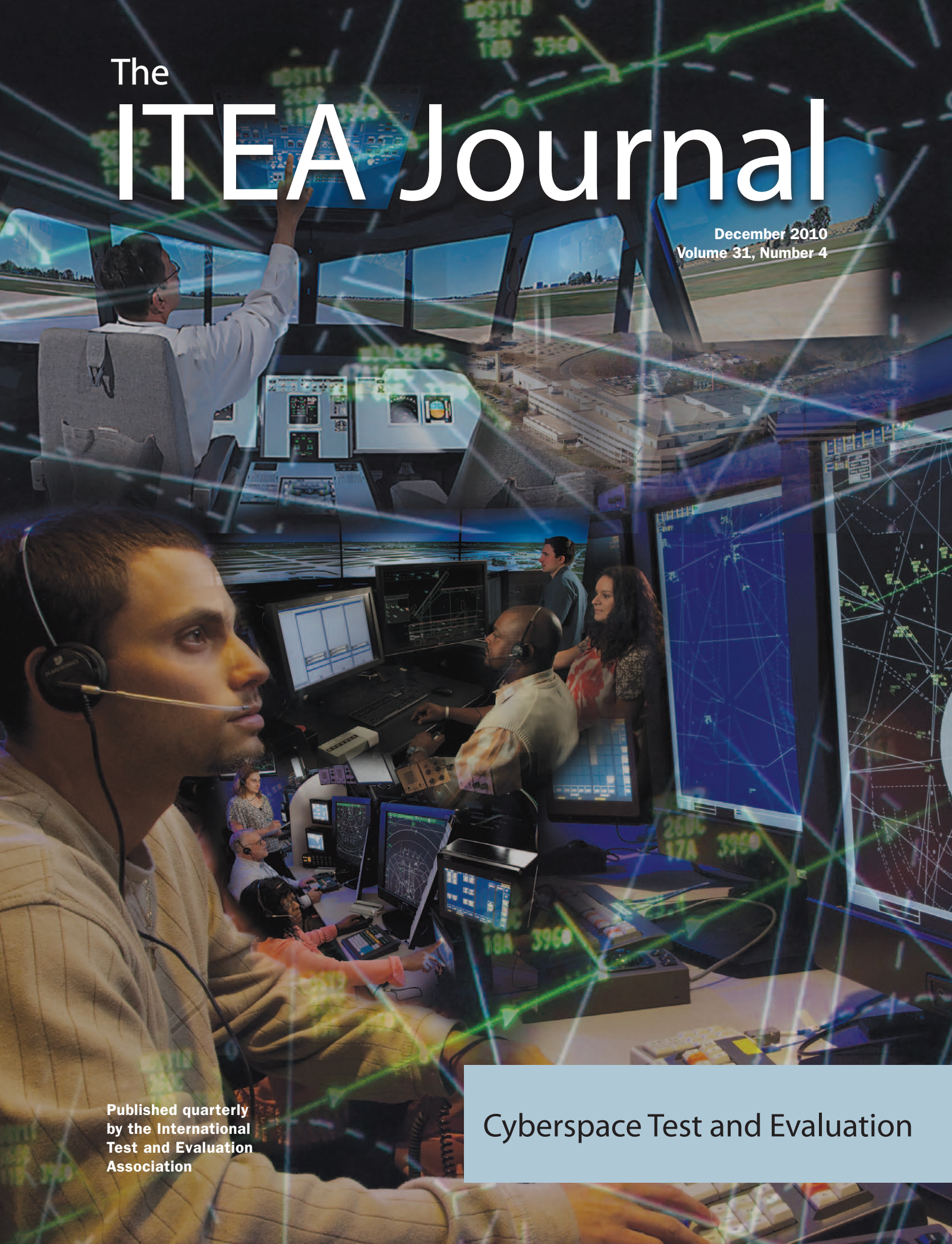
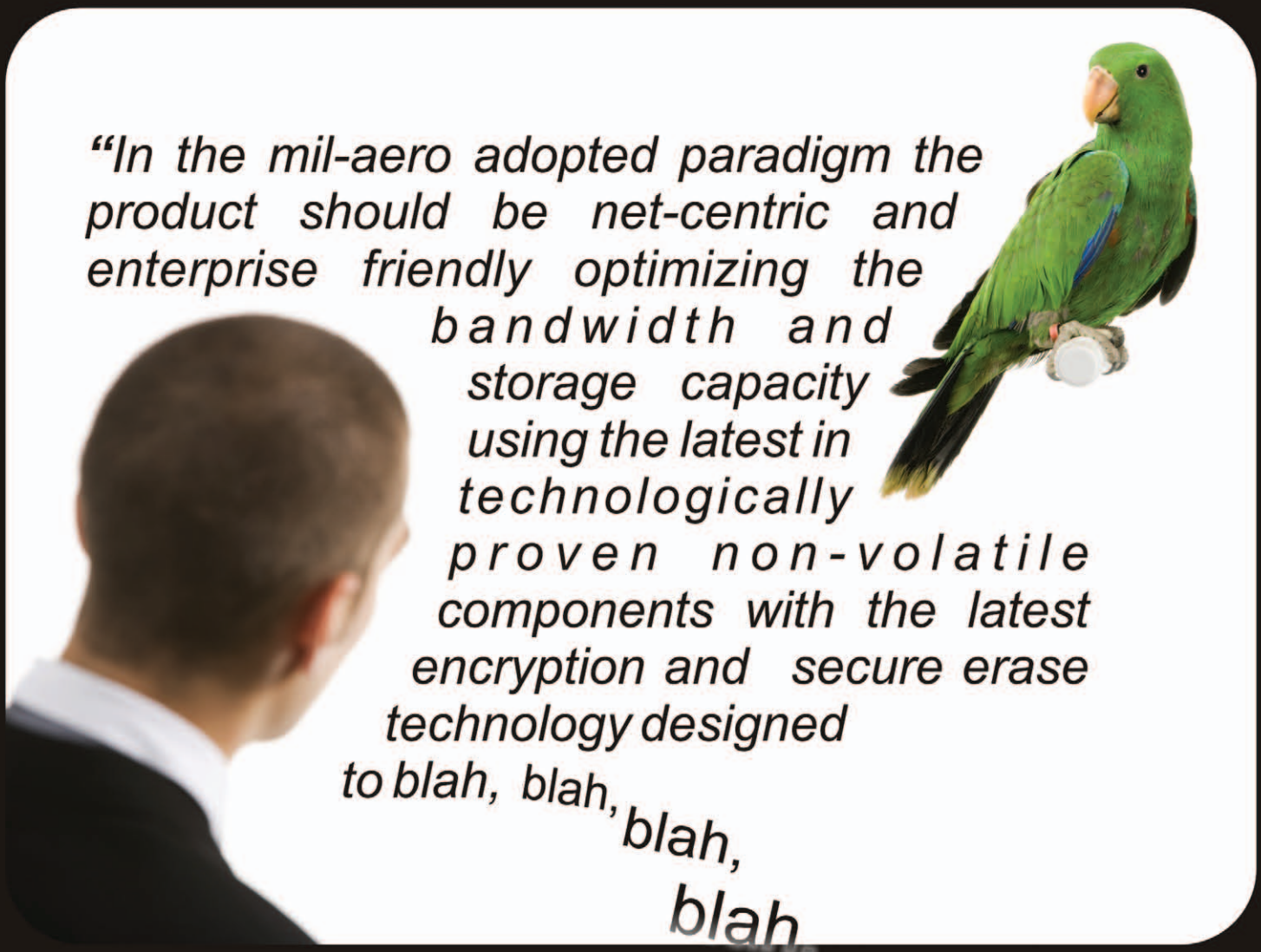


The ITEA Journal

December 2010
Volume 31, Number 4

Published quarterly by the International Test and Evaluation Association

Cyberspace Test and Evaluation



Want a rugged, proven recorder? Turn off the *hot air* and give us a call.

CALCULEX®

132 W. Las Cruces Avenue
Las Cruces, NM 88001
575-525-0131

IRIG 106 Chapter 10 Co-Authors

TAKE YOUR CAREER TO NEW HEIGHTS

CSC

Find out just how far your talent and innovation can take you. We are a global leader because we keep the best on board. That's why CSC rewards your talent with the resources, professional training and diverse opportunities to grow your career.

The results: Freedom to chart your career path. Exceptional mobility. And the chance to learn from the expertise of thousands of talented colleagues worldwide.

We are currently recruiting for immediate openings at U.S. Naval Air Station Patuxent River:

- Software Engineers
- Electrical Engineers
- Field Engineers

For more information on
CSC Applied Technology Group career opportunities contact:
Joe Anderson • 301-737-5708 • jandersoniii@csc.com

www.csc.com/atg

EOE, M/F/D/V

Testing technology in a global environment

Testing in a global environment is a job that our test and evaluation employees take on every day. We bring outstanding technical skills to the toughest problems facing our customers.

Smart people solving hard problems.

www.saic.com

Energy | Environment | National Security | Health | Critical Infrastructure

SAIC®
From Science to Solutions

NYSE:SAI

CONTENTS

The ITEA Journal
December 2010
Volume 31, Number 4

TECHNICAL ARTICLES

DEPARTMENTS

ON THE COVER: The Federal Aviation Administration is in the process of planning and implementing the Next Generation Air Transportation System (NextGen). The goal of NextGen is to efficiently address the current and future challenges facing the U.S. air transportation system. The verification and validation (V&V) of NextGen will require an environment and infrastructure for testing, modeling, and simulating throughout the development and implementation of NextGen capabilities not previously used by the Federal Aviation Administration (FAA). The article, Verification and Validation Capabilities for the Next Generation Air Transportation System, contained in this issue discusses the initiatives that the FAA is undertaking to establish new V&V capabilities and environments for NextGen. Depicted on the cover is the NextGen Integration and Evaluation Capability (NIEC), located at FAA William J. Hughes Technical Center in Atlantic City, NJ. This is one of the FAA's first steps towards the required V&V capability for NextGen. The NIEC leverages existing laboratory and simulation capabilities that are used to develop, test, and maintain the National Airspace System. It is comprised of existing National Airspace System operational systems and high fidelity, real-time simulation capabilities to create an integrated, flexible, and reconfigurable environment to support NextGen research as well as test and evaluation. (Cover graphic courtesy of the Federal Aviation Administration.)

■ ITEA Headquarters: 4400 Fair Lakes Court, Suite 104, Fairfax, Virginia 22033-3899; Tel: (703) 631-6220; Fax: (703) 631-6221, E-mail: *itea@itea.org;* Web site: *http://www.itea.org.*
■ ITEA is a not-for-profit international association founded in 1980 to further the development and exchange of technical information in the field of test and evaluation.
■ *The ITEA Journal* (ISSN 1054-0229) is published quarterly by the International Test and Evaluation Association at 4400 Lakes Court, Suite 104, Fairfax, Virginia 22033-3899. Single issue cover price for *The ITEA Journal* is $20. ITEA membership dues are $50 for individuals, $25 for full-time students, and $800 for corporations. Annual dues include a one-year subscription to *The ITEA Journal*. The annual subscription rate for libraries and other organizations providing timely reference material to groups is $60. All overseas mail (air mail or AOA) requires an additional $20. *The ITEA Journal* serves its readers as a forum for the presentation and discussion of issues related to test and evaluation. All articles reflect the individual views of the authors and not official points of view adopted by ITEA or the organizations with which the authors are affiliated.

POSTMASTER: Send address changes to: ITEA, 4400 Fair Lakes Court, Suite 104, Fairfax, Virginia 22033-3899.

President's Corner

ITEA Journal 2010; 31: 437

I am truly honored to be elected by the ITEA Board of Directors to serve as the Association's President. ITEA has played a significant role throughout my career, both professionally and personally. As President, I plan to focus on ensuring that the Association continues to positively impact the careers of other test and evaluation (T&E) professionals. We celebrated ITEA's 30th anniversary this year. Throughout its tenure, the Association has continually provided relevant connections that T&E professionals need to learn, share, and advance themselves, their organization, and the profession. Those needs are moving targets, however, evolving with the advancement of new technologies and the implementation of new policies. As I listened to the speakers at our recent Annual Symposium, it was obvious that there are a multitude of transformations currently affecting T&E requirements and, in turn, the requirements for ensuring a workforce that can adapt to the resultant changes. Just to name a few, some of the recurring themes that I heard included: recent T&E and acquisition policy changes; mission-based T&E; T&E for agile information technologies; information assurance; data fusion, design of experiments; integrated developmental and operational testing; integrated T&E and systems engineering; rapid acquisition and fielding; testing in an urban environment; effectively involving the tester earlier in the acquisition cycle; and the very timely topic of this *Journal* issue, *Cyberspace Test and Evaluation.* Is our workforce postured to meet these emerging challenges?

Stephanie H. Clewer

As a not-for-profit educational association, I feel it is ITEA's duty to provide relevant, timely, quality educational opportunities for T&E professionals that are aligned with the evolving changes and technological advancements. Our Education Committee is currently compiling potential course topics, as well as researching other avenues (e.g., webinars, online forums) for equipping the current and future T&E workforce with the skills and training required to face the emerging challenges. ITEA is primarily a volunteer organization. I am appealing to each of you to consider supporting the Education Committee in its endeavors through volunteering your time and talents or by providing any comments or suggestions for future educational offerings. ITEA's way forward is an aggressive one and success will be solely reliant on the hard work and determination of our volunteers. I urge anyone interested in assisting in this process to contact me personally at president@itea.org. Change is never easy, but the T&E community needs to adapt to the evolving initiatives; the only way to ensure relevancy of our educational offerings is by sharing best practices and ideas through the close collaboration of our most important resources–our members. Thank you in advance for your support of this important effort!

The 2010 ITEA Annual Symposium was an overwhelming success. On behalf of the Board of Directors, I would like to thank the committee and ITEA Staff for a job well done, especially the contributions of our new Valley of the Sun Chapter. The 2011 Planning Committee is off and running on innovative plans for next year's symposium with a theme centered on "Fostering Partnerships in T&E and Acquisition." Be sure to watch the ITEA website for opportunities to support this important event in Orlando, Florida on 12–15 September.

I would like to personally thank the outgoing ITEA President, **Rusty Roberts**, for his leadership in 2010 as well as **Scott Foisy**, **Tom Macdonald**, **George Rumford**, **Minh Vuong**, and **Rick Shelley**, who recently completed their terms of service in support of the Association. I am pleased to welcome the following newly elected and appointed members to the Board: **George Ryan** (for a 2nd Term), **Mike McFalls**, **Chas McKee**, **Stu Burley**, **Bill Keegan**, **Ted McFarland**, **Keith Sutton** and **Gene Hudgins**. Serving with me on the Executive Committee are **Mark Brown** (Vice President), Mike McFalls (Treasurer), and Chas McKee (Secretary). We have an exciting year ahead of us and I thank all of you for your dedication to the vision and mission of ITEA.

As 2010 comes to a close, the ITEA Events Committee is gearing up for a new year of conferences, workshops, and forums reflecting the current T&E hot topics. I hope to see all of you soon at an upcoming event, starting with the *Live-Virtual-Constructive Conference* hosted by the White Sands Chapter on 24–27 January 2011 in El Paso, Texas.

Issue at a Glance

ITEA Journal 2010; 31: 438

Cyberspace Test and Evaluation. Cyberspace is the fifth combat domain, beyond air, land, sea, and space and is the realm of computers, networks, and software. The terrain of cyberspace is virtual not physical and ever in flux as network topology and system connectivity dynamically change. Cyberspace encompasses government and commercial networks, the communications industry, power distribution, commerce, transportation, and nearly everything that touches our lives and business today. This issue looks at the requirements and challenges imposed on test and evaluation (T&E) by cyber systems and cyber threats.

Brigadier General Brett T. Williams, Director of Communications Systems (J6) at Headquarters, US Pacific Command, presents in the *Guest Editorial* the discussion and debate within Department of Defense senior leadership over the best way to Command and Control cyberspace operations. The Honorable Mr. Edward R. Greer, Director of Developmental Test and Evaluation, contributes his view from *Inside the Beltway* of integrated T&E as the golden key to successful defense development and acquisition. Dr. Steven Hutchison, T&E Executive for the Defense Information Systems Agency, provides an *Invited Article* to explain Section 804 of the fiscal year 2010 National Defense Authorization Act and attendant mandate for agile information technologies. In *Tech-Notes* Timothy Holmes describes the host-based security system as a capability to protect, detect, diagnose and react to cyber threats. Dr. James Welshans, new chair of the ITEA History Committee, interviews a seasoned cyber T&E front line practitioner for *Historical Perspectives*. John Frederick *et al.* outline initiatives that the Federal Aviation Administration is undertaking to establish new verification and validation capabilities and environments for NextGen in their *Featured Capability* article.

The contributed articles begin with recommendations, presented by Pete Christensen *et al.,* from the information assurance policy T&E working group. The working group was established to review Department of Defense policy and guidance that drives T&E requirements for information assurance in acquisition programs. Robert Powell *et al.* illustrate the Information Assurance Range as a systematic, repeatable, and verifiable cyber T&E framework for measuring the abilities and capabilities to protect, monitor, detect, analyze, diagnose, and respond to cyber-security attacks. Chris Watson describes the new Defense Information Systems Agency test, evaluation and certification (TE&C) organizational structure and its goals to provide responsive, mission-focused services and agile testing. Danielle Koester *et al.* revisit the net ready key performance parameter as a measurable and testable evaluation framework for joint interoperability TE&C.

Norman Johnsons discusses six mission-readiness considerations for cyber warfare systems that form a set of basic T&E requirements for informing a mission-readiness or fielding decision. Tim Owen *et al.* explain how the Defense Research and Engineering Network Cyber Security Test Bed will provide a novel environment for testing new cyber security methods. Professor Richard Brooks carefully explores computer security and concludes that test and verification may be more challenging than designing and implementing secure systems. Dr. Anthony LeClerc and Michelle Crosby use open-source modeling and simulation tools for T&E of WiMAX performance on quality of service-constrained tactical edge traffic. Finally, Dr. Charlie Holman and Dr. Andrew Loerch conclude the issue with a procedure useful in predicting biological and chemical warfare agent detector performance against agent in the operational environment.

Guest Editorial

ITEA Journal 2010; 31: 439–441

The Imperative for Shaping Cyberspace

Brig Gen Brett T. Williams

HQ USPACOM, Director Communications System (J6), Camp H.M. Smith, Hawaii

The hot topic in the Department of Defense (DoD) today seems to be cyber, cyber, and more cyber. At the most senior levels, there is significant discussion and debate on the best way to Command and Control (C2) cyberspace operations. Given our reliance on cyber for executing C2 of military operations, this attention is well justified. Unfortunately, our efforts are not always well focused or synchronized, and despite the expenditure of significant resources, we do not yet have a comprehensive plan that addresses our biggest challenges in the cyber domain.

Brig Gen Brett T. Williams

The military imperative for gaining C2 of cyberspace operations comes from the Joint Force Commander's (JFC) requirement to execute C2 of C2. The term "C2 of C2" was coined by Admiral Robert Willard to describe the operational necessity of having Command and Control of the Command and Control architecture. The Admiral's argument is that C2 is what a commander does—it is his contribution to winning the fight. In order to execute his C2 mission, the commander must have a firm understanding of the technology he relies on to make decisions, direct operations, and manage risk. Although not all of the C2 architecture falls within the cyber domain, today's network-centric JFC relies heavily on cyberspace; therefore C2 of cyberspace operations is critical to his ability to execute C2 of C2.

Each Combatant Commander (COCOM) has a position on the best way to execute C2 of cyberspace operations within his area of responsibility (AOR). At the same time, the activation of U.S. Cyber Command (CYBERCOM) has created the impetus to clearly define our doctrine and policy for cyberspace across the DoD enterprise. Defining the proper supported–supporting relationships between the COCOMs and CYBERCOM, Defense Information Systems Agency (DISA), National Security Agency (NSA), and the Services is essential for determining how we are going to execute cyberspace operations in support of mission objectives. Unfortunately, we find that our C2 options are limited by the architecture that defines cyberspace. Cyberspace is a disparate collection of networks, systems, and software that nobody completely understands. It was never designed for military C2, yet we rely on cyberspace to execute the full spectrum of operations from humanitarian relief to warfighting. The Global Information Grid (GIG) as currently constructed severely limits our C2 choices, is too difficult to operate and defend, and costs more than it should. We built cyberspace. We can and should change it.

The professionals of the test and evaluation (T&E) community are well aware of the mad rush to gain complete awareness and control of cyberspace. There are numerous funded and proposed projects focused on cyberspace operations, yet we seem to be missing a roadmap to tell us where we are going. In other words, from a DoD perspective, what should cyberspace look like in the future if we are going to rely on it for national security?

GIG 2.0 is the most recent roadmap. It was introduced in 2008 with the intent of providing the warfighter with an "information advantage." GIG 2.0 focused on five areas: (a) global authentication, access control, and directory services; (b) information and services "from the edge"; (c) joint infrastructure; (d) common policies and standards; and (e) unity of command. GIG 2.0 provided useful motivation for improving our ability to operate in cyberspace, but it did not address the key challenge we face: "It's all one big GIG, so a risk assumed by one is a risk assumed by all." The lack of boundaries in cyberspace means that when the JFC directs operations in cyber, he must always consider the impact on the rest of the GIG. This is a different dynamic than exists in the physical domains, and it drives us to C2 relationships and operational decision making centralized at the DoD level. Additionally, the "one big GIG" factor makes computer network defense (CND) and network operations (NetOps) more difficult, leading some to

focus disproportionately on offensive cyber activities. It is time to update our roadmap and lay out a plan to purposefully shape cyberspace. It is time for GIG 3.0.

The proposed GIG 3.0 capitalizes on existing virtualization techniques to create a cyber Joint Operating Area (JOA) that allows the JFC to execute C2 of cyberspace operations in the same way he executes air, land, maritime, and space operations. GIG 3.0 is a deliberate and proactive game plan to shape cyberspace into a defendable, robust, agile, and secure environment that guarantees friendly freedom of action and denies the same to the enemy.

The basis for GIG 3.0 is a new network environment based on current Multi-Protocol Label Switching (MPLS) technology. This new network environment would be established within the current Defense Information System Network (DISN) and provide the network layer for cyber JOAs—a concept we have defined as the operational network domain. Operational network domains would be created using a set of controlled interfaces to define and separate, from the rest of the GIG, the cyberspace assets and infrastructure that directly support a given operational mission. The controlled interfaces would manage and contain risk in support of the JFC's intent without passing that risk on to the rest of the GIG. At the same time, CYBERCOM and the Services, via the same controlled interfaces, would administer their GIG-wide responsibilities within the JFC's operational cyber domain. An operational network domain would allow the JFC to direct operations and assume risk in his "cyber JOA" just as he does in his geographic JOA. Operational network domains would be flexible, adaptive, easy to establish, and could be controlled via a wide variety of doctrinal C2 constructs.

Within and across the operational network domains, virtual secure enclaves (VSE) would be created using existing commercial off-the-shelf technology (COTS) that has been certified for protecting classified information. These COTS systems use Internet Protocol Security (IPSec) encryption techniques that simplify information sharing with coalition partners and reduce the cost and complexity associated with controlling classified infrastructure. The enclaving strategy also allows us to define key terrain and avenues of approach in cyber, so we can precisely focus our sensors and intrusion analysis to significantly improve our capability for CND and NetOps. Like the operational network domains, VSEs would be extremely agile and would require minimal time to establish. In addition, we would be able to quickly shift services between VSEs to mitigate the effects of physical or logical failures and to enable advanced computer network operations. Finally, the VSEs would employ dynamic electronic keying techniques to facilitate rapid, secure changes to the community of authorized users.

The final component of GIG 3.0 is the Multi-Enclave Client (MEC). The MEC is a work station that allows the user to access multiple VSEs. Currently, most users who require access to several different networks require multiple workstations. The IPSec VSE environment provides the opportunity to employ already approved MEC solutions to access both classified and unclassified networks from a single computer. MEC workstations offer a streamlined method to access information. They reduce costs because there are fewer machines and less supporting infrastructure. And, they offer the potential to reduce overhead because there is less equipment to deploy, and the power requirements are reduced.

Creating enclaved cyber JOAs and accessing them using efficient multi-enclave workstations is only part of the GIG 3.0 roadmap. All of this technology is wasted if we do not develop appropriate tactics, techniques, and procedures (TTP) to take advantage of the technology and the T&E community has a key role in the process. Joint TTP are necessary for operations in every domain, especially cyber. Established TTP allow the commander to issue orders with confidence knowing that the forces assigned to him will execute their mission in a predictable fashion. As with the earlier discussion on C2 options for cyber, it is important that we do not allow the current architecture to restrict our TTP development for cyberspace. There is a synergistic relationship that must exist between technology development and the maturation of cyber TTP. The T&E community should help ensure that there is close integration between the technical experts and the operational community as we develop GIG 3.0. The fact is that the officials in DoD who have the most impact on cyber policy and resources do not typically have the background to advocate for specific technologies. At the same time, the technical experts, who do their best to meet operational requirements, do not always understand the relationship between the technology and the mission. Our test directors have a responsibility to help ensure that these two communities are closely coordinated and aligned as we develop the cyberspace of the future.

Doctrine, policy, C2 relationships, and TTP for cyberspace operations are just as important as they are for operations in the physical domains, but cyberspace is different. It is a domain that comprises live, virtual, and constructive assets that provide real capabilities. We do not completely understand the nondeterministic nature of the cyber domain, but we know we must, and, as a result, we are frantically searching for

ways to execute cyber operations just as we do operations in any other domain. We would like to get to the point where we do not need a separate construct for cyberspace, but for now our perception of the domain and the design of the architecture are forcing us to treat cyber as a special case. We have an urgent imperative to shape cyberspace in a way that we have never done before. The T&E community has a key role in guiding our many disparate efforts, so that in the end the cyber domain meets the requirements of the JFC. ❑

Brig Gen Brett T. Williams is the Director, Command, Control, Communications and Computer Systems, U.S. Pacific Command, Camp H.M. Smith, Hawaii. He is responsible for the communications system across the largest regional combatant command enabling joint and coalition operations. He provides senior leadership and management of Pacific and global communications resources to support the headquarters and the forces of four component commands, four sub-unified commands and all joint task forces.

General Williams was commissioned in 1981 as a distinguished graduate of the ROTC program at Duke University. He is a graduate of Euro-NATO Joint Jet Pilot training and the U.S. Air Force (USAF) Fighter Weapons Instructor Course. He has commanded a fighter squadron, combat operations group, and two combat wings. The general was the Air Combat Command Inspector General, a plans officer at U.S. Central Command, and Chief of Checkmate Division on the Air Staff at the Pentagon. Prior to his current assignment, he was the Commander, 18th Wing, Kadena Air Base, Japan.

General Williams is a command pilot with more than 3,600 hours in the F-15C and more than 100 combat missions in operations Desert Shield, Desert Storm, Southern Watch, Northern Watch, and Iraqi Freedom. He was promoted to Brigadier General in October 2007. He earned a bachelor of science degree in computer science from Duke University, Durham, North Carolina, in 1981 and a master of arts degree in management from Webster University in 1988. In addition, he completed the USAF Fighter Weapons Instructor Course, Nellis Air Force Base (AFB), Nevada, in 1989; and attended the Air Command and Staff College in 1993 and the School of Advanced Airpower Studies in 1994 at Maxwell AFB, Alabama. In 2002, General Williams completed the Advanced Strategic Arts Program at the U.S. Army War College, Carlisle Barracks, North Carolina.

General Williams is currently the Director, Command, Control, Communications and Computer Systems (J6), U.S. Pacific Command, Camp H.M. Smith, Hawaii. E-mail: brett.t.williams@pacom.mil

ITEA Journal 2010; 31: 443–446

The Integrated T&E Continuum, the Key to Acquisition Success

Edward R. Greer
Director, Developmental Test and Evaluation, USD(AT&L)

The words "integrated" and "integration" have appeared for many years in their association with defense acquisition. Although integration has been discussed and written about extensively, making it happen has not been successful in such a non-integrated environment of multiple Services and agencies, multiple contractors, multiple responsible test organizations, and multiple customers. In 1983, Congress looked towards test and evaluation (T&E) officials to take a giant step toward integration in defense acquisition by incorporating responsibility for operational T&E with designated Service and agency Operational Test Agencies (OTAs), and the creation of the Director of Operational Test and Evaluation (DOT&E). This move created an integrated chain of testing, evaluating, and reporting at the completion of major defense acquisition programs (MDAPS) to the two customers of defense acquisition: 1) the warfighter who uses the equipment, and 2) Congress, representing the U.S. taxpayer who pays for the equipment. While this integration of responsibility and authority for operational T&E (OT&E) has been very effective, a drawback is that OT&E by nature requires test items that are near the completion of development so that they can be operated by their ultimate users in an operationally representative environment. Therefore, the majority of OT&E must be accomplished near the end of the development cycle. Here within lies the problem; too much "stuff happens" during the earlier, significantly non-integrated, developmental part of the acquisition process that the two key customers above have no knowledge of or influence over. The result is that OT&E becomes "discovery" of problems that could/should have been dealt with earlier in the process when they would have been much less significant. While integrated test and evaluation has been a recent focus with several policy statements issued, there was no pre-IOT&E stakeholder in place to ensure early integrated testing of systems. In 2009, Congress once again turned to T&E to integrate this part of the process as well with the creation of the office of the Director, Developmental Test and Evaluation (DDT&E). Thus the responsibility of the DDT&E is to assure that developmental test and evaluation (DT&E) is effective, visible, and integrated with OT&E to form a knowledge continuum throughout the entire development and acquisition process.

Edward R. Greer.

Integrated Testing is defined by OSD Memo, "Definition of Integrated Testing," dated 25 April 2008, as follows: "the collaborative planning and collaborative execution of test phases and events to provide shared data in support of independent analysis, evaluation, and reporting by all stakeholders, particularly the developmental (both contractor and government) and operational test and evaluation communities."

From my perspective, the word "integrated" has four key meanings associated with defense acquisition. First, integrated T&E must be an integral part of development and acquisition. Effective and efficient development and acquisition absolutely requires extensive, timely, accurate, and impartial knowledge, and that is the product of good T&E. While the defense development and acquisition process has two customers, the warfighter and the U.S. taxpayer, T&E has a customer list that also includes the program manager, the contractors, the program management team, and the entire development team.

The second meaning of integrated T&E is that contractor and government DT&E must be planned and conducted in a manner such that there is no duplication of effort, facilities, personnel, or other resources. Integrated contractor and government T&E must also include the open sharing of test data in order to achieve efficiencies. Integrated contractor and government DT&E also describe a smooth and efficient transition from very early, mostly contractor conducted, highly technical testing of components and subsystems to the often more government conducted full system technical testing. Government and contractor integrated T&E throughout the entire development will assure a more streamlined and cost effective process and assure that the knowledge gained is used to the maximum extent possible to support

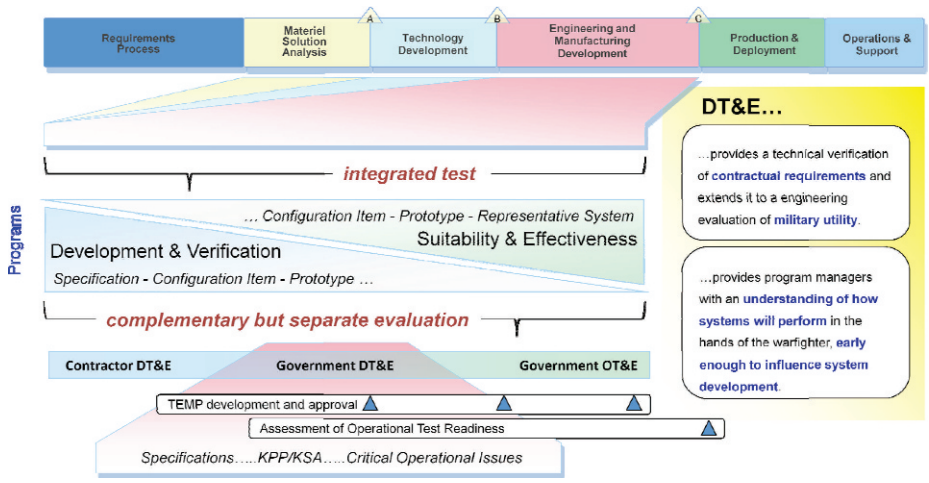


Figure 1. The Integrated T&E Continuum.

timely and cost effective development of effective equipment.

The third meaning of integrated T&E describes the continuance of a smooth and integrated flow of T&E from DT&E with and into OT&E. *Figure 1* shows the resulting continuum of T&E. This continuum ranges from pre-milestone A translation of user requirements to follow-on T&E (FOT&E) and product sustainment post-milestone C. The engineering and manufacturing development (EMD) phase of the system acquisition life cycle is a recognizable transition period from a subsystem engineering effort to a production-representative system evaluation effort. The full spectrum of integrated DT&E and OT&E becomes most evident during this phase, with government DT&E playing an increasingly important role. The government DT&E role, while complimentary to both systems engineering and operational test and evaluation efforts, requires an entirely different set of skills and resources than these other domains. Specifically these are engineering skills and resources focused on developing systems for subsequent operational test and employment. The integrated T&E continuum allows for efficiency across contractor DT&E, government DT&E, and government OT&E. As shown in the blue shaded triangle, systems engineering, when combined with (primarily) contractor test capability, excels at realizing system specifications in component level development. *Figure 1* depicts how this effort continues across the EMD phase, ultimately resulting in system-level prototypes. As the EMD phase progresses, the government test community starts to work with the contractor test community to gain insight into the suitability and effectiveness of the engineering design. DOT&E "owns" the assessment of suitability and effectiveness and is most notably involved in pre-milestone C efforts with (early) operational assessments (OA). A T&E continuum integrates operational assessment with engineering focused verification of contractual requirements, an essential step to assure efficient development and acquisition of operationally effective and suitable systems.

DDT&E provides knowledge to support engineering verification of contractual requirements and engineering evaluation of military weapon systems. This knowledge supports the essential transition from how we expect the system to work to how the user needs it to work for successful employment. Not even the most robustly engineered set of requirements can fully capture the intent, interactions, or dynamics of the operational environment. Therefore, DDT&E provides program managers with an understanding of how systems will perform in the hands of the warfighter, early enough to influence system development. DOT&E provides the assessment of system effectiveness and suitability; however OTAs are not staffed to support daily interactions with the product development community. In addition, while OTAs do well at replicating the user environment, they are not resourced or trained to isolate engineering parameters within that environment and provide technical feedback for development. An integrated T&E continuum assures that both happen as and when they need to for maximum efficiency and effectiveness in system development and acquisition.

My fourth and final characteristic of the word "integrated" applies to my responsibility for bringing together and assuring adequacy of the multitude of capabilities essential to support good T&E for defense

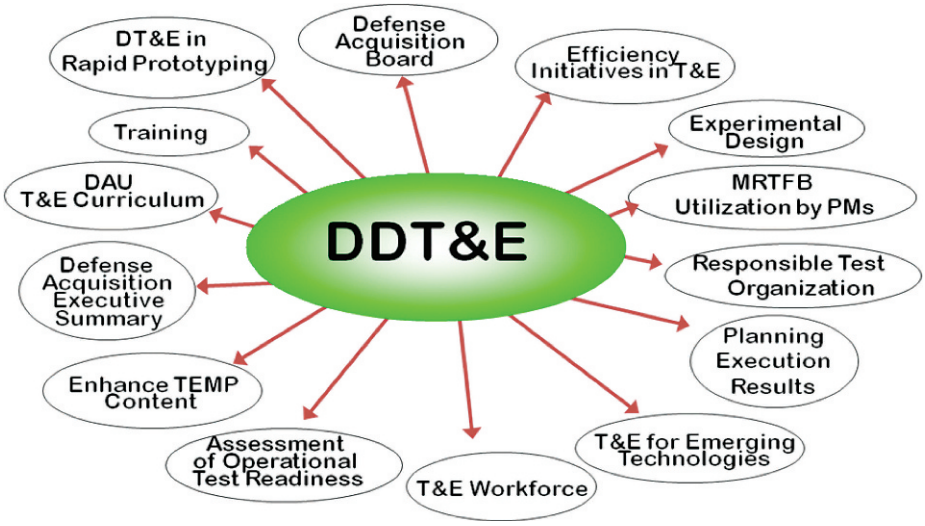


Figure 2. DDT&E Integrated Responsibility.

development and acquisition. As depicted in *Figure 2*, this responsibility ranges from well tested and understood maturing technologies, development and maintenance of a professional T&E workforce, a robust and efficiently utilized test base capability, thorough planning for integrated T&E throughout the entire acquisition program, well organized and responsible test organizations, to effective utilization of knowledge from T&E applied to key acquisition decisions. As part of execution of this responsibility, my organization is working with the Defense Acquisition University (DAU) to improve the T&E training and certification courses and the T&E portion of other related curricula. Another key part of the execution of my responsibility is to integrate and develop methodologies and best practices for T&E of emerging technologies. This includes infrastructure and processes to test hypersonic systems, directed energy weapons, non-lethal weapons, next generation UAVs, data fusion, anti-tamper, cyber, and complex multi-node mobile networks. DDT&E has a key role in the Secretary of Defense's (SECDEF's) efficiency initiatives, streamlining T&E planning and reporting processes and documentation. Closely aligned with this SECDEF initiative is our initiative to assess the cost of doing T&E business. Such an assessment will touch all of our areas of integrated responsibility and provide insights into improvement and metrics for continued monitoring. DDT&E is also committed to how DT&E can be highly focused to enhance, not delay, rapid acquisition. Overall, this integration of responsibility for policy, people, and infrastructure into a single organization positions DDT&E to contribute significantly to more effective and more responsive defense development and acquisition.

As we work together to implement and improve integrated T&E across the continuum, I ask for your help in meeting several key challenges that face the T&E community. Three of the more pressing challenges include T&E in the cyber world, achieving the right balance of T&E within Rapid Fielding, and achieving greater DoD efficiencies within T&E. We must harness the intellectual talent of our skilled workforce to understand and develop effective ways to test and assess system performance and assurance in the complicated world of cyber warfare. Within the initiative to rapidly field weapon systems to the warfighter, we cannot afford the proven and deliberate T&E methodology required in formal acquisition—we must find effective ways to quickly test and assess capabilities and limitations of systems as they are expedited to the front lines. And finally, we owe it to the end user to take a hard look at our processes, policies, and organizations to find significant efficiencies in the way we do business. These challenges must be met in order to deliver affordable weapon systems that work, and I ask your help in meeting these challenges.

Truly, integration is the golden key to successful (effective and efficient) defense development and acquisition. Because the T&E community and processes reach out and touch many key elements of defense development and acquisition, T&E is uniquely positioned to facilitate, guide, monitor, assess, and report the progress and effectiveness of this integration. DDT&E is a key organization within USD(AT&L) assuring that integrated T&E is conducted to significantly improve defense development and acquisition. Without a doubt, knowledge is the power to make it happen and T&E is the conduit for that knowledge. ❑

Edward R. Greer was sworn in as the Director of Developmental Test and Evaluation (DDT&E) on March 15, 2010. He serves as the principal advisor on developmental test and evaluation (DT&E) to the Director of Defense Research and Engineering and the Under Secretary of Defense for Acquisition, Technology and Logistics. Mr. Greer is responsible for developing and revising DT&E policy in support of the acquisition of major Department of Defense (DoD) weapon systems. Other significant duties include reviewing and improving the organization and capabilities of the military departments with respect to DT&E and providing advocacy, oversight, and guidance to elements of the acquisition workforce responsible for DT&E.

Prior to this political appointment and since 2002, Mr. Greer served as the Deputy Assistant Commander for Test and Evaluation (AIR 5.0A), Naval Air Systems Command and Executive Director, Naval Air Warfare Center Aircraft Division (NAWCAD), Patuxent River, MD. As the senior civilian for naval aviation T&E, Mr. Greer was responsible for planning, executing, analyzing, and reporting of all naval aviation T&E spanning a workforce of 6,600 and an operating budget of almost $1B. As executive director, NAWCAD, responsibilities included ensuring that NAWCAD technical, business, and financial objectives were met across a workforce of 14,400 and a total operating budget of over $4 billion.

Mr. Greer joined the senior executive service (SES) in 1998 as director of the Atlantic Ranges and Facilities, NAWCAD, responsible for all facets relating to the development, maintenance, and operation of the range and test facility components of the Navy's principal air combat systems test activity.

From 1995 to 1998, Mr. Greer served as principal deputy program manager of Airborne Strategic Command, Control, Communications; Program Executive Office for Air, Antisubmarine Warfare, Assault & Special Mission Programs. Mr. Greer was responsible for all aspects of acquisition including systems engineering, logistics, training systems and T&E. From 1993 to 1995, Mr. Greer took an assignment in the Pentagon as a staff specialist in the Office of Under Secretary of Defense for Acquisition and Technology, Test, Systems Engineering and Evaluation; Test Facilities and Resources. Prior to 1993, Mr. Greer served in various leadership and engineering positions within the Naval Air Systems Command and was the Navy's representative on the 2007 Defense Science Board Task Force on Developmental Test and Evaluation.

Mr. Greer is a past president of the Southern Maryland Chapter of ITEA. He earned his bachelor of science degree in electrical engineering from the University of Maryland, College Park and received a masters of science degree in management from the Florida Institute of Technology. Mr. Greer is also a graduate of the Defense Systems Management College Program Management Course. E-mail: cdbrown.gm@gmail.com.

TechNotes

ITEA Journal 2010; 31: 447–448

Quick Reaction Test: Host-Based Security System

Timothy K. Holmes
Joint Interoperability Test Command, Indian Head, Maryland
Cesar E. Pie
Cyber Security Research and Solutions Corporation, La Plata, Maryland

Under the leadership and shared vision of the United States Strategic Command, the Defense Information Systems Agency (DISA) Mission Assurance/Network Operations Program Executive Office, the DISA Joint Interoperability Test Command, and other Department stakeholders, the Department of Defense has successfully orchestrated a Global Information Grid–wide initiative in support of the institutionalization of the Host-Based Security System throughout the Department of Defense. The scope of the Host-Based Security System deployment will be worldwide. This vast effort requires a large support infrastructure to be in place and a rigorous testing project that will help expedite the fielding of its unique capabilities.

Key words: Computer network defense; computer system security; cyber-threat; intrusion detection; intrusion prevention.

The Host-Based Security System (HBSS) baseline is a flexible, Commercial-Off-The-Shelf (COTS)-based application. It monitors, detects, and counters known cyber-threats to the Department of Defense (DoD) Enterprise. Under the sponsorship of the Enterprise-wide Information Assurance and computer Network Defense Solutions Steering Group (ESSG), the HBSS solution will be attached to each host (i.e., server, desktop, and laptop) in DoD. The system will be managed by local administrators and configured to address known exploit traffic using an intrusion prevention system (IPS) and host firewall. The Defense Information Systems Agency (DISA) Program Executive Office Mission Assurance and Network Operations (PEO-MA) is providing the program management and supporting the deployment of this solution.

Joint test approach

Under the auspices of the Joint Test and Evaluation Program, the HBSS Quick Reaction Test (QRT) project is focused to develop tactics, techniques, and procedures (TTP) and concepts of operations (CONOPS) in support of HBSS operations. The QRT has taken a joint approach (as well as assessment practices, principles, and strategies used in previous Bulwark Defender exercises) to test formal and informal HBSS configuration policies across the Global Information Grid (GIG) and to develop DoD-specific protection level baselines to address the required level of security needed by the Department. These configuration baselines will provide GIG network defenders with documented TTP and CONOPS for the employment, implementation, and operation of the HBSS throughout DoD (enhancing the warfighter's ability and capabilities to protect, monitor, detect, analyze, diagnose, and respond to cyber threats). The United States Strategic Command (USSTRATCOM) through United States Cyber Command (USCYBERCOM) has instructed the potential use of the QRT test results in upcoming Operational Plans (OPLANS) and will require implementation of HBSS TTP recommendations by their DoD Network Operations (NetOps) Combatant Commands/Services/Agencies (CC/S/A) via Fragmentary Orders (FRAGO) and/or Command Task Orders (CTO).

