problems, i.e., emergent behaviors, early in advanced development.

The program office recognized that even the insertion of simple products like plastic covers and tarps may have a complicating effect on existing TTPs. In order to have a better understanding on the dynamics of the new SoS created by the insertion of these cover materials, the team used a SysML model, Figure 1, to orchestrate the Desert Tempest user demonstration.

MBSE as the Basis for Test Design

To fully capitalize on the Desert Tempest demonstration opportunity, engineers embraced MBSE to dissect

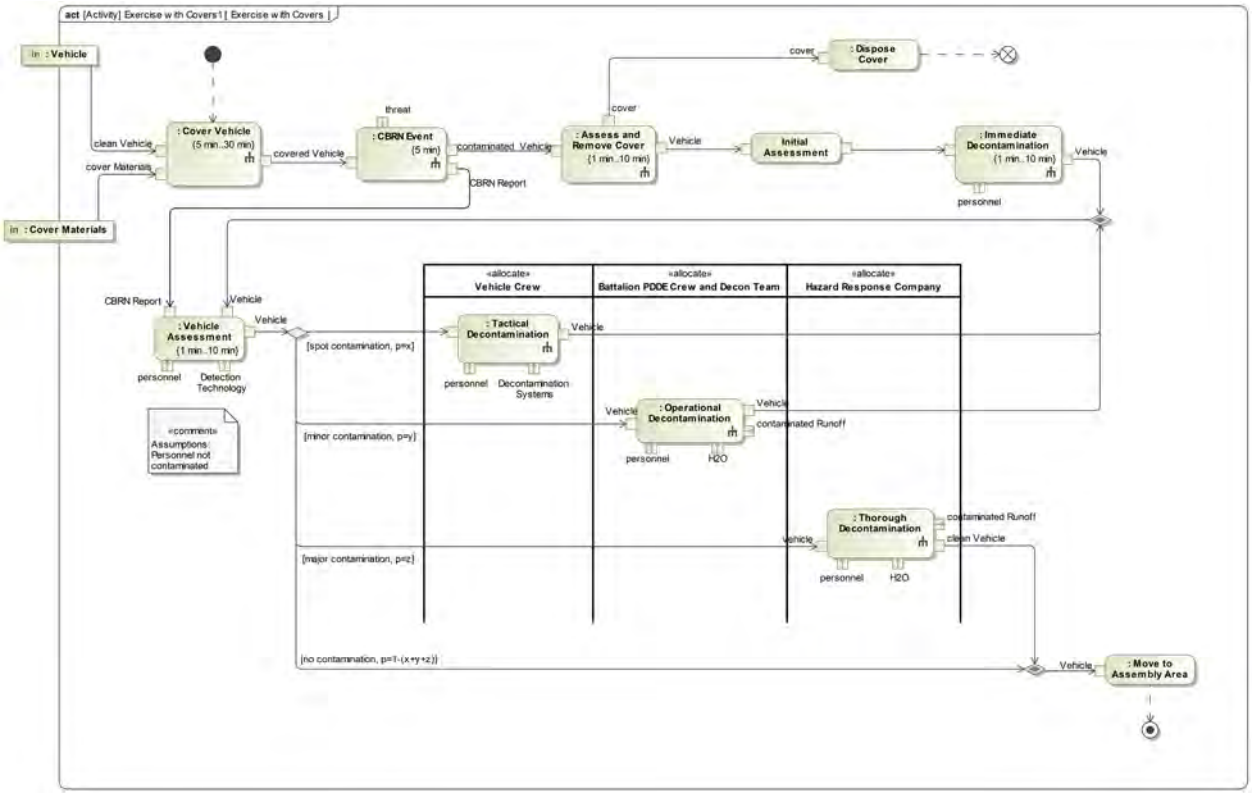


FIGURE 1

DESERT TEMPEST ACTIVITY DIAGRAM

SysML model representation of the utilization of CBRN Covers at the Desert Tempest user event. (Graphic by Daniel O'Neill, JPEO-CBRND)

and understand the procedures of the event. Engineers used SysML as a planning and communication tool to collaborate with representatives from the U.S. Army CBRN School and the U.S. Air Force. Systems engineers explored a mission thread of how these covers and tarps would impact warfighters' actions after a chemical attack on a simulated forward operating base. The team of engineers, program managers, test engineers and combat developers translated doctrinal publications on decontamination to "activity diagrams" (like Figure 1) and system models to understand downstream impacts to the decontamination process caused by the inserted simple tarps and covers. The models clarified complex issues during planning discussions between the team members by providing a common viewpoint on the specific functional elements, specific inputs and outputs element, and planned event outcomes. From these dynamic conversations, system engineers could create new summary views and run high-level simulations for deeper understanding of the complexity of the test. The model enabled the team to visualize the second- or third-order relationships as a systems approach, which would have been difficult to infer utilizing a traditional document-based approach.

Analyzing Emergence and Impacts to Warfighting

Test events can be extremely complex and dynamic, where events must occur in specific orders to gather the results. Modeling provides a common view for all stakeholders to contribute to test planning and ensure that the group reaches common understanding before the event. Demonstration organizers used the model to communicate each scenario and event with the stakeholders.

The model provided insight to potential emergent behavior, particularly on the role of the chemical detectors in the decontamination process. While Army doctrine recommends the use of covers to protect assets from chemical agent contamination in high-threat scenarios, it does not describe the explicit use of covers in TTPs. The model helped the team predict that electronic chemical detectors would have little use in evaluating the contamination levels on uncovered assets because they continued to alarm with large amounts of residual contamination on the ground. While this may seem logical to personnel not well acquainted with CBRN operations, the existing TTPs did not account for mostly uncontaminated equipment in heavily contaminated areas. The SysML model helped the team predict this emergent behavior so that it could be mitigated during the test with non-electronic detectors such as M8 paper and M9 tape. By recognizing the impacts of the insertion of even the simplest of products like tarps and plastic covers into complex operations, test planners can adjust to predicted or impending new behaviors of a system or process. In the case of Desert Tempest, test participants adapted to the use of employing covers and uncovered additional emergent behavior during the test. This presented an issue: how does a warfighter move an uncontaminated asset from a contaminated environment without contaminating the asset? The test subjects developed ad-hoc tactics to move the asset from the simulant-contaminated test site.

Combat developers and user representatives who witnessed the event requested that the program team continue to execute events like Desert Tempest to understand the SoS impacts. They recognized the criticality of understanding emergence in SoS situations to enhance design and product development. MBSE provided a common test picture to enable clear communication between stakeholders and to illuminate likely emergent behaviors in the SoS.

Conclusion

The use of MBSE to drive Desert Tempest highlights emergent behavior as a concern that program managers must address throughout the acquisition process. Information gained through MBSE enables program managers to understand how new materiel solutions will impact the problems they are intended to solve. Exploring areas of emergent behavior works to close these gaps and deliver more effective solutions.

The JPM CBRN Protection plans to continue the use of MBSE in events like Desert Tempest to mitigate the impacts of negative emergent behaviors on development programs. It plans to expand the scope of future events beyond simple covers and tarps, and into more complex decontamination and protection development programs.

Systems continue to become more integrated and complex to deliver a faster and more synergetic way of fighting. Waiting until operational test and evaluation to discover unwanted emergent behaviors leaves program managers with no time and no funding to make major adjustments. The use of MBSE in regular user demonstrations throughout development illuminates risks, allowing program managers to mitigate those risks as early as possible in the acquisition process. Therefore, developing systems without MBSE is inherently risky as program managers are more likely to overlook issues early

in the program life cycle. The combination of MBSE with early SoS testing addresses unforeseen issues before they become too costly and time consuming to fix.

Notes:

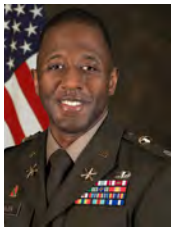
[1] DOD. 2008. "Systems Engineering Guide for System of Systems." Deputy Under Secretary of Defense (Acquisition and Technology) Office of the Under Secretary of Defense (Acquisition, Technology and Logistics). Version 1.0. August 2008

[2] System of Systems Engineering: Innovations for the 21st Century, Edited by Mo Jamshidi, Chapter 7: Emergence in Systems of Systems, written by Charles Keating, 2009. John Wiley & Sons, Inc., Publication

HONORABLE MENTION

Acquisition Reform: "Square Pegs in Round Holes" - Drug Development Doesn't Fit into the Adaptive Acquisition Framework (AAF) Pathways

By the following authors:



Lt. Col. Edwin Kolen

Lt. Col. Amanda Love

Introduction

This article will contend that the Department of Defense should adopt a drug development Adaptive Acquisition Framework (AAF) pathway. The authors will provide evidence that supports the assertion by highlighting statutory requirements, authorities outside of the DOD, process requirements and other challenges that support an additional AAF pathway for drug development. The authors will also define what the pathway should be composed of, and why. Finally, the authors will provide a diagram of the proposed AAF pathway.

Pathway Challenges

Product Managers (PMs) are challenged to lead, learn, develop and manage risk. In exercising their duties, they must get a product or capability to the warfighter. They must provide the warfighter with the product that fulfills the validated requirement, within the cost allocated, and on time. Because of the difficulty in accomplishing these tasks, the DOD has developed an AAF. The DOD has allowed PMs the ability to develop an acquisition strategy for milestone decision authority approval that matches the acquisition pathway processes, reviews, documents and metrics to the character and risk of the capability being acquired. PMs even have the flexibility to choose a combination of acquisition pathways. This is extremely helpful in planning and executing, as risks and schedules are different for each product. However, with drug development, choosing single or multiple pathways is not helpful, as no pathway is adequate for the statutory work and risk associated with delivering this type of capability. In other words, PMs that deliver drug products to the DOD are forced to jam a square peg into a round hole.

If you have ever seen a child attempt to shove a square peg into a round hole, it is fair to assume you witnessed a series of frustrating noises, loud clanging, and finally by some miracle, the child either shoves the square peg into the round hole or finds the square hole. This scene is much like the activities our PMs go through when using the current AAF pathways to support drug development. Eventually, with enough force, frustration and sheer willpower, we get the job done; or, in the words of one of our mentors, "Nevertheless, we deliver." While success occurs, it would benefit the DOD to implement a change and enforce a seventh AAF pathway for drug development.