The HBSS QRT test approach is based on the proven Joint Interoperability Test Command (JITC) Information Assurance/Computer Network Defense (IA/CND) attack-based methodology. Much like a typical war game exercise, the JITC approach uses a red attack/blue defend construct. The concept is red attacking along defined attack vectors, aligned with an anatomy of an attack with detailed scenarios based on the latest Joint Task Force-Global Network Operations (JTF-GNO) J2 observed threats. Blue will use the full range of people, processes, and technologies available to defend against red. Each attack and defend activity is controlled, measured, and

correlated, with analysis focusing on the most effective and suitable scenario as it relates to the warfighter's mission. The operational threat environment replicated by the threat team will aim to target second and third generation threats, as defined in the Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 6510.01E. This is the replication of non-state–sponsored groups utilizing common tools in a sophisticated manner and the replication of state-sponsored groups utilizing a combination of common and uncommon hacker tools and techniques in a sophisticated manner with unlimited resources.

As prioritized by USSTRATCOM, every recommended scenario event has been mapped to its corresponding class of attack (i.e., passive, active, insider, distribution, and close-in) and three of seven stages of an anatomy of attack (i.e., gaining access, escalation of privilege, maintaining access). To support the development of attack scenarios, the JITC created the HBSS QRT Threat Team Working Group (TTWG) to identify, coordinate, and validate the selected scenarios. The scenarios were created by the U.S. Air Force and DISA Field Security Officer and reviewed by the National Security Agency. The JITC, in coordination with the TTWG, will continue to add increasingly sophisticated scenarios over the life of the QRT to render the best possible HBSS configurations and TTP.

Test concept and measures

As part of each QRT event, the threat team will render a series of increasingly sophisticated attacks. The blue defenders will implement a series of candidate configurations of TTP in an attempt to counter the threat. The test concept will measure the relative performance of these candidate configurations and TTPs to identify the best candidate. The measures the QRT will use are taken from the Office of the Secretary of Defense (OSD) Director, Operational Test and Evaluation Core Metrics Manual for Operational Assessments of Information Assurance and Interoperability (DOT&E Core Metrics Manual). This manual contains the performance-based metrics used in the DOT&E-sponsored assessments of IA/CND during Combatant Command (COCOM) exercises. The DOT&E Core Metrics Manual defines the performance measures and metrics, the data elements, and the analysis method, along with associated data collection forms. This Manual has been applied to a variety of COCOM exercises, including Bulwark Defender, to measure the operational performance of the COCOM's IA/CND capability. The metrics are proven, accepted by all OTAs, well understood, and will yield the exact performance-based criteria needed by the HBSS QRT to determine the most effective configurations and TTPs.

Conclusion

The HBSS QRT will be accomplished in two spirals; each spiral will consist of a set of two lab-based events and conclude with an operational test that includes the participation of both U.S. Pacific Command and U.S. Strategic Command. The HBSS QRT was directed on January 6, 2010, with an expected performance period ending January 5, 2011. Upcoming HBSS QRT events will allow the warfighter to establish best practices and obtain lessons learned. The HBSS QRT will provide results that will undoubtedly expand the warfighter's capability to protect, detect, diagnose, and react to cyber threats using effective configurations and improved TTPs. ❑

Mr. Kevin Holmes serves as the JITC information assurance technical advisor, where he develops and maintains the Command's IA policies, methodologies and capabilities. Mr. Holmes joined the JITC shortly after its inception in 1989. He has held a variety of positions within the Command. Mr. Holmes started his JITC career developing software for many JITC instrumentation systems ranging from tactical message protocol analyzers to modeling and simulating Tactical Data Systems. He stood up the JITC IA capability in 2001 and has been working in that area since. Holmes earned his bachelor of science degree in management information systems (MIS) from the University of Arizona and his master of science degree in computer science from George Mason University. E-mail: kevin.holmes@disa.mil

Mr. Cesar E. Pie is chief executive officer of Cyber Security Research and Solutions Corporation (CSRS-Corp). He has extensive program management expertise and has provided subject matter expert support to the JITC for over 6 years in the fields of information system security engineering, information assurance, and computer network operations (computer network attack, computer network exploitation, and computer network defense). Mr. Pie graduated from the University of Maryland University College with a master of science degree from the Computer System Management—Information Assurance Program that is supported by the Department of Homeland Security and the National Security Agency's Center of Academic Excellence in Information Assurance Education (CAE/IAE). Among others, a few of Mr. Pie's certification credentials include Certified in the Governance of Enterprise Information Technology (CGEIT), Information System Security Engineering Professional (ISSEP), Certified Information Systems Auditor (CISA), Certified Information System Security Professional (CISSP), and Project Management Professional (PMP). E-mail: cesar.pie@csrscorp.com

References

DoD. 2008. Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 6510.01E. *Information Assurance and Computer Network Defense.* Washington, DC: DoD.

ITEA Journal 2010; 31: 449–452

History of Cyber Testing and Evaluation—A Voice From the Front Lines

James S. Welshans, Ed.D.
Navarre, Florida

*Our nation does not have a dedicated place to conduct cyber security experiments. The National Cyber Range is DARPA's (*Defense Advanced Research Projects Agency*) contribution to the new federal "Comprehensive National Cyber Initiative," providing a "test bed" to produce qualitative and quantitative assessments of the security of various cyber technologies and scenarios. We will provide a revolutionary, safe, instrumented environment for our national cyber security research organizations to test the security of information systems (DARPA Strategic Technology Office, 2010).*

I'm very honored to join the *ITEA Journal*'s History Committee and will do my best to seek out some interesting perspectives from the early days of test and evaluation in each issue. You might appreciate that my first strategy for unlocking the mysteries of cyber testing revealed a network of organizational genealogies mediated in a language that left my internet browser parked on acronymfinder.com. The good news is that I soon came to my senses and remembered my training in history.

I believe that history is revealed in the lived experiences of everyday people who were in the right place and time to be part of something interesting. Of course, I never expected that anyone in the cyber business would be able to share a "there I was" narrative about the development and testing of a capability for posting explicit YouTube videos on Osama Bin Laden's Facebook site. I contacted a trusted colleague and he recommended an individual who has definitely lived through some interesting times in the cyber business.

Vince Holtmann is a telecommunications engineer who has been actively engaged in testing cyber systems and capabilities for the past 15 years. He began work in the cyberspace field in the mid-1990s as a U.S. Air Force active duty cryptographic technician, where his duties included installing, sustaining, and testing new encryption devices. While on active duty, he did his undergraduate work in computer science. He also holds a master's degree in telecommunications and a master's of business administration degree. After 8 years of service, he left the Air Force. He is currently employed by General Dynamics Advanced Information Systems, a large defense company as a developer and tester of cyber capabilities for the U.S. government.

I telephoned Vince and explained my plan for using his narrative in the journal article. I conducted a telephone interview with Vince. Except for a few icebreaker questions, the interview was an unstructured opportunity for Vince to share his narrative experiences and perspectives learned while in the cyber testing business.

Interview with Vince Holtmann

Welshans

Thanks for offering to share your experience and historical perspectives on test and evaluation of cyberspace. Starting off, can you please explain how you got into that line of work?

Holtmann

"Beginning my AF career as a crypto technician, I fell into the cyber domain from the Information Assurance (IA) and data security angle. Working with these technologies exposed me to the air, space, and cyber domains, as they are all inextricably linked.

"My first cyber range development effort involved the construction of a small laboratory and test range to help customers test collection capabilities over encrypted radio frequency and terrestrial links. From there I moved into a

more formalized Test and Evaluation (T&E) organization. I was a charter member of the [U.S. Air Force's] 346th Test Squadron and also worked for the [U.S. Air Force's] 46th Test Squadron. I also supported many other test organizations such as the Joint Interoperability Test Command (JITC), Air Force Operational Test & Evaluation Center (AFOTEC), and the National Assessment Group (NAG).

"Throughout my 8 years of U.S. Air Force active duty service, I continued to develop T&E ranges to specifically support cyber systems and capabilities, which also included research and development, and demonstration activities. Even before cyber was big, we were always conducting test and evaluation on cyber capabilities. That early experience exposed me to the many technologies and communication media involved in the cyber environment, especially the information assurance aspects of protecting data."

Welshans

Do you feel that your academic background and work experience with the Air Force prepared you to perform cyber test and evaluation? Were there aspects of the cyber testing environment that came as a surprise?

Holtmann

"That's a good question. I think education helped from the technical standpoint to understand how you need to test different things… (i.e., understanding measures of evaluation, measures of performance, measures of effectiveness, those kinds of things). The technical background helped me to determine statistically how those things related and were calculated during the test. Our focus was to ensure that the capabilities we were building and testing for the warfighter would meet their operational needs.

"Some of the Defense Acquisition University courses, such as Test 101 and Test 201 classes provided a baseline understanding of how to plan and conduct formalized T&E. They covered how to build a test plan, how to work out the test procedures, and how to apply those throughout the program's life cycle of development, integration, and fielding. We learned how testing runs pretty much congruently with the whole system engineering life cycle.

"Moreover, there's also the issue of what we call in the military OJT [on-the-job training]. Learning by doing is important in cyber because there are always a lot of things you're not really prepared to deal with [during test preparation and execution]. When you're testing different capabilities, you may not have the most realistic T&E environment to mimic the operational environment. For example, if you're testing a cyber capability to defend against computer attacks from X, you may not have representative real-world attacks from X to use as test data, so you improvise with what you have at your disposal. Under these conditions, it's difficult to determine whether that capability will defend against those attacks."

One technique, run time control, might be used to mitigate this situation by allowing a network to operate at normal speed but to slow down its constituent computers. This would allow more traffic to run on the network, effectively simulating a more realistic operating environment (Kenyon 2009).

Holtmann

"That lends some credibility to the way the government, industry, and academic communities have improved the cyber ranges and the capabilities within them to create more varied and realistic test and evaluation environments. So, where the rubber meets the road, when the warfighter needs to use it, when we need to protect the base, or we need to respond to an attack we know that the capability is going to respond as needed."

Welshans

How does test planning in the cyber environment compare with test planning of other weapon systems? Do your test measures tend toward quantitative performance measures and indicators or do you also use qualitative measures and indicators to judge operational effectiveness and suitability?

"It's really a mix of both quantitative and qualitative. Let me offer an example that might show the similarity between testing an aircraft and testing a cyber capability. Remember that in both areas you have to be concerned with performance parameters like power, throughput, mean time between failures, etc.,… all those types of factors still come into play and fit within the quantitative measure. But specifically for cyber, it really depends on what you're testing against. The qualitative measure looks at human response (e.g., how an operator might respond to a cyber attack, what actions they take next, how efficient are their responses).

"Let's say that you're testing defensive capability Y, such as an Intrusion Detection System (IDS). We'll have to test against established performance parameters. We'll need to verify that the system can process a specified number of events per second. It will have to deal with realistic threats that we've captured from a Computer Emergency Response Team, or another similar function, so that we can do penetration testing against that defensive capability. In this test case, your quantitative measure is the performance of the IDS, while the qualitative is the operator response or

reaction to the attack. The qualitative measurement really helps to improve not only the operator interface with the capability you are testing, but also the improvement of Tactics, Techniques, and Procedures (TTP)."

Welshans

I realize that much of what's done in the cyber domain is highly classified. But can you offer an unclassified "been there, done that" narrative that summarizes the ideas today and puts them in an operational context?

Holtmann

"Sure, I'll talk about a project I supported as a defense contractor working as a tester in the cyber environment. We were supporting a Quick Reaction Capability (QRC) development effort for a customer. The approach we took was to incorporate government test staff within the system development activities. Throughout this effort we developed and refined test cases, involved the operational user to help with usability inputs, and developed training along the way for all involved parties. Because all stakeholders were involved throughout the process, we were able to combine Contractor, Developmental Test, and Operational Test and Evaluation (CT/DT/OT&E) events to deliver a fully functional capability within the tight schedule. This approach has guided our internal process to involve all stakeholders on day one, while continually developing/integrating, testing, and refining to deliver capability early and often to the warfighter.

"Government and industry need to operate with more agility throughout the acquisition, development/integration, test, and fielding activities to respond to the cyber threats that we face on a daily basis. I've heard many government and industry leaders talk recently about moving to a 'Cyber Safari' type of rapid acquisition and test methodology for cyber, where we can work requirements, development, and testing together, what a great idea!

"As the story goes, development is always quick, with agile test and development methodologies bringing all the stakeholders together on day one, so you are developing your capability with all the requirements and all the users involved. You're going to get exactly what they're looking for, and you're testing throughout the entire process to reduce defects early in the process. This means contractor in-plant testing, developmental testing, and operational testing together. You're looking at and refining your measures of performance and measures of effectiveness throughout that whole process, so you have high confidence that the system is going to perform as intended.

"Most important, your test procedures are getting refined, so that when you go through your final test event, even when you combine DT and OT… that speeds everything up because everyone is on the same page for testing and everything is there, all the requirements are met at the end.

"As we're all aware, with shifting government budgets and need to speed capabilities to the warfighter as quickly as possible we need to change the way we do the test business. One of the things that we can offer is combining test events when possible, moving everyone into the process early, and streamlining the QRC-like process for getting capability delivered."

Welshans

So, I'm hearing "Get the testing integrated into the whole spiral development process"?

*"Yes, embed the testing, but not in a spiral development process. Spiral and waterfall development methodologies don't really work for cyber. Agile development is the way to go, with developmental sprints anywhere from 2 weeks to a month. As requirements change, you keep a backlog and work to reprioritize all along the way. If you're going to develop that quickly, of course the testers need to be involved as requirements are changing, test procedures are modified, and MOEs [*measures of effectiveness*] and MOPs [*measures of performance*] are being adjusted.*

"Timelines in the cyber domain require flexibility. It's best to plan to deliver warfighter capabilities as quickly as circumstances allow as the battlefield is in constant motion, resulting in new and altered requirements. You need to ensure that the capability you deliver is going to work because you've been aggressively testing throughout. Get the tester inside the agile development and acquisition life cycle." ❑

Dr. James S. Welshans, Ed.D., is a former active-duty U.S. Air Force fighter pilot, instructor, and war planner. Currently an independent scholar, he is employed as a senior requirements engineer with Teledyne CollaborX, advising the U.S. Air Force Research Laboratory on military C2 projects and technology transition. A founding member of the U.S. Air Force Operational Command Training Program, Dr. Welshans taught strategy and operational assessment to military officers worldwide during major command and control exercises. Dr. Welshans received a bachelor of science in international affairs and history from the U.S. Air Force Academy (1977), a master of science in management (1987), and a doctor of education degree in curriculum and instruction

and educational leadership (2008). He serves on the executive board of the Society for Phenomenology in the Human Sciences. E-mail: lectric6@att.net

References

Defense Advanced Research Projects Agency, Strategic Technology Office. 2010. The National Cyber Range: A National Testbed for Critical Security Research. http://www.whitehouse.gov/files/documents/cyber/DARPA-NationalCyberRange_FactSheet.pdf. (accessed August 27, 2010).

Kenyon, Henry S. May 2009. "Defense Researchers Developing National Cyber Test Range." Signal Online. http://www.afcea.org/signal/articles/templates/SIGNAL_Article_Template.asp?articleid=1928 (accessed August 27, 2010).

Featured Capability

ITEA Journal 2010; 31: 453–457

Verification and Validation Capabilities for the Next Generation Air Transportation System

John Frederick, Hilda DiMeo, and Vincent J. Lasewicz, Jr.
Federal Aviation Administration, Atlantic City Airport, New Jersey
Catherine Jaggard
ASRC Research and Technology Solutions, Atlantic City Airport, New Jersey

The Federal Aviation Administration (FAA) is in the process of planning and implementing the Next Generation Air Transportation System (NextGen). The goal of NextGen is to efficiently address the current and future challenges facing the U.S. air transportation system. The Verification and Validation (V&V) of the NextGen will require an environment and infrastructure for testing, modeling, and simulation throughout the development and implementation of NextGen capabilities that has not previously been used by the FAA. This article discusses the initiatives that the FAA is undertaking to establish new V&V capabilities and environments for NextGen.

Key words: Verification; validation; NextGen; transportation; FAA; aviation; air traffic; simulation; modeling; cockpit; V&V.

Our nation has recently experienced an economic downturn the likes of which has not been seen since the Great Depression. This has slowed the growth rate of U.S. aviation, but delays continue to plague the system and will only grow worse as the number of passengers flying each year in the United States continues to rise. Delays resulting from the constraints of the current National Airspace System (NAS) already cost the United States approximately $9.4 billion annually, and that number will continue to spiral without Next Generation Air Transportation System (NextGen) improvements. New security demands are affecting the ability to efficiently move passengers and cargo. In addition, aircraft noise and pollution are a growing concern. Antiquated systems, processes, and procedures do not provide the desired flexibility needed to economically meet the current and future demands.

The concept behind NextGen is to implement and deploy new technologies, processes, and capabilities that will increase capacity and efficiency while maintaining safety. Several solution sets such as trajectory-based operations and collaborative air traffic management have been identified to provide benefit in the air transportation system. Trajectory-based operations focus primarily on high-altitude cruise operations to provide the capabilities, decision-support tools, and automation to manage aircraft movement by trajectory. Trajectory-based operations will enable a highly desired capability for aircraft to fly negotiated flight paths necessary for full performance-based navigation, taking both operator preferences and optimal airspace system performance into consideration. The collaborative air traffic management solution set provides capabilities to improve traffic flow management system-wide as well as at the tactical, or location-based, level. Collaborative air traffic management supports a more flexible air traffic system capable of in-flight adjustment to alternate, more favorable routings and altitudes as well as the ability to shift traffic operations to match airspace and airport capacity. These solution sets will require FAA laboratory simulation and modeling capabilities that have not been available in the past for the Verification and Validation (V&V) of concepts and systems.

By the year 2018, the Federal Aviation Administration (FAA) expects NextGen-provided benefits to result in a 21 percent reduction in flight delays with 22 billion dollars of cumulative savings. During this period, the FAA expects a cumulative savings of 1.4 billion gallons of fuel, reducing CO_2 emissions by nearly 14 million tons. The increased complexities and valued benefits of NextGen warrant comprehensive V&V toolsets and laboratory capabilities that will provide timely and credible data for concepts develop-

ment, requirements development, risk management, evaluations, and decision support.

Laboratory environments for NextGen capabilities

The magnitude of the challenges presented by NextGen is unprecedented in the FAA. The operational concepts and system-of-systems architecture will be dramatically different than what is currently used to safely operate the NAS. The focus of the NAS operational concept in NextGen is moving from tactical air traffic control to a focus on airspace and traffic management. The NAS architecture with NextGen will transition from an analog, point-to-point system to an integrated, digital, system-of-systems environment that supports net-centric operations. V&V will be critical to the identification and definition of new capabilities and requirements, as NextGen transforms the NAS. Verification ensures that selected work products, product components, and products meet specified requirements and standards, and validation demonstrates whether a product will fulfill its specified purpose when placed in any aspect of its intended environment such as operation. A robust V&V approach is required for the implementation of NextGen. This V&V approach will also be critical to the identification and definition of new capabilities and requirements, as NextGen transforms the NAS. The FAA is taking steps to establish an infrastructure and capability that will focus on the V&V of systems in their intended operational and technical environments using a Live, Virtual, Constructive (LVC) simulation.

The proposed location to develop and establish this LVC environment is at the FAA William J. Hughes Technical Center in Atlantic City, New Jersey. This environment will provide a single integrated framework that advances the V&V of complex, networked, distributed systems operating in the NextGen system-of-systems. With this framework, the FAA will be provided a scalable level of fidelity for V&V based on individual and collective test and evaluation needs. This LVC environment is critical to NextGen implementation activities and acquisition decision support that occurs during all phases of the lifecycle, including mission analysis, investment analysis, solution implementation, and in-service management testing.

NextGen integration and evaluation capability

The NextGen Integration and Evaluation Capability (NIEC), located at FAA William J. Hughes Technical Center in Atlantic City, New Jersey, is the FAA's first step towards the LVC environment *(Figure 1)*. The NIEC leverages existing laboratory and simulation capabilities that are used to develop, test, and maintain the NAS. It comprises existing NAS operational systems and high fidelity, real-time simulation capabilities to create an integrated, flexible, and reconfigurable environment to support NextGen research as well as test and evaluation.

The Technical Center's new NIEC Display Area (NDA) complements this unique platform by collocating and integrating key aviation and NAS components into a single multi-domain visualization environment with advanced data collection capabilities to support integration and evaluation of new technologies and concepts. The base components of the NDA are an air traffic suite, a simulated tower suite, an Unmanned Aircraft System (UAS) suite, a cockpit simulator suite, and a multi-purpose area. Each suite has an integrated voice communication capability that allows for communication between components. The NDA is integrated with other simulation and operational NAS components including data feeds (e.g., weather, traffic flow management, Automatic Dependent Surveillance-Broadcast [ADS-B]) to support high-fidelity simulations that enable researchers to visualize the ripple effect of newly integrated capabilities and technologies across a simulated NAS environment.

In this simulation environment, the research cockpit simulator can be seen flying in the tower simulators out-the-window view. It can also be seen as a target on the air traffic control consoles along with UAS targets, other targets driven by simulated radar data, and ADS-B data. Weather reflectivity data can also be added. If needed, full-up cockpit simulators like those at various National Aeronautics and Space Administration (NASA) facilities or airline training facilities can be integrated into the simulation. The ability to provide a combined environment of legacy systems with future technologies and capabilities also enables the NIEC to support the transition to NextGen.

Simulation

The Target Generation Facility (TGF) and the Distributed Environment for Simulation, Rapid Engineering and Experimentation (DESIREE) are existing simulation engines that are key to conducting NIEC simulations. TGF is a cross-cutting infrastructure that is capable of simulating air and ground traffic, which drives terminal and en route laboratories as well as developmental laboratories. The TGF is a dynamic real-time air traffic simulation capability designed to generate realistic aircraft trajectories and associated digital radar messages for aircraft in a simulated airspace environment. Up to 600 targets (400 piloted) can be generated in one or more concurrent simulation environments. Multiple Terminal, En-Route, and Oceanic airspaces may be simulated individually or

Figure 1. The NextGen Integration and Evaluation Capability (NIEC) at the Federal Aviation Administration William J. Hughes Technical Center.

simultaneously. DESIREE emulates the graphical user interface used in most air traffic control systems. These simulators work together to immerse the subject into a realistic environment that can emulate the past, present, or future air traffic environments.

Air traffic control suite

The NDA contains a reconfigurable air traffic control suite. It has the ability to model up to eight air traffic sectors driven by DESIREE. The sectors are reconfigurable and can be brought up as one of the following: (a) Terminal (STARS), (b) the Future Terminal Work Station (FTWS), (c) Enroute (ERAM), or (d) the Future En Route Work Station (FEWS).

Tower suite

The tower suite consists of the 180-degree out-the-window view and the surface management system. The surface management system has emulations of the Airport Surface Detection Equipment-model X (ASDE-X) and Digital Bright Radar Indicator Tower Equipment (DBRITE). The prototype Terminal Information Display System (TIDS) and Flight Data Management (FDM) displays and software are integrated with the tower suite. A key component of the tower suite is the Virtual Airport Immersion Environment (VAIE), which has the 180-degree out-the-window view. The VAIE is a highly extensible three-dimensional rendering solution for the Target Generation Facility's high-fidelity air-traffic simulator. The VAIE uses advanced rendering techniques to efficiently handle many scene lights—often five per aircraft—that produce highly realistic lighting effects that interact with the terrain and other aircraft in the scene.

Unmanned aircraft system suite

The UAS Modeling and Simulation (UAS M&S) capability currently includes UAS simulators; a four-dimensional trajectory-based operations (4DT)-enabled flight management system simulator, a voice communications simulation platform, automatic de-

Figure 2. The Research Cockpit Simulator (RCS) in the NextGen Integration and Evaluation Capability (NIEC) laboratory at the Federal Aviation Administration William J. Hughes Technical Center.

pendent surveillance-broadcast/radar surveillance, and weather workstations. The UAS M&S capability components interact with systems that are part of the NIEC, including the air traffic control suite.

Research cockpit simulator suite

The Research Cockpit Simulator (RCS) is currently set up as an Airbus A-320 series aircraft but is fully reconfigurable to any current airline transport type aircraft *(Figure 2)*. It has a state-of-the-art touch screen cockpit panel layout that allows pilot commands for inputting and executing commands to the aircraft. The touch screen panels allow the RCS to be easily reconfigured into different types of aircraft. The RCS has a full-size cockpit layout with crew positions for operating transport category aircraft.

Multi-purpose area

The multi-purpose area can be used to display weather data or traffic management data, to operate as a simulation monitoring station or to simulate an airline operations center. Live air traffic data from Traffic Flow Management Production Center and weather data from the NextGen Weather Evaluation Capability can be displayed here.

Evolving to a Live, Virtual, and Constructive (LVC) V&V environment

By evolving to a LVC environment, the FAA will have a single integrated framework that can represent the entire NAS, advancing V&V of complex, networked, distributed systems operating in the NextGen system-of-systems. This framework would provide a scalable level of fidelity based on individual and collective test and evaluation needs providing timely and creditable information to decision authorities using one common dataset and scenarios throughout the life cycle. The multiple fidelity modeling and simulation environments must be able to support early concept validation (lower fidelity, fast-time simulations/models), requirements/design development, and operationally realistic testing (high-fidelity complex simulations/models). In addition to the scalable fidelity characteristics, the nonproprietary and open architecture would make possible in-house engineering modifications to the framework in support of NextGen research and development activities. The type of architecture

solution would set the stage for common datasets and scenarios of varying fidelity with greater flexibility.

The ability to model the legacy NAS and/or the NextGen system-of-systems using a LVC approach with nonproprietary tools in real time, end to end, and open-architecture environment has enormous benefits. This approach provides a technical toolset that can be regularly used to support engineering and acquisition decisions. It can be applied throughout an acquisition life cycle, supporting early concept analysis, through design, developmental test and evaluation, integration, and operational test and evaluation. When implemented in an integrated systematic framework, it can be both a technically effective and a cost-efficient means of understanding the complex and emergent behavior of a system-of-systems. M&S provides an environment to help the technical teams create and evaluate new capabilities for existing systems and consider integration issues that can have a direct effect on the operational user, program costs, and schedule. It provides an open architecture that supports greater laboratory availability to multiple users. M&S can support analysis of alternatives, as well as analysis of requirements and solution options.

Summary

Simulating and modeling the U.S. air transportation system end to end is a difficult challenge. Currently the National Air Space system could have more than 5,000 aircraft flying through it at any one time. Estimates show that flight operations will increase 19 percent at 35 major U.S. airports between 2009 and 2018. This will increase the capacity and complexity requirements for M&S. The current FAA laboratory environments are evolving from a mostly development and test business model emphasis to include the research, analysis, and strategic implementation of the system-of-systems capability required by NextGen. The ultimate goal is to continue to enhance the NextGen Integration and Evaluation Capability and evolve it with other V&V tools to attain a comprehensive Live Virtual Constructive infrastructure. This infrastructure will provide the ability to model and simulate the entire National Airspace System across all involved facilities and functions in real time under all expected loads and variables. ❑

JOHN FREDERICK is a graduate of Drexel University (Philadelphia) with a bachelor of science in computer systems management. Mr. Frederick has over 25 years of test and evaluation (T&E) conduct, management, and oversight experience with the FAA. Mr. Frederick serves as the chair of the Test Standards Board for the FAA and is the International Test and Evaluation Association (ITEA) South Jersey chapter president. He also leads the FAA Acquisition Executives Board V&V Working Group and is the T&E representative for the FAA Technical Center on the FAA Acquisition System Advisory Group. E-mail: John.Frederick@faa.gov

HILDA DIMEO is a graduate of the University of Puerto Rico with a bachelor of science in computer science. Ms. DiMeo has 24 years of experience in laboratory operations and various research and development projects. She is currently the Concepts and Systems Integration (CSI) team manager in the NextGen and Operations Planning organization at the FAA William J. Hughes Technical Center. CSI is composed of four laboratories including the En Route Integration and Interoperability Facility (EIIF), the Oceanic IIF, the NIEC, and the Research, Development, and Human Factors Laboratory (RDHFL). Ms. DiMeo serves as the co-chair of the Simulations Facilities Task Force supporting the National Aeronautics Research and Development Plan. E-mail: Hilda.DiMeo@faa.gov

VINCENT LASEWICZ is a graduate of the University of Scranton with a bachelor of science in electronics engineering. Mr. Lasewicz has 25 years experience in the Technical Center's air traffic control laboratories. He is currently the Laboratory Integration Lead in the Laboratory Services Group. Mr. Lasewicz designed and managed the FAA RDHFL. Mr. Lasewicz has a key role in preparing the Technical Center's laboratories to support testing of the next generation air transportation system. This includes design and development of the Technical Center's new NIEC. E-mail: Vincent.lasewicz@faa.gov

CATHERINE JAGGARD is a graduate of Monmouth University with a master's degree in software engineering. She currently works at William J. Hughes Technical Center for ASRC Research and Technology Solutions under the direction of the Quality and Standard Team AJW-111. Ms. Jaggard has worked throughout the years in many areas including second level support, field familiarization, radar switching systems, configuration management of the radar sites, and quality assurance evaluations. E-mail: cathy.ctr.jaggard@faa.gov

References

FAA. 2010. FAA's NextGen Implementation Plan, March 2010. Air Traffic Organization, NextGen & Operations Planning, the NextGen Integration and Implementation Office. Federal Aviation Administration. http://www.faa.gov/about/initiatives/nextgen (accessed September, 2010).

Invited Article

ITEA Journal 2010; 31: 459–465

Test and Evaluation for Agile Information Technologies

Steven Hutchison, Ph.D.
Defense Information Systems Agency, Falls Church, Virginia

Section 804 of the FY2010 National Defense Authorization Act directed the secretary of defense to develop and implement a new acquisition process for information technology (IT) systems. The law requires the Department of Defense (DoD) to base the new acquisition process on recommendations of the March 2009 Defense Science Board (DSB) Report on DoD Policies and Procedures for the Acquisition of Information Technology. The DSB recommended an agile model for acquiring IT similar to successful commercial practices. Agile software development is a high optempo process that delivers working software at "speed of need." It is highly collaborative, documentation light, and change resilient. Agile focuses short development iterations on priority needs of the customer; in the DoD, the customer is the warfighter. In this model, an iteration is typically 8 weeks or less in duration. This article proposes a means to adopt the DoD IT test, evaluation, and certification (TE&C) process to an Agile model that will ensure TE&C continues to be an enabler of rapid acquisition of enhanced IT for the warfighter.

"Agile Information Technologies"—what does that mean? Agile (with a capital "A") refers to a software development practice that follows the principles of the Agile Manifesto, of course. At this point, everyone with a smart phone should launch the browser and try that slick voice-command feature and check out what comes up. With a little luck, you'll find yourself at agilemanifesto.org. Looking down at the fine print at the page bottom, you'll notice that Agile is not a new idea—at least not new to industry; signed back in 2001, the principles of the Manifesto have been shaping software development for nearly 10 years. If that were only true of software development in the Department of Defense (DoD), I probably wouldn't be writing this article! By the way, there's a good chance that the apps you so readily find to enhance the capabilities of your smart phone were developed using Agile processes; I say that only because if they were developed using more traditional "waterfall" processes, they might not have been there for you to download when you needed them.

Steven J. Hutchison, Ph.D.

And that's the point, right—the capability is there when you need it. In this author's opinion, Agile is about delivery of capability at "speed of need." Agile focuses short development iterations on the *priority needs* of the customer. For those of us in the DoD acquisition arena, the customer is the warfighter, and there should be no doubt that our objective must be rapid fielding of enhanced capabilities to the warfighter. Hence, Agile would seem to be a "no-brainer" for the new DoD information technology (IT) acquisition process.

What *new* DoD IT acquisition process? By the time this article is published, it will have been over a year since the Congress directed the DoD to develop a new acquisition system for IT. The National Defense Authorization Act for FY2010, Section 804, directed the secretary of defense to implement a new acquisition process for IT and report back to Congress in 270 days (which would have been July 2010) with the Department's plans to implement the new process. Section 804 had some remarkably specific language, citing Chapter 6 of the Defense Science Board Report on Acquisition of IT (DSB-IT) (Defense Science Board 2009), published in March of 09, as the model to follow.

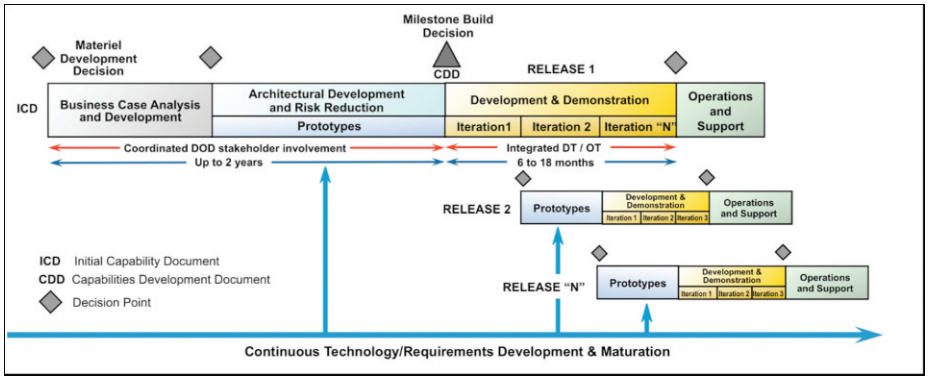


Figure 1. New acquisition process for information technology (Defense Science Board 2009).

So what did the Defense Science Board have to say? The DSB-IT concluded that current acquisition policies and processes (as defined in the DoD 5000 series directive and instruction) "cannot keep pace with the speed at which new capabilities are being introduced in today's information age—and the speed with which potential adversaries can procure, adapt, and employ those same capabilities against the United States" (Defense Science Board 2009). As we marvel at the pace at which new electronic gadgetry shows up in stores, in our cars, and even in our living rooms, it is clear that technological advancements are far more readily available in the commercial sector than in the DoD. Let's face it, if we could push blue force tracking data to the iPhone®, there would already be "an app for that™," and our digital generation soldiers, sailors, airmen, and marines would be using it on the battlefield right now. The DoD *can* improve agility in delivery of IT products. To that end, the DSB-IT recommended a new IT acquisition process that "… is agile, geared to delivering meaningful increments of capability in approximately 18 months or less, and leverages the advantages of modern IT practices" (Defense Science Board 2009). *Figure 1* depicts the DSB-IT model.

The DSB-IT model features are as follows:

- multiple, rapidly executed releases of capability,
- early and continual involvement of the user, and
- integrated testing.

These are all good and necessary features of an IT acquisition system and are at the core of Agile processes. But change is never easy in the DoD, so before we jump in with both feet and say "let's do Agile," we should first take measure of the potential obstacles, so we can successfully overcome them on the road to Agile IT.

Rapidly executed releases of capability are the objective. We hear a lot about rapid acquisition these days; in fact, the wars have been the source of greatest pressure to speed the process, since nothing can get to troops in harm's way fast enough. Our acquisition system today is characterized by cumbersome processes beginning with lengthy, over-specified requirements, which require lengthy, complex development efforts, followed by long, complex test events. We can't just substitute "rapidly executed releases" into the middle of this sequence and expect to have fixed the problem. To achieve rapid releases, we must have a requirements process that acknowledges and fosters evolving user priorities, and an equally agile test process. In other words, we can't focus only on the middle; we have to fix the whole process, end-to-end. Rapidly executed releases must have an underpinning in an agile requirements process; likewise, evolving requirements (read "user priorities") will demand more from our testers than we are currently structured to support. For IT capabilities, getting to Agile will stress the existing testing processes; in fact, the current approach will not work in the Agile IT environment. More on that later.

Early and continual involvement of the user is essential. However, this can be problematic for a Department at war—we simply may not be able to routinely task operating forces to support testing. We are going to have to be imaginative in how we conduct testing; leveraging exercises, experiments, and other venues. We will have to find ways to overcome the tension between testing and training to ensure mutual achievement of objectives. For Agile IT, we will need a user base (beta testers) from each IT community of interest that we can routinely draw from to conduct testing. With a sufficiently large pool of users to draw from, and leveraging other nontraditional test venues, including virtual testbeds, we should be able to overcome the challenges of high optempo deployments and test support.

Integrated testing has been a topic of discussion for decades. Some argue that we've been doing integrated

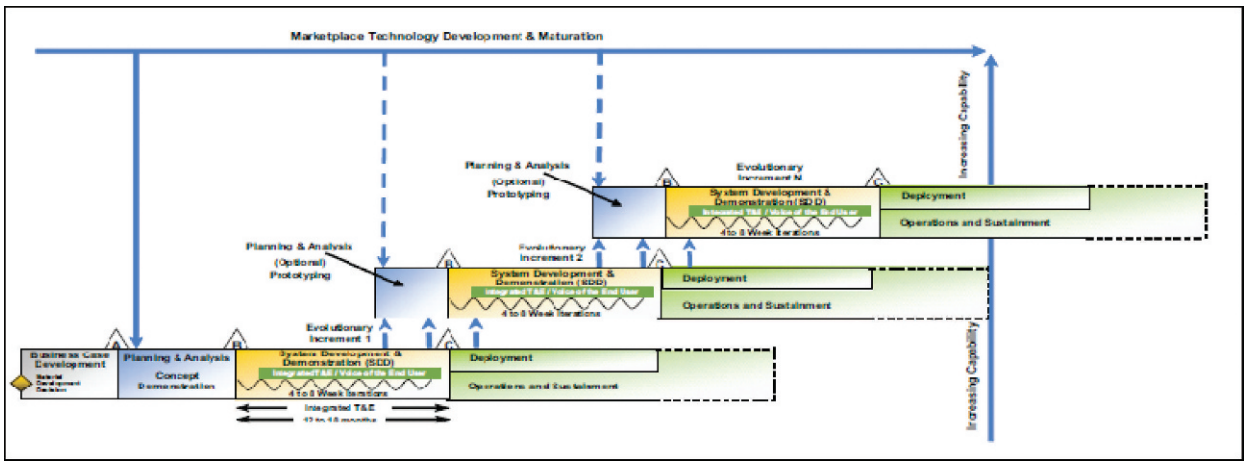


Figure 2. Information technology acquisition management approach (National Academies of Sciences 2010).

T&E all along, others that we need to start doing it. Unfortunately, we have not defined what integrated testing means for IT capabilities. In early 2008, the DoD defined "integrated testing" as, essentially, collaboration between the developmental test (DT) and operational test (OT) communities (https://acc.dau.mil/CommunityBrowser.aspx?id=215765). For IT, that's only half the testers needed; integrated testing of IT involves not only DT and OT but also must include joint interoperability testing and security testing (information assurance). But why do we place all this emphasis on integrated testing? The motivation behind integrated testing is "early involvement" *of the OT community*; as the perception is that the OT folks begin T&E planning late in the process, so developers don't understand how their product is going to be tested once OT starts, and this often results in late discovery of key failure modes, causing further cost and schedule delay. Early involvement is the key to reversing this trend; hence, the mandate for "integrated testing." Integrated testing is really about *testing the capability as it is intended to be used*, and the sooner this starts, the better. In Agile software development, understanding how the capability will be used and tested is the motivation behind the practice known as "test driven development" (Beck 2002). For the DoD to adopt this approach, all of the test, evaluation, and certification (TE&C) organizations (DT, OT, interoperability, and security) will have to bring their needs to the table and make every test event a shared resource. There are, however, strong cultural barriers to this in the DoD, and it is clearly one of the obstacles we must remove to be successful at Agile.

The National Academies study

The DSB wasn't the only group looking at acquisition of IT. DISA sponsored a study by the National Academies of Sciences who released their final report in June 2010 (National Academies of Sciences 2010). *Figure 2* is the study committee's version of an acquisition management approach for IT. The study committee refers to the overarching process as "iterative, incremental development," and their model is generally consistent with the DSB-IT, including the three central points just reviewed: rapid release of capability, continuous user involvement, and integrated T&E. Yet there are also some notable differences. *Figure 3* shows the central part of this model in detail. Notice the green banner "integrated T&E/Voice of the End User." The committee is making an important distinction between integrated testing (as described in the DSB-IT report) and integrating testers and users; that is, it is not enough to know that the system meets requirements, it is equally important to know whether the user thinks the iteration delivers militarily useful capability. Another distinguishing feature of the model is the "sine wave" with the words "4 to 8 Week Iterations" written beneath. Each peak-to-peak transit of the wave represents a complete software development iteration, or "sprint." These sprints are obviously considerably shorter than the DSB-IT's nominal 6-month iterations, and a lot closer to commercial Agile practices. *Figure 4* shows the details of the wave, and as described in the report, "Each iteration will include analysis, design, development, integration, and testing to produce a progressively more defined and capable,

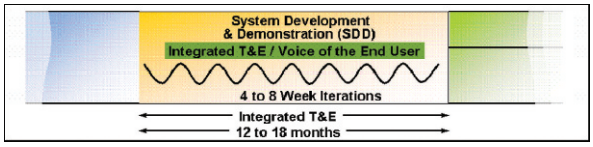


Figure 3. Capability increment in detail (National Academies of Sciences 2010).

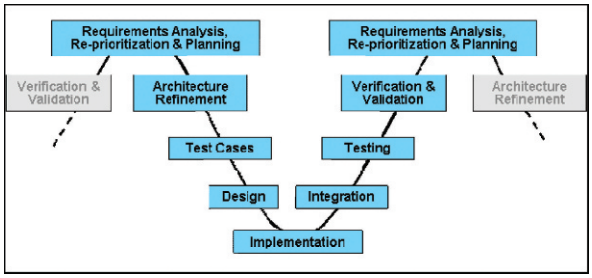


Figure 4. Key elements of the iteration (National Academies of Sciences 2010).

fully integrated and tested product" (National Academies of Sciences 2010). The wave is obviously very similar to what we know as the systems engineering "V," but with several key differences. As we begin following the process down the left-hand side of the V, the iteration begins with requirements analysis and architecture refinement—the latter being an essential consideration for IT. This model then inserts "Test Cases." Note its placement on the left-hand side of the V, before design and coding begins. Here testers translate "user stories" (a description of how the capability is used) into executable test cases. This is "test driven development" and is by definition "early involvement" when *all* testing stakeholders participate in writing the test cases.

Continuing through the iteration, design and build begin, and then "Testing" occurs on the right side. This is *independent* testing with users, not developer testing, but should be understood to be a team effort of all TE&C stakeholders. In the words of the study committee (National Academies of Sciences 2010),

> *"Therefore, an integrated approach to T&E to include the voice of the end user; traditional [DT&E]; [OT&E]; interoperability certification; and information assurance certification and accreditation equities is a fundamental element of this modified acquisition management approach for IT programs. As was the case with the requirements process, this implies a profound change in the T&E process used for such programs."*

Complete integration is the key to T&E at the speed of need.

The current DoD information technology TE&C environment

Our current test and certification process does a good job at helping users and decision makers understand capabilities and limitations, but it can be lengthy, costly, and duplicative. It is not agile. *Figure 5* depicts a high-level view of the Plan-Test-Report (PTR) cycle for IT TE&C. This PTR cycle can take 6 months, although it can be shorter or longer. As the diagram indicates, DT, OT, interoperability, and security testing can and often do occur as separate events, with their respective test teams performing separate analyses and producing separate reports. The process concludes as the various reports inform the milestone decision authority's acquisition (procurement) decision, the Joint Staff J6 interoperability certification, and the designated approving authority's information assurance accreditation. It is a kludge of IT considerations overlaid on a weapons-based acquisition system—but—just as for weapons and major platforms, when it takes years to develop and deliver a new IT capability, this process works. It is just not well suited for Agile IT. What we need is a TE&C model that is fully integrated, less duplicative, less costly, and ultimately one that fuses all test information into a coherent evaluation, so that decision makers better understand capabilities and limitations when making decisions about deploying the capability. What we need is an Agile testing model.