The AAF presently has six pathways with the "Major Capability Acquisition" pathway, and the "Middle Tier of Acquisition" pathway being most pertinent to this article. DOD drug development has traditionally occurred in the Major Capability Acquisition pathway and has recently had opportunities to utilize the Middle Tier of Acquisition pathway. None of these pathways mention, or even allow, the insertion of a key regulatory authority in drug development for the United States and some of the developed world, the U.S. Food and Drug Administration (FDA). PMs can tailor in regulatory information requirements, but the FDA is more than a regulatory requirement.

The FDA has the responsibility for protecting the public health by ensuring the safety, efficacy and security of human drugs, biological products and medical devices. Thus, the FDA truly provides the permission for a drug product to be used. No mention of the FDA or the drug process in an acquisition pathway may lead acquisition professionals to believe that drug development is the same as other products, which is far from true. This leads to problems with following the Middle Tier of Acquisition and Major Capability of Acquisition pathways.

Problems with Following Traditional Acquisition Pathways

There are numerous problems with following the traditional acquisition pathways. The key challenges that drive the need for a new AAF pathway are meeting key performance parameters (KPP), assessing product goals, identifying decision points, establishing manufacturing and acquiring the science and technology necessary for product development.

Medical products that are being developed for the DOD typically have no more than two KPPs that usually require an external regulation and approval process from the FDA. The approval review process ensures safe and effective products are being developed for one of America's most valuable assets, the warfighter. As this regulatory review process is vital for the development of the medical products, the DOD has a separate and distinct acquisition pathway for which products move along.

The DOD and FDA pathways appear to align but have two inherently different goals and decision points. The DOD PM is held to balance cost, schedule and performance for the product delivery at the terminus of the program. While the FDA pathway appears deceptively linear, its sole focus is on the safety and effectiveness of the medical product, with little regard to cost or schedule. This misalignment often moves the medical product along the DOD acquisition pathway much earlier, to fund the necessary testing and clinical trial phases. Clinical trial design is not binary, and many factors are part of the calculation while designing these studies with the best-known science of the time. The FDA evaluates the data at each stage-gate, and makes recommendations for future studies, some of which might be repeated for corrections in the clinical trial design in either the clinical trial phase or the manufacturing phase. The repeated testing requested from the FDA is not planned into the program, and requires funds originally planned for further efforts to be used to continue the process. Another key challenge is that science is ever-changing, and that the accepted scientific practices at the onset of product development may change during the process and require implementation of the new standard.

Manufacturing is another example of the misalignment of parallel processes. Much of the work and effort for manufacturing processes must be well into development to support the further Phase II and III clinical trials, to include but not limited to confirmation of reproducibility, purity determination, stability and shelf-life studies, all following current good manufacturing practices under the FDA review. With much of this work occurring so early in the DOD acquisition pathway, the production and deployment phase and Milestone C appear to be

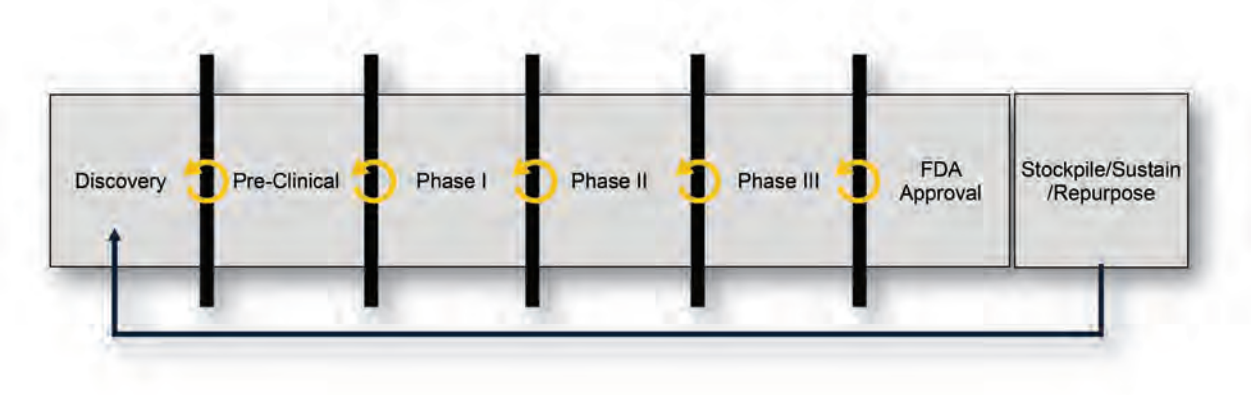


FIGURE 1

Each phase of drug development showing movement to the next phase has a gate that can require more work in the previous phase (Graphic by Lt. Col. Edwin Kolen, joint product manager for JPM CBRN Medical)

needless. The product in development's ability to be used by the warfighter, under these two systems, centers more on the approval from the FDA, with a lesser extent from the Milestone Decision Authority. If the FDA does not believe the product is safe, or has demonstrated an adequate level of efficacy, it will not be placed in a human.

Medical development requires a substantial commitment in the science and technology (S&T) space, on several different fronts, to support capability development. These efforts are typically not fully captured within the scope of the DOD acquisition pathway to support the Materiel Development Decision (MDD), due in part to the alignment of projects to capabilities with an end product in mind. The focus of funding execution versus product development allows for disparate goals from two organizations, S&T and Advanced Development, respectively, to realize the full capacity of the collaboration relationship. Building on the S&T work from multiple inputs such as academia, industry and other governmental partners, allows for more selection and current science to bring a medical product to realization in a more continuous pipeline. The "fail fast, fail smart" mentality needs to be encouraged throughout the organizations for a more agile system.

We assert the need for a functional sponsor that has the responsibility to make resources available for each phase of requirements, and adequately programs and budgets the necessary life cycle cost for execution of the program. The functional manager will also be responsible for all change management needed to execute product development. We recommend removal of the MDD portion in the proposed AAF pathway to better support drug development. The MDD requirement when using the Major Capability Acquisition Pathway is not relevant to drug development. Interagency and sometimes intergovernmental S&T alleviates the need for a mandatory entry point because the maturity of the drug being developed determines what must occur next. Finally, the gateways in which the proposed functional manager provides approval and resources are aligned with receipt of FDA guidance on product development progress.

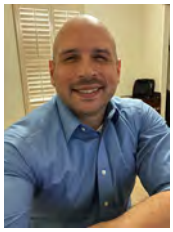
Way Ahead

The DOD must add a drug development pathway to the AAF in order to better align with the FDA, S&T, drug manufacturing and the required clinical studies needed to deliver a safe and effective product to the warfighter. We propose using Figure 1 as the pathway. Figure 1 lists each phase of drug development and shows that movement to the next phase has a gate that can require more work in the previous phase. It also shows the functional manager is aligned with the FDA in decision-making, to ensure resources required are provided for either the next phase or required rework. Figure 1 also shows the operations conducted after FDA approval. Drug development does not end after FDA approval. We also assess if it is possible to repurpose the drug, while maintaining a stockpile and sustainment operations. If the DOD adapts this new AAF pathway, PMs in drug development will no longer attempt to jam a square peg in a round hole. Instead, they will utilize the right tool for the job and get the needed product to the warfighter.

Category: Future Operations

WINNER

Acquisition Cyber Resilience



By the following author:
Carlos A. Natividad

An Army logistics supply vehicle treads along a route, hardened to withstand bullets and explosives, it treads along a tough terrain leading other autonomous military vehicles carrying supplies and personnel along an enemy-contested environment. It uses the leader/follower system to streamline supply delivery. Suddenly, the lead vehicle comes to a stop. The lead, being the head autonomous vehicle, causes a ripple effect among the other autonomous vehicles following it. The lead vehicle operator checks their on-board computer display, which it uses to display a map identifying friendly personnel as well as each autonomous vehicle. This system is also connected to the augmented reality headset the Soldier operator is wearing.

Suddenly multiple enemies start to appear on the map. Both the heads-up display and the on-board computer show that there are several enemy forces spotted around the area. The Soldier operator attempts to reach out for support, but the radios are not working properly. The

Soldier operator then begins to receive a message via text on the software platform from a known contact. The contact instructs them to leave the vehicle, gather the personnel available and return to base. The Soldier operator steps out, weapon in hand, and gathers two more operators. Due to the nature of the convoy being autonomous, the number of personnel is reduced, lethality was reduced and support was heavily concentrated on remote management. The personnel backtrack to the end of the convoy and begin their journey back to base. They rely heavily on the augmented reality headset for situational awareness while they carefully withdraw. After observing the area, a small number of enemy fighters come up to the convoy and seize the assets.

On the enemy side, cyber attackers were able to leverage the Wi-Fi on the systems and have them connect to an enemy hotspot using an "evil twin" attack. They extended the range of their Wi-Fi systems using an amplified antenna. Once they were able to read the network traffic, it became evident that multiple systems could be compromised. The robotic protocols were manipulated to tell the autonomous systems to stop moving, circumventing any operator input. Radio management protocols we identified, attackers used these messages to craft their own and tell the radio to lower the power output and switch to another frequency. This allowed the attackers to limit communication but not create a denial of service. Next, the attackers captured the network traffic used for situation awareness and injected data to create the appearance of enemy forces surrounding the convoy. Adversaries also injected a message telling the Soldiers to make their way back to base and abandon their assets. The enemy forces continue to remotely track the location of the Soldiers through their headsets until they were far enough to capture the convoy.

Taking lessons learned from the current cyber analysis conducted on Army technology systems, this is the reality of the world we are headed into, where the cyber-attack platform has a greater impact on mission operations. To maintain, and increase, a decisive technological advantage against adversaries on current and future battlefields, the Army needs to acquire not only the right hardware but the right software. The cyberattack platform is a software-level problem.

A solution for navigating the current environment may be to acquire software that can attain the resources needed, on demand, in a timely speedy manner. Similar to cloud services that adopt elasticity, where resources are consumed when needed and not used when not needed, software acquisition can also have that flexibility. It can provide the means to allow the Soldier to meet and overcome challenges by delivering capabilities at the moment of need. A cloud infrastructure that supports an on-demand tool repository capable of delivering both defensive and offensive cyber tools on demand would provide solutions for navigating multidomain environments when a cyber threat element is encountered. If access to the cloud is limited or unavailable, then a stand-alone system could be an option.

The modern warfighter now depends more and more on software/data to accomplish the mission. While current conflicts see minimal interference from malicious data actors, the future of conflict will see it more frequently. The interconnectivity of systems over a multidomain environment will enable communication beyond anything the Army has ever used before, but in turn, it will also create a broader landscape where cyber threat actors can exploit system vulnerabilities to affect missions. Given the proposed solution, revisiting the previous scenario has potential to go differently, in favor of the convoy under the cyber threat.