Agile for DoD

So what might an Agile IT acquisition process look like, aside from the DSB-IT's notion of "18-month releases subdivided into iterations"? Agile software development is a high optempo process that delivers working capability at speed of need. It is highly collaborative, documentation light, and change resilient. *Figure 6* depicts an Agile capability development life cycle adapted from the "Scrum" framework for iterative, incremental development. There are many

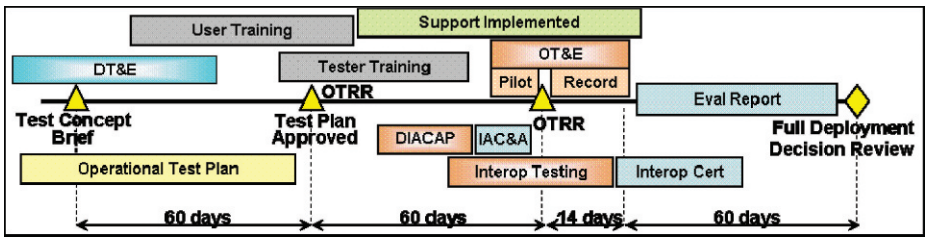


Figure 5. Test, evaluation, and certification of Department of Defense information technology.

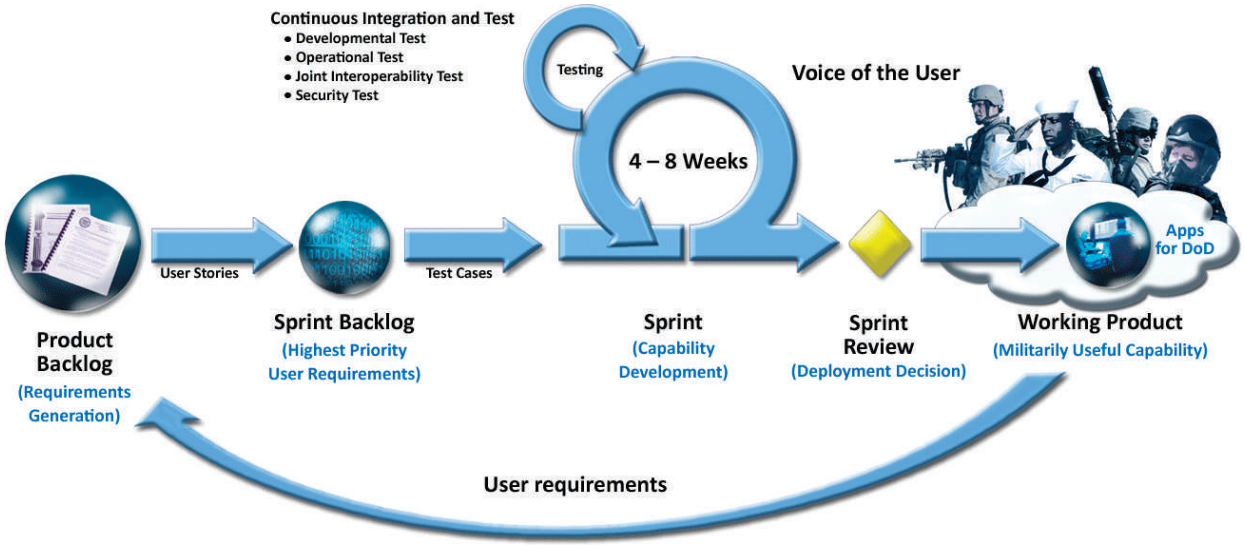


Figure 6. An agile development life cycle adapted for the Department of Defense.

sources of information on Scrum (www.scrum.org) and the Agile life cycle (www.ambysoft.com). Scrum succeeds through team member commitment and by removal of impediments; it enables The Team (a cross-functional group with necessary expertise to deliver a potentially deployable product at each sprint) to self-organize and achieve "hyper-productive" results.

In the model depicted in *Figure 6*, the key stages are "time-boxed," so that development can be accomplished at a sustainable pace. The "product owner" is responsible for articulating the product vision and identifying features in priority order (the commercial sector refers to this list of features as the product backlog). In the DoD, the operational sponsor would likely fill the role as product owner. In Agile, the product backlog evolves over time with priorities updated as features are added and removed to reflect the emerging needs of the customer. This is a critical distinguishing characteristic of Agile software development; resilience to change means that a change in the warfighter's priorities or needs could be just *one sprint away* from delivery.

The Agile process values working software over lengthy documentation (per the Agile Manifesto); therefore, to follow this development practice, we will need to revise the DoD requirements generation process to shift away from rigid requirements definition expressed in capability development documents written years before a product is delivered,[1] to a flexible, priority-driven process responsive to the changing needs of the warfighter. Our interoperability and information assurance certification processes also have to be revised for Agile IT. Likewise, since test activities will be responding to prioritized requirements at each sprint, it is unlikely that we can adequately describe test objectives, scope, and resources as we currently do in a Test and Evaluation Master Plan (TEMP), so we will need to shift the emphasis on detailed descriptions in the TEMP (objectives, scope, and resources) to well-crafted test cases in each sprint.

In the next step, The Team, not the product owner, selects the features from the product backlog that they can commit to develop during the sprint (keeping in mind that the duration of the sprint is a fixed period of time), taking the highest priority items and working down the list. Before The Team can make the commitment, they have to translate user stories into tasks and test cases to better understand the level of effort required to deliver each feature in the product backlog. In this way, The Team takes ownership of the development effort, while assuring the product owner that the highest priority items are included. This short list of priority features constitutes the sprint backlog.

A user story can be described by the simple statement, "As a *role*, I want to *what*, so that *why*." For example, "As an operator, I want to display current blue force locations, so that I have better situational awareness." In the DoD, a "mission thread" is likely to contain numerous user stories. The user story is further decomposed into tasks, and test cases are written before the sprint begins. This is the "test driven development" practice referred to earlier. Test driven development has shown that when developers understand how the capability will be tested, the resultant code has fewer defects. For the DoD, this is the type of early involvement we have been struggling

to achieve; if we can get the complete team of government testers (developmental, operational, interoperability, security) involved this early, we should be able to significantly improve the quality of the product and reduce time to deployment.

In this model, a sprint is typically 8 weeks or less in duration. Once the sprint begins, the product owner cannot change the priorities; any changes will be addressed in the next sprint. During the sprint, items in the sprint backlog are developed and continuously integrated and tested. In the commercial sector, this typically includes unit testing, acceptance testing, and exploratory testing. For the DoD, "Agile Testing" must accommodate the functions performed by government developmental testers, operational testers, joint interoperability testers, and information security testers—but these efforts are integrated and continuous, not separate and serial. When the sprint is complete and working software is ready, a sprint review is conducted at which all stakeholders are present, the capability is demonstrated, and the decision made whether or not to deploy the product.

Agile testing

To shift the DoD IT test and certification paradigm to be responsive to Agile IT programs, we need to move away from the "who does what, when" process (e.g., program manager does DT, the OTA does OT) to a collaborative model built upon shared data and reciprocity of test results that is ultimately an enabling process for delivering working capability. Let's take what's good from our process shown in *Figure 5* and collapse it into a responsive, on-demand, "testing as a service" construct. In other words, let's test smart.

To set the conditions for success of Agile Testing, we must first move away from the linear, serial processes that characterize development and test today. The Agile environment is iterative and collaborative; it exploits the principles of the Manifesto to achieve desired effects. An empowered team can reduce lengthy coordination cycles for document approvals, readiness reviews, etc. Likewise, a team approach will reduce duplication during test execution and publish more comprehensive findings on capabilities and limitations. Empowerment is critical to rapid development and deployment of working capability.

Next there are three key elements in our current *(Figure 5)* process that we must make *persistent* resources in the Agile life cycle; these include user training, tester training, and support structure (help desk). The help desk, as it is intended to support operations, must be in place during every development iteration. Also, since early and continuous involvement of the users is fundamental to success in the Agile environment, we will need to establish a pool of knowledgeable users (beta testers) from each community of interest (C2, business, intel, etc.) to ensure that we can obtain an adequate number of users to test. Likewise, to support the high test optempo, we must be able to draw from a cadre of testers knowledgeable in the systems and services in the capability area, representing all TE&C disciplines. This cadre must be able to engage early, be responsive to evolving user priorities, and execute the PTR cycle in highly compressed time lines.

Not shown in *Figure 5* are additional factors required to support Agile projects, including training our acquisition workforce, providing an enterprise knowledge management capability, and implementing a persistent integration and test environment. As part of improved training for the IT workforce, we need to update our curriculum in the Defense Acquisition University to better prepare our program managers and testers for IT programs in general, and Agile practices in particular. We need a project dashboard for IT programs that provides comprehensive and transparent knowledge management capabilities for all stakeholders. The DoD has spent considerable dollars funding programs in a way that allows them to build their own program-specific system integration labs (SILs). This strategy has failed; in fact, the plethora of SILs has only aggravated the Department's interoperability crisis. A new approach is needed. For example, instead of funding new programs to build more SILs, let's fund a select few SILs across the DoD to serve as a common development, integration, and test environment, and federate them together to ensure access as a shared resource. DISA is providing one such environment in Forge.mil (www.forge.mil), and within this virtual environment, the TestForge.mil will provide robust capabilities for users and testers to ensure capabilities perform as desired. The degree to which we can provide a common environment, common test tools, common methods, data collection, etc., will help all phases of the development process become more agile. A common development, integration, and test environment may eventually provide the foundation for "apps for DoD," similar to the app stores we see supporting our favorite gadgets.

The traditional PTR activities depicted in *Figure 5* can be adapted to the Agile environment, and each has a role; we don't sacrifice rigor in Agile testing. The Capability Test Team $(CTT)^2$ merges and consolidates these PTR activities but does so in a manner that enables each stakeholder to accomplish their evaluation objectives. The CTT is engaged from the outset; so as requirements are prioritized for each sprint, the team translates user stories into test cases. Test cases are risk

based and mission focused, and they address relevant technical parameters, operational issues, interoperability measures, and security measures. In Agile processes, test execution relies more heavily on automation, such as load simulators. Defects that cannot be corrected during the course of the sprint are returned to the work stack; working software is eligible to be fielded. Following the test, the CTT posts the evaluation report to the dashboard, with findings that state whether the capability is effective, suitable, interoperable, and secure. In 8-week iterations, the PTR cycle should be completed in 6 weeks. A single evaluation report could support the acquisition decision, interoperability certification, and the information assurance certification and accreditation. Last, we should modify the deployment decision. Rather than a "full deployment decision review," we should adopt one where we "start small and scale rapidly," with testers in a continuous monitoring role. In this way, we can ensure the capability effectively supports operations at scale, or take corrective actions should a problem arise.

Summary

A new IT acquisition system is coming to the DoD that will feature much higher optempo in development, testing, and fielding. As we evolve our acquisition process to deliver capabilities at the speed of need, test, evaluation, and certification will need to adapt processes to this new environment. The Agile environment will require a capability test team that is empowered to execute the plan-test-report cycle and provide objective assessments of key technical, operational, interoperability, and security metrics necessary for decision makers to understand capabilities and limitations. Key to the approach is to treat all test activities as a shared resource, while being mindful of each test organization's roles and responsibilities. Continuous user involvement, combined with appropriate risk-based, mission-focused testing will ensure TE&C is an enabler of rapid acquisition of enhanced information technologies for the warfighter, and this in turn will help ensure the critical apps that warfighters need are there when they need them. ❑

STEVEN HUTCHISON, Ph.D., is the Test and Evaluation Executive, Defense Information Systems Agency. He is a certified ScrumMaster. E-mail: steven.hutchison@disa.mil

Endnotes

[1]The Defense Science Board Report on Policies and Procedures for the Acquisition of Information Technology, March 2009, reported "… an average of 48 months to deliver useful functionality from the Milestone B decision…."

[2]The capability test team members are empowered representatives of all test and certification organizations and the user community.

References

Beck, Kent. 2002. *Test driven development: by example*. Boston, MA: Addison-Wesley Professional.

Defense Science Board. 2009. *Department of Defense policies and procedures for the acquisition of information technology*. http://www.acq.osd.mil/dsb/reports/ADA498375.pdf (accessed October 7, 2010).

National Academies of Sciences. 2010. *Achieving effective acquisition of information technology in the Department of Defense*. Washington, D.C.: The National Academies Press. http://www.nap.edu/catalog.php?record_id=12823 (accessed October 7, 2010).

ITEA Journal 2010; 31: 466–472

Information Assurance Test and Evaluation Policy Crosswalk for Defense Acquisition Programs

Peter H. Christensen, Susan May, Vijay Rachamadugu, and Robert K. Smith
The MITRE Corporation, McLean, Virginia

This article provides a summary and commentary regarding a recently conducted review of Department of Defense Test and Evaluation (T&E) policy and guidance for Information Assurance (IA) by a DoD working group. The policy review produced several key findings and recommendations, and follow-on actions are in progress to address them. The study confirmed long-standing concerns expressed by the T&E community regarding the need for better IA policy and also identified other concerns beyond the scope of T&E, including IA workforce qualifications, IA requirements definition, IA systems acquisition, contracting and systems engineering, and the need for realistic operational environments to evaluate end-to-end IA and computer network defense capabilities. Material from this entire review is available at: www.acq.osd.mil/dte/docs/IA_Cross_Walk_WG_Report-3-30-10.pdf.

Key words: Acquisition life cycle; computer network defense; contracting; Department of Defense; developmental testing; information assurance; operational testing; platform IT; policy; system engineering; test and evaluation.

This article is based upon a study that was sponsored by a number of U.S. Department of Defense (DoD) test and evaluation (T&E) stakeholders and subject matter experts (SMEs). The study was executed because of the concerns expressed by the Service T&E executives regarding duplication of effort, inefficiencies, and ineffectiveness associated with the standing DoD security certification and accreditation (C&A) processes. As a result, an information assurance (IA) policy Test and Evaluation Working Group (TEWG) was established to review the DoD policy and guidance that drives T&E requirements for IA in acquisition programs.

The review focused on identification of issues that were contributing to failures observed by IA T&E Operational Test (OT) Agencies. Findings were grouped into five categories: (1) General findings; (2) Requirements definition, T&E, systems engineering (SE), and process execution; (3) Platform information technology (PIT); (4) Contracting; and (5) Realistic IA and computer network defense (CND) T&E environments and resources (see *Table 1*).

The TEWG then looked at policy, guidance, and best practices to identify collaborative, integrated IA T&E process to address the full spectrum IA and CND acquisition testing, including all phases of testing. In addition, the team reviewed emerging industry guidance to address mission assurance and systems assurance activities such as Supply Chain Risk Management (SCRM). It was acknowledged that IA must be addressed across the acquisition life cycle beginning with the Joint Capability Integration and Development Systems (JCIDS) process, Systems Engineering Plans (SEP), and Concept of Operations (CONOPS), contracts, contract deliverables, and program reviews. The top level IA activities in the acquisition life cycle are depicted in *Figure 1*.

Findings and recommendations

There was strong agreement among members of the TEWG that IA requirements are documented in many different policy and guidance documents with no concise, overarching, or definitive direction. The JCIDS requirements generation process is specified in the Chairman of the Joint Chief of Staff Instruction (CJCSI) 3170 series. IA and DoD IA Certification And Accreditation (DIACAP) requirements are described in the DoD Instruction (DOD/I) 8500 series.

*Table 1. Impediments to successful information assurance and computer network defense test and evaluation outcomes**

1	**General findings**
	IA policy and guidance needs clarification
	Workforce needs more qualified people with requisite IA acquisition and testing skills.
2	**Requirements definition, T&E, systems engineering, and process execution**
	IA requirements with thresholds and criteria are not identified early and are a critical pre-requisite for system development and T&E.
	JCIDS capability documents do not clearly articulate IA requirements.
	The Joint Staff NR-KPP is focused on process execution rather than technical IA requirements.
	IA policies and procedures are not integrated with the SE process.
	IA is not addressed in PDRs and/or CDRs.
	IA policies and procedures are, in general, focused on the acquisition process beyond Milestone B.
	Requirements documents do not consistently identify which IA controls must be implemented into the system and which controls will be inherited from, and/or integrated into, the supporting enclave.
	In practice, there is a misconception that satisfying C&A technical IA requirements and subsequently achieving ATO is sufficient to support fielding.
3	**Platform IT**
	DoD IA policy does not adequately address PIT, leading to confusion among acquisition program managers and testers.
	DOD 8500 series of documents exempts PIT without a GIG connection from DIACAP, but these systems are still subject to DOT&E IA OT procedures, creating conflict between program managers and testers.
4	**Contracting**
	IA requirements are not consistently included in the contracting or SOW language.
	IT supply chain and other IA risks are not adequately addressed.
5	**Realistic IA/CND** T&E environments and resources
	Realistic operational environments containing representative threats are not consistently used to evaluate end-to-end IA and CND capabilities.

IA, information assurance; T&E, testing and evaluation; JCIDS, joint capability integration and development systems; NR-KPP, net-ready key performance parameter; SE, systems engineering; PDR, preliminary design reviews; CDR, critical design reviews; C&A, certification and accreditation; ATO, authority to operate; IT, information technology; DoD, Department of Defense; PIT, platform IT; GIG, global information grid; DIACAP, DoD IA certification and accreditation; DOT&E, director, operational test and evaluation; OT, operational test; SOW, statement of work; CND, computer network defense.

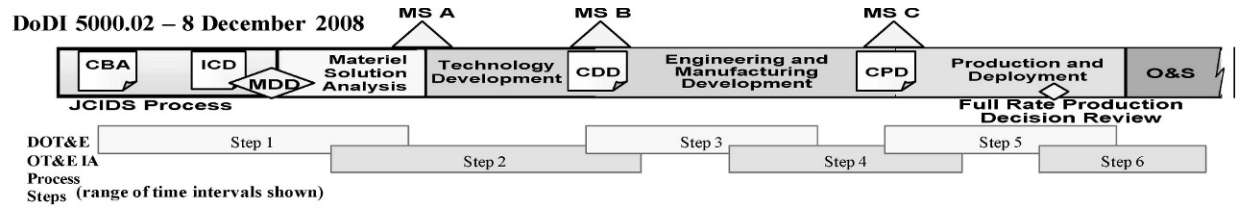
Note: The issues above are grouped by categories, but are not listed in any priority order; also, individual issues may not exist for every acquisition program, or in the practices of all Services and Components.

Director of Operational Test and Evaluation (DOT&E) guidance describes the IA and CND OT process and is currently promulgated as a six-step process that is incrementally executed to provide oversight to IT and NSS programs as they move through the acquisition and T&E process. However, the DOT&E Six-Step process *(Figure 2)* is not codified in DODI 5000.02. Initial IA OT steps seek to verify that system developers plan for and incorporate the proper suite of IA capabilities into the planned material solution. The final steps of the IA OT process are operationally focused to validate that the system and supporting enclave can protect, detect, react, and be restored when a threat is realized. The entire system of systems must collectively function together such that the mission can be executed as described in the Initial Capabilities Document (ICD) and CONOPS.

Adding to the confusion, some IA capabilities are developed specifically for the system being acquired. Other IA capabilities may be inherited from the supporting enclave providing IA services (e.g., Public Key Infrastructure [PKI], patch management, and CND services). The Capabilities Based Assessments and the ICD were found to lack sufficient detail to establish the baseline IA capabilities for the new system or to determine what IA capabilities would be inherited from Computer Network Defense Service Providers (CNDSPs). The DOD Architecture Framework products mandated for systems in the DODD 4630.05 *Interoperability and Supportability of IT and NSS*, and CJCSI 6212 series *Interoperability and Supportability Certification of IT and NSS*, do not provide sufficient insight into required IA capabilities or the inherited capabilities.

To address these issues, the TEWG recommended:

- The JCIDS process should include the requirement to identify and document the Mission Assurance Category (MAC) and Confidentiality Level (CL) assignment of all IT NSS as defined in the DoD Directive/Instruction (DODD/I) 8500 *Information Assurance* series, and to include identification of the Tier III and Tier II CNDSPs, as defined in DODD 8530 *Computer Network Defense*.
- These requirements should be included in the ICD for the DODI 5000.02 Material Development Decision (MDD). If the CNDSP is not



Pre MDD	Pre MS-A	Pre MS-B	Post MS-B	Post MS-C
IA Processes				
JCIDS Process	Materiel Solution Analysis	Technology Development	Engineering and Manufacturing Development	Production and Deployment
Preliminary risk assessment	PPP-Identify CPI, perform MDCI threat assessment	Develop IA input to system acquisition and engineering documents	Perform IA standards conformance, sub-component & software qualification testing	Perform final integrated interoperability, IA & CND, DT&OT testing
Identify & develop IA requirements	PPP-Identify vulnerabilities, perform risk analysis, determine countermeasures	Develop IA & CND performance criteria	Perform DIACAP IA assessments & operational IA vulnerability evaluation	Perform DIACAP IA assessments
Information system categorization - MAC and CL	PPP-Define measures for countermeasure effectiveness	Initiate DIACAP and planning for C&A	Perform preliminary integrated interoperability, IA & CND, DT&OT testing	Perform CNDSP penetration/exploitation performance assessment
Develop Interoperability & IA architecure for NR-KPP	Verify CNDSP & architecture	Develop IA, CND, systems interoperability design	Conduct operational assessment (OT-B)	Conduct IOT&E
Identify CNDSP & architecture	Define IA operations (CONOPS)	Develop IA & CND DT & OT, interoperationbility T&E plan		Verification of correction of deficiencies
	IA systems engineering design analysis	Develop competitive prototypes or prototype the system		
	Identify IA inputs to net-centric and data management strategies	Perform early operational assessment (OT-A)		
	Develop Technology Development Strategy (TDS) to mature to TRL 6	Conduct prototype IA assessments		
	Develop IA TES	Conduct DT IA assessements		
	Establish IPT			
	Establish ITT			
Documentation				
Initial Capabilities Document (ICD)	Program Protection Plan	Test and Evaluation Master Plan (TEMP)	IA test results	Residual risk acceptance reports
DIACAP-IA Acquisition Strategy	Refine IA Acquisition Strategy	Integrated DT/OT test plan	Interim residual risk results	Final residual risk acceptance report
	Technology Development Strategy	Configuration Management (CM) plan		
	Test and Evaluation Strategy	Contract data requirements list		
	Systems Engineering Master Plan	Statement of Work (SOW)		
		DIACAP C&A plan		
Program and Technical Reviews				
	Initial Technical Review (ITR)	System Requirements Review (SRR)	Critical Design Review (CDR)	Assessent of Operational Test Readiness (AOTR)
	Alternative System Review (ASR)	Integrated Baseline Review (IBR)	Test Readiness Review (TRR)	Operational Test Readiness Review (OTRR)
		System Functional Review (SFR)	System Verification Review (SVR)	In-Service Review (ISR)
		Preliminary Design Review (PDR)	Physical Configuration Audit (PCA)	Post Implementation Review (PIR)
				Full Rate Production Decision Review (FRP DR)

Figure 1. Recommended information assurance and computer network defense process in the acquisition cycle.

known Pre-MDD, a requirement should be established for validation of the CNDSP as entrance criteria for the Technology Development Phase to ensure that the information is obtained prior to MS-B and incorporated in the Capability Development Document (CDD).

- The CJCSI 6212 *Interoperability and Supportability Certification of IT and NSS* document should be modified to require that the MAC and CL assignments, and the Tier II and III CNDSPs be documented in the ICD, CDD, and Capability Production Document (CPD).
- DODI 5000.02 should reference and mandate DOT&E IA guidance, which articulates system requirements to the system acquisition process and Program Manager (PM).
- DoD IA curricula should be reviewed to identify gaps in IA training. Training and certification should be added to the DAU curricula for acquisition professionals, and to SE curricula where required to address the gaps. IA training should address the knowledge and skills needed for acquisition program testing, including early phases of systems acquisition and the use of IA Integrated Product Team (IPT), Integrated Test Team (ITT), and IA testers and penetration/exploitation testers. Assurance disciplines, such as IA risk and threat analysis, software assurance, and SCRM also should be emphasized.

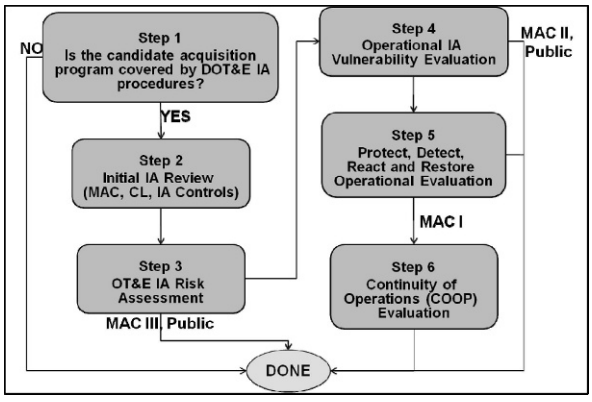


Figure 2. Summary of Director, Operational Test and Evaluation Six-Step Process.

Requirements definition, test and evaluation, systems engineering and process execution

IA requirements are a critical precursor to contracting, SE, and T&E. Capabilities documents and DODD/I 8500 Certification and Accreditation

(C&A) requirements establish qualitative IA performance attributes, such as measures and metrics that must be satisfied during system development and development testing (DT), and certified during the security C&A process. However, capabilities documents usually establish only minimal IA requirements.

The gap between the technical standards defined in the DODD/I 8500 series and the required operational capabilities should be closed or narrowed by earlier definition of operating concepts, operational capabilities, and technical requirements. DOT&E has mandated the IA OT process to evaluate the operational effectiveness of IA in acquisition programs. In order to evaluate operational effectiveness and suitability, DOT&E's suggested framework for IA and CND evaluation includes issues, measures, and metrics that are beyond the performance attributes identified in capabilities documents and the DIACAP requirements. The IA operational requirements should be developed in collaboration with IA systems engineers and an ITT to confirm that the requirements are technically achievable and operationally relevant.

Additional TEWG recommendations include the following:

- An ITT consisting of representatives from the developmental, operational, security, threat and interoperability, and T&E communities should be established as early as possible in the acquisition process. The ITT should work closely with the development team to plan for an integrated DT and OT to the extent feasible. The collaboration of the ITT members is critical to achieving the vision of "test by one, accept by many." The ITT should be an active participant in the SE process and participate in program and technical reviews.
- IA capabilities and requirements should be addressed in the early SE Technical Reviews (SETRs) and translated into robust system requirements, RFPs, and the IT system preliminary design. Translating IA requirements into system requirements and specifications early on will ensure more positive T&E outcomes during later acquisition test phases.
- In order to evaluate end-to-end IA capabilities, IA T&E criteria should include minimum technical thresholds such as measures of performance (MOP) and measures of effectiveness (MOE) that address the operational criteria suggested in the DOT&E Six-Step process.

Platform information technology (PIT)

PIT was an area of confusion and concern for members of the TEWG. The DODD/I 8500 series of documents exempt PIT systems without a Global Information Grid (GIG) interconnection from the IA DIACAP process; however, these same PIT systems are not exempt from implementing appropriate IA controls per DODD 5000.01, nor are they exempt from DOT&E IA OT processes. PIT interconnections (PITI) are not exempted from the DIACAP process. PIT and PITI are addressed in the DODD/I 8500 series but are not addressed in DODD 5000.01, leading to misinterpretation of the PIT exemption as an exemption from applicable IA controls for the subject system. If such an exemption of IA controls is assumed for PIT, an exemption from C&A of PIT systems can be implied. In addition, IA and CND information security issues may not be identified until OT&E. Discovering vulnerabilities during OT&E limits the flexibility of mitigation solutions and potentially increases the cost associated with remediating these vulnerabilities.

PITI exposes systems to IA and computer network attack (CNA) risk. A PITI has readily identifiable security considerations that must be addressed both in acquisition, and operations prior to DOT&E IA operational testing. Examples of PITIs that impose security considerations include communications interfaces for data exchanges with enclaves for mission planning or execution, remote administration, and remote upgrade or reconfiguration.

TEWG recommendations include:

- DODD 5000.01 policy should clarify the need to address PIT IA and C&A requirements.
- DODD/I 8500 series policy should provide additional clarification regarding PIT, specifically as it relates to non-interconnected PIT, and to identify the authority responsible for making a determination that an IT component is PIT.
- DODD/I 8500 series policy should eliminate the blanket PIT exemption in the DIACAP process and reinforce DODD 5000.01 by enforcing the establishment of IA requirements for PIT via the MAC and CL assignments, and requiring IA system C&A. In other words, PIT is DIACAP exempt, but not exempt from IA controls or C&A activities.
- A process should be created that determines criteria for defining
  - whether MAC and CL assignments are required;
  - IA controls that should be required, engineered, and applied;
  - process to certify PIT controls;
  - PIT requirements for Net-Ready Key Performance Parameter (NR-KPP); and

- interoperability test certification requirements for PIT.
- The CJCSI 6212 *Interoperability and Supportability Certification of IT and NSS* should be modified to explicitly address PIT and how it should be handled by the acquisition and testing communities.

Contracting

If the correct requirements are not defined up front and included in the contract, then there is little chance of successful T&E at the end of the acquisition. IA and MA requirements definition begins prior to MDD and includes identifying MAC and CL, developing IA objectives, identifying CND architecture, and performing a preliminary risk assessment. Similarly, there are multiple IA-related activities in subsequent phases. Typically the government issues multiple contracts during the subsequent acquisition phases (e.g., for Materiel Solution Analysis Studies; Competitive Prototypes; Technology Development, Engineering, and Manufacturing Development, Production, and Development; and Operations and Maintenance). Due to multiple phases and contract vehicles, many system acquisitions do not contain sufficient IA and MA requirements definition or contractual language to ensure that a secure, effective, and survivable system is built and fielded. In addition, contracts are often prepared by government staff without advice and assistance from IA SMEs who can ensure that appropriate IA requirements and CDRLs are placed on contract.

To address these issues, the following TEWG recommendations include:

- Government staff should be augmented with IA SMEs to ensure that appropriate IA requirements and CDRLs are placed on contract. IA SMEs should be involved in RFP development, source selection, contract negotiations, and contract monitoring.
- RFPs and contract documents should include explicit language addressing both technical and operational IA requirements. These include system specifications RFPs, contracts and systems assurance (SA) requirements to include SCRM, software assurance, and IA standards implementation (e.g., Federal Information Processing System [FIPS] compliance, Common Criteria).
- Measureable and meaningful IA and CND outcomes should be attached to each milestone decision point. The National Defense Industrial Association (NDIA) System Assurance Committee 2008, *Engineering for System Assurance* document provides recommended topics to be included in contract language.
- The RFP Statement Of Work (SOW) should direct contractors to address IA during preliminary design reviews (PDRs), critical design reviews (CDRs), and all technical reviews, and to participate in the ITT.

Realistic information assurance and computer network defense test and evaluation environments and resources

If the correct requirements are identified on contracts up front, then qualified personnel and resources are also needed to execute IA T&E at the end of the process to confirm that requirements are satisfied. Typically, acquisition T&E support is provided through Services and Components, via a Red Team that will need to adapt their capabilities to meet the acquisition requirement. Their operational responsibilities frequently limit their ability to participate, and their assessment methodologies do not always supply the independent and objective data required for independent evaluation.

Recommendations include the following:

- A single joint and integrated IA and CND T&E methodology included in DODI 5000.02 and amplified in the *Defense Acquisition Guide* (DAG). The T&E methodology should include clearly enumerated T&E objectives and required data needed to accurately measure and evaluate system IA and CND capabilities. Defining Step 5 OT&E process and procedures is particularly important for realistically portraying the cyber threat.
- The Intelligence Community (IC) and other responsible organizations must provide the T&E community and supporting activities with current threat characterization information as applicable to all phases of acquisition and T&E and update it periodically. The responsible supporting information operations organization needs to have coordinated their threat portrayal with the supporting IC organization and be able to lay out the Tactics, Techniques and Procedures (TTP) and application of that threat to the T&E and acquisition communities.
- Acquisition-related IA and CND T&E should be recognized as a critical activity to ensure the security of DoD systems, and stated as such in DODD 8500.1, DODI 5000.02, and the DAG.

- Designated information operations, intelligence, emerging cyber, and other organizations with the responsibility for supporting acquisition T&E requirements should provide timely and sufficient services that portray operationally realistic threats and employ techniques that will satisfy T&E adequacy requirements during T&E events. Services and Components should examine how these supporting threat portrayal services are delivered and determine if acquisition IA and CND T&E requirements can be adequately addressed by existing means. If it is determined that the unique capabilities needed to support acquisition T&E are not efficiently addressed by existing means, then Services and Components should consider establishing IA and CND T&E capabilities with the dedicated purpose of supporting IA and CND acquisition T&E.
- The acquisition T&E community should ensure that testing associated with Step 5 of the DOT&E Six-Step process is performed in the operational environment in which the System Under Test (SUT) will reside after fielding. If the operational environment cannot be used, substitute a realistic environment. This environment should be proposed in the Test and Evaluation Strategy (TES) and Test and Evaluation Master Plan (TEMP) and, if appropriate, approved by OSD.

Conclusion

The Director DOT&E, Dr. Gilmore, and the new AT&L Deputy Director for DT&E, Mr. Greer, agreed with the key recommendations in the report and have taken action to collaboratively make changes to IA T&E policy. Additional major recommendations include the following:

- updates to DoD IA training policies to address support expertise needed for acquisition and T&E processes;
- updates to Joint Staff and DoD Instructions to address the review of IA capabilities and requirements early in the SE process;
- updates to Joint Staff, DoD, and OSD-NII policy and instructions to address technical and operational IA requirements, including CND and NR-KPP;
- updates to DoD policies to address PIT; and
- updates to contracting processes to include IA requirements and to address SCRM.

The specific policy change recommendations have been forwarded to appropriate policy makers for action.

It is critical to emphasize that policy is just paper and what is needed is collaboration between the Capabilities Development, Acquisition Program Managers, Security Certification and Accreditation, and Test and Evaluation Communities to take the required action to apply this policy to acquisition programs. These communities must get involved early in the acquisition process and stay involved throughout the conventional DoD 5000 system development life cycle. Integrated Test Teams involving all stakeholders will help streamline the process. Note that these recommendations must also be considered for the newly proposed accelerated acquisition process for IT systems.

In conclusion, more robust execution of IA processes throughout the system life cycle will help to drive the development of new technologies, which will help to improve the robustness and resiliency of net-centric systems. As new technologies (e.g., Virtualization, Service Oriented Architecture, and Cloud Computing) are introduced, IA and CND policy and processes must be supportive. Attacks will inevitably occur, and new technologies will help the warfighter to respond to sustain continuity of operations and execute the mission. ❑

Peter Christensen is a Senior Principle Engineer with over 30 years experience supporting naval programs. He currently oversees MITRE support to naval sea programs. E-mail: pchris@mitre.org

Susan May currently supports multiple federal government agencies in the areas of security services and operations, security technical and acquisition support, and telecommunications carrier services. Prior to joining MITRE, she developed Managed Security Services for Verizon Business/MCI and NTT/Verio and has managed security engineering teams around the world while serving as Asia Pacific Product Engineering Director for UUNET/Worldcom. E-mail: smay@mitre.org

Vijay Rachamadugu has over 22 years experience in information and network security and enterprise architecture. E-mail: vijayr@mitre.org

Robert K. Smith is a Principle Multi-Discipline Systems Engineer supporting OSD/DOT&E. He has held technical leadership positions with responsibility for acquisition and T&E at several satellite and wireless companies, including COMSAT, Iridium, Nextel, and XM Satellite Radio. E-mail: rksmith@mitre.org

References

Chairman of the Joint Chiefs of Staff Instruction 3170.01G, *Joint Capabilities Integration and*

Development System, 31 July 2008 (updated Feb 2009).

Chairman of the Joint Chiefs of Staff Instruction 6211.02C, *Defense Information System Network (DISN): Policy and Responsibilities*, 9 July 2008.

Chairman of the Joint Chiefs of Staff Instruction 6212.01E, *Interoperability and supportability of Information Technology and National Security Systems*, 15 December, 2008.

Chairman of the Joint Chiefs of Staff Instruction 6510.01E, *Information Assurance (IA) and Computer Network Defense (CND)*, 14 August, 2007.

Committee on National Security System Instruction (CNSSI) No. 4009, *National Information Assurance (IA) Glossary*, June 2006.

Defense Acquisition Guidebook. http://at.dod.mil/docs/DefenseAcquisitionGuidebook.pdf

Director, Operational Test and Evaluation (DOT&E) Memorandum; *Procedures for Operational Test and Evaluation of Information Assurance in Acquisition Programs*, January 21, 2009.

DOD Directive 4630.05, *Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)*, May 5, 2004.

DOD Directive 5000.01, *The Defense Acquisition System*, May 12, 2003.

DOD Directive 8500.1, *Information Assurance (IA)*, October 24, 2002.

DOD Directive 8500.01E, *Information Assurance (IA)*, certified current as of April 23, 2007.

DOD Directive 8570.1, *Information Assurance Training, Certification, and Workforce Management*, August 15, 2004.

DOD Directive O-8530.1, *Computer Network Defense (CND)*, January 8, 2001.

DOD Instruction 4630.8, *Procedures for Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)*, June 30, 2004.

DOD Instruction 5000.2, *Operation of the Defense Acquisition System (including change 1)*, January 4, 2001.

DOD Instruction 5000.02, *Operation of the Defense Acquisition System*, December 2, 2008.

DOD Instruction 5200.39, *Critical Program Information (CPI) Protection within the Department of Defense*, July 16, 2008.

DOD Instruction 8500.2, *Information Assurance Implementation*, February 6, 2003.

DOD Instruction 8510.01, *DOD Information Assurance Certification and Accreditation Process (DIACAP)*, November 28, 2007.

DOD Instruction 8580.1, *Information Assurance in the Defense Acquisition System*, July 9, 2004.

DOD Manual 5200.1, *Acquisition Systems Protection Program*, March 16, 1994.

DOD Regulation 5200.1, *Information Security Program Regulation*, January 14, 1997.

IA Policy Crosswalk T&E Working Group Briefing, September 3, 2009.

Intelligence Community Directive (ICD) 503, *Intelligence Community Information Technology Systems Security Risk Management, Certification and Accreditation*, 15 September, 2008.

Joint Publication 3-13, *Joint Doctrine for Information Operations*, 9 October, 1998.

National Defense Industrial Association, Systems Assurance Committee, *Engineering for System Assurance*, 2008.

[Section 804] – *HR 2647: National Defense Appropriation Act for Fiscal Year 2010*, Section 804, 111th Congress 2009–2010.

The MITRE Corporation, *Slide Presentation: Mission Assurance in DOD Systems Acquisition and Test*, November/December 2009. Adapted from *The Systems Engineering Guidebook for Intelligent Transport Systems*, U.S. DOT, Federal Highway Administration – California Division, November 21, 2009.

Acknowledgments

This article is based on the work of TEWG and was composed of subject matter experts from the DoD, its Services and Components, DISA, and NSA. Participants included: Derek Abeyta, Mike Artis, Thomas Avey, Robert Beck, Ed Beech, Dr. Robert Berger, Larry Burgess, Peter Christensen, Michael Clark, Jeffrey Combs, David Cox, Dr. Judith Dahmann, Michael Davis, Tom Gaetjen, Douglas Garrett, Ralph Harris, Kevin Holmes, Melody Johnson, Kenneth Kiesel, Art King, Shannon Krammes, Ed Kulas, Dan Landin, Larry Leiby, Andy MacBrien, Jerry Manthei, Steve Matthews, Dennis Mattison, Susan May, John Miller, James Morris, Darlene Mosser-Kerner, Martha O'Connor, Patrick O'Connor, Michael Phillips, Vijay Rachamadugu, Ray Subramonian, Mariann Tobias, Timothy Tucker, David Tuteral, Wayne Van Dine, Shelly Wells, and Jack York.

The TEWG would like to thank Mr. Ralph Harris, representing OSD-DOT&E and Ms. Darlene Mosser-Kerner, representing OSD-DDT&E. Their guidance and leadership have made the effort and this document possible in a relatively short time frame, especially considering the complexity of the subject.

ITEA Journal 2010; 31: 473–477

The Information Assurance Range

Robert Powell
Defense Information Systems Agency, Falls Church, Virginia
Timothy K. Holmes
Joint Interoperability Test Command, Indian Head, Maryland
Cesar E. Pie
Cyber security Research and Solutions Corporation, La Plata, Maryland

An effective Information Assurance (IA) posture is achieved when there is confidence that information and information systems are protected against attacks through the application of security services in such areas as availability, integrity, authentication, confidentiality, and non-repudiation. All Department of Defense (DoD) organizations must expect attacks and must incorporate attack-detection tools and procedures that allow them to react to and recover from these incidents and events while still achieving mission success. Since technical mitigations are of no value without trained people to use them and operational procedures to guide their application, it is paramount that in implementing an effective and enduring IA framework, DoD organizations achieve a balance from all three facets of a Defense in Depth strategy: people, operations, and technology. The IA Range seeks to satisfy this strategy.

Key words: CND tactics; computer network defense; IA range; information assurance; T&E.

Cyber threats are asymmetric, surreptitious, and constantly evolving—a single individual or non-state sponsored group anywhere in the world can inexpensively and secretly attempt to penetrate systems containing vital information or mount damaging attacks on critical infrastructures. Moreover, the pervasive interconnectivity of the Global Information Grid (GIG) makes cyber attacks an increasingly attractive prospect for first, second, and third generation threats and adversaries.

In light of the current operational threat environment, the deliberate investments of time, resources, and attention in implementing and maintaining an effective Information Assurance (IA) posture have never been more important or more challenging. The IA Range provides an operational representation of today's GIG IA architecture within a Network Operations (NetOps) construct. Unlike theoretical models, the IA Range is an infrastructural platform designed to integrate distributed and heterogeneous IA architectural systems and solutions with the Department of Defense (DoD) Computer Network Defense (CND) operational hierarchy. The IA range provides DoD stakeholders with an avenue to strengthen the GIG security posture by supporting operational exercises, training network defenders, and testing and evaluating new information capabilities.

Test and Evaluation (T&E) mission

In support of its T&E mission, the IA Range incorporates Defense in Depth design principles to provide DoD organizations with a methodical, repeatable, and verifiable Cyber T&E framework (supported by performance-based metrics indicators) to measure (i.e., quantify and qualify) the abilities and capabilities of network defenders to synergistically integrate *people*, *operations*, and *technology* to *protect*, *monitor*, *detect*, *analyze*, *diagnose*, and *respond* (i.e., contain, eradicate, and recover) to cyber security attacks. In addition to providing for a realistic T&E environment that is segregated from the operational environment (reducing the IA risk and minimizing the technical and operational impacts to zero), the IA Range, as a capability, provides DoD organizations with a venue to measure the cyber security workforce operational performance, the adequacy of in-place cyber security services (near term CND tools and mechanisms), and validate established and mandated IA and CND tactics, techniques, and procedures.

T&E objectives

The IA Range framework will be used to promote a consistent, repeatable, and verifiable T&E venue by which IA and Computer Network Operations (CNO) technical and operational concepts can be validated against requirements and specifications for improvement. Specifically, the IA Range will seek to achieve the following T&E objectives:

- improve cyber security workforce operational performance,
- validate capabilities and services provided by CND tools and mechanisms,
- validate and improve CND tactics, techniques, and procedures,
- validate acceptable level of service of Computer Network Defense Service Providers (CNDSPs), and
- validate IA mitigation strategies for programs of record.

The cyber threat

The cyber threat environment is very dynamic and complex. This environment is predominantly used by well-funded adversaries with strong economic and political motivations and powerful technical capabilities. Today, foreign nations represent the most sophisticated threat. Foreign nations have learned to recognize the value of attacking adversary computer systems, both on the military and domestic front. Foreign nations are currently improving their doctrine and dedicated government-sponsored offensive cyber warfare programs. They are supported by institutional processes and significant resources and have begun to include information warfare in their military doctrine. The second most sophisticated threat and next group of potential adversaries comprises primarily non-state actors who present the most diverse and difficult threat entity to characterize. Non-state actors, including terrorists, have come to recognize that cyber weapons offer them new, low-cost, easily hidden tools to support their causes. The skills and resources of this threat group range from the merely troublesome to dangerous, and while they are unlikely to mount an attack on the same scale as a nation, they can still do considerable harm. The least sophisticated threats are lone or possibly small groups of amateur hackers without significant resources. These inexperienced malicious hackers use common hacker tools and techniques in an unsophisticated manner to attack computer systems and are the source of most attacks.