An Army logistics supply vehicle treads along a route, hardened to withstand bullets and explosives, it treads along a tough terrain leading other autonomous military vehicles carrying supplies and personnel along an enemy contested environment. It uses the leader/follower system to streamline supply delivery. Suddenly, the lead vehicle comes to a stop. The lead, being the head autonomous vehicle, causes a ripple effect among the other autonomous vehicles following it. The lead vehicle operator checks their on-board computer display, which it uses to display a map identifying friendly personnel as well as each autonomous vehicle. This system is also connected to the augmented reality headset the Soldier operator is wearing.

As a direct action of a sudden stop of the autonomous system, a network intrusion app was downloaded as soon as possible to start monitoring the vehicle operational network. The app identified extra systems on the Wi-Fi network and has now blocked them. This detection sends an alert to all personnel on the convoy that a cyber threat has initiated an attack. Another app is now downloaded and installed automatically; it leverages wifi emissions to triangulate nearby Wi-Fi devices. The augmented reality

headset now identifies where the emissions are potentially coming from and points it out to the Soldiers, providing situational awareness of enemy locations. Another app is downloaded and placed on the augmented reality headset with a cyber threat warning level. This app gives the Soldiers a confidence level of the data they see based on warnings provided by the other apps.

A higher warning level allows the Soldiers to rely more on physical awareness over software-based awareness.

They are now situated to defer conflict or fight and overcome the nearby adversaries. The scenario can play out with them sending a warning shot to the identified location of the cyber threat actors or they can switch to manual mode and recover as much of the logistics fleet as they can. Having the capability to dynamically add what software is needed on demand, reduces clutter from having it preinstalled, reduces degradation of the system being used and reduces deployment time for hardware. Automating this process also provides the means to be speedy and provide a user-friendly experience with minimal interaction.

The fabric of tomorrow is not a something worn on our bodies, but it covers us from head to toe. It is not threaded by needle, but instead threaded by a network of systems. The fabric of tomorrow does not fade or get worn by the elements, but it does require due care and diligence to be maintained. Every Soldier is a carrier of multiple threads and every commander a weaver of the fabric. As the Army adopts emerging technologies at a fast pace, technology itself is growing at a faster pace. The Army acquisition process needs to evolve to address the demand that future operations need to have put the right software into the hands of the warfighter as the emerging attack platform grows.

Future operations rely on the data fabric to be woven between systems of systems in a manner that is autonomous, harmonious and secure.

HONORABLE MENTION

Future Operations: Acquisitions for Light Formations

By the following author:
Cpt. Zachary J. Matson

As demonstrated in Ukraine, logistics on both sides of the recent conflict are heavily constrained by their logistics tails. Ukrainian forces struggle to bring enough forces to mass for a successful breakthrough, while Russian forces seemingly neglected this vital warfighting function. To keep up with the increasingly lethal modern battlefield and to support the offense, future logistics platforms must adopt unmanned aircraft systems (UAS) tactics to resupply units on the ground, to extend operational reach and exploit success.

While it makes practical sense to develop modular systems for each brigade and division, the Army's transition to the division as a Unit of Action (UoA) indicates it has realized the necessity to tailor units Modified Table of Organization and Equipment (MTO&E) to respective expected mission type. The Army's armored formations are best employed in unrestricted terrain, while its light formations are expected to fight and win in severely restricted terrain. Mounted formations must prioritize Class III while light formations must prioritize Class V. Because of this, light formations in the future force must organize around rapid resupply during their movements and attacks.

War in Ukraine revealed that successful attacks stalled multiple times because the attacking force ran out of either anti-tank systems or small arms ammunition. U.S. Army formations do not need to waste time acquiring new advanced vehicle platforms to support an offense, since we already possess palletized load systems and trailers at the battalion level, on which a container consisting of logistics UAVs and Class V can be moved and stored. The Conex containers loaded on these logistics vehicles ensure we can ship and store a UAV "hangar" as well as house the appropriate mission-tailored Class V loadout. Army acquisition must focus on developing this self-contained Conex of hanging UAVs that an operator can program with waypoints and a tailored payload from

the Class V in the container on the trailer. While the UAV container would be modular, brigades and battalions would still conduct thorough mission analysis to determine the proper load-out of each Class V container tailored on mission set, (much like engineers' Class IV flatracks are loaded based on planned defensive position).

Urban operations might require less-than-lethal munitions such as flashbangs, and defensive operations in rural terrain would require more Javelin or Tube-Launched, Optically Tracked, Wire-Guided (TOW) missiles. Either a forward support company (FSC) operator or a maneuver company executive officer can update in real time their expenditures based on reporting from platoon sergeants that can tailor the load of each drone that sets upon a predetermined aerial axis of advance. Each drone would have a minimum payload of 50 pounds. While not incredibly heavy, we must favor dispersion of assets and resupply in place of mass. A 50-pound minimum allows for resupply of at least a Stinger or Javelin missile. We cannot expect the future aerial fight to be uncontested, and all strategic power competitors are currently in a race to develop both lethal one-way UAVs and effective air defenses. If we favored a larger autonomous aerial resupply, it is more likely that a single resupply vehicle is targeted and shot down. At our combat training centers, entire combat trains are denied to their respective maneuver units due to a single enemy aircraft destroying it with air-to-ground fires with Family of Scatterable Mines (FASCAM). The squad will continue to be the foundation of the decisive force, and we must focus our acquisitions on equipment that will resupply these units with UAS. Individual aerial logistics drones allow us to keep the squad ready to engage any target and continue fighting. One consideration is where the Palletized Load System (PLS) with Class V are staged and loaded. The Army will continue to use the brigade as the unit of action for the immediate future, and current senior leaders are used to employing the typical brigade combat team construct with a brigade support battalion (BSB) in support. Staging the UAV PLS near the BSB, but not within its visual signature, ensures its survivability on the modern battlefield as enemy forces increase aerial and satellite detection methods. Additionally, UAVs with a 50 km operating range will ensure these logistics elements are far enough from the forward line of troops (FLOT) to maximize survivability. Smaller UAVs require either smaller runways or smaller openings in restrictive terrain and contribute even more to a smaller signature. We must further decentralize logistics and resupply through the company to the squad, as we know that warfare in all domains is trending toward swarm tactics. The 11th Armored Cavalry Regiment "Blackhorse" at the National Training Center recently demonstrated the overwhelming nature of a rotational training unit being confronted with a swarm of UAVs. We must embrace this concept as an institution in every warfighting function to maintain relevance on the modern battlefield. Using a PLS truck and trailer with a "hub" of UAVs rotating to the FLOT, we can keep pace with emerging tactics and technology for the foreseeable future.

Category: Innovation

WINNER

Leveraging Innovation to Modernize Decontamination

By the following author:
Lt. Col. (Ret.) James M. "Mike" Cress Sr.

The current chemical, biological, radiological and nuclear (CBRN) decontamination system is based upon supporting technologies that have remained basically unchanged for decades. While there have been some relatively minor changes to the decontamination process, it is still resource intensive, requiring technical understanding, excessive troop support, massive amounts of water, proximity to the hazard, many hours to complete with sometimes questionable results, a very identifiable, large and difficult to defend layout that presents a signature management challenge. The CBRN technical support available to conduct these activities is typically sparse, often requiring that a unit task organize to conduct what is basically a do-it-yourself operation.

In typical practice, a unit that is contaminated must delay the conduct of its mission, often "going back" for decontamination to restore combat power or logistics delivery capability. With respect to the chemical threat, physics rewards rapid mitigation and complicates the process if it is delayed. The demands of a technology-enabled battlefield require dispersion, agility and signature management that are difficult, if not impossible, to achieve with the legacy decontamination capability.

An agile capability that is tailorable, that requires fewer resources, is capable of being delivered at the point of need and presents a signature less likely to be targeted, has the potential to more quickly return combat power or logistics flow.[1] Early discussions with the user revealed they felt that massively contaminated vehicles and equipment demanded too many resources to support future tactical operations. Leveraging developing programs of record, a crew conducted early mitigation activity that was developed and termed "Tactical Decontamination." The technique used an equipment set that could be on vehicle. A more thorough process was still required but the philosophy of "just enough" prompted research into how equipment becomes contaminated and what would be adequate to mitigate contamination. "Mitigate" is now used in the context of managing contamination, mitigating the hazard to the greatest extent practical to reduce operational risk to warfighters while simultaneously informing maneuver commanders with the requisite knowledge to make risk-informed decisions. There are two primary ways equipment can become contaminated. The agent can be delivered as an "agent rain" or agent can be transferred to the equipment as it passes through a contaminated area. Direct targeting is difficult, but transfer could be common. Of the two, transfer is more easily addressed.

The U.S. Army Combat Capabilities Development Command (DEVCOM) Chemical Biological Center (CBC) manages a robust 6.2 (applied research) portfolio of supporting technologies that, if used in a multi-disciplinary, integrated, redesigned process, could address the limitations of the current system.

FIGURE 1

A Soldier conducts an equipment decontamination mission on May 19, 2013. (Photo by Staff Sgt. Jorge Intriago, U.S. Air National Guard)

CBC conceptualized an ad-hoc process, termed CBRN Insight, (Innovative Novel Systems Integrating Groundbreaking Harnessed Technologies), to engage the user in an innovative, collaborative approach to addressing solution space. The central concept was early and continuous engagement between the CBC and the U.S. Army Maneuver Support Center of Excellence (MSCoE), or other user, to define and build virtual and physical prototypes with the intent of conducting multiple learning events in virtual and physical experimentation. The major challenge was not technology, or the capability to prototype, it was a lack of funding to conduct virtual and physical prototype development. There was a need to generate interest and to seek partners. The CBC liaison officer (LNO), working closely with the U.S. Army CBRN School (CBRNS) and MSCoE, sought approaches that could provide "leap-ahead" capabilities to address user needs. The legacy development approach was cumbersome, unresponsive and expensive, often offering "stovepipe" solutions that were overcome by changes in the evolving operational environment. A virtual team was formed to conceptualize multidisciplinary integrated technology approaches. It was decided to conceptualize leveraging the technology portfolio by defining a cross-disciplinary "capability set" (CAPSET) that addressed the threat, cognitive and physical workload, emerging technologies, alternative operational tactics, techniques and procedures, process outcomes and process time as well as costs. It was decided to create a "quad chart" and a discussion paper to socialize the approach.[2]

Experiment venues supporting Army modernization are oriented upon the priorities of long-range precision fires, next-generation combat vehicle, future vertical lift, air and missile defense, network (cyber) and Soldier lethality. The CBRN threat has the potential to disrupt each of these capabilities to the degree of 30 percent or more.[3] A series of virtual experiments were planned and conducted to inform concepts and requirements developers. This experiment series, collectively titled Combined Arms Maneuver in a Contaminated Environment (CAMCOE), examined the impact of a CBRN environment upon combat operations. The experiment was heavily focused upon maneuver combat operations. Conducted in conjunction with the Maneuver Center and including a contingent from the Marine Corps, as well as significant involvement from the operational force, a number of vignettes were defined and executed in a tabletop exercise. Over 40 operational challenges or "gaps" were identified.[4]

These gaps were defined across the areas of doctrine, organization, training, materiel, leader education, personnel and, to a lesser extent, facilities (DOTMLP-F).

As the scenario vignettes of CAMCOE played out, it became obvious that the legacy approaches to CBRN decontamination were challenging in the current environment and extraordinarily difficult to accomplish in a future conflict against a peer or near-peer competitor. CBRN School and Maneuver Support Center of Excellence established priorities for resolution of these challenges. One challenge was associated with equipment decontamination. Examination revealed that some improvement could be realized by doctrine changes. Those changes were immediately addressed with proposed changes to tactics, techniques and procedures, and the effort was titled Tactical Decontamination, a procedure that incorporated near-term programs of record and modified process. That effort was leveraged to inform the CAPSET. It was clear that a simple insert of a new technology application would not be adequate to support next-generation issues associated with combat with a peer or near-peer competitor. In response, a revolutionary, new conceptual approach was proposed focused upon leveraging emerging technologies, current programs of record and commercial capabilities to realize a semiautonomous process with improved precision, reduced resource burden, the capability to push the process to the point of need, reduce the targetable signature of the process and capable of being tailored to support agile operations while complementing the Tactical Decontamination doctrinal change. A quad chart and supporting discussion paper were prepared and staffed.

The deputy commandant of the CBRNS challenged the CBC team to create a video simulation of an autonomous process to illustrate how integrated emerging technologies could demonstrate the application of autonomous behaviors to a modified equipment decontamination process provided by the MSCoE protection team. Working closely together with MSCoE and CBRNS personnel, a storyboard for the simulation was prepared and handed off to the audio-visual technology developers in the CBC Advanced Design and Manufacturing Division. Inspired by a commercial independent research and development effort, a strawman simulation was developed with a narrative and presented to CBRNS and MSCoE for their approval. The resulting simulation depicted an agile semiautonomous process, that leveraged front-end technical information using a unique item identifier (UII) to inform both humans and autonomous machines of likely transfer locations; a robotic semiautonomous prewash; contamination mapping using colorimetric disclosure technology; precision application of an advanced decontamination solution; automated post mitigation monitoring and a flexible system to label output in a

FIGURE 2

A mitigation specialist remotely monitors semiautonomous spraying of vehicles. (Image from an animation of a conceptual process created by Brianna NcNamara, Chemical Biological Center, Engineering Directorate, Advanced Design and Manufacturing Division)

process with faster process time; the capability to monitor the semiautonomous process from short-range standoff distances; with the capability to deliver mitigation capability to the point of need and return combat power or logistics flow quickly.[5]

Initial funding to form a team and create the video simulation was provided by the director of the CBC, who approved Semi-Autonomous Contamination Mitigation as an in-house innovation project which would leverage the center's innovation funding. Lacking a budget line to conduct prototyping, it was necessary to find funding to resource the plan and conduct a proof of principle. The discussion papers and video simulation helped to secure funding to explore autonomous behaviors and demonstrate proof of principle. The project manager obtained additional funding and leveraged other ongoing efforts to conduct an incremental technology development that integrated a ground robot demonstrator, contamination mapping and robotic precision solution application. Other necessary components of the initiative, such as technical information handoff, post mitigation monitoring and sorting, were partitioned to be addressed later due to a lack of funding.

An ad hoc collaborative team formed with representatives from CBC, MSCoE, the Joint Requirements Office, Defense Threat Reduction Agency – Joint Service Technology Office, Ground Robotics Center, and industrial partners with the goal of conducting an incremental series of demonstrations that would prove the principle of applying autonomous behaviors to the challenge of mitigation of contamination. The demonstration effort would be incrementally leveraging other ongoing technology developments and designing a final integrated proof of principle exercise.

Funding was provided to investigate an unmanned ground vehicle (UGV), a contamination mapping capability and applying autonomous spraying behaviors to surfaces. The other supporting activities were unfunded. The CBC LNO to MSCoE reached out to several academic institutions with a proposal to collaborate on a study of the potential to utilize unique item identifiers to hand off technical contamination and administrative information to humans and to autonomous robotics. The LNO collaborated with the Missouri University of Science and Technology to conduct the study as a senior engineering student design project. The LNO had no funds to offer but agreed to mentor the groups as they conducted the project. The university agreed, and the semester-long project was conducted with three design teams investigating. Students were provided with purpose-designed resource materials and an unclassified discussion of the future combat environment. The project was successful, identifying use cases for quick response

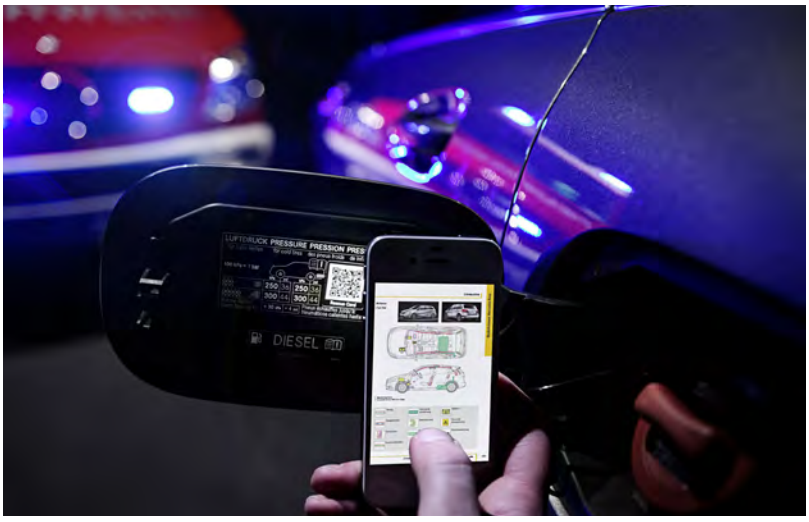


FIGURE 3

Rapid information exchange of complex data is done by a QR code on a Mercedes automobile, which informs first responders of appropriate locations to cut open a wrecked car. (Photo by Car and Driver magazine, June 4, 2013, author Jens Meiners)

(QR) codes informing both humans and machines. Final reports were provided to the project manager and concept developer. One of the more important findings was a commercial equivalent developed by a major automotive manufacturing firm targeting first responders to automotive accidents, advising them on where to cut to extract accident victims.[6]

As a result of the effort, a two-year proof of principle demonstration is planned to follow an incremental prototype development. The MSCoE is periodically advised of progress on the effort and the CBC is actively working with concept and requirements writers on a draft requirements document. Twelve other CAPSET proposals have been prepared and socialized with the MSCoE, resulting in three additional draft requirements documents. This innovative approach leverages Soldier input to shape design and integrates emerging technologies with concepts resulting in state-of-the-art prototype development that informs modernization.

Notes:

[1] Defense Technical Informational Center, Multi-Domain Operations, The Army's Future Operating Concept for Great Power Competition, Technical Report, AD 1083376, 23 May 2019.

[2] Capability Set Proposal, CBRN Visibility of Named Areas of Interest, CBC, Engineering Directorate, CBRN Ignite initiative, 24 February 2022.

[3] DOD Authorization for Appropriations FY86, Hearings before the Committee on Armed Services, U.S. Senate, Ninety ninth Congress, March 1985, Section 3-2, Page 1536.

[4] Combined Arms Maneuver in Contaminated Environment, U.S. Army Maneuver Center of Excellence, ATZK-CIC, 19 October 2017.

[5] Semi-Autonomous Contamination Mitigation (SACM) Video Simulation, AFC, CBC, Engineering.

[6] Mercedes adds QR codes to Cars in Effort to aid First Responders, Car and Driver magazine, June 4, 2013.

HONORABLE MENTION

Predicting Medical Countermeasure Product Acquisition Success: Developing Highly-Reliable Medical Products

By the following authors:

David Booth, PE

Renae Malek, Ph.D.

Introduction

The U.S. Department of Defense (DOD) relies on the medical countermeasures (MCMs) that treat chemical warfare agent (CWA) exposure, delivered through autoinjectors (AIs), to be highly reliable, meaning a failure rate of not more than one device per 100,000 devices produced. Product design frameworks and methods play a large part in helping product design teams achieve their product performance and reliability goals. Design-outcome predictive frameworks and methods are more effective for "designing in" product quality and reliability than reactive design frameworks, like the build-test-fix (BTF) method typically used in the DOD acquisition processes.

The Joint Program Executive Office for Chemical, Biological, Radiological and Nuclear Defense (JPEO-CBRND) Joint Project Manager for Chemical, Biological, Radiological and Nuclear (JPM CBRN) Medical researched and created a novel design-outcome predictive framework called the Improved Product Reliability Development Framework (IPRDF) and associated methods. This framework is being used to help manufacturer design teams meet stringent reliability requirements set by the U.S. Food and Drug Administration (FDA). When teams were trained in Design for Six Sigma (DFSS) and IPRDF methods, three AI development projects using IPRDF, in less than a year and a half, reached and exceeded the FDA 99.999 percent device reliability target, with a

95 percent confidence level; by comparison, AIs designed only using reactive design frameworks achieved at most 99.7 percent reliability.

Product Design Frameworks

Design frameworks and development methods have significant impacts on a product's performance. Often, if a product does not work properly, is taking too long to bring to market, or ends up costing too much, it is the result of a poor design process. It is possible to predict with relatively good accuracy how reliable a product design is, as it is being designed. This is accomplished by choosing design-outcome predictive frameworks and methodologies that allow the design team to quickly learn about their product design and make rapid changes, bringing about superior product performance. This leads to the desirable benefits of predicting and driving product reliability, rather than reacting to the lack of it. This visibility is especially important when designing high-reliability MCMs.