Improve cyber security workforce operational performance

As shown in *Figure 1*, the IA Range promotes improved cyber security workforce operational performance through performance metrics to measure both a simulated opposing force's cyber attack activities and friendly network defenders protecting, monitoring, detecting, analyzing, diagnosing, and responding to the cyber attacks. Strategically, an Opposing Force (OPFOR) is employed in this environment to execute cyber attack scenarios. The steps a hacker may follow will be broadly divided into seven phases, which include footprinting and scanning, enumeration, gaining access, escalation of privilege, maintaining access, network exploitation, and covering tracks. This is the most effective framework to test network defenders because it forces the warfighter to consider all aspects of an attack—the best way to defend our networks is to think like the enemy. Defined by DoD requirements, these scenarios will be strategically designed to exercise different classes of attacks (e.g., passive, active, insider, close in, distribution) and their corresponding threats (i.e., nation state, non-nation state, etc.). Every scenario includes elements such as the expected actions, conditions, standards, operational threat environment options, associated risks, event stoppers, and applicable training audience. If successful, the OPFOR will challenge security assumptions and strategies, expose operational and technical weaknesses, and stimulate fresh thinking about the enterprise security posture. This construct provides a simplistic approach, agile and flexible enough to be expanded into a more complex assessment model.

Validate capabilities and services provided by CND tools and mechanisms

A CND tool or mechanism is a device that provides one or more of the following capabilities and services: protection, monitoring, detection, analysis and diagnosis, and/or responding (i.e., containing, eradicating, and recovering) from incidents and events. To support CND emerging technologies, the IA Range provides a stable environment to more effectively and efficiently improve the design, implementation, and calibration of new CND technologies. This includes validating the capabilities and services provided by these devices as well as the implications and tradeoffs of implementing different and alternative security technology strategies throughout the GIG.

In addition, since the scale, complexity, and diversity of the components, systems, infrastructures, and operational environments comprising the GIG are unprecedented in the DoD, no one solution fits all; yet all solutions must adhere to a common set of guiding principles, common lexicon, and consistent set of capabilities and activities that govern system design and evolution, thus enabling interoperability. With this in mind, the IA Range provides an ideal environment

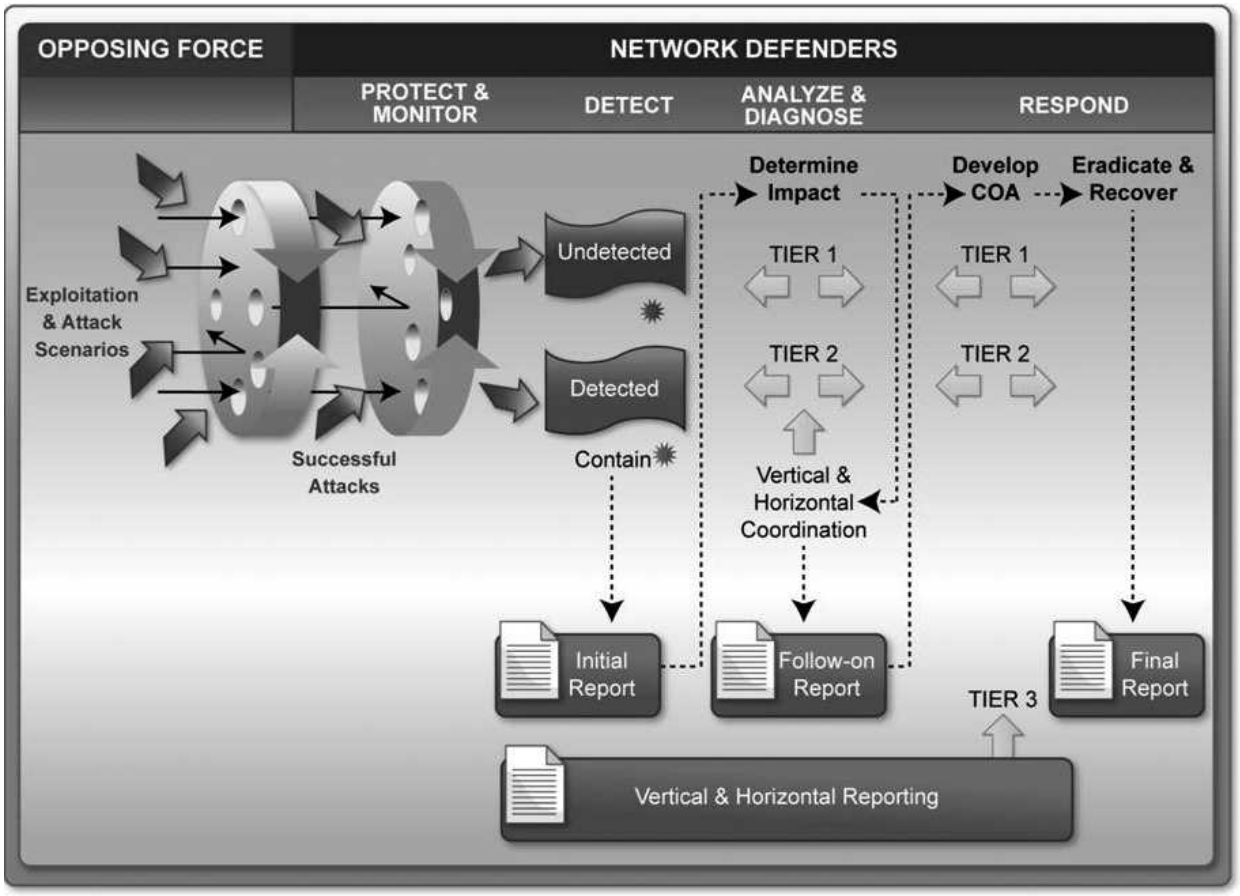


Figure 1. Cyber security assessment framework.

for testing the effectiveness and efficiency of tools and technologies, both for the purpose of improving technologies still in the research and development stages and for testing existing deployed mechanisms, thus validating architectural models of IT systems and infrastructure at large scales (i.e., Demilitarized Zone). This ensures that individually and collectively, CND tools and mechanisms contribute to the overarching DoD strategic IA plan; support the full spectrum of solutions involving any combination of doctrine, organization, training, materiel, leadership and education, personnel and facilities; and promote the maturity of these capabilities from concepts to realized Defense in Depth capabilities.

Validate and improve CND tactics, techniques, and procedures

When implementing CND technologies, it is important to note that each element of the *people*, *operations*, and *technology* triad plays a role in the cyber security of critical infrastructures. Well-documented Tactics, Techniques, and Procedures (TTPs) can often help to overcome potential vulnerabilities in a security product, while poor implementation can render good technologies ineffective. In order to mitigate risk and operate DoD networks in an organized and cohesive way, it is important to lay the framework for operation and administration of CND. The efforts from this strategic area help the warfighters effectively fight cyber threats by ensuring clear guidance, consistency of operations, and high readiness throughout the DoD enterprise.

In support of this effort, the IA Range will be used to validate and improve CND TTPs across the enterprise and achieve an optimal readiness posture. The IA Range can influence the development of TTPs necessary to systematically implement IA and CND for the GIG. Identification and establishment of standard TTPs are a critical initial step in deploying cyber security solutions to meet GIG operational requirements. In a net-centric environment, TTP development needs to be dynamic and aligned with GIG IA and CND activities and technology advances to maximize the benefits of achieving the GIG vision. As the technology evolves, supporting TTPs must be updated accordingly to complement the emerging technological capabilities.

Validate acceptable level of service of CNDSPs

DoD Manual O-8530.1-M, "*Computer Network Defense Service Provider Certification and Accreditation Process*," defines a measurement-driven Certification and Accreditation (C&A) process for evaluating the performance of DoD CNDSPs. The term CNDSP is used to describe the providers of CND and incident response services in DoD that incorporate services similar to those provided by Computer Emergency Response Teams (CERTs) and Computer Security Incident Response Teams (CSIRTs). Unlike traditional C&A, which calculates the security risk for a given system and certifies that the security controls in place for that system adequately mitigate that risk, the C&A of a CNDSP assesses the degree to which that provider assures a minimum standard of service to its DoD subscribers. Assuming specific GIG architectural design requirements, the IA Range could be used to validate that general CNDSP services meet predefined criteria. These criteria could be captured for example by utilizing metrics to measure the adequacy of the services the CNDSPs provide in four main categories:

- **Protect**—includes vulnerability analysis and assessment, CND red teaming, virus protection, subscriber protection and training, information operations condition implementation, and IA vulnerability management;
- **Monitor**, **Detect**, **Analyze and Diagnose**—includes network security monitoring and intrusion detection; attack sensing, warning, and indications; and situational awareness;
- **Respond**—includes containment, eradication, recovery, and incident reporting;
- **Sustain Capability**—includes memoranda of understanding and contracts; CND policies and procedures; CND technology development, evaluation, and implementation; personnel levels and training/certification; security administration; and the primary information systems that support the CNDSP.

Validate IA risk mitigation strategies for programs of record

The IA Range can be an effective tool for evaluating complex programs of record. Programs of record may encompass globally distributed systems, through numerous distributed organizations, a wide range of technologies, and the effects of interdependencies among systems. The IA Range can facilitate validation of recurring IA mitigation strategies and improve Programs of record capabilities and effectiveness. IA risk mitigation involves prioritizing, evaluating, and implementing the appropriate risk-reducing controls (recommended from the risk assessment process). Because the elimination of all risk is usually impractical or close to impossible, the IA Range could be used, for example, to validate the least-cost approach and the most-appropriate controls to decrease mission risk to an acceptable level, with minimal adverse effect on GIG resources and mission.

In addition, because of a Defense in Depth strategy, in the context of the DoD IA C&A process, the IA Range could be used to validate IA control inheritance. IA control inheritance is a common state in which an IA control, along with the control's validation results and compliance status, is passed, or "inherited," from an originating Information System (IS) to a receiving IS for the purposes of C&A. The sharing of IA control compliance status and evidence allows C&A practitioners to model an environment where security mechanisms are shared across multiple ISs. Inheritance eliminates testing redundancy by passing the actual results, associated validation artifacts, and compliance status from the originating IS to each inheriting IS. The IA Range could be used to validate some of these test results.

Conclusion

The DoD IA Range will surely prove invaluable for warfighting organizations looking to measure the effectiveness of enterprise tools and TTPs prior to their release into the production network. The realistic operational environment offered by the IA Range can be custom tailored to meet the assessment needs of a small-scale test effort, as well as a larger-scale enterprise program of record evaluation that requires multiple tools, services, and agency participants. It will strengthen IA awareness and the overall security posture of networked systems throughout the DoD. ❑

Mr. Robert Powell hangs his hat at the Defense Information Systems Agency's office of Field Security Operations, Arlington, Virginia, and is the program manager for the DoD IA Range. Mr. Powell is a summa cum laude graduate of Shenandoah University, Winchester, Virginia, and holds numerous industry certifications to include the Certified Information Systems Security Professional. E-mail: robert.powell@disa.mil

Mr. Kevin Holmes serves as the Joint Interoperability Test Command (JITC) information assurance technical advisor, where he develops and maintains the Command's IA policies, methodologies and capabilities. Mr. Holmes joined the JITC shortly after its inception in 1989. He has held a variety of positions within the Command. Mr.

Holmes started his JITC career developing software for many JITC instrumentation systems; ranging from tactical message protocol analyzers to modeling and simulating tactical data systems. He stood up the JITC IA capability in 2001 and has been working in that area since. Holmes earned his bachelor of science degree in management information systems (MIS) from the University of Arizona and his master of science degree in computer science from George Mason University. E-mail: kevin.holmes@disa.mil

Mr. Cesar E. Pie is chief executive officer of Cyber Security Research and Solutions Corporation (CSRS-Corp). He has extensive program management expertise and has provided subject matter expert support to the JITC for over 6 years in the fields of information system security engineering, information assurance, and computer network operations (computer network attack, computer network exploitation, and computer network defense). Mr. Pie graduated from the University of Maryland University College with a master of science degree in Computer System Management—Information Assurance Program. This program is supported by the Department of Homeland Security and the National Security Agency's Center of Academic Excellence in Information Assurance Education (CAE/IAE). Among others, a few of Mr. Pie's certification credentials include Certified in the Governance of Enterprise Information Technology (CGEIT), Information System Security Engineering Professional (ISSEP), Certified Information Systems Auditor (CISA), Certified Information System Security Professional (CISSP), and Project Management Professional (PMP). E-mail: cesar.pie@csrscorp.com

References

DoD. 2003. *Department of Defense Computer Network Defense Service Provider Certification and Accreditation Manual,* O-8530.1-M. Washington, DC: DoD.

ITEA Journal 2010; 31: 479–484

DISA Test, Evaluation, and Certification: A New Organizational Construct

Chris Watson
Office of the Test and Evaluation Executive,
Defense Information Systems Agency, Arlington, Virginia

Test, evaluation, and certification (TE&C) is an essential part of the Department of Defense (DOD) acquisition system. As the DOD moves forward with the implementation of a new acquisition process for information technologies, the Defense Information Systems Agency (DISA) must lead from the front. The DISA TE&C organizations bring tremendous expertise across all information technology (IT) TE&C disciplines: developmental testing, operational testing, joint interoperability test and certification, and security testing or information assurance certification. However, we must evolve beyond our traditional methodologies to provide the same rigorous services in the agile IT environment. This article describes the new DISA test and evaluation organizational structure and the goals that we have established to responsive, mission-focused TE&C services that enable rapid acquisition of enhanced information technologies for the warfighter.

Key words: Test, evaluation, and certification; joint interoperability; DISA organization and goals; agile testing; virtualization; test automation; TestForge.mil.

The Defense Information Systems Agency (DISA) is committed to advancing the art and science of test, evaluation, and certification (TE&C) of information technology (IT) and national security systems (NSSs). The DISA TE&C mission is to provide responsive, agile, and cost-effective interoperability; other tests, evaluations, and certifications; or both to support rapid acquisition and fielding of enhanced net-centric warfighting capabilities.

Clearly, TE&C is an essential element of the Department of Defense (DOD) acquisition system. As the DOD moves forward with agile IT acquisition concepts, DISA must be at the forefront of shaping the supporting policies, processes, and joint TE&C environment. DISA TE&C organizations must progress toward the use of distributed test methodologies that provide realism and promote joint mission effectiveness. DISA's early and continuous involvement throughout the IT acquisition life cycle with service proponents, operational sponsors, and industry developers will help ensure that agility is achieved.

DISA TE&C organization

DISA recently restructured its testing organization. The new structure better aligns test and certification activities with the agency's strategic objectives. DISA TE&C organizational elements are aligned under the DISA's test and evaluation (T&E) executive, and include the Office of the Test and Evaluation Executive (TEO), Joint Interoperability Test Command (JITC), and the Test and Evaluation Management Center (TEMC). DISA TE&C organizations and facilities are located in Fort Huachuca, Arizona; Indian Head, Maryland; and Falls Church, Virginia. The Falls Church organization and testing labs will move to Fort Meade, Maryland, in April 2011, as part of the Base Realignment and Closure. *Figure 1* depicts the overarching DISA TE&C organizational structure.

Collectively, DISA TE&C organizations and associated facilities serve as the IT test bed in the Major Range and Test Facility Base (MRTFB) and provide capabilities and infrastructure for end-to-end system engineering and execution of distributed, net-centric testing of core technologies and mission-enabling applications supporting the joint warfighter. The DISA MRTFB is a national asset that provides full spectrum TE&C services in support of DOD, other government agencies, and industry.

The DISA T&E executive provides oversight of all DISA T&E activities. The TEO is responsible for serving in advisory and support roles within various Office of the Secretary of Defense, DISA, and joint governance groups (*Figure 2*). The TEO influences

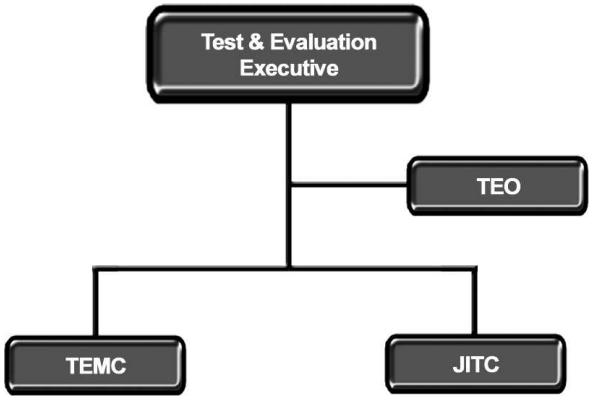


Figure 1. Defense Information Systems Agency Test, Evaluation, and Certification organizational structure.

DOD IT TE&C strategies, policies, procedures, and investments. The TEO organizational structure consists of the deputy T&E executive, administrative staff, and an advisory staff. The Interoperability Policy and Certification Panel (IP/ICP) lead serves as DISA's voting member on the Military Communications and Electronics Board IP/ICP and represents the DISA T&E executive at various senior-level Office of the Secretary of Defense T&E working groups and advisory boards. The Joint Test & Evaluation Methodology Transition director works in cooperation with the operational T&E director to improve the ability to conduct testing in a joint environment and validates the capability test methodology to define and use a distributed, live, virtual, constructive test environment to evaluate joint mission effectiveness. The Joint Test & Evaluation (JT&E) liaison supports the JT&E Program and serves as a conduit to DISA for all chartered and proposed JT&E efforts and quick reaction tests. Lastly, the strategic planning and communications chief serves as the principal adviser for defining organizational planning and outreach strategies associated with all TE&C elements within DISA.

Joint interoperability test command

As designated by the Joint Chiefs of Staff, JITC certifies IT and NSS interoperability and net-readiness for joint military operations (*Figure 3*). In addition to serving as an operational test agency, JITC serves as the responsible test organization for various DOD program offices. JITC works closely with the warfighting combatant commanders during exercises and contingency operations, providing them on-the-spot evaluations of problem areas and viable mission-oriented solutions. The laboratories at JITC operate as an MRTFB. JITC's global reach extends to the entire spectrum of DOD, federal government, private industry, and allies in support of command and control, intelligence, and defense reform initiatives. JITC deals directly with vendors to provide critical preacquisition test results. This early involvement in development results in better systems at lower cost.

JITC's mission is supported by a blend of military, civilian, and contractor personnel, including engineers, computer scientists, and technical and operational experts. JITC government personnel provide technical direction, policy decisions, schedules, and program cost controls in the management of JITC daily operations. The organization is primarily composed of divisions and portfolios and is aligned with the warfighting mission areas to provide consistent practices and processes across the testing disciplines (developmental, operational, interoperability, and security) and support the implementation of a risk-based test strategy that enables agile testing and rapid fielding. Divisions offer business and internal services to JITC to perform its mission, and the portfolios execute the JITC mission and address customer requirements. JITC elements are as follows:

- The *Operational Test & Evaluation Division* conducts operational testing of IT and NSSs acquired by DISA and other DOD organizations to ensure capabilities are effective, suitable, interoperable, and secure. This division assists in the preparation of critical operational issues and develops, defines, and publishes measures of effectiveness, measures of suitability, and measures of performance. It also directs and approves operational T&E methods for data collection, reduction, and analysis.
- The *Business Management Division* provides management and oversight of all JITC business,

Figure 2. Office of the Test and Evaluation Executive organizational structure.

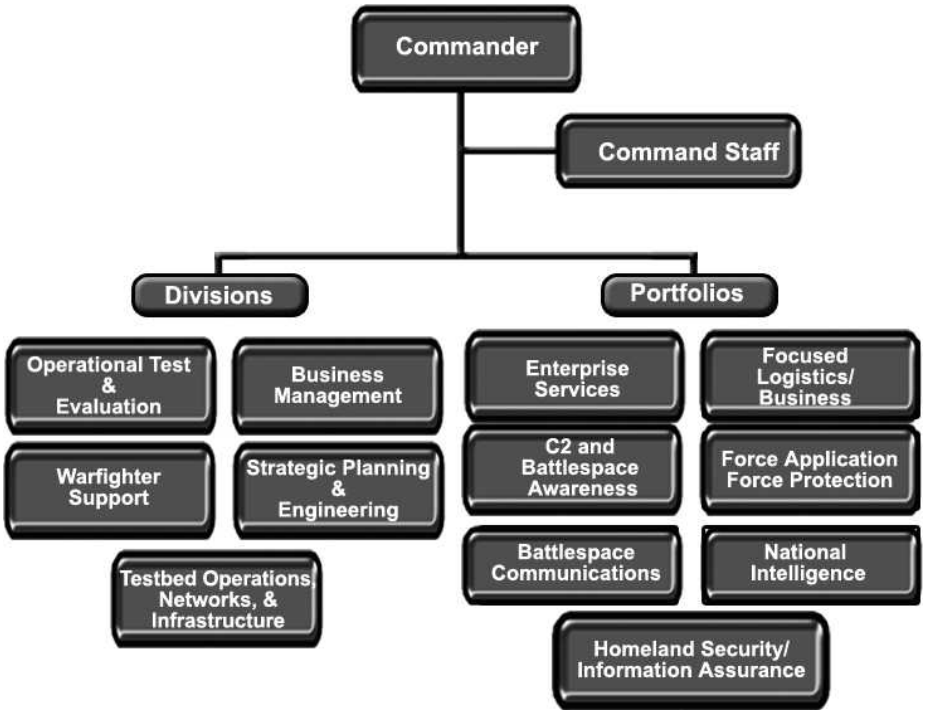


Figure 3. Joint Interoperability Test Command organizational structure.

personnel, training, contracts, and security operations in support of JITC's mission, goals, and objectives while obtaining or providing best-value goods and services for JITC's workforce. This includes command support activities, corporate-level management of proposals, and contracts or agreements. This division also serves as the MRTFB focal point.

- The *Warfighter Support Division* assists the JITC commander with setting command priorities and moderating the operational tempo in support of day-to-day command operations. It provides exercise and contingency support to the warfighter and combatant commander by participation in combatant commander exercises, deploying to contingencies, and providing a 24/7 technical support hotline.
- The *Strategic Planning & Engineering Division* provides leading edge test engineering, instrumentation, and operations services to the JITC divisions and portfolios in support of the overall JITC mission. This support includes defining and coordinating the integration of test engineering best practices, oversight of key acquisition test programs, and establishing standard practices for instrumentation development.
- The *Test Bed Operations*, *Network & Infrastructure Division* plans for and maintains functional test beds, local and wide area networks, and laboratories at JITC. It provides timely facilities infrastructure and logistics support services resolution to JITC's test portfolios and divisions.
- The *Enterprise Services Portfolio* supports the fielding of global net-centric solutions by providing continuous and effective T&E services to DISA and DOD joint acquisition programs within the enterprise services construct.
- The *Focused Logistics and Business Portfolio* serves as the focused logistics and business mission area responsible test organization for the DOD and other federal agencies. It also assists programs in the transition to a capability-based net-centric environment.
- The *Force Application or Force Protection Portfolio* conducts interoperability assessments, standards conformance, and interoperability certification testing of force application or protection systems and joint tactical data links in hardware-in-the-loop and operationally realistic environments to validate the implementation of approved standards and certify system interoperability in a joint environment.
- The *Command and Control (C2) and Battlespace Awareness (BA) Portfolio* mitigates risk to C2 and BA community programs and activities by providing developmental and interoperability T&E support and certification services with the goal of enhancing C2 and BA systems capabilities

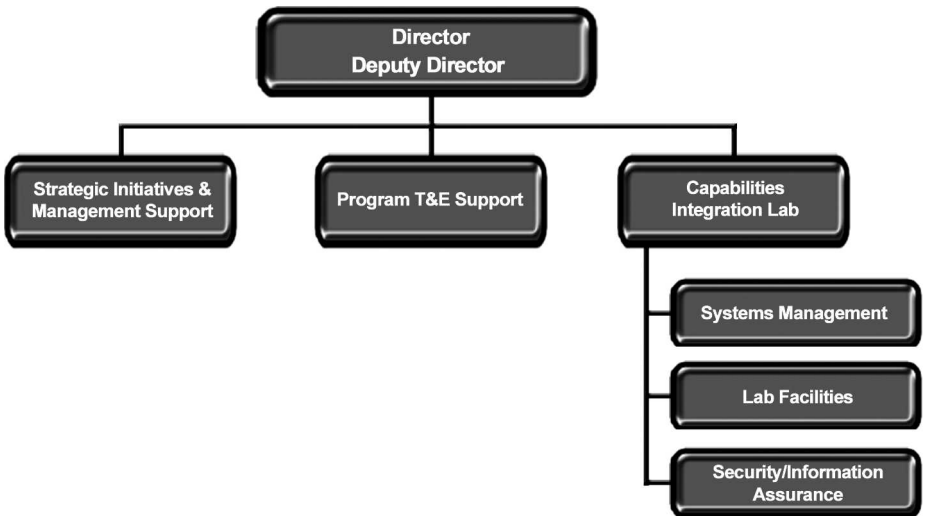


Figure 4. Test and Evaluation Management Center organizational structure.

and performance in support of joint and coalition warfighters.

- The *Battlespace Communications Portfolio* supports the warfighter with direct technical assistance and through testing of secure and nonsecure voice, video, and data communications. It characterizes performance and mitigates risk as net-centric transport solutions are introduced to the global information grid.
- The *National Intelligence Portfolio* mitigates risk to national intelligence community programs and activities by providing support through developmental and interoperability T&E and certification efforts to enhance national collection or dissemination systems capabilities and performance.
- The *Homeland Security or Information Assurance Portfolio* provides the full range of testing services, technical support, coordination, and oversight to the DOD, Department of Homeland Security, and other federal, state, and local agencies to ensure seamless acquisition, integration, and Information Assurance (IA) of systems supporting the DOD and the National Command Authority.

Test and Evaluation Management Center

The TEMC is a staff organization responsible for strategic management of agency test resources. TEMC provides TE&C oversight and guidance to DISA acquisition programs to ensure consistent application of sound T&E methodologies and processes. TEMC has highly skilled and motivated computer scientists, electrical engineers, operations research analysts, IT specialists, and management analysts who establish, review, and enforce TE&C strategies, policies, and procedures for DISA acquisition programs. They represent DISA, as well as champion strategies within the TE&C community.

The TEMC Strategic Initiatives & Management Support Branch is responsible for TEMC resource management in the areas of personnel, finance, and contracting and supports the daily operations mission by executing all aspects of logistics, training, facilities, security, base realignment and closure management, and internal controls. The Program T&E Support Branch provides guidance in the implementation of agile T&E strategies and methodologies and supports the DISA campaign plan by formalizing procedures to provide TE&C services to the DISA development community at large and assist in planning test events necessary to provide the information and confidence that DISA program capabilities are ready for implementation. The Capabilities Integration Lab Division operates and maintains the DISA test infrastructure, providing on-demand test suites, operational network connectivity, collaborative environment, multiple security levels, and technical support services. It works to ensure program system integration through implementation of seamless integration of software capabilities within required security framework and leveraging operational network infrastructure (*Figure 4*).

The TEMC laboratory is also an element of the MRTFB. With DISA laboratories scheduled to move to Fort Meade beginning in 2011, the TEMC is dedicated to making the relocation as transparent as possible by minimizing disruption to services and programs.

DISA campaign plan

In January 2010, Lieutenant General Carroll F. Pollett (DISA director) formally established a cam-

paign plan to focus on the nation's need for a force that is ready and capable of performing the full range of military operations. The DISA campaign plan defines the major focus areas and goals that will enable DISA to meet the demands of the warfighter. The campaign plan is centered on "lines of operation" and supported by "joint enablers" that provide the framework for strategic planning, budgeting, and task prioritization or execution. The plan lays out the methods by which DISA will satisfy its goals and achieve its objectives.

Within the campaign plan, the three lines of operation are as follows:

- enterprise infrastructure,
- C2 and information sharing,
- operate and assure.

The joint enablers are the process and governance areas that support the lines of operation. The nine joint enablers are as follows:

- acquisition,
- contracting,
- engineering,
- information and knowledge management,
- people,
- planning,
- resources,
- spectrum,
- testing.

The DISA TE&C strategic plan coincides with the overarching DISA campaign plan joint enabler for testing, which outlines the priorities in clearly stated 2- and 4-year actions for accomplishing the TE&C mission.

DISA TE&C objectives and goals

The primary DISA TE&C objectives are as follows:

- ensuring mission-focused agility through rapid development of mission-oriented test plans that permit objective assessments of technical and operational capabilities and limitations;
- improving TE&C by ensuring integration and synchronization of efforts among proponents, operational sponsors, developers, and testers;
- ensuring use of consistent, sound, repeatable TE&C strategies that can be executed at all levels, by any test organization, and that, when executed, yield similar results.

Early program involvement and enhanced methods or processes for executing TE&C will lead to rapid deployment of IT and NSS capabilities that are operationally effective, suitable, interoperable, and secure. To improve TE&C processes, DISA has established three aggressive goals:

1. provide efficient, responsive joint interoperability TE&C and other capabilities as a service;
2. establish an on-demand TE&C environment that provides enhanced virtualization and access to federated capabilities that serve the TE&C community;
3. develop and retain a highly qualified and professional workforce to ensure the success of agile TE&C activities.

To achieve these goals and objectives, we must introduce new strategies that allow us to adapt to rapidly changing technologies, ensure that we stay engaged with the program offices to help them find and fix problems early, stay objective in our assessments, and make the right investment decisions to keep us relevant in the on-demand world of IT. Strategies for satisfying DISA TE&C goals include the following:

- enhance the execution of the IT and NSS TE&C mission in accordance with DOD policy and federal law;
- enhance the execution of DISA's operational test mission;
- reduce TE&C timelines in support of agile acquisition through implementation of the capability TE&C model;
- enhance the ability to execute security (IA) TE&C;
- work with capability portfolio managers to ensure a system of system testing in a joint operational context;
- implement a network pilot that supports development, integration, and TE&C;
- improve infrastructure and federate capabilities across DOD;
- implement a virtual environment in support of TE&C;
- maintain a focus on recruiting, hiring, and retaining a workforce of trained, experienced TE&C professionals.

Tasks and initiatives associated with respective DISA TE&C strategies are assigned and tracked for accomplishment to verify whether goals have been met and objectives have been satisfied within established timelines. Several key initiatives will allow DISA to satisfy their strategic TE&C goals and objectives.

For example, DISA TE&C organizations will support IT acquisition reform in accordance with National Defense Authorization Act Section 804 by establishing new test approaches that merge TE&C

events (i.e., development testing, operational testing, net-ready key performance parameter validation, and IA) more concurrently.

Initiatives

DISA currently provides a software development environment known as Forge.mil (see www.forge.mil).

For TE&C, we envision TestForge.mil as a virtual environment that enables developers, users, and testers to rapidly verify new software that satisfies user needs. The environment promotes collaboration among key stakeholders, synchronization of development and testing, and integration of team members, and combined execution to satisfy the decision-making needs of all test customers. TestForge provides on-demand access to testing capabilities throughout the development life cycle and enables capabilities that support continuous integration and service virtualization. TestForge currently provides support for testing within the development cycle on agile projects. This includes support for defect management, automated unit, functional and regression testing, and static code analysis through a continuous integration environment. In the near future, TestForge will provide full support for all testing activities including performance, scalability, reliability, interoperability, operational, net-ready key performance parameters, and IA. TestForge will be a key element of an enterprise test and integration capability that provides access to common tools, methodologies, and support.

The IA Range is an infrastructural platform designed to integrate distributed and heterogeneous IA architectural systems and solutions and the DOD Computer Network Defense (CND) operational hierarchy to provide DOD stakeholders with a venue to strengthen the global information grid security posture by supporting operational exercises, training network defenders, and testing and evaluating new cyber capabilities. DISA Field Security Operations manages the IA Range and ensures that it provides a realistic Internet environment and tools in which to test application security, as well as train personnel in computer network operations. Field Security Operations intends for the IA Range to allow for network services found at the NetOps tiers 1–3 and provide a joint service environment for cyber exercises and CND AP training. In support of its DISA TE&C mission, the IA Range incorporates in-depth defense design principles to provide DOD organizations with a methodical, repeatable, and verifiable cyber T&E framework (supported by performance-based metrics indicators) designed to measure (quantify and qualify) the capabilities and limitations of network defenders to synergistically integrate *people*, *operations*, and *technology* to *protect*, *monitor*, *detect*, *analyze* and *diagnose*, and *respond* (contain, eradicate, and recover) to cyber security attacks. DISA TE&C facilities will use the IA Range to promote a consistent, repeatable, and verifiable T&E venue by which IA and CND technical and operational concepts will be validated against requirements and specifications for improvement.

To further professionalize the DISA TE&C workforce, the DISA T&E executive sponsors several events and efforts. The DISA T&E forums are quarterly professional development events and are open to all DISA acquisition professionals and contractors and to guests. The T&E forums have featured nationally recognized speakers from the testing community. The bimonthly T&E management symposiums focus on specific issues related to DOD test processes, procedures, and methodologies.

Conclusion

DISA TE&C organizations are well prepared to conduct mission-focused and agile testing across all IT portfolios, and they strive to continuously improve efficiency through use of virtualization, enhanced test automation, collaboration, and federation across DOD's overall distributed joint test infrastructure. Through conscious investment decisions, sensible allocation of resources, and new, innovative strategies, DISA TE&C organizations will enable rapid acquisition of enhanced capabilities for the warfighter. ❑

Chris Watson serves as the chief of strategic planning and communications for the DISA TEO. In this capacity, Mr. Watson serves as the DISA T&E executive's principal adviser for defining overarching organizational planning and outreach strategies associated with all T&E elements within DISA. He has supported the DISA T&E organization in various capacities for more than 22 years and has published more than 20 articles associated with T&E processes, capabilities, and events of interest. He serves as the DISA T&E liaison to the Joint Atlantic & Chesapeake Ranges Cooperative and the Federal Laboratories Consortium. E-mail: chris.watson@disa.mil

ITEA Journal 2010; 31: 485–494

Net-Ready Key Performance Parameter: A Measurable, Testable, and Operationally Relevant Means of Assessing Joint Interoperability

Danielle M. Koester
Chief, Engineering & Policy Branch,
Joint Interoperability Test Command (JITC), Fort Huachuca, Arizona
Shaina Williams
Command and Control Systems Branch, JITC, Fort Huachuca, Arizona
Kathleen Powers
Senior Systems Engineer,
Northrop Grumman Mission Systems, Fort Huachuca, Arizona
Karen Vincent
Senior Test & Evaluation Engineer,
Northrop Grumman Mission Systems, Fort Huachuca, Arizona

In an effort to overcome community difficulties regarding the testability of the Net-Ready Key Performance Parameter (NR-KPP), the Joint Interoperability Test Command, as the Department of Defense's sole Joint Interoperability Certifier, has established and implemented a detailed approach for defining, testing, and evaluating the NR-KPP consistent with the Chairman of the Joint Chiefs of Staff Instruction 6212.01E. This methodology provides a measurable, testable, and operationally relevant approach to NR-KPP test and evaluation for Joint Interoperability Certification.

Key words: Joint interoperability certification; Joint Interoperability Test Command; test data; DoD architecture framework (DODAF); information exchange, requirements.

The Net-Ready Key Performance Parameter (NR-KPP) was formalized in the Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 6212.01C dated November 20, 2003. Since that time, CJCSI 6212.01 has undergone two major revisions resulting in the current CJCSI 6212.01E dated December 15, 2008 (CJCSI 2008). With each revision, the NR-KPP has grown in size and complexity resulting in both confusion and anxiety for program managers across the Department of Defense (DoD). Arguments have been made that the NR-KPP is neither measurable nor testable. Additionally, it is often viewed as not being operationally relevant. The fact that "Net-Ready" is not a traditional KPP in structure has often been a source of confusion as well. In order for systems in the Department to be secure, interoperable, and able support the mission at hand, it is critical that there is a clear understanding of what the NR-KPP is, how to implement it, and how to test, evaluate, and certify for Joint Interoperability in accordance with the CJCSI 6212.01E.

Interoperability policy and guidance

Governing the Joint Interoperability Certifier role are several policies, the most important of which is Title 10, Section 2223, of the United States Code, which gives the DoD Chief Information Officer (CIO) the responsibility of ensuring interoperability of information technology and national security systems. The certification role has been delegated to Joint Interoperability Test Command (JITC) by the DoD CIO. From a practical standpoint, however, the CJCSI 6212.01E is the instruction that is most referenced with respect to roles and responsibilities for joint interoperability evaluation and certification within the Department. The JITC serves as DoD's sole Joint Interoperability Certifier, in addition to their role

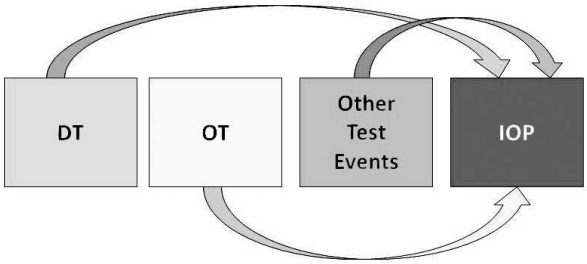


Figure 1. Life cycle test events serve as data points for interoperability certification.

as one of five DoD Operational Test Agencies (OTA). JITC also provides "in the field" support with any interoperability-related issues through the JITC Hotline (1-800-LET-JITC).

Joint Interoperability Test Certification process

In order to issue a Joint Interoperability Test Certification (the proper name for the JITC certification), the interoperability certifier must evaluate a system for compliance with each element of the NR-KPP. The NR-KPP is the evaluation framework used to determine whether or not a system will receive a Joint Interoperability Test Certification *(Figure 1)*. This evaluation uses data collected during developmental testing, operational testing, security testing, demonstrations, exercises, or any other reliable source of test data. The goal is to leverage data and test events to the maximum extent possible, in order to reduce or eliminate the need to conduct separate interoperability testing. For this reason, it is highly recommended that programs involve the interoperability tester early in the life cycle. By being involved early, interoperability testers are able to influence or participate in test events that can be used to collect data for interoperability certification. In the long run, program managers save money by funding the interoperability test agency early, greatly reducing the need for separate interoperability test events.

The Joint Interoperability Test Certification process starts with a Joint Staff certified requirements document. Requirements documents such as Capability Development Documents (CDD), Capability Production Documents (CPD), or Information Support Plans (ISP) are certified by the Joint Staff J-6 for interoperability and supportability. This certification of requirements provides the foundation for issuing the Joint Interoperability Test Certification *(Figure 2)*. Without Joint Staff certified requirements, a Joint Interoperability Test Certification is not possible; although an "assessment" may be given, pending approval of requirements.

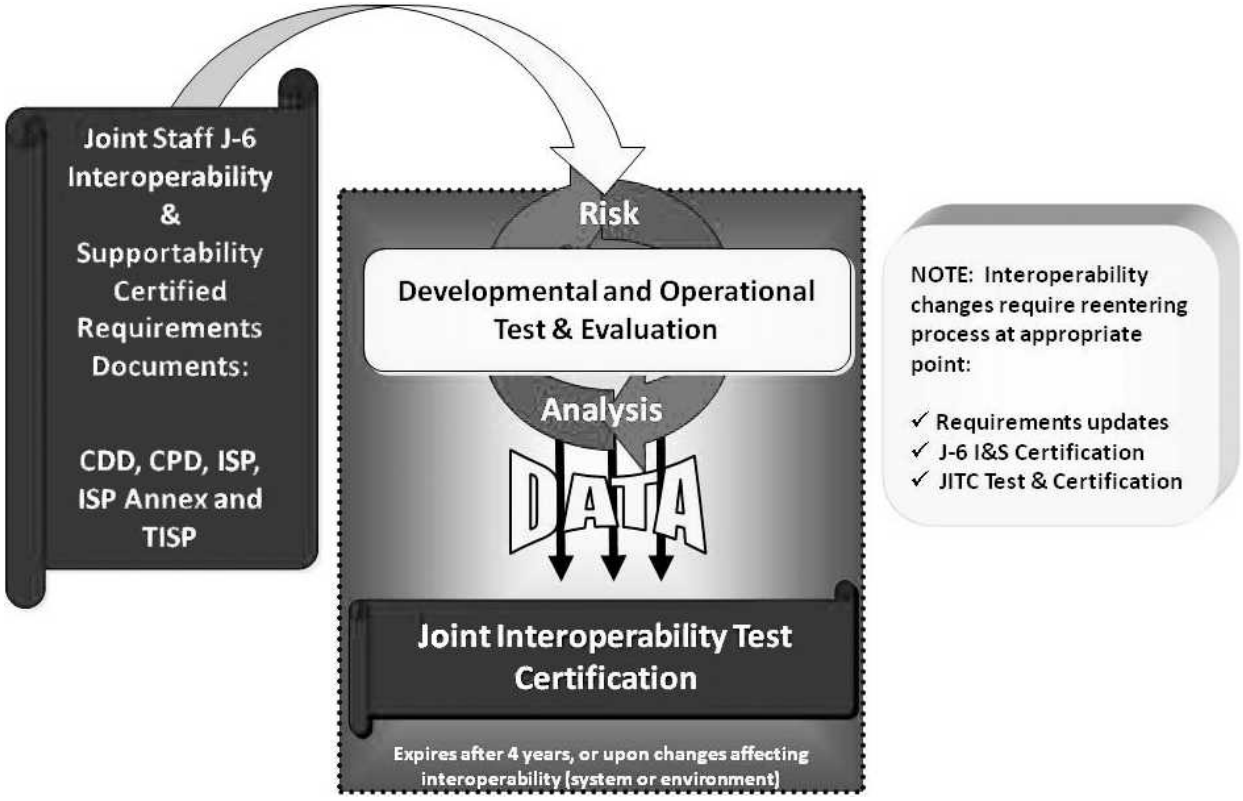


Figure 2. Joint interoperability test certification process.

Table 1. The net-ready key performance parameter.

KPP	Threshold	Objective
Net-Ready: The capability, system, and/or service must support Net-Centric military operations. The capability, system, and/or service must be able to enter and be managed in the network, and exchange data in a secure manner to enhance mission effectiveness. The capability, system, and/or service must continuously provide survivable, interoperable, secure and operationally effective information exchanges to enable a Net-Centric military capability.	The capability, system, and/or service must fully support execution of joint critical operational activities and information exchanges identified in the DoD Enterprise Architecture and solution architectures based on integrated DODAF content, and must satisfy the technical requirements for transition to Net-Centric military operations to include: 1) Solution architecture products compliant with DoD Enterprise Architecture based on integrated DODAF content, including specified operationally effective information exchanges 2) Compliant with Net-Centric Data Strategy and Net-Centric Services Strategy, and the principles and rules identified in the DoD Information Enterprise Architecture (DoD IEA), excepting tactical and non-IP communications 3) Compliant with GIG Technical Guidance to include IT Standards identified in the TV-1 and implementation guidance of GIG Enterprise Service Profiles (GESPs) necessary to meet all operational requirements specified in the DoD Enterprise Architecture and solution architecture views 4) Information assurance requirements including availability, integrity, authentication, confidentiality, and non-repudiation, and issuance of an Interim Authorization to Operate (IATO) or Authorization to Operate by the Designated Accrediting Authority (DAA), and 5) Supportability requirements to include SAASM, Spectrum and JTRS requirements.	The capability, system, and/or service must fully support execution of all operational activities and information exchanges identified in the DoD Enterprise Architecture and solution architectures based on integrated DODAF content, and must satisfy the technical requirements for transition to Net-Centric military operations to include: 1) Solution architecture products compliant with DoD Enterprise Architecture based on integrated DODAF content, including specified operationally effective information exchanges 2) Compliant with Net-Centric Data Strategy and Net-Centric Services Strategy, and the principles and rules identified in the DoD Information Enterprise Architecture (DoD IEA), excepting tactical and non-IP communications 3) Compliant with GIG Technical Guidance to include IT Standards identified in the TV-1 and implementation guidance of GIG Enterprise Service Profiles (GESPs) necessary to meet all operational requirements specified in the DoD Enterprise Architecture and solution architecture views 4) Information assurance requirements including availability, integrity, authentication, confidentiality, and non-repudiation, and issuance of an Interim Authorization to Operate (IATO) or Authorization to Operate by the Designated Accrediting Authority (DAA), and 5) Supportability requirements to include SAASM, Spectrum and JTRS requirements.

Once the system requirements have been analyzed, a risk analysis must be conducted to determine exactly what will be tested to achieve the threshold level of the NR-KPP. This determination is made based upon the requirements that are deemed as "Joint" and "critical" for interoperability. After the risk analysis is complete and data elements for certification identified, data collection begins. If test events are not available for leverage, interoperability testers will need to conduct separate test events. Test data are then analyzed to determine whether or not a system will receive a Joint Interoperability Test Certification.