By contrast, the typical DOD acquisition process operates using a top-down design framework of BTF to develop systems and products. This design philosophy is embedded in DOD's technology readiness levels (TRLs) and integrated TRLs for MCM products. The pressure and urgency to reach TRL levels results in the early release of technology and hardware that harbors problems and flaws, bringing about cyclic rounds of testing and fixing problems in the lab or field. This results in delays as teams work to discover the source of these failures, pushing project timelines to the right and increasing project costs. The BTF framework does not permit design teams to predict reasonably accurate product performance and reliability before the system is built. This postpones fielding critical systems that meet the U.S. military services' need.

To understand how development benefits from employing predictive design frameworks and methods, let's look at a particular medical device, the AI.

The EpiPen® is a commercially available AI that contains the drug epinephrine and is used to treat severe environmental allergic reactions. Similarly, first responders treating severe opioid overdose effects frequently use an AI containing the drug naloxone.

The DOD, under the JPM CBRN Medical, has numerous acquisition activities to develop lifesaving emergency-use AIs that contain a variety of drugs to combat CWA exposures. Likewise, when CWAs are inhaled or absorbed through the skin, they can act within seconds or minutes to incapacitate, cause severe symptoms, and/or cause death. AIs are ideal devices for service members to deliver lifesaving drugs to both themselves and their battle buddy, as these devices are robust enough to survive in austere military settings. They can deliver a drug through chemical protective garments, and reliably deliver the correct dose under a range of operational conditions.

For example, the DOD partnered with pharmaceutical company Kaléo Inc. to develop a 10 mg naloxone AI, based on their previously developed 2 mg AI. In February 2022, the FDA approved this higher-dose naloxone AI for military personnel and chemical incident first responders to treat highly potent opioid exposure, including exposure to opioids like carfentanil. It was fielded in the summer of 2022 to specialized units at high risk for exposure. Additional acquisition efforts managed at the JPM CBRN Medical include developing AI devices containing drugs to counter the severe adverse effects of nerve agent poisoning. Their partner, Aktiv Pharma Group Inc., is developing a scopolamine AI using an innovative design, to deliver a drug that acts in the brain to stop the central effects of nerve agent poisoning.

Emergent BioSolutions Inc., is collaborating with the JPM CBRN Medical on two projects. The first, the Dual Drug Delivery Device (D4), is an AI that can deliver two drugs, atropine and 2-PAM (Pralidoxime), to treat cholinergic symptoms and restore breathing. The second effort is to produce an AI that delivers the anticonvulsant drug diazepam.

The JPM CBRN Medical, working with Rafa Laboratories Ltd., received FDA approval on August 8, 2022, for its AI that delivers the drug midazolam to treat seizures. As such, the midazolam AI can be used to stop seizures resulting from nerve agent poisoning.

Major Defense Acquisition Programs and Major Automated Information Systems often leverage DOD test facilities to conduct developmental and operational testing to evaluate system performance, coordinating through the defense test and evaluation community. In medical acquisition, the product sponsor conducts developmental and operational testing, with the FDA acting as the final approver. According to the April 2020 FDA draft guidance titled, "Technical Considerations for

Demonstrating Reliability of Emergency-Use Injectors Submitted under a Biologics License Application, New Drug Application, or Abbreviated New Drug Application," "FDA recommends that emergency-use injectors include design control specifications for successful injection reliability of 99.999 percent with a 95 percent level of confidence." That translates to one detected failure per 100,000 injection attempts; AI manufacturers using the BTF model struggle to meet these FDA reliability requirements. All JPM CBRN Medical's AIs in development will need to meet these robust FDA design requirements.

Predictive Versus Reactive

Predictive design frameworks and methods produce products that are notably more reliable and do this more quickly than reactive design methods. In Figure 1, a traditional BTF design framework is compared with a predictive framework like DFSS, showing these contrasting characteristics.

The iterative system-level testing approach in a reactive design framework like BTF does not allow the design team to quickly learn about critical sub-level parameters that are impacting performance. A predictive design framework and its methods feature a controlled process for identifying and iteratively optimizing critical parameters at all sub-levels, to ensure that when the system is assembled, it performs as expected. Design problems are eliminated **before** they appear at the system level.

Figure 2 depicts BTF loops continuing in multiple cycles until the design meets the product requirement inputs. It is difficult for design teams using this framework to determine what design or manufacturing process aspects contributed to testing failures. Typically, teams using this framework will need four to six BTF cycles, with six to 10 months per cycle, to meet the input requirements. Meeting the FDA's reliability requirements using these methods is difficult and sometimes impossible. One company spent 13 years working to reach their AI input requirements and were still not successful.

A fundamental shift from BTF was needed to produce a design that met the FDA's stringent reliability requirements. The JPM CBRN Medical acquisition team researched and created a novel adaptation of DFSS' design-outcome predictive methods, which is key in helping manufacturing design teams successfully create highly reliable AI designs. Known as the IPRDF, it provides an accurate way for design team members to predict and quickly improve their design capability and reliability. This improvement features a tighter coupling of DFSS methods, risk assessment and risk

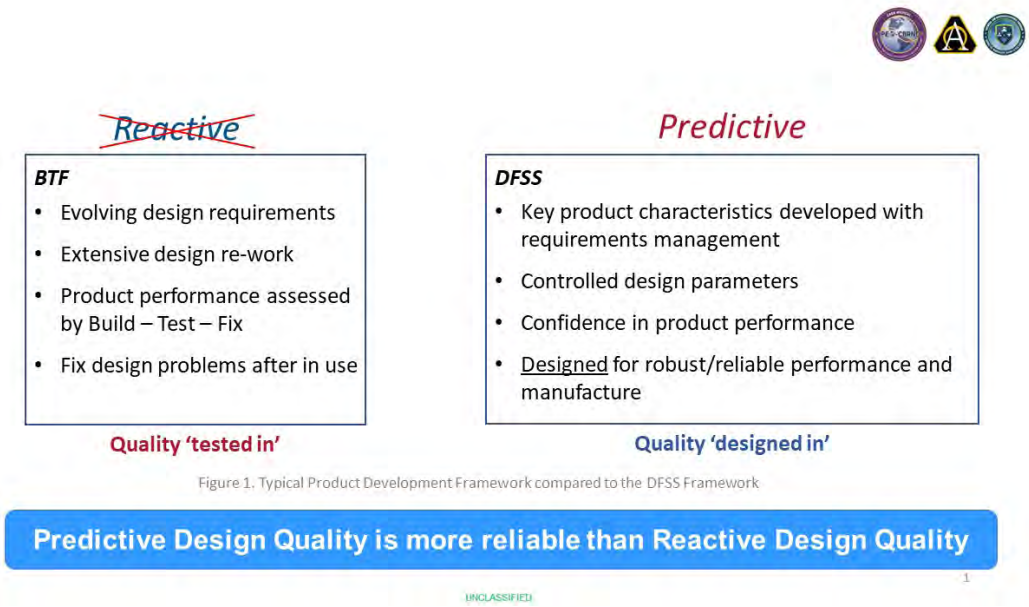


FIGURE 1

Typical product development framework compared to the DFSS framework. (Graphic by David Booth, process adviser, supporting JPM CBRN Medical)

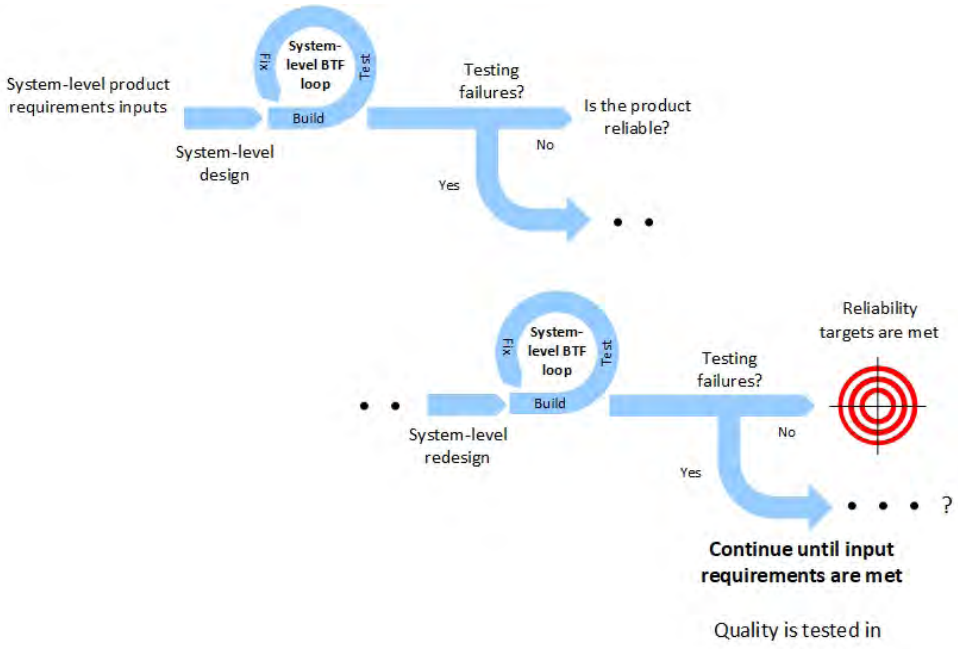


FIGURE 2

Build-Test-Fix reactive framework model. (Graphic by David Booth, process adviser, supporting JPM CBRN Medical)

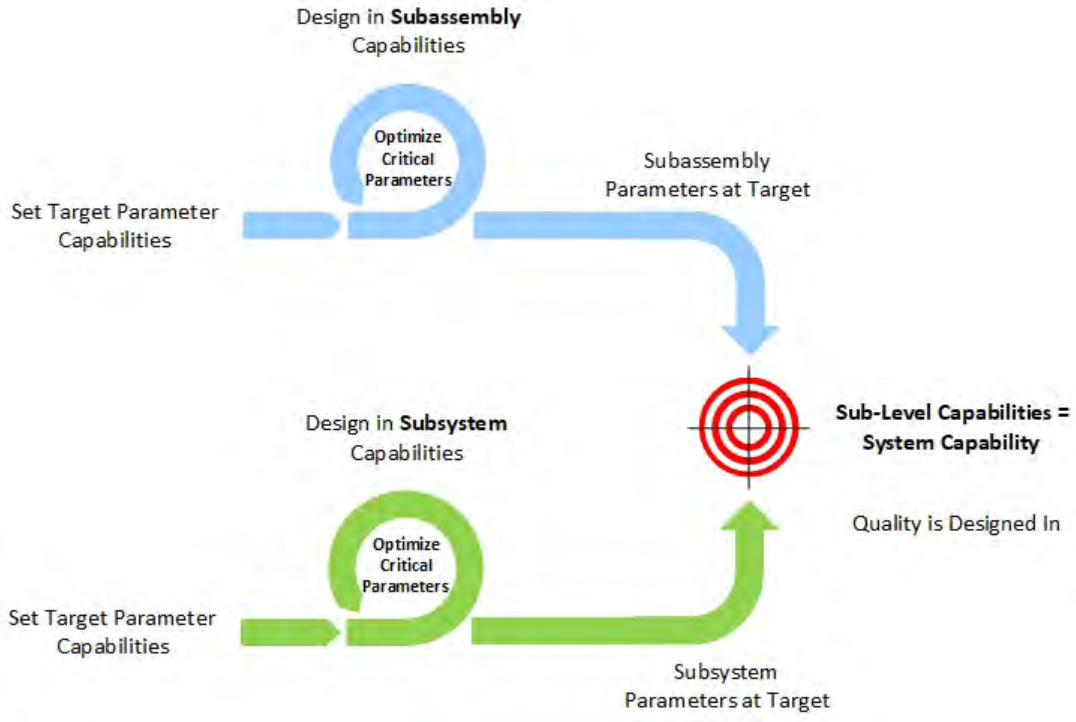


FIGURE 3

Design-outcome predictive framework model. (Graphic by David Booth, process adviser, supporting JPM CBRN Medical)

management, by iteratively updating the design's fault tree analysis with failure probabilities taken from critical parameter testing. The design engineers can quickly identify design weaknesses. In another innovative tactic, the government team is training manufacturer design teams in this new method and demonstrating real time product performance improvements.

The predictive model in Figure 3 shows how subassembly and subsystem critical parameter capabilities equal the capability of the system. Target sub-level parameter capabilities are determined at the start of the design in the design-outcome predictive framework, to ensure that product reliability and robustness meet user expectations. These parameters are optimized by revising the sublevel parameter levels to include the manufacturing process level. Sublevel parameters are easier and quicker to optimize. The effects of internal and external stresses can be traced throughout the design, as well as their effects on mitigated critical parameters. This results in a system that, when assembled, performs at the reached sublevel capability targets. Reliability targets are realized when capability targets are met.

To date, three AI designs have met their design input requirements, as well as met and surpassed the FDA's reliability requirements. Aktiv used the IPRDF to demonstrate FDA-compliant reliability in their scopolamine and 2-PAM AIs. Testing demonstrated that their product input requirements will be handily met. Emergent BioSolutions is developing an atropine and 2-PAM AI and a diazepam AI. This manufacturer's design and manufacturing processes have followed the same development strategy, attaining similar design success.

Each company's design teams were not trained in the DFSS framework when the four projects started. One company engaged a consultant for a week to train their design and leadership staff. The other company's team did not receive formal DFSS framework training; however, the acquisition team provided ongoing DFSS training for both companies and mentored their engineers in the IPRDF. Prior to starting these projects, the companies' design staffs relied exclusively on the BTF framework for their development strategies.

It took both teams about a year to become proficient in DFSS and the IPRDF. From that point, it took the companies between 1.3 and 1.5 years to reach their design and, particularly, their reliability goals. To date, the teams are not fully trained in IPRDF execution and have more to learn. However, they have adopted these value-adding strategies as part of their business models, and each team feels that without using the IPRDF, they would not have been able to achieve these levels of design success.

Conclusion

Design-outcome predictive frameworks and methods used for designing AI MCMs are demonstratively effective in producing reliable products, more so than reactive design methods. No MCM developed to date by acquisition teams using a BTF framework has been able to come close to the level of FDA-required reliability as achieved by the IPRDF. Even with partial implementation, the IPRDF demonstrates superiority in providing design visibility, resulting in opportunities to create a better, more reliable product.

Diazepam. (Photo by Denis Alias, principal engineer, Emergent BioSolutions Inc.)

Midazolam. (Photo by Addie Barel, QA manager, Shalon Chemical Industries Ltd.)

Category: Lessons Learned

WINNER

Fielding Military Health Status Wearables

By the following authors:

William J. Tharion

Swati Maeder

Maj. (Ret.) Robert Jones

Understanding the challenges, solutions and lessons learned for acquisition and fielding of a real-time wearable health status system for military users.

Throughout the summer of 2022, regardless of where we live in the U.S., we all experienced heat wave after heat wave and its uncomfortable effects. For first responders that answer the call to chemical, biological, radiological, nuclear and/or explosive (CBRNE) threats wearing full Level A hazardous material (HAZMAT) personal protective equipment (PPE), we can only imagine the life-threating impact hot environments have on them. Fortunately, just in time for this unprecedented summer heat, one group of first responders was fielded an early warning real-time physiological status monitoring (PSM) system to help mitigate heat strain through improved decision making and avoid the potentially deadly effects of the heat, as they serve to protect the American public. This PSM system fielding was the first of its kind for the Department of Defense (DOD) with a complicated set of actions and procedures to be followed. Having a talented integrated product team (IPT) and motivated customer leadership working together might seem like the ideal acquisition scenario, but we were traveling into uncharted territory. We hope our lessons learned will help others as they navigate their own unique acquisition challenges.

What are the Challenges and Operational Needs?

The National Guard Bureau (NGB) Weapons of Mass Destruction – Civil Support Team (WMD-CST) formally identified a need for real-time monitoring of health status. However, wearable systems for military decision making are more complex than typical retail wearable systems. The WMD-CSTs support civil authorities at domestic CBRNE incident sites and represent a critical emergency first responder capability for the nation. During their missions, the WMD-CST survey team members are at significant risk of heat injuries when they wear their PPE.

The WMD-CST Medical Working Group identified a capability gap to improve the safety of their downrange personnel through health status monitoring. Historically, downrange personnel monitor each other using the "buddy method," where individuals assess each other through verbal communication and by paying attention to any abnormalities in physical disposition (e.g., signs of ataxia, flushed or pale skin and mental disorientation). Challenges with the "buddy method" include three main issues. First, most personnel are highly motivated to do their jobs and do not readily admit to feeling ill or in need of a break. Second, PPE physically compromises team members' ability for assessing their partners (e.g., masks impose muffled speech and reduce visibility of facial changes and suits generally impair or restrict movement that can be visually observed as clumsiness). Lastly, onset of changes in health status can occur rapidly and unpredictably, making recognizing them when they occur very challenging. Figure 1 illustrates some of the types of vigorous training that personnel conduct in PPE.

The Joint Product Director (JPdD) Chemical Detection and Mobile Analytics (CDMA) CBRNE Rapid Acquisition Division (C-RAD) Aberdeen, Maryland, office, through direction from the Joint Program Manager Sensors (JPM Sensors) and the Joint Program Executive Office for Chemical, Biological, Radiological and Nuclear Defense (JPEO-CBRND) received this

FIGURE 1

TYPICAL WMD-CST TRAINING

The 47th WMD-CST in Mississippi practices man-down rescue during brief training periods (approximately 20 minutes) resulting in increased core temperatures. (Photos by William Tharion, U.S. Army Research Institute of Environmental Medicine (USARIEM))

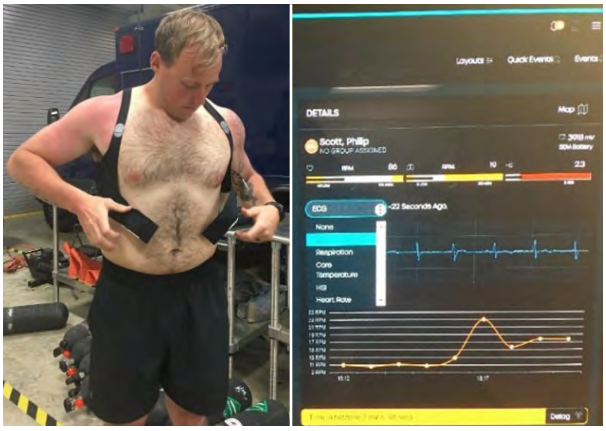


FIGURE 2

WEARABLE MONITORING SYSTEM THAT PROVIDES REAL-TIME PHYSIOLOGICAL DATA FOR MILITARY DECISION MAKING

A 47th WMD-CST (Mississippi) Soldier putting on the wearable monitoring system. A data dashboard provides real time information to support decision making.

capability gap from the NGB. The C-RAD team through their Commercial Off-the-Shelf Modernization (COTS-MOD) process and in close collaboration with the U.S. Army Research Institute of Environmental Medicine (USARIEM) in Natick, Massachusetts, provided solutions to this challenge.

FIGURE 3

DEMONSTRATION OF MONITORING SYSTEM

Robert Jones, Chemical Detectors and Mobile Analytics (CDMA) team, demonstrates the PSM system and explains its capability to 47th WMD-CST (Mississippi) health care provider, Maj. Richard Lachney.

A PSM system was determined to be the appropriate solution for addressing this operational gap (Figure 2). For this PSM solution to be acceptable for use, it needs to be valid, reliable and allow for rapid decision-making by health care providers (HCPs). Additionally, the system must pass human factors needs (e.g., acceptable to wear) and functionality assessments for the user group (in this case, communication requirements for moving data from downrange personnel to an HCP decision maker typically 1,000 meters or more away).

The C-RAD team procured and fielded a PSM system that provides the WMD-CSTs with assessments of heart rate, respiration rate, skin temperature, estimates of core body temperature, a heat stress index measure and alerts for a man down through body motion data. The team also worked to ensure that proper new equipment training (NET), system set-up and logistical support was provided to all 57 WMD-CSTs. The fielding process included setting up systems for the teams and providing a 2-day NET. This process began in April 2017 and was completed in May 2022 (Figure 3). The following are the lessons we learned throughout this process.

Lesson 1: It Takes a Village

There were no medical-grade PSM systems listed on the General Services Administration (GSA) Global Supply website; therefore, it took multiple organizations to

make this acquisition a reality (Figure 4). Because some PSM systems are commercially available, the COTS MOD process was leveraged to rapidly acquire a solution. The challenge then remained in putting together HCPs that could represent the WMD-CST community and matching them with subject matter experts (SMEs) who understand and can describe the technology tradespace to ensure the chosen system could be modified to meet the WMD-CST needs. To this end, JPdM CDMA and USARIEM organized their IPT with three key HCP representatives from WMD-CST, and a SME from Naval Air Systems Command (NAVAIR) to provide expertise in software systems and communications. Additionally, JPdM DCMA also brought expertise on the contracting and acquisition strategy.