Requirements analysis

So, is the NR-KPP measurable and testable? What gets measured or tested? And how does that relate to the ability to accomplish the mission? It is important to note that the NR-KPP as a stand-alone item is, in fact, not testable. The reason for this is that the NR-KPP is an *evaluation framework* for joint interoperability and not the actual system-level requirements. The measurable and testable requirements are derived from a system's architecture, generally structured in terms of the DoD Architecture Framework (DODAF). For example, as seen in *Table 1*, the NR-KPP requires that a system be able to support execution of its joint critical operational activities (JCOA); however, it is the system's Operational View-5 (OV-5) that actually defines *what* those JCOAs are. Also important to note is that, while DODAF does prescribe specific content for architectures, it does not prescribe *format*. This is especially important for program's that are operating on limited funding because it allows for reuse of contractor developed system design artifacts, regardless of format.

For interoperability test, evaluation, and certification (TE&C), each system JCOA must be evaluated for

- secure, timely, accurate, complete, and useable information exchanges (operationally effective information exchanges);

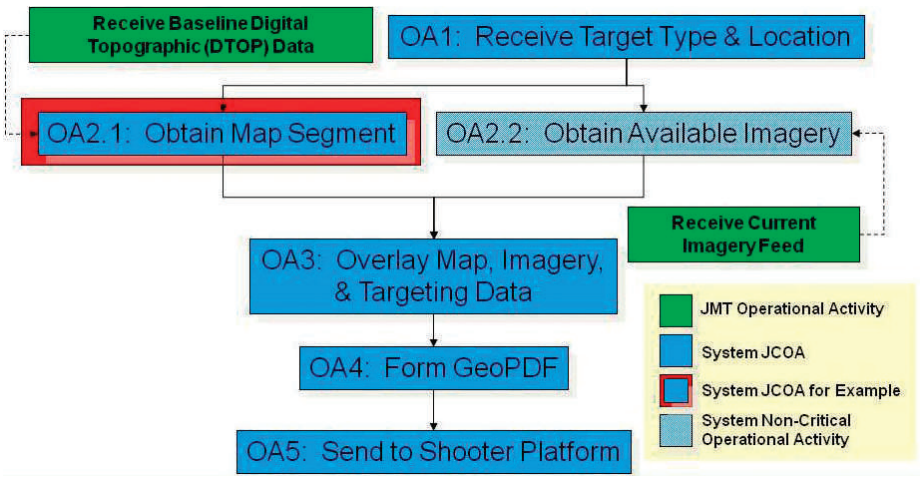


Figure 3. Notional Operational View-5 for Notional Mission Planning Enroute Augmentation System.

- enterprise-level shared data and services that are visible, accessible, understandable, secure, and interoperable (net-centric data and services strategies); and
- standards that have been properly implemented, resulting in no critical deficiencies (Global Information Grid [GIG] Technical Guidance [GTG]).

These are defined as elements 1–3 of the NR-KPP (see *Table 1*).

In addition, the system as a whole must have the information assurance and supportability compliance requirements in place (elements 4–5 in *Table 1*). With respect to information assurance, the system must have completed the requirements for certification & accreditation (C&A), typically through the DoD Information Assurance Certification and Accreditation Process (DIACAP) (although there are other C&A processes that may apply to systems) resulting in interim authority to operate (IATO) (Threshold) or authority to operate (ATO) (Objective). For supportability, the system must ensure that

- any Global Positioning System (GPS) receivers procured are Selective Availability/Anti-Spoofing Module (SAASM) compliant,
- any radio solutions that operate in the Joint Tactical Radio System (JTRS) range are JTRS solutions or that a JTRS waiver has been given by Assistant Secretary of Defense for Networks and Information Integration (ASD[NII]), and
- for spectrum-dependent systems, a Stage 4 DD Form 1494 is in place.

Since information assurance and supportability requirements are relatively static in nature, we will focus on the dynamic requirements defined by NR-KPP elements 1–3 from *Table 1*.

Identify JCOAs

Let us use a fictional example to illustrate this concept. In this fictional example, the Notional Mission Planning Enroute Augmentation System (NMPEAS) is our proposed system under test. Let us also assume that there is an established and accredited joint mission thread (JMT) for mission planning that has been developed by the appropriate operational sponsor. The mission thread defines the activities that must occur to execute mission planning and is tied to the appropriate Universal Joint Tasks to define tasks and metrics for mission accomplishment. The JMT is constructed of various operational activities, two of which are supported by NMPEAS. These operational activities, as shown in *Figure 3*, are

- receive Baseline Digital Topographic (DTOP) data, and
- receive current imagery feed.

The NMPEAS Operational Activity OA2.1: Obtain Map Segment provides a capability that enables "Receive DTOP Data." Simply put, "receive DTOP data" is an activity of the *joint mission thread* (mission planning), and "obtain map segment" is an activity of the *system* that supports the thread activity. There may be a number of system activities that, together, provide the overarching capability defined in the thread. In this example, we will use "obtain map segment" as our representative JCOA for defining measurable and testable criteria for interoperability.

Identify operational information exchange requirements

For our representative JCOA, we must now establish the information exchange requirements (IER) necessary to support execution of that activity,

Needline ID	IER ID	IE Name & ID	Content	Scope	Accuracy	Language	Sending OP Node	Sending OP Activity
NL02 NL03	IER020	IE002: Target Area DTOP	Target area topographic map segment	One or more missions	Resolution 1:25,000	N/A	ON5: Intelligence Cell	**OA2.1 Obtain Map Segment**

Receiving OP Node	Receiving OP Activity	UJTL/ METL	Trans. Type	Trigger Event	Criticality	Periodicity	Timeliness
ON1: Targeting Cell	**OA2.1: Obtain Map Segment**		Automated map segment request/ response	NMPEAS User Request	Critical	As needed	<30 seconds

Figure 4. Notional Mission Planning Enroute Augmentation System Operational View-5 information exchange requirements example.

using the system's OV-3. As shown in *Figure 4*, there is an IER associated with OA2.1 (IER 020), which requires a 30-second "round trip" on a request/response for map data between the intelligence cell and the targeting cell (operational nodes). This is an example of a measurable and testable requirement associated with the NR-KPP. To determine whether or not this IER is "operationally effective" it must take place within a 30-second window, as stated in the operational requirements. Additionally, the data must be complete, accurate, secure, and usable to the warfighter in the conduct of the mission.

Identify system data exchange requirements

At the next level of decomposition, IER 020 is broken out into system data exchanges (SDEs), as defined in the system's SV-6 (see *Figure 5*). This notional example shows a request (SDE021) that must take place within 10 seconds, and a response (SDE022) that must take place within 15 seconds. This supports our operational requirement of a 30-second round-trip time. In addition, the SDE must be able to meet the defined throughput requirements, the data received must be complete, accurate, secure, and usable to the warfighter in the conduct of the mission.

Identify net-centric data and service requirements

Once the data exchanges for evaluation have been identified, the system must be analyzed for use of net-centric data and services. This is important since many systems will be providing data and services to the enterprise for use by other systems. If those data and services are not readily available for consumption, capabilities will be degraded. While the Data/Service Exposure Verification Tracking Sheets are the mandated method of documenting data and services provided to the enterprise, a good system architecture will clearly show what data and services are being

Info Exch ID	System Data Exch ID	System Interface Name/ID	Data Element Name	Content	Format Type	Media Type	Data Standards
IER 020	SDE021	NMPEAS link to enclave LAN	Target area map segment request	Target coord, map segment boundary length	SOAP	Electronic	W3C SOAP v1.2 W3C, XML 1.0 (5th ed) IETF, RFC 2616 1,1 IETF STD 7, 9/91 IETF STD 5, 9/91 IEEE Std 802.3 2008
IER 020	SDE022	DTSS link to enclave LAN	Target area TOPO map segment	TOPO map segment centered on target coord	TFTP	Electronic	MIL-PRF-89037A, 5/99 MIL-STD-2401, 1/94 IETF STD 33, rev 2 IETF STD 7, 9/91 IETF STD 5, 9.91 IEEE Std 802.3 2008

Sending System	Receiving System	Trans. Type	Triggering Event	Criticality	Periodicity	Timeliness	Throughput
NMPEAS	DTSS	Automated request	NMPEAS request "Get Target Area"	C	As needed	<10 s	6 req/min
DTSS	NMPEAS	Automated response	NMPEAS target area map request	C	As needed	<15s	4 resp/min

Figure 5. Notional Mission Planning Enroute Augmentation System SV-6 example.

Table 2. Net-centric data and service requirements for interoperability.

Net-Centric Data Requirements	Net-Centric Service Requirements
Data is Visible Post discovery metadata in an Enterprise Catalog: Department of Defense (DoD) Discovery Metadata Specification (DDMS) conformant discovery metadata is posted in the Net-Centric Enterprise Services (NCES) Enterprise Catalog or other compatible/federated enterprise catalog that is visible to the Enterprise. Use appropriate keywords for discovery: Discovery keywords should reflect common user terms, be appropriate for mission area or data type, be understandable, and conform with MDR requirements that map back to COI identified mission data.	**Services are Visible** Publish a description of the service or access mechanism - Descriptions (metadata) for the service or access mechanism are published in an enterprise service registry, e.g., the NCES Service Registry. Comply with enterprise-specified minimum service discovery requirements - The data access mechanism complies with enterprise-specified minimum service discovery requirements, e.g., a Universal Description, Discovery and Integration (UDDI) description to enable federated discovery.
Data is Accessible Post data to shared space: Data asset is available in a shared space, i.e., a space that is accessible to multiple end users. Provide access policy: If data is not accessible to all users, a written policy on how to gain access is available and accurate. Provide serving (access) mechanism: Shared space provides serving (access) mechanisms for the data. I.e., a service provides users with access to the data. Publish active link to data asset: The Enterprise Catalog DoD Discovery Metadata Specification (DDMS) entry contains an active link (e.g., Uniform Resource Identifier (URI)) to the data asset.	**Services are Accessible** Provide an active link to the service in the enterprise catalog - Active link (e.g., Uniform Resource Identifier (URI)) to the specified service is included in the enterprise catalog metadata entry (i.e., metacard) for the specified service. Provide an active link to the service in the NCES Service Registry - URIs as the operational end points for services shall be registered in the NCES Service Registry by referencing the WSDL (that is in the MDR).
Data is Understandable Publish semantic and structural metadata - Semantic and structural metadata are published in the Enterprise Catalog. Register data artifacts in DoD MDR - XML schema definitions (XSD), eXtensible Markup Language (XML) instances, data models (such as entity relationship diagrams) and other appropriate artifacts are registered in the DoD Metadata Registry (MDR).	**Services are Understandable** Publish a description of the service or access mechanism to the NCES Service Registry - Metadata for the service or access mechanism are published in the NCES Service Registry. Publish service artifacts to DoD MDR - Web Service Description Language (WSDL) documents, and other appropriate artifacts are registered in the DoD Metadata Registry (MDR). Provide service specification or Service Level Agreement (SLA) - A service specification or Service Level Agreement (SLA) exists for services and data access mechanisms.
Data is Interoperable Base vocabularies on Universal Core (UCore) - Semantic vocabularies reuse elements of the Universal Core (Ucore) standard. Comply with COI data-sharing agreements - Semantic and structural metadata conform to interoperability agreements promoted through communities, e.g., Community of Interest (COI). Conform to DDMS - All metadata, including record-level database tagging and in-line document tagging, complies with DDMS.	**Services are Trusted** Operate services in accordance with SLA - The service meets the performance standards in the SLA Include security mechanisms or restrictions in the service specification - The service specification describes security mechanisms or restrictions that apply to the service Enable continuity of operations and disaster recovery for services - The service has a defined and functional Continuity of Operations Plan Provide NetOps Data (NetOps Agility) - Services and data access mechanisms provide operational states, performance, availability, and security data/information to NetOps management services, e.g., Enterprise Management, Content Management, and Network Defense services
Data is Trusted Provide information assurance and security metadata - All metadata, including record-level database tagging and in-line document tagging, includes data pedigree and security metadata, as well as an authoritative source for the data (when appropriate).	**Use of Core Enterprise Services (CES)** - Core Enterprise Services (CES) are used in accordance with DoD CIO mandates

provided. In this example, NMPEAS is not providing any data/services to the enterprise, but since a SOAP request is used in communication with DTSS (see *Figure 5*) there is, more than likely, a Web service being provided by DTSS that provides the requested map information. Clearly, if the DTSS service is not readily available for use, then NMPEAS will not be able to successfully execute IER020. All net-centric data and service assets must comply with the requirements defined in *Table 2*, tailored as necessary in the Joint Staff certified requirements document, in order to be readily available for use across the enterprise.

Identify high-risk standards

Using the JCOAs as a guideline, the system's Technical View-1 (TV-1) is analyzed to determine what standards are implemented that support a JCOA and are high-risk (i.e., military unique, critical to interoperability, etc). *Figure 5* ties the standards to the specific data exchanges that support JCOAs. In this example, perhaps SOAP 1.2 is considered a "high-risk" standard due to known interoperability issues with other Web service standards. The system would be tested for proper implementation of this standard and, ideally, would have a detailed implementation profile

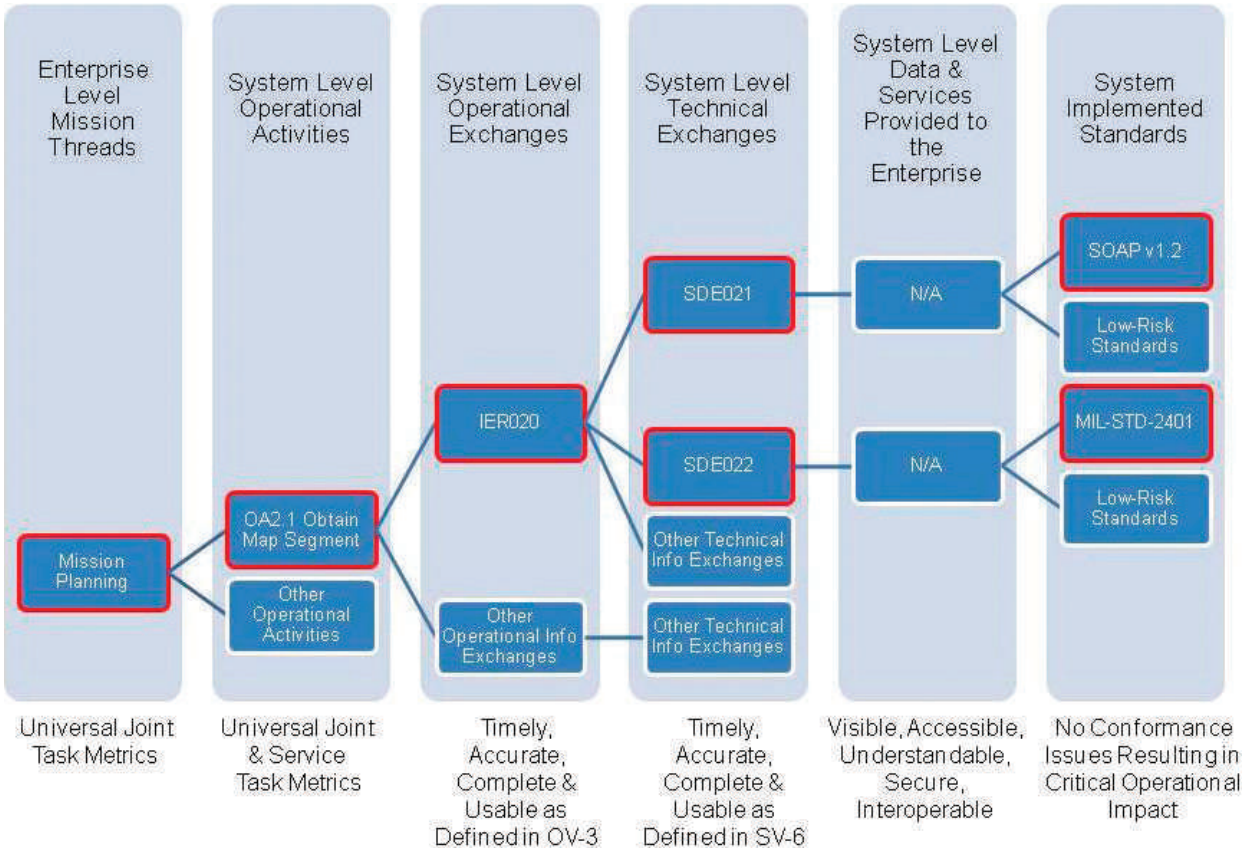


Figure 6. Requirements decomposition into notional test measures for interoperability (Notional Mission Planning Enroute Augmentation System [NMPEAS] Joint Interoperability Certification requirements in red).

that states exactly *how* the standard is being implemented, as is the vision of GIG Technical Profiles.

Document interoperability test criteria

Upon completion of a detailed requirements analysis, test criteria can be easily defined and documented. The goal is to identify these criteria early in the system life cycle, so that program managers can plan for testing, and testers can better plan to leverage each other's events and data. The vision is that testers can test together but evaluate independently to ensure that tester's needs are met and program managers are able to maximize testing return on investment through reuse of test events and test data. These interoperability test criteria, if included in program documentation such as the Test and Evaluation Master Plan (TEMP), will provide the test community and program managers early visibility into interoperability test and certification requirements. A notional breakdown of requirements and measures can be seen in *Figure 6*.

Test, evaluation, and certification

When assessing compliance with the NR-KPP, it is important to test in an operationally realistic environment. This ensures that the results of testing will mirror the system's behavior when fielded in the operational environment. For example, if loading conditions during testing do not represent the conditions of fielding, then test results regarding the timeliness of information exchanges could misrepresent how the system will behave when in the field. This is especially critical when evaluating the first two elements, operationally effective information exchanges and compliance with the Net-Centric Data and Services Strategies. *Table 3* gives high-level information regarding test and reporting for the NR-KPP. Detailed test procedures are available in the JITC NR-KPP Testing Guidebook (DoD 2010).

Upon completion of test and evaluation, a determination is made as to the certification status of the system under test. *Table 4* provides detailed information regarding the different types of interoperability certifications, a description of each, and the fielding recommendation associated with them.

Conclusion

The NR-KPP provides a measurable and testable evaluation framework for joint interoperability test,

Table 3. Net-ready key performance parameter test and evaluation procedures.

NR-KPP Element	Test Procedure	Evaluation
Operationally Effective Information Exchanges	Assess timeliness, accuracy, completeness and usability of information exchanges that support JCOAs in an operationally realistic environment.	System must meet all information exchange requirements that support joint critical (T)/all (O) operational activities.
Net-Centric Data and Services Strategy Compliance	Assess net-centric services and data for visibility, accessibility, understandability, trust and interoperability (VAUTI) IAW JITC NR-KPP Testing Guidebook	System must meet all VAUTI requirements for net-centric data and services that support joint critical (T)/all (O) operational activities.
GIG Technical Guidance	Evaluate system for proper implementation of high-risk standards through conformance testing or reuse of test results from approved organization.	No critical standards conformance-based deficiencies were identified in DT and OT by a combination of government and/or commercial verifications or JITC standards testing or conformance certifications that included all high-risk standards in the TV-1 that support joint critical (T)/all (O) information exchanges.
Information Assurance	Verify system receipt of IATO/ATO, ensure system was tested in approved IA configuration, and as necessary, conduct additional IA scans.	System tested in approved IA configuration, no issues identified during IA scans, and receipt of an IATO (T)/ATO (O).
Supportability	Verify system has met requirements for SAASM, Spectrum and JTRS.	GPS receivers procured are SAASM compliant (T/O) Spectrum dependent system have Stage 4 DD 1494 (T/O) Radios are JTRS solutions or a waiver has been received from ASD(NII) (T/O)

evaluation, and certification. When viewed in the context of joint mission threads and system solution architecture products, it provides a comprehensive means for evaluating joint interoperability that is operationally relevant. A step-by-step process, as shown in *Figure 7*, defines how system solution architectures are easily decomposed into clearly defined test measures providing the test community and program managers the chance to plan for test execution and test data reuse among key stakeholders. While often mistaken as solely a technical requirement or merely a paperwork "compliance" check, the NR-KPP provides the means to tie together technical, system, and operational requirements into meaningful measures. ❑

Ms. Danielle Koester is Chief of JITC's Engineering and Policy Branch within the Strategic Planning and Engineering Division. She has over 10 years of experience in both government and industry focusing on the research, development, engineering, test and evaluation of Information Technology and National Security Systems. Ms. Koester holds a bachelor's degree in mathematics from the College of Saint Elizabeth, Morristown, New Jersey, and a master's degree in systems engineering from Stevens

Table 4. Interoperability certifications as per ''Interoperability and Supportability of Information Technology and National Security Systems'' (CJCSI 6212.01E 2008).

Certification	Description	System can be fielded? (Y/N)
Standards Conformance Certification	System is certified for conformance to a standard/standards profile	No
Joint Interoperability Test Certification	Full system certification. System meets at least all critical interoperability requirements	Yes
Limited Joint Interoperability Test Certification	System meets subset of critical interoperability requirements	Yes, with Interim Certificate to Operate (ICTO)
Interim Joint Interoperability Test Certification	Capability module has adequately demonstrated interoperability for at least all critical threshold requirements identified in the increments	Yes
Special Interoperability Test Certification	Certification is based on J-6 approved requirements other than the NR-KPP, e.g., use of Unified Capability Requirements (UCR) for voice switches	Yes
Non-Certification	Critical operational impacts expected. Provides a warning to the Warfighter.	No
Interoperability Assessment	PM would like to determine interoperability status. System may lack J-6 certified requirements.	No

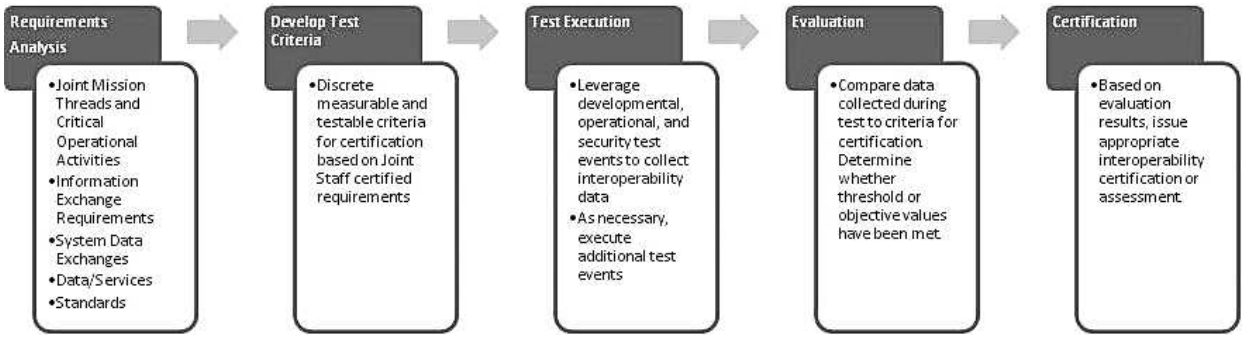


Figure 7. Net-ready key performance parameter test, evaluation, and certification process.

Institute of Technology, Hoboken, New Jersey. Previous assignments include Capability Test Team Lead for the Net-Enabled Command Capability, Project Lead for the Network Enabled Battle Command (NEBC) program, and Information Management Integrated Product Team Lead for the Objective Force Warrior program. A member of the Defense Acquisition Corps, Ms. Koester holds Level III DAWIA certification in Systems Planning, Research, Development and Engineering and Test & Evaluation Engineering. She is the current vice-president of the Huachuca Chapter of the International Test and Evaluation Association.

SHAINA WILLIAMS is a Test Officer in the Command and Control (C2) Systems Branch within the C2 Battlespace Awareness Portfolio at the Joint Interoperability Test Command. She manages and performs Joint Interoperability Test and Evaluation (T&E) activities that include developing, coordinating, and managing the planning, execution, reporting, budget, and contractor support required to meet the T&E requirements for DoD Information Technology and National Security Systems. Ms. Williams holds a bachelor's degree in computer information systems from Wayland Baptist University and is currently pursuing her master's degree in systems engineering. E-mail: shaina.williams@disa.mil

Ms. KATHLEEN POWERS works for TASC, Inc., as a senior systems engineer supporting JITC's Strategic Planning and Engineering Division. She has 16 years of experience in communications and systems engineering, focusing on signal processing software development as well as T&E processes. Ms. Powers holds a bachelor's degree in electrical engineering from Clarkson University, Potsdam, New York, and a master's degree in electrical engineering from John Hopkins University, Baltimore, Maryland. Ms. Powers is a member of the Institute of Electrical and Electronics Engineers and holds a U.S. patent for a "System for recognizing signal of interest within noise." E-mail: powersk@ieee.org

Ms. KAREN VINCENT is a Senior Test and Evaluation Engineer working for TASC, Inc., supporting the Joint Interoperability Test Command's Strategic Planning and Engineering Division. Ms. Vincent has more than 25 years as a systems engineer for the acquisition, architecture development, engineering, and testing of command, control, communications, computers, intelligence, surveillance, and reconnaissance systems. Ms. Vincent holds a bachelor of science degree in electrical engineering and computer science engineering from Northern Arizona University. Previous assignments include 3 years as project director for the States U.S. Army Information Systems Engineering Command's Image Product Library Bandwidth Expansion and Engineering Web Development projects, 4 years as North American Air Defense Command/U.S. Space Command Architecture Development project team leader, 2 years as the U.S. Air Force Tactical Data Link Message Standard representative to the Joint and North Atlantic Treaty Organization Data Link Working Groups, and 4 years as Project Manager for the Peacekeeper and Minuteman Ballistic Missile Systems Integration and Electromagnetic Compatibility project. Ms. Vincent is a member of the Defense Acquisition Corps, holding a Level II certification in Acquisition.

References

CJCSI. 15 December 2008. CJCSI 6212.01E, "Interoperability and Supportability of Information Technology and National Security Systems." 20 July 2010. http://www.dtic.mil/cjcs_directives/cdata/unlimit/6212_01.pdf (accessed October 18, 2010).

DoD. 2 December 2004. DoDD 8320.02, "Data Sharing in a Net-Centric Department of Defense." 1 October 2007. http://www.dtic.mil/whs/directives/corres/pdf/832002p.pdf (accessed October 18, 2010).

DoD. 22 June 2010. JITC NR-KPP Testing Guidebook, version 1.0. 20 July 2010. https://www.us.army.mil/suite/doc/23429848 (accessed October 18, 2010).

DoD CIO. 9 May 2003. "Department of Defense Net-Centric Data Strategy." 1 October 2007. http://www.defenselink.mil/cio-nii/docs/Net-Centric-Data-Strategy-2003-05-092.pdf (accessed October 18, 2010).

DoD CIO. March 2007. "Department of Defense Net-Centric Services Strategy." 1 October 2007. http://www.jcs.mil/j6/DoD_NetCentricServicesStrategy.pdf.

DoD CIO. 11 April 2008. "Department of Defense Defense Information Enterprise Architecture, Version 1.0." 18 August 2008. http://www.defenselink.mil/cio-nii/cio/diea/products/DIEA1.0-Final.pdf.

Sizemore, Nicky. 23 July 2010. "Use of Architecture Products for Evaluating Info Exchange." JITC Internal Architecture Training Briefing.

ITEA Journal 2010; 31: 495–498

Test and Evaluation of Cyber Warfare Systems: Basic Requirements

Norman E. Johnson
SDS International, Ft. Meade, Maryland

The Department of Defense requirements process is designed for systems that will provide decades of service. Well-considered requirements are important for getting it right the first time; however, the Department of Defense does a poor job of articulating requirements for Cyber Warfare Systems that may become obsolete within months. Nevertheless, there are six Mission-Readiness Considerations that form a set of basic requirements that should be evaluated by test and evaluation to inform a mission-ready or fielding decision: safety, security, interoperability, legality, effectiveness, and suitability. Each of these considerations is discussed in detail.

Key words: wartime acquisition environment; capability overlap; obsolescence; mission-readiness; technical risk; interoperability; safety; information assurance; effectiveness; suitability; legality.

Requirements in the Department of Defense (DoD)

Requirements form the foundation for acquisition. They provide overseers with justification to fund an acquisition effort; they provide developers with design objectives; they provide testers with parameters to measure; and they provide decision makers with success criteria.

The DoD requirements process is described in Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 3170.01G and the Joint Capabilities Integration and Development System (JCIDS) Manual (CJCSI 2009; JCIDS 2009). The process focuses on identifying capabilities needed to perform a mission, capabilities currently available, and the gaps between them. Once the gaps are identified, a process is initiated for closing them. This process includes examining all aspects of doctrine, organization, training, leadership, education, personnel, facilities, and policy. If changes in these areas do not satisfy the gaps, a materiel acquisition program is initiated. It is a top-down, mission-driven process that is generally very good, but it has its weaknesses.

Since it is not a bottom-up process, front line warfighters have very little input. The people who are out there getting shot at sometimes have some excellent ideas on what is really needed to prosecute a war. The process flatters itself by providing an environment to drive technological breakthroughs, but it tends to ignore independent breakthroughs that could provide undreamed of capabilities. For example, motorized tanks and machine guns were huge technological achievements that appeared on the scene not too long after the civil war, but Robert E. Lee would never have dreamed about asking for something like that. The process has many moving parts and is deliberative, ponderous, and slow. This is not a fatal problem for ships, tanks, and aircraft. Those acquisition efforts result in products that provide service for decades, so it is vitally important to set a firm foundation in well-considered requirements. They have to get it right the first time. Cyber warfare systems, on the other hand, are subject to Moore's Law and could become obsolete in a matter of months. They provide capabilities that must stay inside the enemy's decision loop timing, so a drawn-out requirements process is absolutely fatal. Even when the gaps are identified, users have difficulty articulating what is needed to fill them. If you do home handyman chores, how many times have you gone to the hardware store thinking, "I can't really describe what I want, but I'll know it when I see it."

The DoD does a poor job of articulating requirements for cyber warfare systems. This is not to cast aspersions on requirements organizations who strive mightily to do the right thing. They are simply overwhelmed by a wartime culture of urgency and the need to quickly get cutting edge technology into the field in order to stay one step ahead of a very clever and resourceful enemy. In contrast to DoD's 3170.01 process (CJCSI 2009), most "requirements processes" for cyber warfare systems are driven by technological innovations. The research and development (R&D)

teams come up with a spectacular capability, and the forward-leaning product teams rapidly produce it and get it into the field with very little testing. This approach has its weaknesses as well.

The requirements and acquisition teams breathlessly try to keep up with the necessary documentation to satisfy overseers and justify funding. This documentation is supposed to be for planning and program guidance, but in this environment it is just an irritating formality. The products that are hastily pushed into the field have very little in the way of concept of operations documentation, training, or logistics support. The designs of urgently needed products frequently do not include reliability or maintainability features. As a result, front line users may spend large amounts of valuable time away from mission duties as they learn how to use the new capability or coax it to work properly. Time saved at the front end of the process (by avoiding a rigorous requirements process) is spent in larger quantities at the back end: "pay me now or pay me more later." Some good ideas cascading out of the R&D brain trust and fielded by product teams are redundant with capabilities already in the field. A more rigorous requirements process would vet these ideas and minimize the capability overlaps. Front line users frequently get unexpected and unrequested capabilities dropped in their laps with an overly sunny briefing, if they get one at all, from the developer or Program Manager (PM). Since many of these capabilities have come straight from development, the users end up doing unstructured beta testing that takes them away from direct mission duties.

When this undeclared beta testing is complete, the users have figured out how to use the capability in a productive manner and have even become a little dependent upon it. After all, it was *supposed* to provide a better capability than the legacy systems. The new system, however, may not have all the features of the old one, so the user ends up employing both. The system gets integrated into operations without formal considerations of safety, security, interoperability, legality, effectiveness, or suitability, which brings us back to requirements. Without documented requirements, these considerations for mission readiness are hollow anyway. How can a decision maker determine if a system is safe, secure, legal, interoperable, effective, or suitable without corresponding metrics? How can he/she even determine how much risk is being assumed? These metrics, and their associated threshold and objective values, flow from well-considered requirements, which can then be measured and evaluated by a robust test and evaluation (T&E) process.

We may not be able to achieve well-considered requirements in the short turn-around times inherent with cyber systems, but it turns out that the six mission-readiness considerations mentioned above are associated with professional communities that maintain standards of acceptability that can be applied to cyber system development programs. With no formal requirements, PMs, developers, testers, and decision makers could anchor themselves to the associated communities to successfully deploy a quick-reaction cyber warfare system capability.

Safety

This is always the first concern, but with software-intensive systems, it is usually not a major concern. Department of Defense Instruction (DoDI) 5000.02 (DODI 2008) indicates that a Programmatic Environmental Safety and Health Evaluation (PESHE) is required by statute (Title 42 U.S.C. 4321). PMs and other acquisition officials are required to identify, consider, manage, and comply with environmental, safety, and occupational health issues early in the acquisition process. A PESHE, conducted by an appropriate safety organization, provides an estimate of the safety risks of a newly developed or developing capability. This in turn provides the necessary insight for a decision maker to weigh risks and benefits associated with a particular capability. This effort is not a test (the T part of T&E), but it is definitely an evaluation (the E part of T&E).

Security

This is another word for information assurance (IA), which is defined in the glossary of CJCSI 3170.01G as

> *"information operations that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities."*

IA ensures controls are in place to avoid, detect, reduce, and/or recover from a realized threat.

Before a developer can connect a system to a network to move forward with developmental testing, they must obtain an authorization from the designated approving authority (DAA) for the system to be accessed. For most DoD systems, the DAA is the Defense Information Systems Agency (DISA). Before DISA approves a newly developed product, it must undergo certification and accreditation (C&A) testing as described in DoDI 8510.01, Defense Information Assurance Certification and Accreditation Process (DODI 2007). This process embraces the idea of IA controls, as defined in DoDD 8500.1 and DoDI

8500.2 (DODD 2002, DODI 2003), as the primary set of security requirements for all cyber warfare systems. The IA controls are determined based on the system's Mission Assurance Category Confidentiality Level. An authorization from the appropriate DAA gives an acquisition decision maker the necessary confidence in the IA of a newly developed system to support continued progress.

Interoperability

Interoperability is defined in the glossary of CJCSI 3170.01F as

> *"the ability of systems, units, or forces to provide data, information, materiel, and services to and accept the same from other systems, units, or forces and to use the data, information, materiel, and services so exchanged to enable them to operate effectively together. Information technology and National Security Systems interoperability includes both the technical exchange of information and the end-to-end operational effectiveness of that exchanged information as required for mission accomplishment."*

The metric for interoperability is the Net-Ready Key Performance Parameter (NR-KPP) standards, which comprise the following elements:

- solutions architecture compliant with the DoD Architecture Framework;
- compliance with net-centric data and services strategies;
- compliance with applicable Global Information Grid Technical Guidance;
- compliance with DoD IA requirements, as discussed above; and
- compliance with supportability requirements.

The NR-KPP is a requirement for any capability that touches the Global Information Grid. That includes just about every DoD cyber warfare system capability. Interoperability testing involves testing to evaluate the ability of a system to exchange information with other systems or components and to use information that has been exchanged, without harm. The strategy for testing interoperability should be included in the T&E Master Plan and must comply with CJCSI 6212.01E (CJCSI 2008).

The PM must coordinate with the Joint Interoperability Test Command (JITC) to obtain an Interoperability Certification. As a practical matter, JITC will normally leverage other tests to accomplish this step. When the evaluation is complete, JITC provides an Interoperability Certification. This certification is good for a maximum of 4 years. However, if there is a major change to the system it will have to be recertified earlier.

If there is an urgent operational requirement to field a system or capability but the required documentation to evaluate interoperability is not yet available, an Interim Certificate to Operate (ICTO) may be obtained. The ICTO is issued by the Military Communications-Electronics Board Interoperability Test Panel and provides the authority to field new systems or capabilities for a limited time (up to 1 year), with a limited number of platforms to support developmental efforts, demonstrations, exercises, or other operational use. During this time it is expected that the PM will work with JITC to ultimately obtain an Interoperability Certification.

Legality

The Office of General Council reviews new capabilities for compliance with legal restrictions. This is not a T&E function, but it is an evaluation and an important risk area for decision makers to consider before making a mission-ready decision.

Effectiveness and suitability

Operational effectiveness is defined in the glossary of CJCSI 3170.01G as the "measure of the overall ability to accomplish a mission when used by representative personnel in the environment planned or expected for operational employment of the system considering organization, doctrine, supportability, survivability, vulnerability, and threat" (CJCSI 2009). It is a measure of how well a capability prosecutes the mission for which it was designed. Developmental T&E (DT&E) evaluates and characterizes the performance of a new capability, but that doesn't mean it evaluates how well the capability can perform the mission. For example, a BMW automobile is a beautifully engineered piece of equipment and performs wonderfully; but if the mission is to haul rocks, it falls decidedly short. The purpose of operational T&E (OT&E) is to point that out through an effectiveness evaluation.

Operational suitability is defined in the glossary of CJCSI 3170.01G as "the degree to which a system can be placed and sustained satisfactorily in field use with consideration given to availability, compatibility, transportability, interoperability, reliability, wartime usage rates, maintainability, environmental, safety and occupational health, human factors, habitability, manpower, logistics, supportability, logistics supportability, natural environment effects and impacts, documentation, and training requirements" (CJCSI 2009). Suitability is almost interchangeable with supportability or sustainability. It includes all the "-ilities" and is especially concerned with reliability and maintainabil-

ity. It complements an OT&E effectiveness evaluation by assessing the infrastructure and processes that support operational use and that facilitate the capability's effectiveness over its entire life cycle. As with the other five considerations, the decision maker must evaluate the risks associated with a capability's suitability before making a mission-ready decision.

Evaluation of effectiveness and suitability is heavily dependent upon stated operational requirements such as system availability, user interface, and data volume and velocity needs. The independent Operational Test Agency (OTA) responsible for the effectiveness and suitability evaluation develops critical operational issues (COIs) based upon stated requirements. From the COIs flow the measures of effectiveness and measures of suitability, and, at the next level of detail, the measures of performance. Using this information, the OTA develops operational scenarios to gather the necessary data for evaluation. COIs are usually based upon formal requirements, but these are frequently lacking in this wartime culture of urgency saturated with technological innovations. Nevertheless, the OTA can develop COIs based upon developer intentions, perceptions of user expectations and needs, and threat environment. These COIs would not carry the same weight of authority as COIs built upon formal requirements, but they would nevertheless facilitate an evaluation of operational effectiveness and suitability. At the very least it would provide an independent assessment of system capabilities and limitations to inform a mission-ready decision, and to minimize off-mission time for the front line users as they integrate the new capability into their normal processes. When contemplating a mission-ready decision, the decision maker must review the capabilities and limitations, as presented in OT&E reports, and assess the risks associated with releasing it at a particular point in time.

Conclusion

Developmental test and evaluation is a PM tool to uncover, understand, and mitigate technical risk. Site acceptance test and evaluation is a Site Commander tool to ensure that a new cyber warfare system being installed at the site is compatible and will aid the mission, or at least not hinder it. Between these two types of testing in chronology is OT&E. OT&E is a milestone decision authority tool to ensure newly developed cyber warfare systems are effective and suitable before they are employed for mission operations. The OT&E is the last chance to ensure that risks associated with safety, security, interoperability, legality, effectiveness, and suitability are characterized well enough for the decision maker to properly balance the net risks against the net benefits to make a well-informed mission-ready decision in a hectic, urgency-driven, wartime environment replete with technological opportunities, but short on formal requirements. ❑

NORMAN JOHNSON is currently employed by SDS International as a senior advisor for Operational Test and Evaluation (OT&E) for the National Security Agency, Ft. Meade, Maryland. He began his career in T&E in 1986 when he attended the U.S. Air Force Test Pilot School at Edwards Air Force Base (AFB), California. He was a project test pilot on the B-1B development program and later moved to Chief Test Pilot on the Joint STARS development program. During Operation Desert Storm he logged 250 hours of combat flight time in command of the experimental prototype E-8A reconnaissance aircraft. He was director of T&E at the Air Force's Electronic Systems Center, Hanscom AFB, Massachusetts, and spent 5 years at the Pentagon in the Developmental T&E section of the Office of the USD(AT&L). From that office he took his Air Force retirement as a Colonel in 2004. Mr. Johnson has a bachelor of science degree in aerospace physics from the University of Colorado, Boulder; a master's degree in aviation management from Embry-Riddle Aeronautical University, Daytona Beach, Florida; and a master of science in national security strategy from the National Defense University, Washington, D.C. E-mail: nejohnson@cox.net

References

CJCSI 3170.01G. Joint Capabilities Integration and Development System, 1 Mar 09.

CJCSI 6212.01E. Interoperability and Supportability of IT and NSS Systems, 15 Dec 08.

DODD 4630.5. Policy for Interoperability and Supportability of IT and NSS, 5 May 04.

DODD 5000.1. Defense Acquisition System, 12 May 03.

DODD 8100.1. Global Information Grid Overarching Policy, 19 Sep 02.

DODD 8500.1. DOD Information Assurance, 24 Oct 02.

DODI 4630.8. Procedures for Interoperability and Supportability of IT and NSS, 30 Jun 04.

DODI 5000.02. Operation of the Defense Acquisition System, 2 Dec 08.

DODI 8500.2. IA Implementation, 6 Feb 03.

DODI 8510.01. DOD Information Assurance Certification and Accreditation Process (DIACAP), 28 Nov 07.

DODI 8580.1. IA in the Defense Acquisition System, 9 Jul 04.

Joint Capabilities Integration and Development System Manual, 1 Mar 09.

ITEA Journal 2010; 31: 499–511

Joint Sensor: Security Test and Evaluation Embedded in a Production Network Sensor Cloud

Tim Owen, Rob Scott, and Roy Campbell, Ph.D.
Defense Research and Engineering Network,
High Performance Computing Modernization Program, Lorton, Virginia

A great security posture inherently requires that cyber operations employ the latest discoveries in emerging security research to keep in step with trends in attack methodologies. The most trenchant cyber security research to date employs actual network data to ensure sensing algorithms and defense methodologies are effective in real-world scenarios. This approach often requires discernments to be made as temporally close to the observed events as possible to allow rapid adaptability of the security posture upon detection of an anomaly. Traditional security architectures, on the other hand, are static and are managed as a centralized, homogenous, symmetrical framework of visibility and interception. Even though access to the data collected from such an environment provides some accessional improvement to researching new algorithms and detection methods, these incremental offline advancements are vetted in a sterile, non-real-time environment without the benefit of sequent responses or adaptive determinations accoutered by a production environment. The primary goal of the Defense Research Engineering Network Cyber Security Test Bed is to leverage emerging network protocols and recent distributed computational techniques to create a cloud of sensors built on tractable computer server platforms that enables cutting-edge security to coexist with current security infrastructure directly inside the production network. The transition time of the latest cyber research from theory to practice will be significantly reduced while intrinsically revolutionizing the approach to engineering network security architectures. By creating a true proving ground by which the science of new algorithms and detection methods can interact directly with raw (as opposed to filtered, sensed, or captured) traffic in real or near-real time in a safe and controlled way, the proposed test bed will provide meaningful advances that can appreciably address the ever-changing landscape of cyber attacks.

Key words: Adaptive; cloud; Defense Research and Engineering Network (DREN); detection; live; network; security; sensor; test bed.

It is an easy sell, at least on the surface, to discuss the introduction of new detection and protection techniques into the traditional network-centric security posture. Just beneath the surface, however, it is clear that traditional architecture has been engineered with specific requirements in mind and purposefully uses a relatively simplistic model: make it persistent (or make it static), consistent (centrally manage and control it), homogenous (use the same tools everywhere), and symmetrical (see both sides of all connections) wherever possible. The solution is the result of a steady evolution from deploying detection and protections in key locations on a network boundary in a Draconian fashion based on event history to modernizing by adding layers of automation, such as firewall or intrusion protection system (IPS) signature subscription services and domain policy for maintaining system vulnerability patching for up-to-the-day readiness. Practically, a circumscribed "defensible" perimeter represents both a sphere of visibility and control and a clear demarcation of responsibility, while reducing the complexity of management of enterprise-wide security solutions and systems within the boundary. Therefore, introducing complexities into that equation can easily translate to more manpower and effort as

well as the opportunity for errors that can easily hide real problems.

In contrast to traditional defense, today's threat is dynamic, decentralized or distributed, heterogeneous (using various means and methods and attack vectors), and asymmetrical. It connotes a style of using a diverse platform to launch a barrage of threats and even turn the defense mechanisms against themselves to deny service, compromise systems, malign applications, exfiltrate data, and then (as if that were not enough) use those systems to launch subsequent assailment—all without being detected firsthand and often not until long after the event. It then comes as no surprise that efforts are now placed in a variety of avenues to aid in identifying malicious content, anomalous traffic patterns, and even behaviors of the programmers developing malware. The security architecture that takes advantage of all of these developments by delivering more comprehensive and compatible features that improve detection, investigation, and mitigation is far more likely to yield the significant gains required to remain afloat in the face of cyber storms.

It is not, however, as simple as replacing one paradigm with another or one tool with a newer one. It is primarily a philosophical transition from the historical function of security to seek out and categorically block incoming antagonists to a more surgical and focused reaction to maintain as much operational normalcy as possible while defeating specific intrusions. In making that transition, tools cannot necessarily just be upgraded in place or abandoned for newer ones. The nature and function of the newer tools rely heavily on hardware and processor capabilities and fit into more fluid data communications structures not entirely compatible with the existing installed base of components, protocols, or data formats. Likewise, research and development of these new tools and techniques using only data that is captured using the traditional methods may also lack the perspective to uncover new tactics and unleash new response mechanisms. Instead, there must be a way to leverage existing capabilities to create measures of usable data, as well as grant access for the next generation of detection and defense algorithms to be proven within the current architecture with real and real-time data to smooth the transition and transform the defense strategy.

It is precisely this gap that a neoteric sensor platform can help fill by injecting research methodologies and tools into the existing architecture. A replacement for traditional sensing appliances, this solution combines current sensing techniques with an isolated modular space within which to test new tools and strategies on a multipurpose hardware platform directly within the production environment. The goals of such a device are to continue to provide existing capabilities, enhance those capabilities with small doses of new techniques for detection and protection, and significantly reduce the development cycle from research to production for quality tools. These nascent methodologies must be implemented without breaking performance or compromising operations and be directly subject to the same inimical traffic to both better sense the anomalies initially and provide clear value by uncovering threats and activities not previously detected.

Divergence of attack and defense style

Many security professionals feel the approaches for cyber defense of the past need to be amended or augmented to find new attacks so that we may continue to "meet mission in the face of cyber warfare." Alternatively, some people go further to identify cyber warfare as a fifth combat arena (*The Economist* 2010) behind land, sea, air, and space. The latter camp builds an argument by identifying three unsound assumptions with the former camp:

- The boundary is structurally defensible (which does not account for mobility),
- The threat is more readily tractable on the existing dimensions being defended (in the face of multifarious attack),
- Automation is equivalent to readiness (which both relies on an asynchronous mechanical client update system and intrinsically trusts the content and structure of resultant code).

A read of this year's Verizon 2010 Data Breach Investigations Report (Baker et al. 2010) may in a sense reiterate the assumptions and propagate the impression that the most significant issues in cyber security are resolved by better deploying the existing technologies. Their statistics, generated in collaboration with the U.S. Secret Service as a study of existing cases of breaches, indicates that 61% of the cases were discovered by a third party, 85% were not considered difficult to accomplish, and a whopping 96% of studied breaches could have been avoided with the use of some form of low- or median-level mitigation. The conclusions were based on one glaring fact: in 86% of the cases, victims had evidence of the breach in their log files. Taken at face value, this type of study shows the need for bolstering and continuing to emend existing installed solutions that mitigate known vulnerabilities, but it does not necessarily mollify the need for a broader perspective on warfare or keeping even worse from happening. Perhaps more germane to the argument is that the method of the study might indicate a marginal disconnect or divergence between

defense and attack style simply because the data being used to develop conclusions, or in turn, new tools, was uncovered using conventional data and visibility.

Though the Verizon report shows hackers still have open to them several "paths of least resistance," simply closing those paths does not secure against the broader, more organized, mature, and insidious threat that cyber warfare proponents assert. And while the report further catalogs the expanse of the threat, the conclusions are focused on closing the known holes and implementing processes to look for more holes. While this retrospective admonition has merit, efforts based on this distractive construct of integral improvement not only diverge from the attack style but also propagate the limitation to invest in and support development of modernized capabilities. In gist, what is being asked is to fundamentally change how defense is enacted. The real imperative of cyber warfare is to defend against something of which we have no knowledge, arriving as a previously undiscovered zero-day attack, and entering on one or more vectors about which we do not know and over which conventional defense has little control or visibility. Even so, outfitted with the latest weapons on each of the vectors, the strategy focused on finding something new to block may in practice allow the attacker to use defense systems and practices against themselves, whereby an effort to block the traffic in a gross motion may result in a self-inflicted denial of service. Summarily, war in the cyber realm contends for the need to stop just defending, bring the various vectors into a unified interdependent defense model, and have concentrated reactions specific to the attack. Further maturity is then needed in a strategic shift from force protection to surgical response with focus on precision mitigation, low false positives, inoculation or learning where possible to defend against repeat or similar attacks, and effective and immediate recovery of systems that have been attacked.

The mobility and dimensionality notwithstanding, with the perceived necessary central approach to manpower, management and reporting, ease and consistency of tools (i.e., homogeneity), and automation (e.g., updates and filter list managers), the detection and pragmatic block of all possible mechanisms and signatures to avoid any potential known types of attack simply is not scalable. Antivirus powerhouse Symantec announced in its publicly available quarterly report that it created 457,641 new malicious code signatures in the second quarter of 2010, down from 958,585 in the previous 3 months (Symantec 2010). McAfee indicated earlier this year that growth in new malware recorded remains around 40,000 pieces per day (Muttik 2010). (How many signatures can an IPS run before a significant drop in performance occurs?) The signature convention of blocking all possible inroads based on historical attacks is unsustainable. Moreover, these staple products use an asynchronous method of update, whereby the new malware must be identified, submitted to the vendor for processing, and then downloaded, with a periodic client update to be installed on a computer to detect and then possibly mitigate a future infection by the known malware. Considering the incredible capabilities of worms and other attacks like Conficker and Aurora, perhaps a deficiency in the current model that is even more sobering than scale is time.

By the time the press had come out about Google being under attack by Aurora in January 2010, at least 34 other organizations had indicated they had come under the same attack. Ongoing worm research has also indicated that, through similar techniques, as many as 1 million hosts can be compromised by a worm in as little as 0.5 to 1.0 seconds (Stanisford et al. 2004). So even the most robust traditional security just does not scale to protect from initial attack and does not learn fast enough to keep the compromise from spreading. Details now known about the Aurora attack indicate that the attack was so diversified, used encryption and obfuscation techniques of a complexity not seen before, and came from such a spectrum of sources as to avoid traditional detection. In just these few examples, it becomes clear that time is not on the side of traditional processes and even the best of traditional security is not geared to detect, let alone respond to, the changing threat. To wit, after further study, botnet expert David Dagon of Georgia Tech provided a telling rejoinder that beyond the network-based security not preventing the spread, "the network *is* the infection" (Dagon 2005). Therefore, the defense style must, by virtue of functionality, now be transformed from an irresolute, static, and isochronal response to a dynamic, flexible, and predictive one to detect sooner and more effectively thwart the ever-changing attack.

More to the point, the evidence on all fronts drives home the requirement to bolster the advancement or replacement of traditional tools aimed at dynamically updating host defense and anomaly recognition, prime the ontogenesis of detection and containment techniques, and incite the discovery of new tools and algorithms designed to see new kinds of attacks before infiltration. Those all begin with access to data. Typically, new tools are developed using simulated data, network replay, or analysis of collected sensed data combined with data stores of log files and similar system-specific information. Any systematic approach to innovation by requirement features access to that

data, at least as a tenuous first step in progressive ingenuity. However, storage directly affects capability (i.e., you can only store so much for so long) and retrospective analysis directly affects network bandwidth (i.e., all this sensed data must be backhauled to a central location for processing). Therefore, even in this first phase, generally any data collected must be limited by some suspicion threshold that triggers capture before caching locally and then compressing for transmission to the depository. Care must be placed on the right rule sets to balance the amount of data being captured and the bandwidth and storage required to retain it. (At what decay rate does the data collected from such attacks become unusable for improvement or development of new strategies?)

The other shoe

"Botnets" are not just quite prevalent today but all the rage, creating a marketplace that is both highly sophisticated and inexpensive. It has been reported widely in recent months that hackers are having what some call a "fire sale," whereby an interested party can buy a "botted" computer for a slice of time for as little as $0.02. That creates an inexpensive attack infrastructure that is not only voluminous and widespread but also highly adaptive and dynamic. Imagine being an upstart hacker needing to test a new algorithm, distributed denial of service, or a malware solution for data exfiltration from a company or even a federal agency. Being able to rent a large infrastructure of botted machines from around the world for the price of a few hamburgers would surely facilitate a large-enough attack source or malware hosting facility with sufficient obfuscation as to provide immediate results on the validity of the code while avoiding detection of the actual traffic going into and out of the Internet access gateways, let alone tracing of the sources or criminals moving as quickly as the shadow of the cloud under which they hide (Delbert et al. 2010). Further, the high availability and variety of different systems in diverse locations make it possible for hackers to rent the appropriate facility to reduce the hacker test-to-production life cycle for their malicious wares. The proverbial shoe is clearly on the other foot.

In stark contrast, researchers in retrospective-based defense system development rely heavily on large, expensive, summarily classified or otherwise unavailable (and as a result, often quite stale) data sets with rigid posture and limited scope to test their ideas. Trying out new tools is not only complicated and time consuming but also costly and often delayed enough that researchers cannot know whether the ideas will bear results until just before or even after the finished product is sent to market. Even more likely, the research takes so long and costs so much money that the resultant technology is already stale or unusable and is insufficiently up-to-date with the malicious world against which it was being designed to protect. Behavioral heuristics (detection of traffic anomalies), code obfuscation and encryption detection, infection detection and quarantine, and cyber genetics certainly all have value and are being funded and pursued more than ever, but all face this same dilemma. Without early testing of ideas on quality offline data, intermediate validation of budding algorithms using increasingly real-time traffic, or full-scale evaluation of the resultant solution in real time in a real environment, the cycle from idea to production expands to a nearly untenable and mostly unsustainable ambit. It then seems relatively imperative to find new ways to get data to the science or, even better, get the latest science more fugacious access to the data to bring that science to market faster. Further, engaging the mature tool sets in this final stage of access to contextual traffic for evanescent validity, the construct is finally broached for ongoing support of the research, stimulating both evolutionary and revolutionary adaptation to the threats while improving the effectiveness of the installed security base.

Newer defense systems generally begin to abandon signatures that require mechanical updates to a large database running on the appliance supplanting them with software or even Application-Specific Integrated Circuit (ASIC)–based algorithms that look for particular behavioral patterns in the traffic or anomalies in the data. Detecting certain ways a malicious code will try to behave to avoid detection, phone home, receive remote instruction, or seek to further infiltrate are more and more known by analysts and researchers to the point of guessing that if that pattern of traffic occurs, it may well be malicious in nature. Some researchers have gone further to indicate that programmers operate with similar behavioral patterns and are more easily detected. The desire to remain anonymous, to fragment traffic to avoid header analysis and the sheer numbers of resources around the world to enlist as an attack source are all clear indicators of a need for suspicion, and inclusion of these characteristics reduces false positives significantly. In some cases, these kinds of indicators are being built into the tool sets scanning data in retrospect and into IPS and content scrubbers watching traffic patterns, but in other cases, it is a unique research algorithm searching public information for human behaviors and configuration patterns. For example, how a Domain Name Service (DNS) server is configured in support of a domain might indicate the administrator's desire to

remain low key. A broad study of publicly available DNS information may uncover a trust model or likeliness of becoming malicious at a later date. Cordoning off traffic to and from those addresses, domains, or network neighborhoods for more intense scrutiny would be more palatable because it reduces the amount of traffic that requires such scrubbing and the hardware and bandwidth required to watch with intensity.

This particular type of discovery is not exactly easy to do but does not necessarily require access to live traffic. Yet information being learned from such research becomes a more critical part of the overall protective mechanism and must be integrated into the comprehensive defense posture. Were the shoe on the other foot, or more precisely, were the shoe in the production environment designed to assimilate or accommodate the other shoe being developed across multiple research communities, the ability to test the capability on the operational foot would provide profound help in bringing both capabilities to bear on protecting the network. Unfortunately, the current architecture is often device based, or even ASIC based, and introduction of new algorithms and tools is not simple. And incorporation of the solutions others have found is even more incoherent (reminiscent, to maintain the allegory, to the intelligence fiasco of *Tall Blond Man with One Black Shoe*). Instead, research from various fields and intelligence gained from those fields need to be married in a new approach to dynamic security posture.

In complement, several security vendors, as well as federal institutions and federally funded university institutions, have made significant strides in Internet Protocol (IP) trust models. By using both collected data from a worldwide installed base of sensors and firewalls, as well as security alerts and massive data stores of attack data, researchers have been able to create incredible databases used to categorize bad agents, agents who may work with bad agents (guilt by association), and hosting or network providers and supporting bad agents (autonomous systems that provide a safe haven for agents that generally do bad things). Cognate to these approaches, innovations such as Milcord's Botnet Threat Intelligence has been able to identify malicious content providers by rapid changes in DNS information or the hosting of large numbers of domains across a very small number of IP addresses, a behavior known as fast flux (Caglayan et al. 2010). Colorado State University's Border Gateway Protocol (BGP) Monitoring System (Yan, Massey, McCracken, and Wang 2009) has vastly improved the capability of identifying suspect organizations based on route changes found in BGP route tables from around the world. And there have been several ventures into genetic and immunization models for dynamic defense, worm quarantine, and other means to identify and prevent the spread of malicious worms and Trojan-based attacks. These efforts, and others as they arise, need to be verified in the real environment, as well as incorporated into the overall attack strategy of the enterprise.

The Defense Research and Engineering Network (DREN), being the wide area network service provider for the Department of Defense's Research, Development, Test & Evaluation community, is in a unique position to collaborate with these types of research in pursuit of the development of a robust and dynamic security posture servicing a mature and complicated environment. This solution is principally delineated into five elements:

- Identify (mainly through intelligence) historically or potentially malicious players (some through behavioral analysis), networks, or "neighborhoods" before they attack, and handle traffic to or from those entities appropriately;
- Detect or sense suspect traffic patterns as early as possible to identify and contain events as they are under way;
- Combine near-real-time alerting and response (or countermeasures) with retrospective analysis to get to quick reactions as events occur (or are suspected to be occurring), as well as full details shortly thereafter;
- Use dynamic networking capabilities to create a tiered approach to protection and prevention, creating a mechanism for best-in-class protection being provided by different devices, potentially even in different locations;
- Facilitate the research in all these areas by providing access to data with appropriate controls and platforms so that new solutions can be proven and brought to bear sooner.

Through collaboration on several diverse projects with other federal and federally funded agencies and programs to pursue each of these elements, DREN can readily vouch that significant research has already been done in many areas such as improved analysis, heuristic-based detection, and even behavioral analysis of the attacker, all to provide increased intelligence of who the bad guys are, where they tend to live, and what they look and act like. Those data points and projects have increased and continue to help increase the vital ability to defend the ever-changing environment in pursuit of an ever-evolving mission. Integration of these research elements, by redeveloping the architecture to make it compatible with influx of intelligence

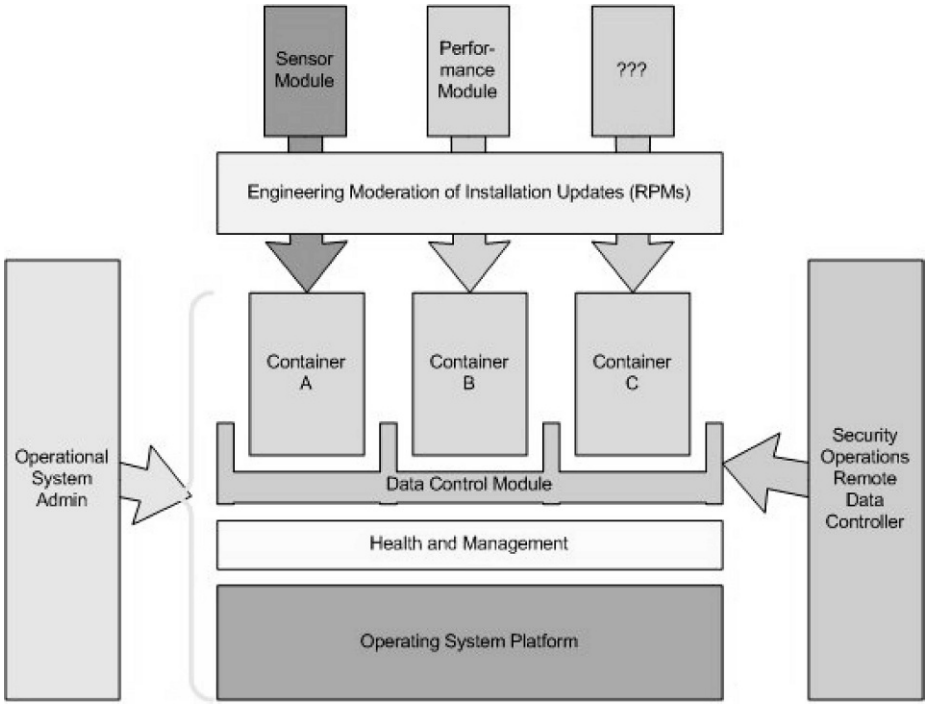


Figure 1. Joint Sensor functional architecture.

and rethinking the data structures to support analysis from both internal and external sources, provides the pivotal pieces to migrate the traditional architecture in pieces to a more robust and nimble posture. Being a wide area provider, however, puts DREN in a unique position to focus our efforts on the final of these elements, namely, getting data to offline scientific research and getting the results of that science into the environment for proof and innovation. For this reason, the Joint Sensor (JS) project was initiated to concentrate our proficiencies for the betterment of cyber research in pursuit of that grand defense solution.

The DREN JS

The crux of the DREN security architecture that spans all five critical elements of strategic defense is the invention of a new multipurpose platform, the JS (see *Figure 1*). This platform services both real-time and retrospective analysis tools, will be fed in places by dynamic network redirection of suspicious traffic identified through intelligence feeds and other mechanisms, and will make access to data more readily available for proving research in a real environment. While the main idea being conveyed is to allow testing assets to sit next to or on top of a device already providing production sensing, the JS platform is more broadly valuable in that the platform is capable of supporting some of the more rudimentary requirements posed by a security operation with a dynamically changing deployment strategy—namely, full or partial reimaging, traffic-specific sensing, and functional participation in a cloud-based distributed environment.

The key to the JS project's success over the various historically incompatible uses (operational, data mining, and research algorithms) is its component design as an appropriately sized, multipurpose computing platform with data connectivity allowing for the collection of sensors to act as a fully capable, distributed, node-parallel computing platform. To gain the advantages of this, various methods of data separation and protection must be applied internally to a system and then externally to how they are connected to the network. The system's specifications were also selected as being able to support the more recent advances in virtualization and process isolation, making it possible for the various elements to coexist without treading on one another. Then, in addition to having enough capacity to operate correctly when at full network flow load, the design of the system allows for other uses when the network load is normal and far less than full capacity.

Computational techniques and hardware for a given price point have advanced far enough to apply better than simple signature techniques to improve cyber security. Given the multicore, large memory system that is required to deal with a high-bandwidth or denial-of-service attack, a significant amount of processing power would be available at all other times

for nonoperational uses. Classic design of sensing requires many sensors located at the network data. This means that the JS systems across DREN mostly will be available as a large, distributed-processing computing capability. Advances in scheduling, memory use, data mining, and parallel techniques would allow this capacity to perform research and test functions without interfering with operational function as a classic security sensor. A key advantage to this approach is that the same network flows (Rajahalme, Conte, Carpenter, and Deering 2004) that are being examined in the normal ways can be examined, mined, and vectorized by both emerging applications and research sampling methods.

In addition, with the bandwidth available at off-use periods on the high-performance DREN network, both existing and new methods in the area of data cross-correlation can be researched and developed as a stage toward integration with a response mechanism. When combined with tools such as BGP Flow Specification (FLOWSPEC) and other network data copying and redirection techniques, network flows of interest can be sampled or piped through other resources such as those available from the High Performance Computing Modernization Program for even more advanced and intense algorithms. These algorithms, working on live data that is representative of both normal and intrusion-type flows, can lead to new techniques of detection, elimination, and even potential cleansing to deal with the ever-changing threats. Even in the area of existing operational sensing, the JS project can add a new capacity by providing communications and computational frameworks for doing simple distribution and redistribution of signature and threat analysis processing across all nodes, shifting work from heavily used systems to barely used ones. Techniques can be applied to cross-correlate data and findings across all nodes such that, for example, network flows seen in more than one location are only processed or analyzed once in the path. Moreover, signature hits can be multicast to the other nodes to increase monitoring of related flows or to change scheduling in recognition of a high load event spreading across the network.

Data separation in the joint sensors will have many facets. Initially, the standard mechanisms are process core binding and data isolation, combined with hardware-supported memory protection. The operating system was selected to be able to take advantage of securing mechanisms available now or being added incrementally, such as security-enhanced Linux, containerization, and full virtualization. Since a large reason for both the operational and the research use of a JS system is to capture the full network traffic at the location, a mechanism will be developed to act as data controller for that network capture. A single capture will be passed to one or more existing modules or methods of analysis. A more controlled and possibly restricted copy of the data would be made available to research algorithms on the system. A sanitized and restricted data set could be made available on the system (most likely to a separate virtual machine on the system) for use by external and affiliated researchers. In addition to all of these methods local to the system, the data controller could send a full or subsampled set of the data using an encrypted path to other resources for further analysis or research algorithm processing. This last method could also be used to make diagnostic captures based on a filter definition fed from a remote, fully authenticated control station. Similarly, controls could be passed into the system, such as to satisfy data requests from law enforcement, which could include instructions for the data controller to apply special encryption to the data and pass multiple copies to distinct and appropriately controlled archival systems.

All processes will be fully vetted before deployment on the JS. In addition, extra steps can be deployed to ensure proper function even while running a research module. Some such modules can be subjected to additional memory and processing restrictions (core affinity, central processing unit utilization, and memory allocations), as well as techniques such as memory leak monitoring and process destruction, to ensure no deleterious effects on the mainline processing of the system. In addition to these mechanisms within the operating system, new techniques provided by libraries and processor features will add virtualization capabilities to provide further isolation. These methods include containerization, which allows a process to run on the main operating system but with no access except as defined to the operating system and leaves the process unaware and incapable of interaction with other processes on the system. A further step would be to do full virtualization, where a module would exist with its own operating system and copy of the data without interaction with the host operating system, any process on that host system, or any data or process of another guest virtual machine. This technique also allows for any Intel-based operating system or appliance-like package that is completely different or incompatible with the RedHat Enterprise host operating system to run locally and have the captured data set available (using internal host or guest network interfaces).

These systems are homed to the DREN network. By its mission, DREN is a high-performance, high-capacity network to transport Department of Defense research and development, science and technology, test

and evaluation, and modeling and simulation data. As the transport and security of the data results of the sensor function need to be assured, this is another place where separation and control techniques need to be used. The DREN architecture provides several mechanisms that are useful to this need. First, multiple layer-3 IP virtual private networks can be used with varying amounts of separations to ensure connectivity and monitoring of the JS system; and delivery of its data can be handled in a separate and preferentially queued way. The path of data to CERT operations and internal research systems would use this method. The redirection and cloning of data using BGP FLOWSPEC techniques would also use similar layer 3 methods available. At the next level, DREN can provide isolated layer 2 paths. Using virtual private local area network service in a configuration developed for another project on DREN, the console implementation will use a layer 2–separated path from the operations control points to the sensors while not allowing traffic between the sensors. This console implementation provides connectivity to the onboard integrated Dell Remote Access Controller interface, which implements a full Intelligent Platform Management Interface 2.0 capability and then some. What this means is complete control of the system from a remote location with console functionality—both serial and graphic, as if locally connected—but only from predetermined locations. In addition, this has the capacity to mount a remote image that appears as if a digital video disc was inserted into the system.

Using this combination of tools, a complete system boot from the remote image; preparation, install, and customization of the operating system; and inclusion of all add-on modules can occur across DREN in a private, controlled manner. This can occur remotely in about 35 minutes, in contrast with 25 minutes when using local media in the local installation lab setup. This capacity not only provides full control to ensure that the sensor remains fully functional at its operations mission but also allows it to be adaptable and even completely remoldable without significant shipping costs, travel, distributed manpower, or downtimes that are longer than necessary. Since this is a limited virtual private local area network service deployment of layer 2 connectivity, its separation from any other DREN function is high, and the locations with access to this remote console capability can be tightly controlled to restricted, on-network sites. Using the system's other interfaces, additional paths will be set up to manage the system, collect data for the operational CERT functions, communicate with the other JS systems, and have the capacity to set up temporarily unique captures and data paths over DREN. Having these interfaces and paths allows the use of the features inherent to DREN to provide high-capacity, secure communications where data protection and integrity are ensured.

Expectation engineering

The final piece of the sensor bed puzzle is engineering the willingness to support such an intricate solution. The success of even getting such an emergent test bed deployed within an operational environment boils down to three key elements, at least in terms of bringing to bear the right framework to create and sustain the environment, as well as to provide sufficient verdure to attract willing parties and sustain harmonious living within it. These three elements are as follows:

- Providing access for the researchers to real operational data sets (traffic, data store, central storage, or other appropriate capability, whether on the device or in a controlled shared space), as well as to the test sensor packages in the cloud for managing and making changes to the product;
- Indirect but immediate sharing of algorithms to security operations that provide visibility into attack vectors not otherwise seen using traditional sensing and showing intrinsic value for the arrangement;
- Guaranteeing some level of control but, more importantly, significant levels of visibility for network and security operations into the function of test capabilities and the process whereby the first two key elements are managed and delivered.

In an environment where security is prime, there has historically been a separation and isolation between operations and research, usually upheld in reality by dividing activities on network segments (e.g., demilitarized zones, border zones, and lab networks), as well as temporal separation between live traffic sets and data being offered for research. Simply put, there has been limited access to the live network by anything other than stable and secured applications and devices. To facilitate this test bed and provide benefit to both operations and research that are nearer real time and lasting in effect, some of those conventions need to be broken down, and the research must be meticulously inserted to maintain the original character of security. At the outset, this translates to not only best practices but also sophisticated operational security measures on the joint sensor, as well as in the processes of securing the applications before use. To make network security operations a willing participant, these additional functional requirements for the sensor test bed mean leveraging stable and tried operating systems, middle-

ware, and application configurations in the field. Perhaps far more important to success and willingness, there needs to be visibility access granted to security operations—not just into the additional software but also into the processes and procedures of how those elements are managed and maintained. Controls must be implemented on how information is shared with the software and, in turn, from that software to its management systems, source coders, and stakeholders. But more rudimentarily, this leads to an emphasis on visibility into the process of fielding a package into the sensor test bed so that operational security can inject reviewing hinge points and affect policies at various review stages. An engineering resource internal to the organization that will take the research participant, along with the operations participant, through the process from concept to field trial gives all parties sufficient voice to ensure the solution is engineered within expectation and guidelines.

This progression is also a phased approach, whereby the research participant begins with access to sterile data with which to run algorithms to do a rudimentary proof of concept offline, followed by an experimental initial offering in a lab environment using real but not real-time data, quickly proceeding to a similar scenario where live or nearly real-time streams of operational data are tested for verification of algorithms, as well as constructive processes such as management and alerting. These earlier phases give the researchers the opportunity to test their theories before expenditure of operational man-hours and resources for field deployment and to create a more trusted expectation once field testing is approved to begin. Through this phased process, another of the key elements is awarded participants: algorithms and actual results using live data can supply researchers with validation of the algorithms and demonstrate to operations with evidence that these algorithms are of value. Once in the field, a more intimate relationship between researchers and operations (or at least the output of the test sensor and the input of the operational security mechanism), brokered by the internal engineering capacity, will give the security participants more immediate value by finding issues their tools would not otherwise have found. Conclusively, these algorithms, running in parallel to existing capabilities, provide a number-for-number cross-correlation of results, false positives, and detection rates as all are subject to the same traffic.

Ultimately, the grandiose concept of a cloud of test sensors built on the back of the production sensors requires as much operational nuance as it does technical innovation to ensure environmental policies are enforced, participants have valid expectations, and real results have both immediate and long-term impact. In the DREN JS project, the supporters of the former methodologies have been enlivened by the opportunity to provide input to the building of the sensor and the process whereby the sensor will be managed, and part of that enlivenment was directly created by an enlightenment of seeing new sensor technology find real issues in data that the incumbent technology had not seen. Billing the new technology not as a replacement of the existing methodologies but, instead, as an enhancement to them would not have created willingness without the proof of real data and visibility into how the system would fit into the architecture.

Dynamic network support

In general, the effectiveness of intrusion detection systems, intrusion prevention systems, and even firewalls is like real estate—location, location, location—and in general, prime location is at the enterprise edge facing the wide area network. In the case of DREN, a wide area network service provider, the edge is an asymmetrical collection of geographically diverse network access points connecting the network to a variety of upstream and downstream entities, such as tier 1 and regional Internet service providers, direct and private peers, and of course, customers. This renders the key location to see the most traffic a less-than-optimal location to see both sides of any given conversation. As best current practice for a wide area network is still "hot potato routing" (getting packets off your network as fast as possible via the closest connection along the path to the destination), the capability to synchronize bidirectional conversations is impractical and nearly impossible to manage. However, significant capabilities in network equipment can now facilitate "symmetrizing" predetermined connections or "flows"[1] such that the traffic to or from a particular prefix or protocol of interest can be dynamically redirected to a remote-triggered black hole, sink, or scrub (see *Figure 2*).

A remote trigger is a means to dynamically tell a network device (usually a router) to redirect traffic with certain parameters (source IP address, destination IP address, IP protocol, and transmission control protocol/user datagram protocol source and destination port) as it hits a filter or access list, sending this traffic to a black hole (a means to drop the traffic), sink (a collector designed to capture the traffic for analysis rather than just drop it), or a scrub network. A scrub is a collection of tools that can be in line at a separate location somewhere in the network cloud used for monitoring or performing stateful inspection, intrusion protection, or content filtering, and allowing valid traffic to proceed unchanged to its original destination.

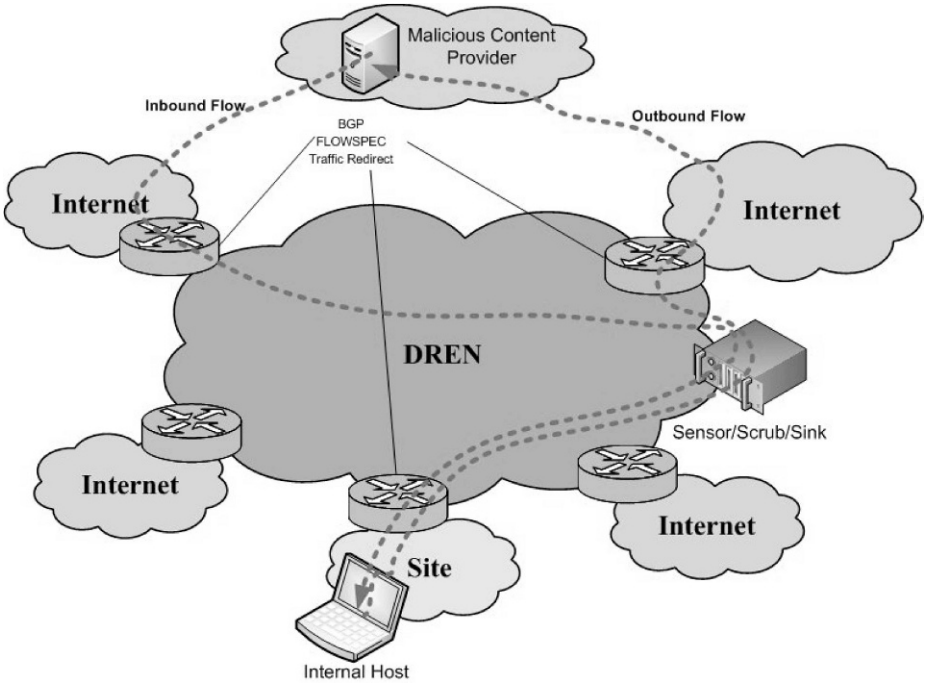


Figure 2. Dynamic redirect using Border Gateway Protocol Flow Specification.

This scrub network redirection is facilitated by configurations and protocols designed to temporarily modify the path of the traffic within the network without giving any indication to external entities that the redirect is occurring. Even better, because the network can be affected bidirectionally, traffic through the scrub is now symmetrical, and both sides of the suspect conversation can be monitored through a single inspection point.

Because this redirection is now available, it is no longer required that you have all the right tools at every possible location, and tools at specific locations can be specialized to focus on particular protocols or traffic types. For example, consider a subscription service to malicious URLs or an intelligence feed of alerts about suspected "botnet" addresses. It is possible to inject this intelligence into the network so that the boundary devices (facing the ISP and the customers) upon receiving any packets associated with these suspect addresses and/or protocols can be redirected to the scrub (or sink). There the tools can now see both sides of a connection in order to accurately determine malicious content. For the purposes of a sensor test bed, you no longer are required to have sensors at every site to be of significant value. An algorithm that focuses on malicious web traffic, email scanning, DNS attacks, or any application-specific determinism can now sit in a single or a few locations and achieve complete visibility into all interesting traffic for focused testing.

One particular element, a new network layer reachability information protocol of BGP known as FLOWSPEC, allows a system (such as an sFlow collector or analysis tool) to publish "rule sets" in the fashion of particular flow or traffic parameters in a BGP session with a specific action (such as discard or redirect). This gives the security operations the capability of dynamically updating filters on routers across the wide area simultaneously. Used in conjunction with virtual route forwarding tables and protocols like multiprotocol label switching, FLOWSPEC enables dynamic blocking—or better yet, redirection—based on information gained from outside sources, deep packet inspection, or retrospective analysis. In conjunction with a sensor test bed, particular traffic patterns of interest can be "symmetrized" and sent to a set of tools for better isolation and tighter focus of research algorithms. In the context of the phased approach mentioned earlier, dynamic redirect could surgically separate known-suspicious packets and send copies or temporarily divert that traffic through a controlled, laboratory-type environment without having the test software residing in the production environment or touching valid, sensitive data.

As an aside, this capability can change with the perspective of the researcher. As indicated earlier, it is possible to redirect traffic based on an intelligence feed, the outcome of internal analysis, or other such means of identifying peculiar or suspicious traffic. Likewise,

just this part of the overall mechanism is a means to research emerging algorithms or tools in that the choice of what traffic is diverted to a particular sensor or scrub center may be determined by the work of a new tool or even an outside research project. Today, feeds from Milcord, security vendors, lookups from the BGP Monitoring System, and others are all possible candidates for a redirect to an algorithm-specific sensor or protection system, making it readily possible to divide and conquer and thus reducing overall performance and bandwidth requirements on any individual system and constructing a defensible boundary one protocol or application at a time. Other methods for identifying things for redirection can also be tested safely, including research such as cyber genetics, man-in-the-middle botnet investigation, and immunity algorithms for identifying bad patterns and other negative characteristics. This thinking goes quite well with the distributed parallel computing capabilities of a collection of joint sensors across DREN.

In the end, dynamic network support is critical to facilitating the next generation of traffic protection, sensing, and enterprise-wide dynamic security architecture with a focused attack response. In the meantime, for the purposes of a test bed, it becomes quite powerful in facilitating the first phases of proof of concept for new algorithms and tools before they are put in the production realm. This extra step in the process provides sufficient "warm up" time for the security operations teams to assess or remove any question before putting any risk on the network. Similarly, the ability to send only the traffic that needs to be seen by the particular algorithm, selected specifically for its suspicious or known malicious nature, means the tool does not have access to sensitive data but does still get sufficient real and real-time traffic to perform the research. Any anomalies detected or protections proven through this dynamic redirect give the research considerable value and provide security operations tremendous insight into the function of these new tools—without putting them in production.

Next steps

The first opportunity to improve the development cycle of interesting new tools from concept to production is to provide data sets to researchers for early analysis. Once the algorithms that are implemented in the tools are proven and improved through access to production traffic, the logical next step is to develop a means to incorporate what the algorithm detects into the overall, aggregated analysis and response system of security operations. Systems and algorithms developed through research around the world result in new intelligence feeds and alerts that can feed the central aggregate analysis in the production environment, as well as those rule sets indicated in flow data and BGP FLOWSPEC deployments. Likewise, these tools being developed and possibly deployed as products in other networks and research environments should then result in new alert feeds made available to this network as production tools. The aggregation of these data streams is critical in the next generation of security architectures.

A project under way at the Naval Research Laboratory in Washington, D.C., is taking this concept and creating a sort of cross-correlation system. Tools such as host-based security systems, firewall and IPS databases, malicious uniform resource locators, and other subscriptions are all being synchronized to create a multidimensional set of target parameters. DREN has a similar function being developed, whereby a scripting system is used to indicate whether particular IPs are showing up in multiple intelligence feeds. Certainly, any IP or prefix or autonomous system number that appears in multiple lists should be regarded as a more serious threat and can be more closely scrutinized. In addition, taking data from multiple solution sets from various vectors can help create a richer attack vector analysis and present analysts and dynamic watch systems with a sort of trust model of dangerous protocols or "bad neighborhoods." Just as long lists of individual known bad IPs is hard to digest and incorporate in a watch list or analysis tool, too many tiny fragments are that much harder to distribute through protocols on the network. Therefore, being able to combine knowledge from multiple sources and different types of information into a general attack and protection pattern simplifies the architecture and provides a more robust response system.

As previously indicated, dynamic protection also engenders the focused response as a measurable outcome to be researched during this project. The researchers that are creating the algorithms should be working in concert with the security professionals to develop response mechanisms and methodologies as part of developing the detection and prevention strategies. Mitigation recommendations and progressions for various traffic types or attack intensities, reduction of false positives, inoculation against repeated attacks, and means whereby infiltration can be recovered from must be incorporated into the defense strategy as each technique for discovery is pursued. Expecting the vendors and researchers to provide both new alerts and sustainment is critical in the thought processes required in making a marketable product, as well as an integrated tool for use in the environment.

One next step in the sensor test bed project is to develop the mechanisms and processes whereby potential suitable research initiatives can begin taking advantage of this new solution. These must be finalized and put into a quality management system. The goal of this programmatic development is to better understand the nuances of how to select the most valuable and most mature tools first and get immediate benefit from the program. In parallel, as a measure of effectiveness of the program and the tools it produces, we must also focus on improving the political relationships and creating solutions that are more immediately usable by the broader federal community, even while still in the infant stage. The tools being produced through the test bed should not be limited to use within DREN and should also promote the development of (or compatibility with) community-centric capabilities such as shadow-mirror databases, standardized data structures and formats, reporting templates, and alert communications systems. A tool being developed through the JS test bed may bring to bear components where national or vendor-specific collections of attack signatures and threats—like McAfee's IP Trusted Source or Symantec's AV database—would benefit the community greatly and much earlier than traditional procurement processes afford. A shadow-mirror is a duplication of a vendor database that receives updates from the vendor system (being populated by submissions and alert feeds from all over the world) but then becomes the internal collection point of new additions discovered in the wild within the community (rather than reporting them to the publicly available system). It is called a shadow because the sensitive information from the environment is kept internal, but the lessons learned (from attack) are available from both inside and the Internet at large. Any tool that is introduced into the test bed would also be required to create a module for this central collection and continue to provide updates for the life of the product, whether it is eventually sold into the federal market or not.

Conclusion

The DREN Cyber Security Test Bed will provide a novel environment for testing new cyber security methods. The following active elements will be implemented as individual, well-contained modules: traditional government off-the-shelf intrusion detection software, traditional commercial off-the-shelf intrusion detection software, active network performance software, and experimental cyber security code. The test bed will be embedded in a production network, thereby providing real traffic to all modules to generate in situ results for comparison, contrast, and correlation. This collocation of cutting-edge security with existing security infrastructure (embedded in a production network) will dramatically expedite the transition of posited network and data protection concepts to proven adaptive cyber security algorithms.

The success of the program relies on not only quality technical implementation but also sound operational and expectation engineering. Creating processes that allow for visibility and interaction from security operations and providing nearly immediate results back to researchers and operations will solidify the value of a given tool and the program as a whole. Bridging the gap between product research and support for the federal environment in the shape of new data feeds, comprehensive aggregate analysis, and response solutions, the goal becomes furthering the overall process, not just the posture of the enterprise security architecture. With so many new attack styles and dimensions, the most valuable outcome of this project will be the new way of approaching the problem. ❑

Mr. Tim Owen received his undergraduate degrees in telecommunications engineering technology from Capitol College in 1989 and physics and science education from North Carolina State University in 1992. He is the chief engineer for WareOnEarth Communications, Inc., and is a key member of the DREN engineering staff. E-mail: towen@hpcmo.hpc.mil

Mr. Rob Scott received his bachelor's degree in communications media from the University of Maryland in 1986. He is currently the chief technology officer of GeoWireless, Inc., and is a key member of the DREN engineering staff. E-mail: rob@hpcmo.hpc.mil

Dr. Roy Campbell received his doctorate in electrical engineering from Mississippi State University in 2002. He currently serves as the program manager for the DREN. E-mail: rcampbell@hpcmo.hpc.mil

References

Baker, W., et al. 2010. 2010 data breach investigations report. http://www.verizonbusiness.com/resources/reports/rp_2010-data-breach-report_en_xg.pdf (accessed October 13, 2010).

Caglayan, A., Toothaker, M., Drapeau, D., Burke, D. and Eaton, G. 2010. Behavioral patterns of fast flux service networks, *Hawaii International Conference on System Sciences (HICSS-43) Cyber Security and Information Intelligence Research Minitrack*. Koloa, Kauai, Hawaii, Jan. 5-8, 2010. http://csdl2.computer.org/comp/proceedings/hicss/2010/3869/00/02-02-05.pdf (accessed October 10, 2010).

Dagon, D. 2005. Botnet detection and response: The internet is the infection. OARC Workshop. http://www.caida.org/workshops/dns-oarc/200507/slides/oarc0507-Dagon.pdf(accessed October 13, 2010).

Delbert, R., et al. April 2010. Shadows in the cloud: Investigating cyber espionage 2.0, JRo3-2010. http://www.nartv.org/mirror/shadows-in-the-cloud.pdf (accessed October 10, 2010).

Economist. July 2010 War in the fifth domain.

Muttik, I. 2010. Coorperation is key to internet security. McAfee Security Journal, 2010 (issue 6): 20–24. http://www.mcafee.com/us/local_content/misc/threat_center/articles/summer2010/msj_article05_cooperation_is_key_to_internet_security.pdf (accessed october 13, 2010).

Rajahalme, J., Conta, A., Carpenter, B., and Deering, S. 2004. IPv6 flow label specification, *Network Working Group Request for Comments, RFC 3697*. Reston, VA: The Internet Society, http://www.ietf.org/rfc/rfc3697.txt (accessed October 13, 2010).

Staniford, S., Moore, D., Paxson, V., and Weaver, N. 2004. The top speed of flash worms, In *Proceedings of the 2004 ACM Workshop on Rapid Malcode*, October 2004. http://www.icir.org/vern/papers/topspeed-worm04.pdf (accessed October 10, 2010).

Symantec. 2010. Symantec Corp. FY2011 2Q Report. http://www.symantec.com/business/theme.jsp?themeid=threatreport (accessed October 13, 2010).

Yan, H., Massey, D., McCracken, E., and Wang L. 2009. BGPMon and NewViews: Real-time BGP. In *Proceedings of the Institute of Electrical and Electronics Engineers International Conference on Computer Communications*, April, Rio de Janeiro, Brazil. http://www.ieee-infocom.org/2009/demos/5%20-%20BGP%20Mon.pdf (accessed October 13, 2010).