Through this IPT, a set of PSM system requirements and product specifications were generated. Then, a candidate system was chosen, and independent testing was conducted by the Army Test and Evaluation Command (ATEC) in Aberdeen, Maryland. Once the system was tested and approved, an Acquisition Decision Memorandum (ADM) was formalized and approved by JPEO-CBRND for the procurement. Finally, a NET was developed by JPdDM CDMA CRAD in collaboration with SMEs from the product vendor and USARIEM.

Lesson 2: Process and Product Improvement are Continuous

In 2016, procurement funding was available to outfit 12 select teams, to be fielded in 2017. The planned budget did allow for the other 45 teams to have systems fielded beginning in 2019. This budgetary programming was fortuitous, as a number of valuable lessons learned came from the first 12 teams' experiences that would provide insights for better deploying PSM systems to the remaining 45 teams. Additional issues were identified using formal market research surveys and focus groups that enabled solutions for fielding to the last 45 teams. The initial 12 teams had product upgrades and a new enhanced NET resulting from this process. Some of the key technical areas worked on, including communications, Bluetooth requirements, customization of system alarms and refinement of training documents, are specifically outlined below.

Communications. Long-range communications for pushing data from downrange personnel used a legacy radio network that all teams already had in place. However, in some cases these systems were quite old and unreliable. By 2019, all teams had acquired the Persistent Systems LLC, in New York, MPU5 radio systems for other non-PSM related purposes. These MPU5 systems served as a more

FIGURE 4

THE ACQUISITION VILLAGE

This acquisition required subject matter expertise and cooperation from many organizations, systems and communications. (Illustration by Matt Bartlett, USARIEM)

reliable long-range communications platform, allowing the PSM system to be used as intended.

Relaxation of the no Bluetooth Requirement. During the 2017 fielding, DOD software security requirements prohibited use of Bluetooth technology. This posed a challenge, as part of the intended communications system relied on use of a cellphone carried by the user that obtained and processed data from the sensors prior to the long-range data transmission. The PSM system would typically communicate locally or in short ranges using Bluetooth. However, due to the prohibition of Bluetooth, which was lifted by 2019, the body-worn sensor system needed to be wired to the cellphone. Tethering of the phone created an additional technological step and some associated human factors challenges. Long-term, systems such as the one acquired by the WMD-CSTs could operate without Bluetooth because they have an open-architected communications structure and could use a tunable narrow-band radio or other types of systems. The COTS MOD process enabled rapid acquisition, making tethering the system to the phone an addressable short-term solution.

Individualization of Alarms. Initially, the system had standard settings that included an auditory alarm and a change in displayed color statuses triggered by high or low health state readings. For example, if an individual's heart rate dropped below 40 beats per minute (bpm) or above 180 bpm, an auditory alarm and a color change of the data on the system dashboard would be initiated. Feedback from the HCPs indicated there could be large individual differences among their team members and they wanted the ability to individualize these alarms by team member. This product capability was added by 2019.

Improved New Equipment Training (NET). A revised NET was adopted that provided more hands-on training with less PowerPoints and relied on a more practical "crawl, walk, run" approach. Following this, all team members attending the NET would learn about all aspects of the system. Initially in 2017, a team member would only learn about the part of the system they were using. Associated with improvements in the NET, trainers were now required to become certified by passing a written and practical test on the material they had been taught, signifying their readiness and ability to teach the NET. This more rigorous qualification of instructors also improved the transfer of knowledge.

There were many other smaller changes adopted from the feedback from the teams, but the above list highlights how important it is to seek continuous product and process improvement in response to customer needs. Continuous feedback is a key part of the acquisition process during the sustainment phase. Formal feedback from a diverse set of teams to understand their unique situations and challenges using the PSM system is still being obtained through product surveys and focus groups. Understanding the use cases though post-PSM system deployment surveillance monitoring should yield valuable information for future WMD-CSTs' use of PSM systems, but also help guide development and use of PSM technologies more broadly for the DOD.

Lesson 3: Flexibility is Important, Especially During the Period of COVID-19

The need to be flexible with the contract period of performance (PoP) was necessary during the COVID-19 pandemic. There were time periods when COVID-19 restrictions reduced or halted the ability for fielding and NET. Available resources supported only one fielding per week and scheduling became increasingly compact due to COVID-19 restrictions, and no-cost PoP modifications to the contract were required. Effectively implementing these modifications required good working relationships between the contracting officer and the vendors. Prompt, clear, and open communication between JPdD CDMA C-RAD leadership, the vendor and the contracting office ensured these actions took place.

Lesson 4: Continued Engagement with User Community During Sustainment Phase

Communication between teams and from the program management office and USARIEM helped improve user acceptance. For example, a new HCP from one of the teams not using the PSM system because of team turnover, was motivated by the PSM IPT to use the system. The HCP was put in contact with a WMD-CST team that was an advanced user of the system and was provided that team's standard operating procedure to allow the novice PSM use team to become operational with the PSM system.

Conclusion

Fielding of PSM systems to all 57 WMD-CSTs was a major undertaking. It was the first acquisition of its kind and required transfer of material and knowledge to a valued customer. There were a number of challenges presented that were overcome during this acquisition.

This paper illustrates the process and provides valuable lessons learned by our acquisition team. Success of this acquisition was based on lessons learned described here but these lessons likely apply to others as well.

For more information regarding wearables and the science behind various systems, you can contact William Tharion at william.j.tharion.civ@health.mil. For information on the use of the COTS MOD process for acquisition, especially in the CBRN arena, contact Swati Maeder at swati.maeder.civ@army.mil.

Disclaimer: *Citations of commercial organizations and trade names in this paper do not constitute an official Department of the Army endorsement or approval of the products or services of these organizations. The opinions or assertions contained herein are the private views of the authors and are not to be construed as official or as reflecting the views of the Army or the DOD.*

HONORABLE MENTION

Early Cyber Technical Assessment (Quantifying Cyber Metrics and Maturity Early in a Software Development Cycle)

By the following authors:

Angel Pomales-Crespo

Deryk Gannon

Christel Petrizzo

Introduction

Most Army software development today is performed using the Agile methodology of the development-operations-security (DevOpsSec) process, where cybersecurity is introduced at the end of the development process (or in Agile, at the hardening sprint, sprint H), usually only aligned with risk management framework (RMF). In addition, most software is not penetrated assessed until a "red team" is paid for (normally during formal test and evaluation events). This late cyber testing and the necessary late fixes has led to increases in costs, schedule and possibly non-secure applications in warfighter hands during deployment.

Product Manager (PdM) Tactical Cyber and Network Operations (TCNO) has changed our process to one which embraces building cybersecurity early in the system or application development (one could say a "DevSecOps" process). Software cybersecurity is not always seen by the user, and so it is not quantified or measured fully even at late stages of software development. The introduction of Early Cyber Technical Assessment (ECTA) provides programs the ability to start quantifying applications' cyber maturity early in the development process. ECTA provides meaningful cyber metrics and cyber maturity findings that track against penetration risk, vulnerabilities exposure, cyberattacks and potential system or mission performance degradation. Some of the key cyber metrics assessed are cybersecurity hardening of the software, implementation of least privileged access, protection level against cross scripting, ensuring reduced attack surface, access control mechanisms and validating software supply change integrity. Cyber metrics provided and evaluated by ECTA in applications' development enable program managers to discover and address negative findings (vulnerabilities, design flaws, lack of code quality, increased attack surface, reduced mission availability, etc.) and/or adjust the software application architecture early to correct those findings. Also, ECTA enables applications' cyber architecture to keep pace with attack surface and mitigate threat vectors. In essence, programs leveraging ECTA's methodology within a DevOpsSec process ensure applications are delivered within cost, performance and schedule, while also delivering a cyber-hardened product to function correctly in today's cyber challenged world.

1. The ECTA Process

As depicted in Figure 1, Step 1, ECTA starts with the earliest version of software, even beta or < v1.0 software.

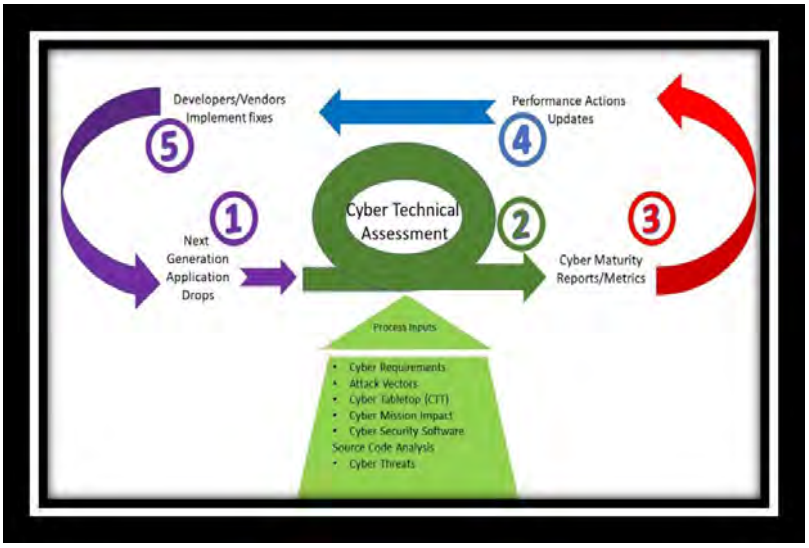


FIGURE 1

Early Cyber Technical Assessment (ECTA) maturity process. (Images created by the authors)

ECTA enables baselining software cybersecurity maturity and provides program cyber metrics. This also allows risk reduction on software performance (minimizing cyber impacts on warfighter's missions), and avoids cost increases and schedule overruns. ECTA can be adopted anywhere within a software life cycle by providing key cyber metrics and increase cybersecurity. However, organizations adopting ECTA later, may be limited in their ability to adjust the software architecture agilely.

As depicted in Figure 1, Step 2 is the Cyber Technical Assessment (CTA). This is conducted at a cyber range with a Cyber Security Evaluation Team (CSET). CSET conducts a white-box cyber assessment offering the ability to collaborate in the assessment with application subject matter experts (SMEs), software developers and users to plan, design and execute the cyber assessment. The CSET offers the ability to provide new and unseen prospective of attack surface of an application's software. This assessment enables CSET access to user manuals, and applications' software design documents to properly design and execute the cyber assessment. The CTA activities include:

- Validating fixes and mitigations from previous cyber assessment.
- Assessing applications' software cybersecurity assurance, security architecture and implementations of cybersecurity best business practices.
- Measuring the applications' implementation of data confidentiality and integrity regarding current DOD cybersecurity doctrine.
- Assessing the applications' cybersecurity risk while performance mission functions.
- Identifying the applications' cybersecurity weak and stress points, to provide cyber metric to monitoring during development.
- Risk reduction for user operational tests that also include cyber assessments.