Zetter, K. 2010. Google hack attack was ultra-sophisticated, new details show. *WIRED*, January 14, 2010. http://www.wired.com/threatlevel/2010/01/operation-aurora/ (accessed October 13, 2010).

ITEA Journal 2010; 31: 512–517

Would You Like Vulnerabilities With Your Computer System?

Richard R. Brooks, Ph.D.
Holcombe Department of Electrical and Computer Engineering,
Clemson University, Clemson, South Carolina

Computer and network development is difficult. Translation of needs into specifications is an art, as is verifying that a technical design fulfills the specifications. Unfortunately, while these seemingly intractable problems are necessary for verifying system security, they are not sufficient. This article presents the difficulty of security verification. The first topic we consider is the economics of the commercial off-the-shelf market. Unfortunately, economics, more so than technical issues, is the driving force behind the prevalence of vulnerabilities. The second topic we examine is that security architectures typically are defined within a limited scope. We discuss the Secure Sockets Layer and Transport Layer Security technology that is the basis of e-commerce. A large number of vulnerabilities were disclosed recently that negate its security guarantees. Finally, we discuss side-channel attacks. Once again, security is circumvented without the need to directly attack the protocols. Small amounts of information leakage can be used over time to circumvent well-designed security systems.

Key words: Economics; power analysis attacks; security testing; security vulnerabilities; side-channel attacks; timing attacks.

Computer and network systems are difficult to reliably design, develop, and deploy. Specifications are written to fulfill perceived needs. Verifying that specifications match those needs is hard, as is verifying that a design satisfies specifications. Developing a test regime to verify that a final hardware system fulfills specifications is challenging.

When one contrasts hardware with software, there are many factors that should make hardware harder to verify than software. Both software and hardware depend on the logical consistency of their design, but hardware systems are subject to wear and tear and degrade over time. Each physical instance of a machine is of necessity unique owing to manufacturing issues.

Despite this, software systems are typically considered harder to test and verify. This is often blamed on complexity. To verify all possible paths through a software system to check for errors, incompatibilities, and side effects is not practical since the number of tests will suffer from combinatorial explosion. Unfortunately, even this prohibitively expensive, exhaustive testing approach is not adequate as there are bugs that appear only when a given set of instructions is repeated exactly multiple times. (Ilja gives examples of security relevant bugs that surface only after the same commands are given three times in a row [Ilja 2007].)

There is another reason, beyond system complexity, that computer systems are insecure. Computer system security depends on external factors. No matter how well a piece of hardware or software is designed, analyzed, and tested; security is hostage to factors a tester cannot control.

This article explores this problem in some depth. We look at how and why contemporary computer system security is compromised from outside. In the "Economics of computer systems" section, we survey how market economics encourages the production of insecure and unreliable software and hardware. The "Security scope" section illustrates how a good security design can be negated by assumptions about its execution environment. The "Side-channels" section shows how attackers observing system artifacts can break security. The test and evaluation community needs to be aware of these dangers and vulnerabilities. We close the article with a set of possible countermeasures.

Economics of computer systems

There is a growing body of research involving interactions between information security and economics (Anderson and Moore 2008). Current market incentives reward behaviors that do not safeguard the well-being of the public.

Hardware and software markets have *network externalities*: the value of an investment depends in large part on whether or not other parties make the same purchase decision (Katz and Shapiro 1985). These markets are "tippy"; miniscule differences in quality or perception result in major differences in profitability. In our industry, network externalities often result in markets where one product dominates. This explains the historically dominant market positions of the IBM PC, Microsoft Windows, and Intel processor architecture (Besen and Farrell 1994). The need to be the dominant player induces pressure to be "first to market" with new applications. Arriving early usually tips the market enough to dominate it. In this "winner take all" context, actions that improve product quality and security, but delay delivery, can be fatal to an enterprise (Dekel and Scotchmer 1999). Ross Anderson of Cambridge says: "If [Bill] Gates had put proper access controls in [Microsoft] Windows … from day one … then Steve Jobs would be a very much richer man …" (Anderson 2010).

This is exacerbated by software being a "lemon market" (Akerlof 1970), with information asymmetry between buyer and seller. The buyer cannot reliably distinguish between quality goods and shoddy products. Under these conditions, buyers choose the lower-priced product. Shoddy products are produced more cheaply, driving quality products from the market. Other factors contributing to the poor quality of computer systems include the following:

- The "Microsoft Philosophy"[1] of "we'll ship it on Tuesday and get it right by version 3" (Anderson 2010) is exacerbated by the ease of distributing patches over the Internet.
- There is little financial incentive to test rigorously. It is common to use clients as unpaid software testers to gradually find errors in programs (Rice 2008).
- Software becomes larger and more complex over time. New versions are released to increase the number of features instead of reducing the number of errors. Since industry perceives that this matches user demand (Gates 1995), this trend continues in spite of a survey by the Standish Group indicating that 45 percent of computer program features are *never used* (De Luca 2002).
- End User License Agreements (EULAs) tend to deny liability for damages due to software failures. This lack of liability is codified both in the Uniform Computer Information Transactions Act (UCITA), which is law in Virginia and Maryland. The Computer Fraud and Abuse Act (CFAA) passed by Congress in 1984 states, "No action may be brought … for the negligent design or manufacture of computer hardware, computer software or firmware." (U.S. Congress 1984).

These factors encourage the industry to quickly produce large quantities of poorly analyzed programs. There is little financial incentive to do otherwise and much to gain.

The consequences of poor software quality for consumers and the economy as a whole are immense. Dr. David Rice cites National Institute of Standards and Technology studies showing the annual cost of insecure software to the United States as conservatively $180 billion[2] (Rice 2008). He also cites a market research survey, which finds that 75 percent of computers connected to the Internet have been infected and used to distribute spam. In addition, numerous cases exist where software errors have proved fatal (Bogdanich 2005, Miller et al. 2010, and Norton-Taylor 2010). The case of the Therac-25 radiation therapy machine, where a faulty user interface resulted in patients being fatally irradiated, is a frequently cited case of a fatal computer software bug (Miller et al. 2010).

In summary, security requires extra time and money. A lack of security is hard to detect and quantify, but a higher price tag is obvious. These market forces displace high-quality products with insecure and dangerous ones. The purchase price is less, but the cost resulting from lost information, time, and lives is greater.

Security scope

We now consider systems that are designed to be secure. These designs are subjected to rigorous peer review, implementations are widely used and tested, errors are exposed, and patches are quickly distributed. This sounds like the ideal approach. A good example is the ssl (secure sockets layer), now known as tls (transport layer security). This is the basic security infrastructure relied on by e-commerce applications. Ssl/tls currently provides little real security, because it relies on assumptions that do not hold in practice.

When an ssl/tls session starts, the client and server exchange authentication certificates that establish identity and provide public keys. Authentication certificates are cryptographically signed to ensure their authenticity. The public keys encrypt messages that are exchanged to securely establish a session key, which is used to encrypt the rest of the session. More details can

be found in Nicholls and Lekkas (2002). The protocol has been thoroughly analyzed, and we may assume it is cryptographically sound. So, why isn't it secure?

The first problem is that network routing is insecure. Internet protocol (IP) addresses are found using the Domain Name System (DNS). DNS is not secure (Kaminsky 2008a, 2008b, 2009b; Young and Aitel 2004). It is possible to create rogue DNS servers or to introduce fake DNS entries into the local DNS cache. This is exacerbated by the ability to poison the Address Resolution Protocol (ARP) cache (Young and Aitel 2004). There are also implementation problems like the flaw that was corrected in 2009 (Kaminsky 2008a).

In principle, the use of X.509 certificates makes up for the DNS being insecure. Certificates are cryptographically signed by a trusted third-party certificate authority (CA) to establish the identity of each party without doubt; however, most sites use self-signed certificates, which do not establish identity (Kaminsky 2009a). Some CAs sell certificates without verifying the purchaser's identity (Molnar et al. 2009), violating the assumptions on which ssl/tls is based). But ssl/tls is backwards compatible with outdated cryptographic techniques that allow certificates to be forged (Molinar et al. 2009). In addition, popular browsers accept certificates from more than 200 root CAs, including foreign governments (Soghoian and Stamm 2010).

Ssl/tls security can be circumvented in other ways as well. When a certificate is requested, it is valid to tell the other party to try again later, and later, and later … (Marlinspike 2009a, 2009b). Ssl/tls is mainly used in tunneled html sessions. There are tools available that perform man-in-the-middle attacks on these html sessions and that are almost impossible to detect (Marlinspike 2009b; Soghoian and Stamm 2010). A bug was fixed in 2009 where node names with embedded null characters allowed nodes to masquerade as other nodes; for example, msnbc could have legitimately created a valid "www.foxnews.com\0.msnbc.com" certificate that every browser would have accepted (Marlinspike 2009b).

The basic problems of ssl/tls all come from elements external to its main design including

- relying on other insecure protocols,
- assuming due diligence by third parties,
- having no verification that software tools are correctly implemented, and
- having incomplete protocol specification.

Side-channels

Side-channel attacks exploit information gained from monitoring a system's physical environment. Since they are frequently used against cryptography, we discuss attacks on cryptographic algorithms to illustrate this problem. The mathematics of cryptographic algorithms is analyzed minutely to avoid any information leakage, but side-channels exploit implementation details of the protocol that inadvertently leak information about keys and/or cleartext data. Well-known side channels include timing, power consumption, and electromagnetic emanations (tempest). The doctrine of red–black separation has been developed to combat side-channel vulnerabilities. Secure processing is performed using strictly separated power infrastructure, frequently within a Faraday cage.

Power analysis side-channel attacks use variations in power consumption of different operations. The power consumption of an operation depends on the inputs. Different operand values cause different switching activities in the memory, buses, datapath units (adders, multipliers, logical units), and pipeline registers of processors. Among these components, the processor datapath and buses exhibit more data-dependent energy variation than memory components (Ye et al. 2000). Power analysis attacks have varying degrees of sophistication. Simple power analysis (SPA) (Kocher, Jaffe, and Jun 1998) uses only a single power consumption trace for an operation. From this power trace, an attacker can identify the operations performed (e.g., whether or not a branch at point p is taken, or if an exponentiation operation is performed). Combining power consumption information with knowledge of the underlying algorithm can be used to reveal the secret key. Differential power analysis (DPA) is a common higher-order power analysis approach. This scheme uses power profiles from several runs and uses the data-dependent power consumption variation to break the key (Kocher, Jaffe, and Jun 1998). In Goubin and Patarin (1999), the secret key is guessed by using 1,000 sample inputs and their corresponding 1,000 power consumption traces. Many researchers have investigated the potential for both invasive and noninvasive attacks. An overview of these techniques is presented in Dhem and Feyt (2001) and in Kommerling and Kuhn (1999). Kocher, Jaffe, and Jun (1998) provide a detailed description of the SPA and DPA techniques. The difference between these two attacks is that DPA is more sophisticated and involves statistical analysis using a larger sample set.

Timing side-channel attacks exploit time artifacts of computational systems. For ssh, one timing side-channel attack exploits the fact that interactive mode transmits one packet per keystroke. Due to the layout of keys on the QWERTY keyboard, some key pairs are typed more quickly than others. Statistical analysis of this information can identify sequences of keystrokes. In Song, Wagner, and Tian (2001) they manually

construct a hidden Markov model (HMM) for harvesting passwords from interactive ssh sessions. For noninteractive sessions, timing attacks can exploit the fact that ssh pads only to 8-byte boundaries to infer approximate payload lengths. A similar methodology is used in (Zhu et al. 2005) to thwart the anonymity provided by mixing networks such as Tor. If attackers can eavesdrop at mixed network entry and exit points, they can collect interpacket timing information. In Zhu et al. (2005), interpacket timings of all entry and exit points are cross-correlated to calculate the mutual information between all entry–exit pairs. This technique reliably identifies the correct communications paths using sample sizes on the order of seconds to tens of seconds. Surprisingly, this attack works better on larger networks than on smaller ones.

A divide and conquer approach can use power difference for Advanced Encryption Standard (AES) encryption done with two different secret keys to crack the secret key within hours. We developed a hardware/software co-design approach to foiling this attack (Brooks et al. 2005; Saptura et al. 2003). Dual rail logic can process all data and its complement. This results in a flat power consumption profile no matter which cleartext and secret key are used. It also consumes over 80 percent more power and generates over 80 percent more heat. We added tags to the compiler, signaling which variables to secure. All data derived from those variables use dual rail "secure instructions." The use of compiler tags results in only a 15 percent energy consumption overhead.

For timing side-channels, as described in English and Hamilton (1996), we use HMMs to observe state transitions and infer semantic information from timing data. Unlike English and Hamilton, our approach requires no a priori knowledge of system structure. The HMM can be inferred directly from observed data. In addition, we can detect interactively whether or not we have collected enough training data to adequately learn the system. In our recent research, we have extended these attacks by inferring HMMs directly from observed process behaviors (Brooks et al. 2009; Schwier 2009). HMMs have been inferred that detect the language being used in interactive ssh sessions (Bhanu 2010), detect protocols being used in tunneled communications (Bhanu 2010; Craven 2010), and violate the privacy goals of Tor (Craven 2010).

This means that security verification cannot be limited to analyzing the attacks that an approach was designed to counter. Verification also needs to analyze all detectable consequences of system use. This, unfortunately, puts the test community in a position where they need to be somewhat omniscient. The Department of Defense strategy of red–black separation that physically isolates secure components makes a lot of sense in this regard. It is, however, not applicable to systems like the Global Information Grid.

Conclusions and suggested countermeasures

Our final conclusion is that security verification may be more challenging than designing and implementing secure systems. The deck is stacked against test and verification in many ways:

- The fact that a company is still in business almost guarantees that their computer hardware and software are insecure.
- It is not enough to verify the security of the system under test, constant vigilance is required to verify that all assumptions about external factors are valid.
- Even if a system fulfills all the given security requirements, it is quite likely that it leaks information in subtle ways that can be exploited.

The mathematics of cryptography is "almost never" the weak link in system security Ferguson and Schneier (2003). Systems are compromised more often through either social engineering or implementation errors. Unfortunately, implementation errors and human gullibility are difficult factors to test.

Some countermeasures are possible, however. While individual consumers in the open market are unable to distinguish between valuable and shoddy products, the testing community could perform a valuable service by demanding accountability and financially punishing producers of vulnerable systems. This could tip the market in a positive direction.

Verification needs to account for all aspects of the system. If a system depends on external authentication of participants, care needs to be taken that certification authorities are reputable and accountable. Protocols need to have conformance tests. Due diligence by all parties must be assured.

Side-channel attacks can be nullified by normalizing resource usage. If implemented naively, this is prohibitively expensive. Our work in Brooks (2005) shows, however, that it is possible to do this in a targeted manner to reduce overhead. For smart-card applications, our approach requires 15 percent additional overhead.

When verifying security, care must be taken not to simply verify advertised security features. It is necessary to analyze the entire ecosystem of the application. ❑

Richard Brooks, Ph.D., is principal investigator (PI) on research programs currently funded by the U.S. Army

Research Office (ARO), Office of Naval Research (ONR), and BMW Corporation. These research projects are in coordination of combat missions among autonomous combat vehicles (ARO), situation and threat assessment for combat command and control (ONR), and security analysis of cellular networks used for vehicle remote diagnostics (BMW). Dr. Brooks' current research interests include game theory, strategic reasoning, information assurance, use of statistical physics insights for distributed systems design, and fusion of heterogeneous real-time sensor feeds. He was PI of the Mobile Ubiquitous Security Environment (MUSE) project sponsored by ONR as a Critical Infrastructure Protection University Research Initiative (CIP/URI). It concentrated on creating distributed countermeasures to overcome large-scale network attacks such as distributed denial of service and worms. Dr. Brooks was co-PI of a National Institute for Standards and Technology (NIST) project defining the security standards and protection profiles for the International Standards Organization building automation control network (BACNET) networked building control systems standard. Dr. Brooks was co-PI of a Defense Advanced Research Projects Agency (DARPA) Information Systems Office program coordinating air campaign command and control and PI of the Reactive Sensor Networks (RSN) project sponsored by DARPA Information Exploitation Office (IXO). RSN explored collaborative signal processing to aggregate information moving through the network and the use of mobile code for coordination among intelligent sensor nodes. He has received DURIP awards from ONR and ARO that support the study of networked systems interacting with the real world. His Ph.D. dissertation received an exemplary achievement certificate from the Louisiana State University graduate school. E-mail:rrb@acm.org

Endnotes

[1]References made to Microsoft Corporation should not be interpreted as stating or implying that their approach to software construction is worse than elsewhere. These references are due more to Microsoft adapting properly to its environment and being more successful than competitors.

[2]Rice 2008 estimates losses from Hurricane Katrina to be approximately $100 billion.

References

Akerlof, George A. 1970. The market for "lemons": Quality uncertainty and the market mechanism. *The Quarterly Journal of Economics* 48: 488–500.

Anderson, R. 2010. *Information security – Where computer science, economics and psychology meet*. http://www.tech.dmu.ac.uk/STRL/news/annual-seminar/STRL-ADS-2009.m4v (accessed March 2010).

Anderson, R., and T. Moore. 2008. Information security economics – And beyond. In *Lecture notes in artificial intelligence, Proceedings of the 9th International Conference on Deontic Logic in Computer Science,* Luxembourgh, 49. Berlin, Germany: Springer-Verlag.

Besen, S. M., and J. Farrell. 1994. Choosing how to compete: Strategies and tactics in standardization. *Journal of Economic Perspectives* 8: 117–131.

Bhanu, H. May 2010. Timing side-channel attacks on SSH. Master's thesis, Clemson University.

Bogdanich, W. 2010. "Radiation offers new cures, and ways to do harm," *New York Times*, January 23, 2010. http://www.nytimes.com/2010/01/24/health/24radiation.html?pagewanted=1 (accessed Month day, year).

Brooks, R. R. 2005. *Disruptive security technologies with mobile code and peer-to-peer networks*. Boca Raton: CRC Press.

Brooks, R. R., J. M. Schwier, and C. Griffin. 2009. Behavior detection using confidence intervals of hidden Markov Models. *IEEE Transactions on System Man and Cybernetics, Part B: Cybernetics* 39 (6): 1484–1492.

Craven, R. May 2010. Traffic analysis of anonymity systems. Master's thesis, Clemson University.

Dekel, E., and S. Scotchmer. 1999. On the evolution of attitudes towards risk in winner-take-all games. *Journal of Economic Theory* 87: 125–143.

De Luca, J. 2002. "Requirements – The budgeting syndrome," *Feature Driven Development (FDD) Newsletter Issue 7*. City, Country: The Standish Group International, http://www.featuredrivendevelopment.com/node/614 (accessed January 2010).

Dhem, J.-F., and N. Feyt. 2001. Hardware and software symbiosis helps smartcard evolution. *IEEE Micro* 21 (6): 14–25.

English, E., and S. Hamilton. 1996. Network security under siege: The timing attack. *IEEE Computer* 29 (3): 95–97.

Ferguson, N., and B. Schneier. 2003. *Practical cryptography*. Hoboken, NJ: Wiley.

Gates, Bill. 1995. Interview with Bill Gates. *Focus Magazine* 43: 206–212.

Goubin, L., and J. Patarin. 1999. DES and differential power analysis: The "duplication" method. In *Proceeding of CHES '99, Springer Lecture Notes in Computer Science,* 1717, pp. 158–172.

Ilja. 2007. A collection of random things, look at what I found under the carpet. In *Proceedings of the 24th Chaos Computer Congress*, Month day, Berlin, Germany. http://events.ccc.de/congress/2007/Fahrplan/events/2296.en.html. (accessed May 2010).

Kaminsky, D. 2008a. "Black Ops 2008 – It's the end of the cache as we know it," *Black Hat USA 2008*. https://media.blackhat.com/bh-us-08/video/bh-us-08-

Kaminsky/black-hat-usa-08-Kaminsky-blackops08-hires.m4v (accessed August 2009).

Kaminsky, D. 2008b. DNS rebinding packet tricks. In *Proceedings of the 24th Chaos Computer Congress*, January 2008, Berlin, Germany. http://dewy.fem.tu-ilmenau.de/CCC/25C3/video_h264_720x576/25c3-3023-en-making_the_theoretical_possible.mp4 (accessed August 2009).

Kaminsky, D. 2009. Why we were so vulnerable to the DNS vulnerability. In *Proceedings of the 25th Chaos Computer Congress*, January 2009, Berlin, Germany. http://dewy.fem.tu-ilmenau.de/CCC/25C3/video_h264_720x756/25c3-2906-en-why_were_we_so_vulnerable_to_the_dns_vulnerability.mp4.torrent (accessed August 2009).

Katz, M. L., and C. Shapiro. 1985. Network externalities, competition, and compatibility. *The American Economic Review* 75: 424–440.

Kocher, P., J. Jaffe, and B. Jun. 1998. *Introduction to differential power analysis and related attacks*. http://www.cryptography.com/public/pdf/DPATechInfo.pdf (accessed October 11, 2010).

Kommerling, O., and M. G. Kuhn. 1999. Design principles for tamper-resistant smart card processors. In *USENIX Workshop on Smart Card Technology,* May 10–11, Chicago, Illinois. http://www.usenix.org/events/smartcard99/full_papers/kommerling/kommerling.pdf (accessed October 11, 2010).

Marlinspike, M. 2009a. "Defeating OCSP with the character '3'," *Blackhat 2009*. http://www.blackhat.com/presentations/bh-usa-09/MARLINSPIKE/BHUSA09-Marlinspike-DefeatOCSP-PAPER2.pdf (accessed August 2009).

Marlinspike, M. 2009b. New tricks for defeating SSL in practice," *Blackhat DC 2009*. https://www.blackhat.com/presentations/bh-usa-09/MARLINSPIKE/BHUSA09-Marlinspike-DefeatSSL-PAPER1.pdf (accessed August 2009).

Miller, K., T. Camp, L. Smith, K. D. Johnson, and B. Moska. 2010. A history of the introduction and shut down of Therac-25. *ComputingCases2010*. http://computingcases.org/case_materials/therac/case_history/Case History.html (accessed January 2010).

Molnar, D, et al. 2009. MD5 considered harmful today. In *Proceedings of 25th Chaos Computer Congress*, January, Berlin, Germany. http://dewy.fem.tu-imenau.de/CCC/25C3/video_h264_720x756/25c3-3023-en-making_the_theoretical_possible.mp4.torrent (accessed August 2009).

Nicholls, R. K., and P. C. Lekkas. 2002. *Wireless security: models, threats, and solutions*. New York: McGraw-Hill.

Norton-Taylor, R. 2010. "MoD knew of Chinook flaws before fatal crash, says father," *Guardian*, January 4, 2010. http://www.guardian.co.uk/uk/2010/jan/04/chinook-death-crash-new-evidence (accessed January 4, 2010).

Rice, D. 2008. *Geekonomics*. Upper Saddle River, NJ: Addison-Wesley.

Saputra, H., N. Vijaykrishnan, M. Kandemir, M. J. Irwin, R. R. Brooks, S. Kim, and W. Zhang. 2003. Masking the energy behavior of DES encryption. *IEE Proceedings: Computers and Digital Techniques* 150 (5,22): 274–284.

Schwier, J. July 2009. Pattern recognition for command and control data systems. Doctor of philosophy dissertation, Clemson University.

Soghoian, C., and S. Stamm. 2010. Certified lies: detecting and defeating government interception attacks against SSL. http://files.cloudprivacy.net/ssl-mitm.pdf (accessed April 2010).

Song, D. X., D. Wagner, and X. Tian. 2001. Timing analysis of keystrokes and timing attacks on SSH. In *10th USENIX Security Symposium*, Washington, D.C. http://www.usenix.org/events/sec01/.

U.S. Congress. 2010. The Computer Fraud and Abuse Act, Title 18, Part 1, Chapter 47, 1984. http://www.law.cornell.edu/uscode/18/1030.html, Accessed January 2010.

Ye, W., N. Vijaykrishnan, M. Kandemir, and M. J. Irwin. 2000. The design and use of SimplePower: A cycle-accurate energy estimation tool. In *Proceeding of the 37th Design Automation Conference,* June 5–9, Los Angeles, CA.

Young, S., and D. Aitel. 2004. *The Hacker's Handbook*. Boca Raton, FL: Auerbach Publications.

Zhu, Y., X. Fu, R. Bettati, and W. Zhao. 2005. Anonymity analysis of mix networks against flow correlation attacks. In *Proceedings of IEEE Global Communications Conference (GLOBECOM)*, November. http://ieeexplore.ieee.org/xpl/mostRecentIssue.jsp?punumber=10511 (accessed September 2010).

Acknowledgments

This material is based upon work supported by, or in part by, the U.S. Air Force Office of Scientific Research contract/grant number FA9550-09-1-0173. Opinions expressed are those of the author and not the U.S. Department of Defense.

ITEA Journal 2010; 31: 518–524

Test and Evaluation of WiMAX Performance Using Open-Source Modeling and Simulation Software Tools

Anthony Leclerc, Ph.D. and Michelle Crosby
SPAWARSYSCEN Atlantic, North Charleston, South Carolina

Recently, various efficient WiMAX quality of service–based uplink scheduling algorithms have been proposed. These algorithms have been analyzed theoretically and in many cases evaluated unilaterally using ad-hoc random simulation. A novel integration of open-source and freeware modeling and simulation software tools for performing comparative analysis of uplink scheduling algorithms is presented. This integrated open-source modeling and simulation solution is used to evaluate the effect on performance of various uplink scheduling algorithms within a real-world quality of service–constrained tactical-edge scenario.

Key words: IEEE 802.16; M&S; network simulation; open-source; QoS; uplink scheduling; WiMAX.

The Institute of Electrical and Electronics Engineers (IEEE) 802.16 standard (IEEE 2004; IEEE 2006), also known as Worldwide Interoperability for Microwave Access (WiMAX), includes specifications for fixed and mobile broadband wireless access (BWA). Deployment of WiMAX is particularly attractive in tactical military settings where "cells" of high-data rate wireless connectivity must be established rapidly and relatively inexpensively (see *Figure 1*).

The 802.16 standard prescribes several quality-of-service (QoS) classes, which help ensure the reliability and timeliness of critical tactical edge (TE) applications such as voice over internet protocol (VoIP), real-time situational awareness (SA), and command and control (C2).

A typical configuration for WiMAX, called point-to-multipoint (PMP) mode, involves two types of communication stations: (a) base station (BS) and (b) subscriber stations (SS). The BS (perhaps located at the command center) regulates all communication in the cell network. Data are transmitted from the SS to the BS in the uplink direction and from the BS to the SS in the downlink direction. Sagacious allocation of available bandwidth "slots" in the uplink direction is crucial to QoS of WiMAX at the TE.

The amount of bandwidth each SS is allowed to have in the uplink direction is dynamically determined by the BS in the form of an "uplink scheduling algorithm" (Khalil and Ksentini 2007; Belghith and Nuaymi 2008). This algorithm is not specified in the 802.16 standard, thus giving WiMAX implementers the option of choosing, or even designing, optimized uplink schedulers that meet specific needs. For instance, one may seek to maximize the system throughput while maximizing the number of transmitted data packets with hard deadlines. An efficient uplink scheduling algorithm at the TE should consider the QoS constraints imposed by characteristic TE application traffic while seeking to maximize the throughput of the system (Yu 2008; Pishdad and Rabiee 2008; Piro et al. 2010; Wongthavarawat and Ganz 2003; Mohammadi, Akl, and Behnamfar 2008b).

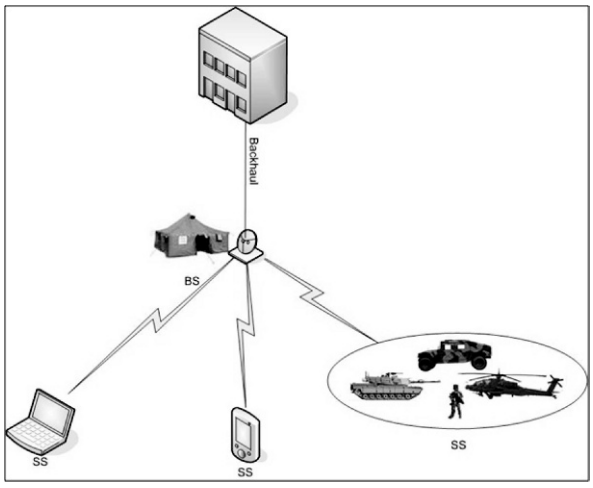


Figure 1. Simple tactical-edge Worldwide Interoperability for Microwave Access (WiMAX) depiction.

Approaches

Test and evaluation (T&E) of WiMAX QoS using existing and proposed uplink scheduling algorithms requires an environment flexible enough to select and implement different uplink schedulers. A field test with physical hardware utilizing field-programmable gate arrays (FPGAs) with the ability to reprogram new uplink schedulers is theoretically possible. Currently, however, most equipment used for WiMAX field tests within the Department of Defense (DoD) do not contain FPGA components. In addition, few testers possess the requisite expertise with hardware description languages (HDLs) and programing tools in order to program FPGAs. Even given FPGA-endowed equipment, HDL tools, and programmer resources, field testing of alternative WiMAX QoS configurations and algorithms would be cumbersome and costly.

A more flexible, rapid, and cost-effective way to test and evaluate WiMAX QoS is to use discrete event simulation, a high-fidelity form of modeling and simulation (M&S). A discrete-event network simulator emulates the behavior of an interconnected network and applications, including detailed processing through all layers of the protocol stack. In the case of WiMAX, this should include an accurate media access control (MAC) and physical layer (PHY) implementation of the 802.16d and 802.16e specifications with PMP mode and the Wireless Metropolitan Area Network Orthogonal Frequency–Division Multiplexing (MAN-OFDM) PHY layer. These two specifications are also known as fixed and mobile wireless, respectively. Examples of network simulators that claim to accurately implement the 802.16d/e standards include ns-2/ns-3 (NSNAM), OPNET (OPNET Technologies, Inc.), and QualNet (Scalable Network Technologies).

Two important requirements for our T&E of WiMAX QoS with new and existing uplink scheduling algorithms are cost and modifiability. The two simulators ns-2 and ns-3 are open-source. For comparison, OPNET is proprietary software requiring the purchase of multiple licenses and support options at a current cost approaching $60K. An integrated graphical user interface (GUI) is lacking in ns-2/ns-3, requiring C/C++ programming in order to configure the simulation. OPNET, on the other hand, possesses a mature and intuitive GUI for configuration.

Cost and ease of configuration aside, the greatest argument for using an open-source simulator is the ability to modify and add source code. T&E of existing and proposed uplink scheduling algorithms requires the ability to incorporate a significant amount of logic into the simulator that goes beyond simple configuration. Proprietary M&S tools may offer the user a limited ability to configure "built-in" algorithms or add some process code but often provide no mechanism to significantly modify existing algorithms or implement new algorithms. When such a provision is available, the modification or implementation of the algorithm is realized as C or C++ code.

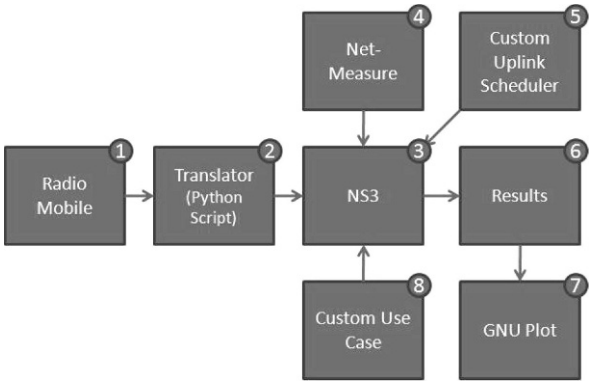


Figure 2. Integrated architecture.

Solution components

We propose and utilize integrated solution architecture for T&E of WiMAX performance on QoS-constrained TE traffic (see *Figure 2*). The solution represents a loose coupling of five open-source and freeware software tools. We briefly describe each of the five tools in this section and, where relevant, address validation acquirements.

ns-3

The ns-3 simulator was selected because it is actively developed on multiple fronts, written entirely in C++, and has a rich set of WiMAX modules. Initial funding to develop ns-3 was provided, in part, by the National Science Foundation in 2006. Since then, the ns-3 development effort has attracted the support and interest of several major academic departments and organizations including the Electrical and Computer Engineering Department at the Georgia Institute of Technology, the Electric Engineering Department at the University of Washington, and the Google Summer of Code.

Ns-3 consists of a simulation core engine, a set of models, example programs, and tests. The ns-3 testing environment provides model validation and testing tools and encourages the publication of validation results. Characteristics of the ns-3 development effort include

- strict implementation of IEEE specifications;
- broad international use and contribution;
- continuous academic, corporate, and public scrutiny of the source code;
- academic "validation" through published articles and conference presentations; and
- extensive testing.

A search on the Association of Computing Machinery (ACM) portal for articles involving the keyword, "ns-3", identifies nearly 500 articles. Searching with the additional keyword, "WiMAX" yields 20 articles spanning respected conferences such as SIMUTools, WICON, SIGOPS, SIGCOMM, AAA-IDEA Interperf, and ValueTools.

It is difficult to guarantee the correctness of large-scale software simulators, including commercial simulators. Rather, qualities such as those listed above build confidence in the simulator's correctness, including validation and verification.

In the language of the ns-3 documentation (ns-developers@isi.edu 2010), "ns-3 must be correct, robust, performant and maintainable." In summary, each of these test criteria is addressed as follows (with excerpts from the ns-3 testing documentation):

- Correct: "The ns-3 testing environment provides tools to allow for both model validation and testing, and encourages the publication of validation results."
- Robust: "The ns-3 testing environment provides tools to allow for setting up and running test environments over multiple systems (buildbot) and provides classes to encourage clean tests to verify the operation of the system over the expected "domain of applicability" and "range of accuracy."
- Performant: This is a concise neologism that is used to describe the design goal that ns-3 must be "powerful and fast enough to get the job done. In the ns-3 test framework, we provide support for timing various kinds of tests."
- Maintainable: "The ns-3 testing framework provides tools for automating the process used to validate and verify the code in nightly test suites to help quickly identify possible regressions." These regressions include local regressions, remote regressions, unmasked regressions, and performance regressions.

Radio Mobile

As mentioned, ns-3 lacks a GUI. This condition not only diminishes usability but also denies the user the ability to graphically specify network topologies. A freeware tool called Radio Mobile (RM) (Coude n.d.) exists that predicts the performance of a radio system by using digital terrain elevation data. RM additionally provides a GUI for the layout of wireless network devices on top of a rendered topography. The output of RM can be used to configure ns-3 for more realistic scenarios, which include topology, distance, and signal properties.

RM is based on the U.S. Department of Commerce National Telecommunications and Information Administration Institute for Telecommunication Sciences (NTIA/ITS) Irregular Terrain Model (ITM) (Longley-Rice). This software has been in use since 1988. RM's publication history is less extensive than ns-3, with only a few articles appearing in *Radcom* (Brown 2006) and *AntenneX* (Brown 2009). Comprehensive T&E of RM is not present in the literature. However, our use of RM is intended to more accurately characterize the environment in which our TE scenario will be deployed. We are interested in the following output from RM:

- topology of the TE scenario,
- accurate distance measures between BS and SS, and
- approximate radio propagation qualities.

We have validated the output of the first two items by inspection. Furthermore, RM provides a three-dimensional view of the BS and SS stations as well as vectors illustrating, with color, the signal loss as a result of the environment. This interface provides a quick "sanity check" of the outputted numerical results. Since the built-in ns-3 propagation model is the only other environment model we have available, the reasonable approximation of radio propagation produced by RM is a significant improvement.

Gnuplot

Gnuplot is an open-source cross-platform command-line–driven graphing utility. It was created for visualization of mathematical functions and data interactively and has been under active development since 1986. Gnuplot is used extensively in the scientific community. A search on the ACM portal for articles involving the keyword, "gnuplot", identifies nearly 300 articles. Our use of gnuplot is for the two-dimensional visualization of performance metrics such as throughput.

Net-Measure

Net-Measure (code.google n.d.) is a C++ class that "wraps" the performance monitoring capability of ns-3 (FlowMonitor) into an easy-to-use interface. In addition, Net-Measure provides interval-timed captures of network metrics so that performance plots can be visualized (with gnuplot) over time. The implementation of the class is one C++ file.

As Net-Measure relies on the correctness of the ns-3 FlowMonitor, a personal review of the single source file implementation was sufficient to verify the correctness of the implementation. We validated, to

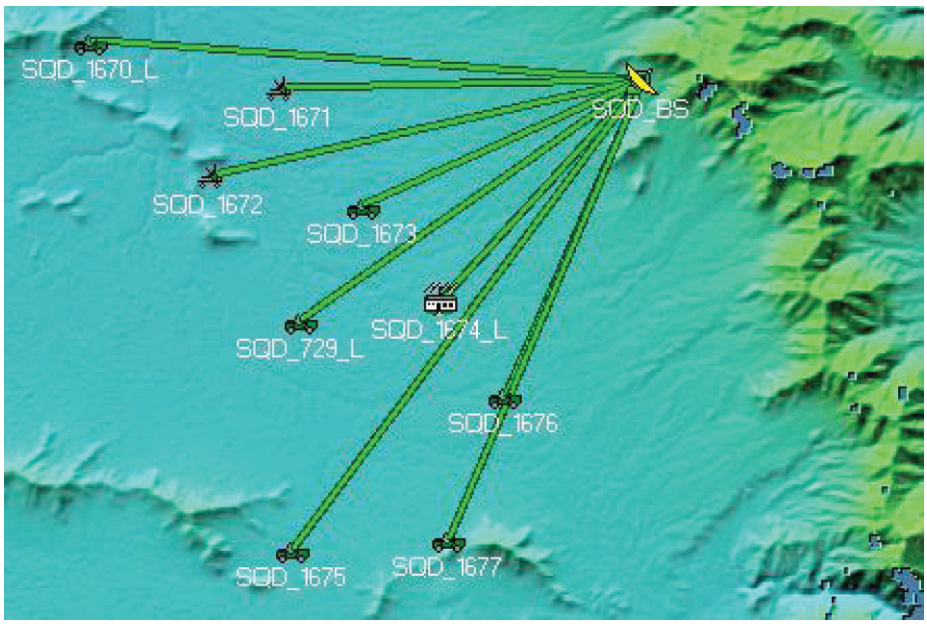


Figure 3. Worldwide Interoperability for Microwave Access (WiMAX) platoon configuration.

our satisfaction, the results of Net-Measure on three "built-in" WiMAX examples within ns-3.

Python script

A Python script is utilized to translate the output results of RM into a more succinct text form that will be imported into our ns-3 simulation. This script is short, and its correctness is easily verified by observing the source code. We validated the correctness of the results by comparing the translated output with the input from RM.

Integrated solution details

Figure 2 illustrates the integration and coordination of the various tools described in the previous section. We now describe the flow through this solution architecture with a specific TE use case.

A likely deployed isolated squad WiMAX cell scenario was obtained from the Communications-Electronics Research, Development, and Engineering Center (CERDEC) (see *Figure 3*). The topology of this deployment is not atypical of general WiMAX topologies, including commercial layouts. CERDEC also supplied simulated traffic; characterizing traffic types, rates, QoS priorities, and timings for a squad deployment.

The traffic data from CERDEC is not real data, but rather representative data obtained from the traffic generation tool, TGEN. The data has been "sanitized" for security reasons but still represents a realistic TE traffic flow pattern with multiple QoS constraints, including situational awareness, command and control, and voice.

Our integrated solution commences with the layout of a squad topology in a selected region using RM [1] as shown in *Figure 2*. The output of RM is then converted with a python script into a form amenable to ns-3 [2]. A simulation run consisting of the custom use case [8], Net-Measure module [4], and a command-line–specified uplink scheduler [5] is initiated. The plot output results of the ns-3 simulation are then viewed using the Gnuplot utility [7].

This integrated solution is not unwieldy. Since we are concerned with the impact of the uplink scheduling algorithm on throughput (with QoS constraints), steps [1] and [2] need only be performed once. Components [3, 4, 5, 6, and 8] are either "hardwired" into the code, or automatically configured/selected as a result of the input. Only step [7] needs to be performed separately after each simulation run.

Results

Figure 4 compares the performance of three different scheduling algorithms. The graph is a preliminary comparison graph we constructed utilizing a simplified simulation. We initially coded this simple simulator to verify the results of one particular published article (Mohammadi, Akl, and Behnamfar 2008b), which demonstrated an "optimal" uplink scheduling algorithm in the form of a modified 0/1 Knapsack problem.

The simple simulation compares the different scheduling algorithms in a theoretical manner in that

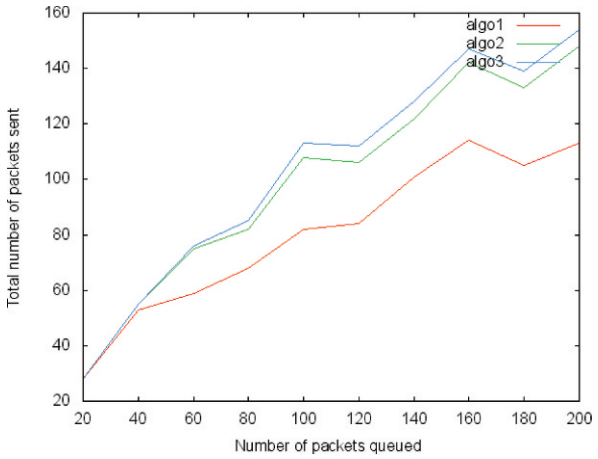


Figure 4. Simple simulation results.

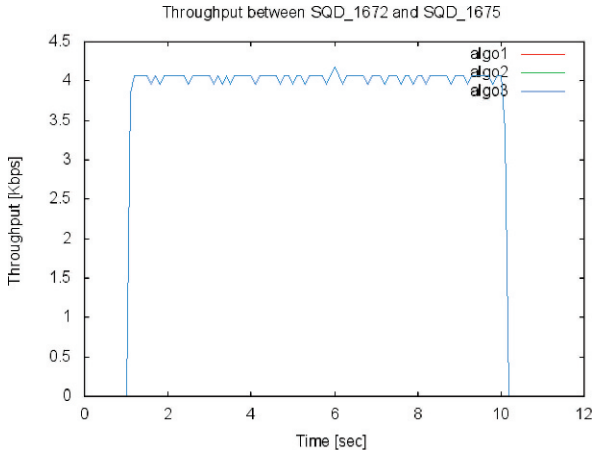


Figure 5. Net-measure results.

the vast majority of the WiMAX infrastructure and protocols are not modeled. For instance, protocol stacks, specific application data, and propagation characteristics are not modeled. The simple simulator consists of less than 1,000 lines of code and is typical of many simulations that appear in journal articles comparing WiMAX scheduling algorithms (Mohammadi, Akl, and Behnamfar 2008a, 2008b; Wongthavarawat and Ganz 2003).

From *Figure 4*, we see that as the number of packets waiting to be sent (queued) at the SS grows, then the different algorithms distinguish themselves by performing better or worse in terms of the number of packets actually sent. Theoretically speaking, it appears that Algorithm 3 is superior.

The TE-use case consists of a set of nine squad member SS and one control center BS (see *Figure 3*). In this figure, the BS is depicted as a parabolic antenna with the label SQD_BS. All other icons on the map are squad members. A green connecting line between the BS and an SS indicates a high-quality signal strength radio link. The distance between the BS and each SS ranges from 14 km to 32 km. Each SS consists of a 2-meter high omnidirectional antenna and uses Binary Phase Shift Keying (BPSK) 1/2 modulation. Three different uplink scheduling algorithms were evaluated.

Simulation results using the TGEN squad traffic with multiple scheduling algorithms indicated no difference in performance. *Figure 5* summarizes the results of the comparison by measuring the throughput over time for traffic between two arbitrary nodes. All three uplink algorithms yielded similar throughput. Performance between other pairs of nodes behaved similarly.

For this TE scenario, the results of our simulation indicate that any uplink scheduling algorithm can be used with no significant change in performance. These results don't contradict the simple simulation results. Rather, they simply indicate that, for this scenario, the choice of uplink scheduler is not a factor on performance.

We note that the nature of the TGEN squad traffic is fundamentally multicast. Though ns-3 supports multicast within many models, the documentation is unclear about how to establish multicast groups attached to a BS. The results presented here substitute unicast traffic in place of multicast traffic. Nevertheless, we expect the results to be the same, as the traffic volume in the uplink direction would not increase significantly.