The CSET reviews program cybersecurity documentation as a method to determine proposed attack surface, which is essential input to CTA and collaborative cybersecurity assessment. Examples of inputs include:

- Cyber Requirements – Applications' cybersecurity requirements.
- Attack Vectors – Similar application known exploits.

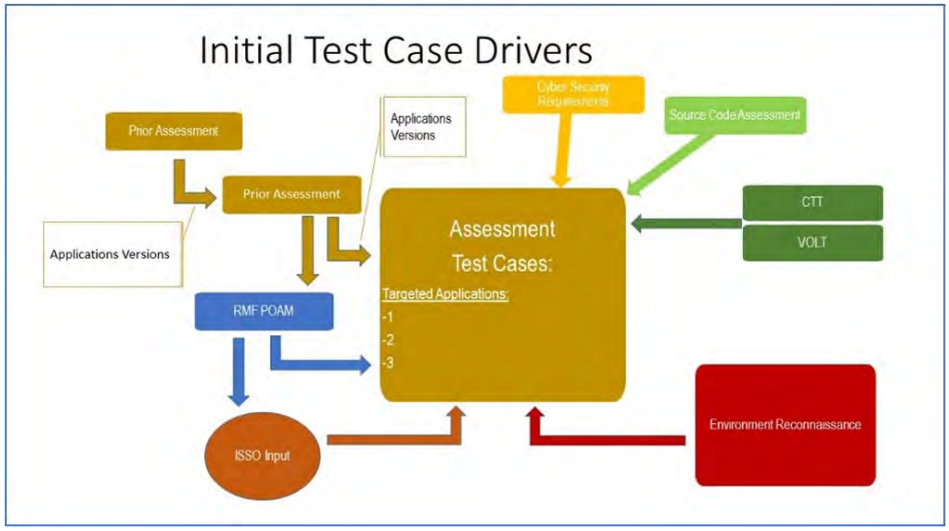


FIGURE 2

Cyber Assessment – test case development.

- Cyber Tabletop (CTT) – Document threats to function and mission impact.
- Cyber Mission and Criticality Impact – User community defined availability statement of applications.
- Cybersecurity Software Source Code Analysis – Detailed source code review for weakness, issues, old libraries calls and supply chain.
- Vulnerability On-Line Threat – Generated by intelligence community.

Review of CTA inputs and baseline applications' documentation, CSET develops test cases around the cyber metrics already described, as depicted in Figure 2, to evaluate the applications against the documented proposed attack surface. The last activity the CSET conducts is an environment reconnaissance to develop test cases that the CSET captures during their initial hands-on review of the software applications.

After the test cases are set, the CSET begins evaluating the applications, and develops and executes the "exploit" of the application per the test cases. The CSET attempts exploits throughout the assessment. During the assessment, the SMEs will assist the CSET to evaluate impact. The SME also assists the CSET in adjusting exploits, using their knowledge of the application. The team documents their findings throughout the assessment, captures how the exploit worked or not, and the application's behavior during the test.

At the conclusion of the assessment, the CSET performs a final close-out of their documentation by fully capturing exploits, findings and artifact data. This is recorded for any future re-execution of the findings, either by another assessment or to correct the vulnerabilities via enhanced software development. The CSET also provides demonstrations to SMEs, allowing for collaboration in near real time, to develop recommendations and mitigations. Finally, the CSET captures all validated fixes from previous assessments to ensure the assessment report closes those weaknesses out.

As depicted in Figure 1, Step 3, the CTA produces an output of a report with findings of the assessment. The report details the CSET's recommendations of technical fixes required or user procedure updates. The report also includes the steps and screen captures that the CSET executed to record the findings. Keynote in the report is capturing verified fixes that were implemented and documenting previously found cyber vulnerabilities that are no longer present.

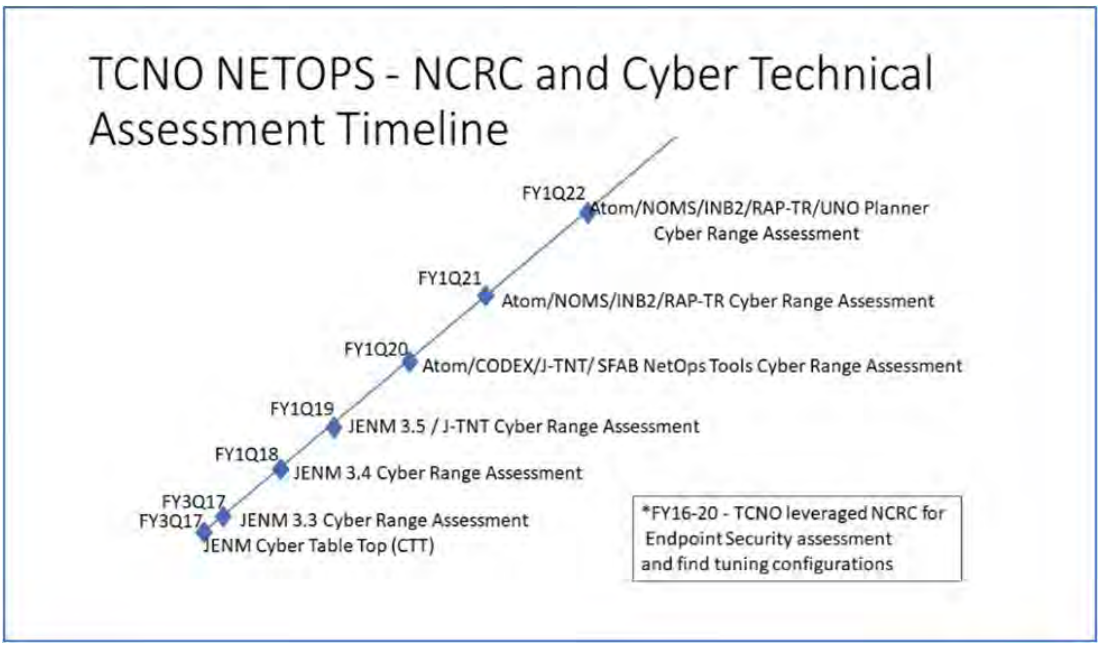


FIGURE 3

TCNO annual cyber technical assessment timeline.

As depicted in Figure 1, Step 4, a working group (WG) is established of program managers and cyber engineers to review the CTA report and bin actions. The binning of actions refers to how the program plans to address the cyber findings. Typically, applications' cyber weaknesses are binned into technical fixes for developers and vendors, where these organizations have to change security architecture (i.e., adoption of zero-trust models and least privileges), integrate security protection mechanisms (i.e., integration of encryption, firewalls and public key infrastructure), adjust configurations (i.e., hash and signing source code), or rewrite software. Other binning actions include updating training, manuals or procedures, addressing user hygiene (i.e., password), implementation of security patches, implementation of configuration management and supply chain management processes, developer security training and control processes, implementing security into Agile software sprint development process, and/or the updating or clarifying of applications' cybersecurity requirements. The WG also derives cyber maturity and metrics from the assessment report. These metrics are overlaid onto applications' performance attributes to drive cyber weakness priorities for fixing, thereby informing a program's cost, schedules and the contracting process to enable these fixes by the vendors when required.

As depicted in Figure 1, Step 5, the final step is for the developers, vendors, system engineers, logicians and technical manual writers to address the assigned actions to perform and implement fixes and mitigations. The developers review the details of the cyber assessment report and provide technical assessment impacts to resolve the vulnerabilities. As fixes are implemented, the applications are prepared for the next iteration of the CTA. The timeframe between CTA is usually six months to one year.

2. The PdM TCNO Experience

PdM TCNO conducts annual ETCA of the Unified Network Operations (UNO) prototypes and product lines, as part of its rapid development and acquisition process. These ECTAs validate cybersecurity and provide improvement recommendations to securely operate in cyber-contested domains ahead of product delivery. Every year, TCNO integrates its current year prototypes and developments into cyber ranges located at the institutionally funded DOD National Cyber Range (NCR). Figure 3 depicts TCNO's annual assessment during

rapid prototype and agile development. The NCR and CSET assess these TCNO applications (ATOM, NOMS, UNO Planner, etc.) against cybersecurity/attack surfaces to measure and document cyber threat impacts and to advance the applications' cybersecurity and hardening.

PdM TCNO's cybersecurity strategy embeds annual cybersecurity assessments of the UNO Middle Tier of Acquisition prototypes and other PdM product line systems. A key part of this cybersecurity assessment is to address potential vulnerabilities and identify mitigation steps, including software improvements and additional vendor software requirements. NCR cyber engineers and CSET, working alongside the PdM TCNO cybersecurity team, leveraged a cyber tabletop methodology, which simulates incident scenarios with hands-on participation, to identify cyber threat vectors that could potentially render TCNO products vulnerable to cyber-attacks at the application level. These identified threat vectors are translated into test cases for the next cyber technical assessment.

Finally, TCNO has been taking these ETCA findings back to vendors for necessary corrections. As a result of TCNO's adoption of annual ECTA methodology during rapid development, TCNO's prototypes/applications/system have performed well in cyber "red team" assessments during operational tests with minor or no findings and are deemed "cyber security survivable" by the test community.

3. Summary

The Early Cyber Technical Assessment (ECTA) provides a great capability and opportunity to identify cyber and information assurance vulnerabilities very early in an applications' life cycle, while helping to support program goals for secured performance, communications and data integrity. This process enables PdM TCNO to establish cyber metrics throughout a system life and address the cyber risks through these cyber metrics. The aim of ECTA within a DevOpsSec environment is delivering continuous cybersecurity improvements by verifying how sound is software security and identifying and implementing fixes for vulnerabilities before the next software delivery. TCNO's lessons learned by moving to the ECTA process will benefit other product managers (PMs). By addressing cyber findings early into program development and building cybersecurity at its earliest point, ECTA enables PMs to minimize risk on software performance while avoiding both the increased cost for software fixes at the last minute, and schedule overruns which would normally come at the tail end of development. Certainly, the ECTA approach is one that is sound from a cybersecurity, technical and economic point of view to the benefit of the PM, the acquisition community and the software capability provided to the U.S. Soldier.