Conclusion and future work

We have demonstrated integrated solution architecture for T&E of WiMAX performance on QoS-constrained TE traffic using open-source modeling and simulation tools. The solution is general in that it can be applied to other WiMAX performance-affecting variables such as modulation type, radio frequency, terrain profiles, and traffic type.

For the specific TE squad use–case we investigated, the choice of uplink scheduling algorithm resulted in no detectable degradation in performance. Our belief is that the limited volume of the TGEN squad traffic does not saturate the available bandwidth in the uplink direction. Thus, algorithms that seek to optimize bandwidth allocation perform no better than simple algorithms. With larger-scale scenarios involving more loquacious network applications, we anticipate differences.

We identify five promising avenues for continued work using this architecture. First, the characteristic multicast nature of TE communications should be modeled. The multicast facility is present in ns-3 but requires further research to determine how to use it at a

WiMAX BS. Second, larger-scale simulations, perhaps at the platoon or even battalion level, can be pursued. Third, WiMAX TE scenarios involving a broader range of applications exhibiting greater traffic volume and more varied QoS constraints can considered. Such a set of applications might include tactically important text chat, white board, streaming video, and application sharing. Fourth, a level of validation can be obtained by implementing the same scenario in another simulator (e.g., OPNET). Fifth, the development of a GUI to "seamlessly" integrate the various open-source and freeware tools would be a useful endeavor.[1] ❑

Dr. Anthony Leclerc works with the Testing and Evaluation Department in Code 59330. He has worked at Space and Naval Warfare in Charleston, South Carolina, for 10 years. He is also a professor in the Computer Science Department at College of Charleston, South Carolina. He earned a doctor of philosophy in computer science from Ohio State University in 1992. E-mail: anthony.leclerc@navy.mil

Michelle Crosby also works in Code 59330 and supports the Testing and Evaluation department. She has worked at Space and Naval Warfare in Charleston, South Carolina, for 8 years. She earned her bachelor of science degree in computer science in 2004 at the College of Charleston, South Carolina. E-mail: michelle.crosby@navy.mil

Endnotes

[1]Disclaimer: The authors' affiliations with SPAWAR Atlantic are provided for identification purposes only and are not intended to convey or imply the above organization's concurrence with or support for the positions, opinions, or viewpoints expressed by the authors.

References

Belghith, A., and L. Nuaymi. 2008. Comparison of WiMAX scheduling algorithms and proposals for the rtPS QoS class. In 14th European *Wireless Conference, 2008* Electronic Proceedings, June 22–25, 2008, Prague. Berlin: VDE Verlag Gimbh.

Brown, I. D. 2006. An introduction to radio mobile. *Radio Communication* October: 79–82.

Brown, I. D. 2009. Radio mobile—What can it do for you? *antenneX* 147: 1–11.

CERDEC. (n.d.). *CERDEC U.S. ARMY RDECOM*. http://www.cerdec.army.mil (accessed July 1, 2010).

code.google. (n.d.). *Tutorial—ns3-wireless-planning*. http://code.google.com/p/ns3-wireless-planning/wiki/Tutorial (accessed July 1, 2010).

Coude, R. (n.d.). Radio Mobile Web site. http://www.cplus.org/rmw/english1.html (accessed July 10, 2010).

IEEE. (2004, October). Standard for local and metropolitan area networks, Part 16. *IEEE 802.16-2004*. New York: IEEE.

IEEE. (2006, February). Standard for local and metropolitan area networks, Part 16: Amendment 2 and Corrigendum 1. *IEEE 802.16e/D12*. New York: IEEE.

Khalil, A., and A. Ksentini. 2007. Classification of the uplink scheduling algorithms in IEEE 802.16. *IWDYN'07 Workshop*. Rennes, France: INSA Rennes.

Mohammadi, A., S. G. Akl, and F. Behnamfar. 2008a. Optimal linear-time uplink scheduling algorithms for WiMAX. In *Proceedings of the IEEE Vehicular Technology Conference*, September 21–24, 2008, Quebec, Canada, 19–24.

Mohammadi, A., S. G. Akl, and F. Behnamfar. 2008b. QoS-based Optimal Logarithmic-TimeUplink Scheduling Algorithm for Packets. *Proceedings of the IEEE international symposium on Personal, Indoor and Mobile Radio Communications (PIMRC)*. Cannes, France.

NSNAM. (n.d.). *The ns-3 network simulator*. http://www.nsnam.org/ (accessed July 1, 2010).

OPNET Technologies, Inc. (n.d.). *Application and network performance with OPNET*. http://www.opnet.com (accessed July 1, 2010).

Piro, G., M. A. Ismail, L. A. Griecoq, and T. Turletti. 2010. An improved IEEE 802.16 WiMAX module for the ns-3 simulator. In *International Conference on Simulation Tools and Techniques for Communications, Networks and Systems & Workshops archive*. March 15–19, Torremolinos, Spain. Malaga, Spain: ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering).

Pishdad, L., and H. R. Rabiee. 2008. An optimization based uplink scheduler for IEEE 802.16 networks. In *2008 International Conference on Computer and Electrical Engineering*, December 20–22, Phuket, Thailand. 482–486. Washington, D.C.: IEEE Computer Society.

Scalable Network Technologies. (n.d.). *Scalable networks*. www.scalable-networks.com (accessed July 1, 2010).

Wongthavarawat, K., and A. Ganz. 2003. IEEE 802.16 based last mile broadband wireless military networks with quality of service support. In *Military communications conference*, October 13–16, Boston, MA, 779–784. Piscataway, NJ: IEEE.

Yu, C. Z. 2008. An enhanced uplink scheduling scheme for IEEE 802.16 metropolitan area networks.

In *Proceedings of the international Conference on Mobile Technology, Applications, and Systems*. Yilan, Taiwan: ACM.

Acknowledgments

We acknowledge the critical work done by CERDEC on our behalf. In particular, we thank Scott Newman (Chief) and Jinwoo Park within the System Engineering Analysis Branch at CERDEC. Scott Newman was instrumental in guiding us quickly to manageable TE use-case. Jinwoo generated and sanitized the important TGEN data. Both Scott and Jinwoo engaged in numerous e-mail discussions and one enlightening conference call.

We also acknowledge the time given us by Tao Rocha and the rest of the Wireless Network Branch at SPAWAR Atlantic. Members we deliberated with on WiMAX use cases in the U.S. Navy include John Paul Kalapurakal, Tim Schmitz, and Andrew Kelly.

Finally, we thank the Innovation Program at SPAWAR Atlantic for providing us with the opportunity to research, test, and evaluate an innovative technology with tools that we would otherwise not have the time to investigate. We trust our efforts have contributed to field.

ITEA Journal 2010; 31: 525–530

Chemical and Biological Test and Evaluation—Detector Agent Simulant Relationship

Charlie Holman, Ph.D.
Army Test and Evaluation Command, Alexandria, Virginia, and Biology and Mathematics Departments, Claflin University, Orangeburg, South Carolina
Andrew G. Loerch, Ph.D.
Systems Engineering and Operations Research Department, George Mason University, Fairfax, Virginia

Realistic testing of chemical and biological defense systems requires an actual warfare agent. But use of such an agent is restricted to laboratory containment chambers, which are not realistic. This state of affairs has driven the chemical and biological defense community to integrate developmental testing and operational testing. Systems are challenged with both agent and simulant in laboratory containment chambers during developmental testing. A simulant is a substance that resembles the agent from the perspective of the system under test. A three-step procedure is described in this article to relate performance when challenged with simulant during operational testing to performance when challenged with agent. The procedure is based on classical logistic regression and judgment. If there is no statistical difference in performance between the agent and the simulant, then the results of the field test with the simulant can be used to predict agent performance. If there is statistical difference in performance between the agent and the simulant, but that difference is small and the system under test performs better when challenged with the agent than with the simulant, then the simulant performance is a lower bound to agent performance. What is defined as small difference is a matter of judgment. A graphical method is provided to provide insight as to the magnitude of the difference. In all other cases, the logistic regression can be used to predict performance based on operational test challenge concentrations and other parameters from the operational test.

Key words: ALO; chemical and biological defense systems; detector; evaluation; logistic regression; simulant.

An Operational Test (OT) is intended to be a realistic representation of how the system under test will be used by its intended operators in the intended operating environment. An OT includes actual warfighters executing combat missions and using the system under test in the same manner that they would use it in combat. Realistic testing of chemical and biological defense systems requires the use of an actual warfare agent. However, because of treaties, public laws, and a desire not to harm test participants, testers, the general public, or the environment, neither chemical warfare agents nor biological warfare agents are released during operational tests or any field test. Testing with an actual warfare agent is restricted to the laboratory in containment chambers. Unfortunately, these containment chambers are not realistic environments. This state of affairs has driven the chemical and biological defense community to integrate agent chamber Developmental Testing (DT) with OT (Holman and Berkowitz 2009).

There are three methods by which the chemical and biological test and evaluation community combines or integrates the realism of actual biological or chemical agent chamber testing with the realism of actual warfighters executing missions in combat like environments. These three methods are (a) conducting DT with systems before and after OT, (b) modeling and simulation, and (c) developing agent–simulant relationships (Holman and Berkowitz 2009). A simulant is a relatively harmless substance that has some of the properties of agents and can be released into the environment.

Conducting agent DT with systems before and after OT can provide keen insight into determining whether using a system in the operational environment will degrade its performance. This type of testing has been used most extensively with protective garments. New Joint Service Lightweight Integrated Suit Technology (JSLIST) protective garments and JSLIST garments that went through 15, 30, 45, and 60 days of OT wear were tested in DT. The DT included swatch tests with liquid and vapor chemical warfare agent and whole system tests with simulant. As a result of this testing, curves were developed that predicted degradation in protection based on the amount of wear (Musgrave et al. 1997).

Modeling and simulation were used to integrate developmental agent chamber tests with simulant OTs for the Joint Service Lightweight Standoff Chemical Agent Detector (JSLSCAD). The JSLSCAD performance was modeled with a hierarchy of three models: (a) a vapor cloud model, (b) a scanning model, and (c) the JSLSCAD model. During the validation and verification process, the model accurately predicted performance of the JSLSCAD when challenged with simulant in open air field tests. The modeling and simulation effort was the backbone of the JSLSCAD performance evaluation (Holman et al. 2007).

Modeling and simulation was also used to evaluate the Joint Biological Standoff Detector System (JBSDS). In this effort, field measurements of the cross-sectional infrared back scatter, ultraviolet backscatter, and ultraviolet florescence of simulant were replaced with laboratory measurements for actual agent and were played back in the system software using the other parameters that were recorded in the system software during simulant release (Shirakawa et al. 2008).

Early efforts at developing an agent–simulant relationship were simply to bound a detector's performance against an agent with its performance against two simulants (Musgrave et al. 1997, 2000). Fitch et al. (2004) recommended developing both better methods to perform an agent–simulant relationship and better biological simulants. He proposed using simulants that are phylogenetically similar to the agents. These Agents of Like Origin (ALO) include the vaccine strains.

This article describes an approach based on logistic regression and judgment to develop an agent–simulant relationship and combine chamber agent test results with OT results, so that an operationally relevant evaluation can be made on chemical warfare and biological warfare agent detectors. This approach was used and is currently being used to evaluate the Joint Biological Point Detection System (JBPDS) (Holman et al. 2008; Moe et al. 2010). Biological warfare agent LE and its ALO-killed simulant are used as an example throughout this article.

Concentration

At some high concentration of an agent, a detector will always detect that agent. This high concentration is above the detection threshold, and the probability of detection is unity. At some low concentration of an agent, a detector will never detect that agent. This low concentration is below the detection threshold, and the probability of detection is zero. As the concentration of agent increases from a level that is undetectable, the probability of detection increases. The probability of detection as a function of concentration tends to be s-shaped or a sigmoid as depicted in *Figure 1*. There are many different sigmoid functions, but the logistic regression model is especially useful to model detection performance (Holman and Berkowitz 2009).

Concentration is the independent variable that has the most pronounced effect on detector performance (Holman and Berkowitz 2009).

As a general rule of thumb, the sigmoid curve is steeper (or vertical) in the laboratory than in the field. This is likely because chamber air when filtered lacks many of the impurities found in the environment. The impurities increase the variability in the detector performance. In addition, there is less measurement error, and hence less variability of response in a chamber than in the field environment.

Agent–simulant relationship procedure

The procedure described here involves testing the detector with an agent and a simulant in a chamber at various concentrations, so that a logistic regression model can be developed. The procedure then consists of three steps:

- Step 1: test of hypothesis – Test to see if there is any statistical difference between the performance of the detector when challenged with a simulant or agent in the laboratory. Ensure that sample sizes are sufficient to adequately control error. If there is no statistical difference in the performance of the detector challenged with agent or simulant, then use the simulant to predict detector performance without a transformation.
- Step 2: analysis of the difference – If step 1 demonstrates that detector performance when challenged with agent is statistically different from its performance when challenged with simulant, determine both the directionality and magnitude of the difference. If detector performance for an agent is always better than performance against a simulant, and if the difference is judged not to be too great, then field performance against a simulant can be used to form a lower bound of performance. If the

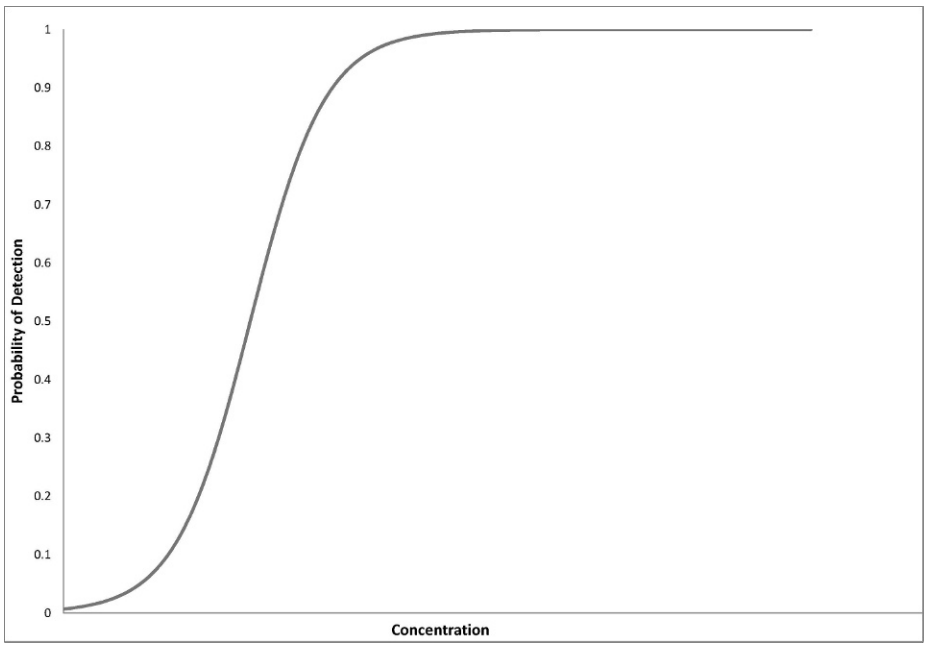


Figure 1. S-shaped or sigmoid curve depicting the relationship between agent detection and agent concentration.

detector performs well enough against this lower bound, we know that the detector will perform better against the agent.

- Step 3: For all other cases, use the logistic regression model to predict performance.

Step 1: test of hypothesis

For the JBPDS LE example, the hypothesis is as follows:

- H_o: JBPDS performance is the same with either killed LE ALO or live LE agent.
- H_a: JBPDS performance with killed LE ALO is different from its performance with live LE agent.

A classical logistic regression statistical model was constructed for the probability of detection as a function of concentration to determine if the JBPDS detection performance differed between the agent LE and the killed LE ALO simulant. The random component is binary 0 or 1 for no detection or detection (also no identification or identification), respectively. The explanatory variables for this model are agent or simulant concentration, and agent or simulant. The Detection Model is as follows (Allison 1999; Agresti 1996; Hosmer and Lemeshow 1989):

$$\text{logit}(\pi) = \log(\pi/(1-\pi)) = \alpha + \beta_1 S + \beta_2 x$$

$$P(\text{detect}|x,S) = e^{\alpha+\beta}1^{S+\beta}1^{x}/\left(1+e^{\alpha+\beta}1^{S+\beta}2x\right),$$

where π = probability of detection; α = shift parameter; $S = 1$ if live agent, 0 if killed ALO; β_1 = agent flag shape parameter; x = concentration; and β_2 = concentration shape parameter.

For this model, hypothesis is now equivalent to

- H_o: $\beta_1 = 0$
- H_a: $\beta_1 \neq 0$

The test statistic is the likelihood-ratio test statistic: $-2\log(L_0/L_1) = -2(L_0 - L_1)$, where L_0 is the likelihood function without β_1, and L_1 is likelihood function of the full model. This test statistic is chi-squared with degrees of freedom equal to the difference in the number of parameters between the two models.

As can be seen in *Table 1*, JBPDS detection performance when challenged with a live LE biological warfare agent is statistically different from its detection performance when challenged with killed LE ALO simulant (P value = .0437). Also, as would be expected, detection performance is a function of concentration (P value = .0161) *(Table 1)*. The Maximum rescaled R-squared is 0.8077 for this model. Live LE and killed LE ALO detection results are based on 62 challenges at various concentrations. The Hosmer and Lemeshow goodness-of-fit test chi-square value is 0.3962 with 6 degrees of freedom, which produces a P value of .99. The deviance goodness-of-fit statistic is 14.50 with 56 degrees of freedom and a P value of .99. Neither goodness-of-fit test is statistically significant, which suggests that the model is a reasonable fit.

It is interesting to note, that the difference in detector performance between the LE agent and killed

Table 1. LE versus killed LE agents of like origin analysis of maximum likelihood estimates.

Parameter	DF	Wald Chi-square	Pr > Chi-square
Intercept	1	5.8085	0.0159
Natural log of concentration	1	5.7941	0.0161
Live LE or killed LE ALO indicator	1	4.0665	**0.0437**

DF, degrees of freedom; Pr, probability; ALO, agents of like origin.

LE ALO simulant is caused by an inherent difference in the detection of the LE agent and LE ALO and is not caused by the killing process. There is no significant statistical difference in how JBPDS detects live LE agent or killed LE agent (P value = .4564). Nor is there any significant statistical difference in how JBPDS detects live LE ALO or killed LE ALO (P value = .6447). There is, however, a significant statistical difference in detector performance between live LE agent and live LE ALO (P value = .0335).

Since detector performance when challenged with agent is statistically different from its performance when challenged with simulant, we proceed to step 2 to determine both the directionality and magnitude of the difference. Actually, regardless of the outcome of the statistical test, step 2 provides insight as to the nature of the agent–simulant relationship.

Step 2: analysis of the difference

Since the dependent variable is binary, detect or fail to detect, many of the traditional plots used to provide insight into linear regression are of minimal benefit.

Keen insight may be provided by creating a function that is the difference between the predicted probability of the detecting agent–given concentration and the predicted probability of the detecting simulant–given concentration and plotting that function against concentration. In our LE example, we create the following function:

$$\text{LE\_DIF} = P(\text{Detect LE}|\text{Concentration}) - P(\text{Detect Killed LE ALO}|\text{Concentration}).$$

Figure 2 depicts a plot of LE_DIF and concentration. The X axis on this chart has been shifted to create an unclassified figure.

From this plot the following can be determined:

- The simulant-killed LE ALO accurately predicts detector performance for LE agent at high and low concentrations.
- The maximum difference in expected detection performance between challenges of LE and killed LE ALO is 0.62.
- The difference in the probability of detection between live LE and killed LE ALO
  - exceeds 0.60 over a range of 5 Agent Containing Particles per Liter of Air (ACPLA),
  - exceeds 0.20 over a range of 23 ACPLA.
- Detection performance when challenged with agent LE is greater than when challenged with LE ALO at the same concentration.

It is not surprising that the simulant-killed LE ALO accurately predicts detector performance for LE agent at high and low concentrations. At some low concentration, the JBPDS can detect neither killed LE ALO nor LE agent; hence the difference is zero. At some high concentration, the JBPDS always detects both the killed LE ALO and LE agent; hence the difference is zero.

The maximum difference in expected detection performance between challenges of LE and killed LE ALO is 0.62. Since the maximum value of a probability is unity, 0.62 is quite large.

The difference in the probability of detection between live LE and killed LE ALO that exceeds 0.60 occurs over a concentration range of 5 ACPLA. The difference in the probability of detection between live LE and killed LE ALO exceeds 0.20 occurs over a concentration range of 23 ACPLA. Both of these concentrations are quite small. A difference of 5 ACPLA is in the noise of measurement error. For field trials, concentration typically ranges from 1 to 16,000 ACPLA. Hence, the magnitude of the difference in detection performance is actually quite small.

The function LE_DIF is formed by subtracting the expected probability of detection of the killed LE ALO given concentration from the expected probability of detection of the live LE agent given concentration. Since this function is always zero or positive, it is clear that the JBPDS detects LE agent at a particular concentration at least as well as it detects killed LE ALO. Hence, the performance when challenged with the simulant-killed LE ALO is a lower bound on what the performance would be if challenged with actual LE agent. If the system performs well enough against killed LE ALO, then we know that it will perform better when challenged with actual LE agent.

If the difference in performance between the agent and the simulant is relatively small, and if the system detects agent better than it detects simulant, then the simulant performance in the field can be used as a lower bound of the performance when challenged with agent.

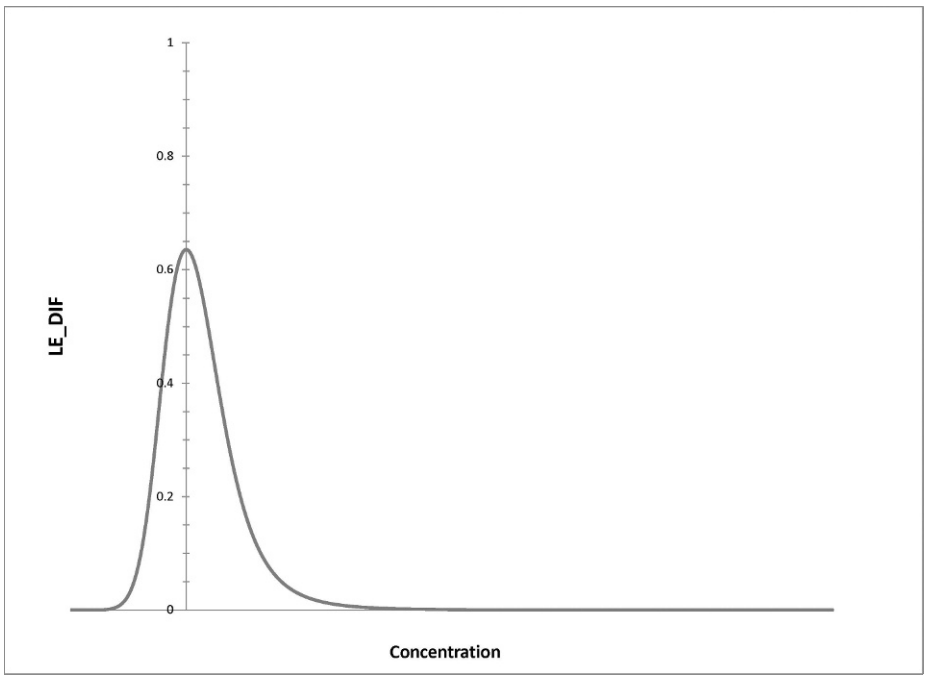


Figure 2. Joint Biological Point Detection System detection performance. In this plot, LE_DIF = P(Detect LE|Concentration) − P(Detect killed LE ALO|Concentration). DIF = difference and ALO = agents of like origin. (Concentration has been shifted and values left off to create an unclassified figure.)

Step 3: use the logistic regression model to predict performance

The logistic regression model follows and is described above. $P(\text{detect}|x,S) = e^{\alpha+\beta 1^S 1^x} / \left(1 + e^{\alpha+\beta 1^S 1^x}\right)$ can always be used to predict detector performance against agent given concentration. Soldier performance can be incorporated by factoring in releases that would have been missed as a result of maintenance or soldier inattention. As a means of validation, the equation can also be used to predict performance against simulant. The predicted results against simulant can then be compared with the actual simulant performance.

There are two limitations with step 3. First, test results are being estimated by an equation based on concentration as opposed to being measured. Second, since field testing is limited to simulant and no agent, it is being estimated by extrapolation as opposed to interpolation.

Conclusion

The procedure defined in this article is useful in predicting biological warfare agent and chemical warfare agent detector performance against agent in the operational environment based on testing with both agent and simulant in the laboratory during developmental testing and on testing with simulant in the field during operational testing. This method has been used to predict the performance of the Joint Biological Point Detection System and is currently being used on developmental detectors. ❑

CHARLIE E. HOLMAN, Ph.D., is Chief of the Chemical and Biological Defense Evaluation Division at the U.S. Army Test and Evaluation Command in Alexandria, Virginia. He has 20 years of experience in evaluating chemical and biological defense systems. He received a bachelor of science degree in biology from Pennsylvania State University, University Park, Pennsylvania; a master of science in biology from Bloomsburg State University, Bloomsburg, Pennsylvania; a master of mathematics from the University of South Carolina, Columbia, South Carolina; and a doctor of philosophy in biodefense from George Mason University, Fairfax, Virginia. He is a member of both the International Test and Evaluation Association and Military Operations Research Society. On August 16, he became a member of the faculty at Claflin University, Orangeburg, South Carolina. E-mail: holmancharlie@earthlink.net

ANDREW LOERCH, Ph.D., is an Associate Professor and the Associate Chair of the Department of Systems Engineering and Operations Research at George Mason University. He holds a master of science in operations research from the Naval Postgraduate School, Monterey, California, and a doctor of philosophy in operations research from Cornell University, Ithaca, New York. He is also

a retired Army Colonel with 26 years of active federal service of which 15 years was spent as a military operations research analyst. He is a Past President and Fellow of the Military Operations Research Society. He is an associate editor of Military Operations Research, and is the editor of the MORS newest publication, Methods for Conducting Military Operational Analysis. Dr. Loerch directs the track in Military Applications of Operations Research in the master's program in Operations Research at George Mason University. He presently receives funding through the Joint IED Defeat Organization. He also holds a black belt in Tae Kwon Do, is the principle bassoonist in the NOVA Manassas Symphony Orchestra, and is a huge fan of the New York Yankees. E-mail:aloerch@gmu.edu

References

Agresti, A. 1996. An introduction to categorical data analysis. New York: John Wiley & Sons.

Allison, P. D. 1999. *Logistic regression using SAS*. Cary, NC: SAS Institute and Wiley.

Fitch, J. P., B. P. Mark, W. Colclasure, M. Coleman, P. E. Coyle, H. H. Hill, N. B. Jackson, et al. 2004. *Review of test and evaluation methodology for biological point detectors*. Washington, D.C.: The National Academies Press.

Holman, C. E., and R. Berkowitz. 2009. Chemical and biological defense test and evaluation—A hallmark of integrating DT and OT. *ITEA Journal* 30: 381–385.

Holman, C. E., M. Moe, C. T. Russell, C. Jennings, R. Bartholomew, and D. Anderson. 2008. "Technical note: Whole System Live Agent Test (WSLAT) methodology and performance assessment." U.S. Army Test and Evaluation publication September 2008.

Holman, C., I. Kuria, N. Dunn, J. Timmerman, S. Colegrove, P. Serguievski, J. Kleimeyer, et al. 2007. "Report of the modeling and simulation of the Joint Service Lightweight Standoff Chemical Agent Detector (JSLSCAD)." U.S. Army Test and Evaluation publication March 2007. (Classified at the secret level; information used in this article was only unclassified.)

Hosmer, D. W., and S. Lemeshow. 1989. *Applied logistic regression*. New York: John Wiley & Sons.

Moe, M., C. E. Holman, D. Kao, E. Heaps, C. Jennings, and A. Thomas. 2010. "Abbreviated system evaluation plan for the Whole System Live Agent Test (WSLAT) phase II of the Joint Biological Point Detection System (JBPDS)." U.S. Army Test and Evaluation publication April 2010.

Musgrave, D., and C. Holman. 1997. "Biological Integrated Detection System (BIDS) pre-planned product improvement program IOTE test and System Evaluation Report Evaluation (SER)." U.S. Army ATEC Report, Alexandria, Virginia.

Musgrave, D., C. Holman, S. Tackett, K. Finanger, J. Fuller, R. Jernigan, T. Hillard, and C. Sleeper. 2000. "System Evaluation Report (SER) for the Biological Integrated Detection System (BIDS) Pre-Planned Product Improvement (P3I) System Evaluation Report (SER)." U.S. Army Test and Evaluation publication May 2000.

Musgrave, D., N. Dunn, F. Gasiorowski, J. Winters, S. Tackett, and C. Holman. 1997. "System evaluation report of the Joint Service Lightweight Integrated Suit Technology I (JSLIST I) Developmental and Operational Tests (DTs and OTs)." U.S. Army Test and Evaluation publication April 1997.

Shirakawa, K., C.-T. Russell, and C. E. Holman. 2008. *Estimating Performance of a Standoff Biological Detector*. MOR SS June 10–12, 2008, New London, Connecticut: U.S. Coast Guard Academy.

Chapter News

Emerald Coast Chapter

The Emerald Coast ITEA Chapter hosted a luncheon on September 28 at the Eglin AFB Enlisted Club Lounge. The guest speaker was **Col Michael E Gantt**, Commander 53rd Wing, who presented a discussion on "DT/OT Integration." The 53rd Wing comprises approximately 2,000 military and civilian people at 17 locations throughout the US and is responsible for fighter, bomber, and remotely piloted air vehicle operational testing and evaluation, and tactics development and evaluation in the areas of electronic combat, armament, avionics and aircrew training devices. Col Gantt's topic of discussion was Integrated Testing (IT), which is the combined effort of performing Development Test and Evaluation

Col Michael E. Gantt

(DT&E) and Operational Test and Evaluation (OT&E). IT requires a collaborative partnership between all the stakeholders, which includes the users, acquisition program offices, developers, and the Developmental/ Operational testers.

Col Gantt noted that while the acquisition program offices are the catalyst of better IT and should take the lead in all IT initiatives, the testers must collaborate to the fullest extent possible to make systems better. Examples of successful programs that used robust, fully integrated DT/OT testing included the B-1 Sniper ATP, F-22 OFP Testing, and F-15 Combined Test Force. In concluding, Col Gantt stressed the need for AF PEOs to solicit Program Managers (PMs) to lead efforts to improve integrated test, and the focus of these PMs should be to establish and sustain robust, responsive, and inclusive Integrated Test Teams (ITTs). The focus of program ITTs should be to charter applicable stakeholders to conduct "clean sheet" studies of how to improve IT within the acquisition program. The focus of testers should be on collaborative test planning, facilitated by a common analysis methodology.

■ ■ ■

Chapter Locations

NORTHEAST REGION
Vacant, Vice President

CONNECTICUT & RHODE ISLAND
Narragansett Bay Chapter
Vacant

MASSACHUSETTS
New England Chapter
Michael E. Keller, Sr., President
Boston, MA

NEW JERSEY
South Jersey Chapter
John Frederick, President
Atlantic City, NJ

EAST REGION
Robert A. Vargo, Vice President

EUROPE
European Chapter
Steve Lyons, President
United Kingdom

ISRAEL
Israeli Chapter
Aaron Leshem, President
Haifa, Israel

OHIO
Miami Valley Chapter
Stephen Tourangeau, President
Dayton, OH

MARYLAND
Francis Scott Key Chapter
https://www.sksi.net/fskitea/index.html
John B. Schab, President
Aberdeen, MD

Southern Maryland Chapter
Bill Darden, President
Patuxent River, MD

DC/NORTHERN VIRGINIA
George Washington Chapter
http://gw-itea.org
Michael Wetzl, President
Washington, DC

VIRGINIA
Tidewater Chapter
Brian C. Ensogna, President
Virginia Beach, VA.

SOUTHEAST REGION
Mike McFalls, Vice President

ALABAMA
Rocket City Chapter
Leigh Christian, President
Huntsville, AL

FLORIDA
Central Florida Chapter
David P. Grow, President
Orlando, FL

Emerald Coast Chapter
http://itea-ecc.org
Robert A. Crist, President
Eglin AFB, FL

GEORGIA
Atlanta Chapter
http://iteaAtlanta.org
Alvan Kimbrough, President
Smyrna, GA

SOUTH CAROLINA
Charleston Chapter
Philip Charles, President
Hanahan, SC

Volunteer Chapter
Nickolas Frederick, President
Arnold AFB, TN

SOUTHWEST REGION
Gregory D. Lamberth, Vice President

COLORADO
Rocky Mountain Chapter
http://www.itea-rmc.org
Christopher Mayette, President
Colorado Springs, CO

ARIZONA
Huachuca Chapter
Johnathan Woodruff, President
Sierra Vista, AZ

Valley of the Sun Chapter
Robert A. Olson, President
Scottsdale, AZ

NEVADA
Southern Nevada Chapter
Steve L. Moraca, President
Las Vegas, NV

NEW MEXICO
Roadrunner Chapter
Stephen "Buzz" Sawyer, President
Albuquerque, NM

White Sands Chapter
Douglas D. Messer, President
White Sands, NM

UTAH
Great Salt Lake Chapter
Jefferey D. Peterson, President
Dugway, UT

WEST REGION
Keith Sutton, Vice President

CALIFORNIA
Antelope Valley Chapter
http://www.iteaavchapter.org
Michael Berard, President
Edward AFB, CA

Channel Islands Chapter
Christopher J. Weal, President
Point Mugu, CA

China Lake Chapter
Bettye R. Moody, President
China Lake, CA

Greater San Diego Chapter
Jack Sears, President
San Diego, CA

WASHINGTON
Pacific Northwest Chapter
Jon Hanan, President
Seattle, WA

PACIFIC REGION
Stewart V. Burley, Vice President

AUSTRALIA
Southern Cross Chapter
Peter G. Nikoloff, President
Edinburgh, South Australia

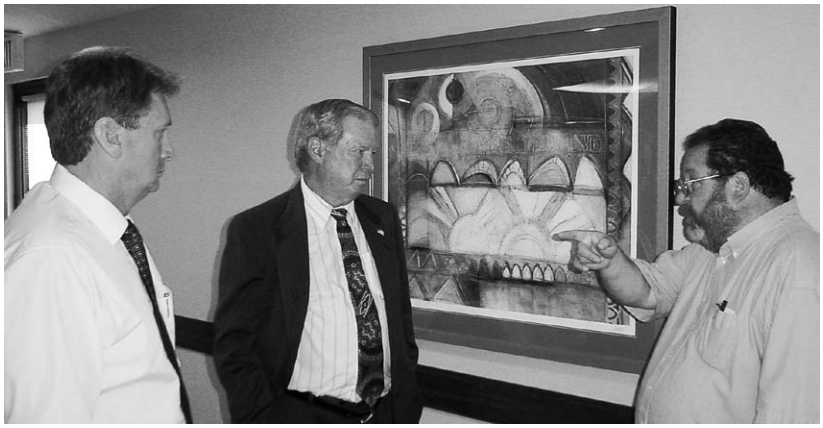
HAWAII
Mid-Pacific Chapter
Sandy D. Webster, President
Kekaha, HI

Greater San Diego Chapter

Luncheon Highlights JTRS Program and Testing: The Greater San Diego Chapter hosted **Mr. Greg Adams**, Test and Evaluation Lead for the Executive Director for Joint Program Executive Office (JPEO), Joint Tactical Radio System (JTRS) Enterprise Integration (EDEI) Staff, at its August Luncheon. Greg gave a comprehensive overview of the JTRS program and the unique testing plan developed for the family of radios JTRS will ultimately produce. The JTRS family of software programmable radios will provide the vital terrestrial leg of the tactical networking capability being developed to extend the global information grid (GIG) to ground, air, and seagoing forces. Based on a series of interoperable networking waveforms, the JTRS product line will provide flexible networking capability to tactical forces at "the tip of the spear." In coordinating the testing of this range of new capabilities, Greg's approach integrates the testing efforts of the individual services test agencies to ensure that the JTRS family of radios is interoperable and capable of meeting key performance parameters as individual radios and waveforms are fielded.

In addition to Greg's highly informative talk, the usual socializing, networking and door prize drawing were the highlights of the luncheon.

Greater San Diego Chapter president Jack Sears thanks Greg Adams, Test and Evaluation lead for JPEO JTRS, for his presentation at the Chapter's August luncheon.



Greg Adams, Test and Evaluation lead for JPEO JTRS, discuss the JTRS test and evaluation program with members at the Greater San Diego Chapter's August luncheon.

■ ■ ■

Francis Scott Key Chapter

The Francis Scott Key Chapter leadership would like to thank the ITEA Board of Directors and Awards Committee for recognizing FSK members, **Cathy Pritts** (DDT&E) as the recipient of the ITEA Energizer Award, and **Dr. Michael Barton** (Trideum Corporation), recipient of the Board of Directors Award at this year's ITEA Annual Symposium. Both Mrs. Pritts and Dr. Barton are exceptional members of ITEA and their awards were truly deserved. Also, as a testament to the local members and their dedication to this chapter, we are pleased to inform you that we received the Chapter of Excellence Award for contributing effectively to ITEA's mission and goals to help ITEA in furthering the professional and technical interests of the Test and Evaluation community.

In October, the Francis Scott Key chapter kicked off its fall luncheon series. On October 6, **Dr. Steven Hutchison,** Test and Evaluation Executive, Defense Information Systems Agency, was our invited keynote speaker. Dr. Hutchison's presentation was titled, "Test and Evaluation for Agile Information Technologies." We thank Dr. Hutchison for his time and for his very thought provoking presentation. The adoption of the DoD IT Test, Evaluation, and Certification (TE&C) process to an agile model hopes to ensure that TE&C continues to be an enabler of rapid acquisition of enhanced information technologies for the Warfighter. Special thanks to **Diane Eberly,** Army Evaluation Center and Dr. Michael Barton for their help hosting a successful luncheon.

Our fall 2010 and spring 2011 luncheons will continue to be scheduled for the first Wednesday of the month. The schedule includes November 3, December 2, March 2, April 6, and May 4. If you are in the Aberdeen area and your schedule permits, please come and join us. Guests are always welcome.

As 2010 comes to a close, the Francis Scott Key Chapter looks

ahead to a very busy and productive 2011. The chapter is in the planning stages of a local event where testers, evaluators, researchers, and developers can share their views on how they can work more closely together to ensure T&E is efficient while adding maximum value in the acquisition process. Please mark your calendar for March 2; we hope to see you there. In addition, the Francis Scott Key chapter is also in the planning stages of hosting quarterly educational seminars free of charge to the local community. The chapter is fortunate to have multiple leading experts in many areas within T&E and plans to utilize their knowledge. The chapter hopes to help educate a new transitioning workforce to the area by providing 2-hour technically intensive talks on topics which will help broaden the knowledge of T&E professionals in the area. Proposed topics might include: Systems Engineering, Design of Experiments, T&E of Intelligence, Surveillance, Reconnaissance (ISR) Systems, Survivability and Lethality T&E. If you have ideas on potential subject topics or if your company would like to sponsor a session; please contact chapter president **John Schab** (Georgia Tech Research Institute) at john.schab@gtri.gatech.edu. We are always open to suggestions and forever seekingvolunteers.

Finally, 2011 is going to be a huge year of transition for the Aberdeen area as a result of BRAC. We welcome all newcomers to the area, and we extend an open invitation to all of our ITEA events. We hope you become involved in our local chapter as you settle in at Aberdeen as we are always looking for new ideas and suggestions. If you have interest in becoming an active member of our local Board of Directors or filling one of our officer positions or would just like more information about our chapter, please contact John Schab at the email address listed above. We look forward to meeting you.

■ ■ ■

George Washington Chapter

The George Washington Chapter elected new officers to two-years terms starting in September. Former Vice President **Mike Wetzl** was elected President and former Secretary **Lou Husser** became Vice President. **Mike Bell**, who was previously the chapter's Program Chair, became Secretary. **Erika Chan**, who recently joined the chapter, was elected Treasurer. While presiding over his first luncheon meeting as President, Wetzl praised the accomplishments of previous President **Chas McKee**, who had just been elected to the ITEA Board of Directors.

At its luncheon on September 23rd at the Army Navy Country Club in Arlington, VA, the George Washington Chapter heard **Captain Austin Gould**, USCG, Program Manager of the CG-926 Research, Development, Test and Evaluation (RDT&E) office. He described the test and evaluation support CG-926 provides to Coast Guard Programs. He spoke on USCG capabilities in test planning, providing guidance for TEMPs, robust developmental testing, asset Verification Progress Reports and of supporting test

Captain Gould addresses GW Chapter.

New GW Chapter officers (left to right) President Mike Wetzl, Vice President Lou Husser, Secretary Mike Bell, and Treasurer Erika Chan.

execution. Gould pointed out that developmental testing builds towards Operational Test Readiness Reviews which determine readiness for IOT&E. The USCG uses the US Navy COMOPTEVFOR for the majority of the OT&E for Coast Guard systems and has a memorandum of agreement for this support. His office has expertise in aviation, surface, C4ISR and logistics T&E. He gave several examples of tested systems including three surface vessels: National Security Cutter, Fast Response Cutter, and Response Boat Medium, as well as three aviation examples: C-144 Ocean Security aircraft, MH-65 Helicopter Upgrade, and MH-60T Helicopter Upgrade. Gould said that test execution by the office includes on site test management, post-event briefings, and objective data reporting. After a Q&A session, chapter president Mike Wetzl presented Captain Gould an ITEA globe as a memento of the occasion.

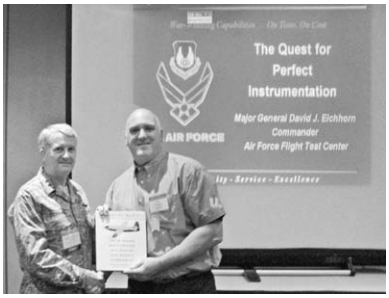
■ ■ ■

Southern Nevada Chapter

"Test Instrumentation Workshop Held in Las Vegas Successful"
This year, the Southern Nevada Chapter hosted the 14th Annual Test Instrumentation Workshop in Las Vegas. The new location and incorporating training into the program with the theme, *Test and Training Enterprise: To boldly go... to common solutions for Test and Training Instrumentation* proved to be a record breaker for attendance and tutorial participation. Both the Antelope Valley (AV) and China Lake Chapters assisted the Southern Nevada Chapter in hosting its first event.

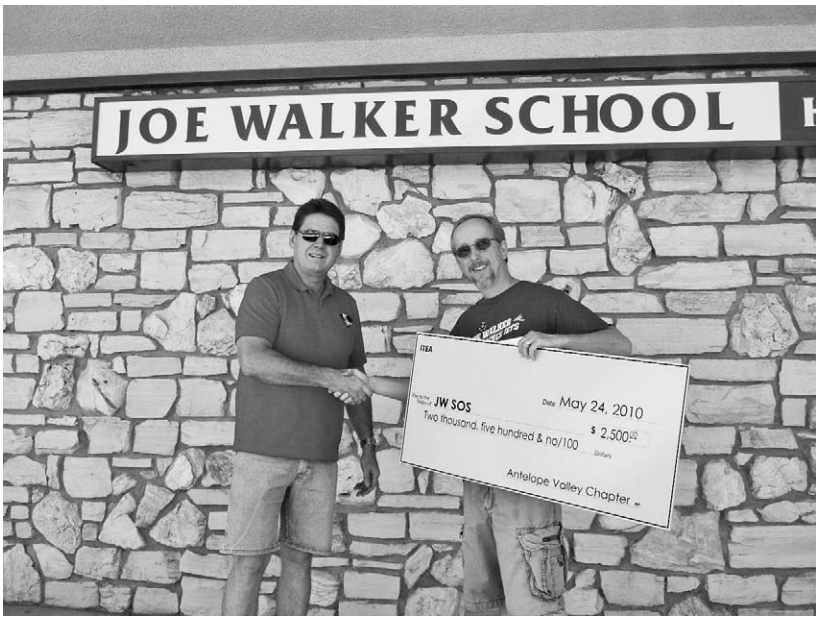
Overall, there were 327 registered attendees and 103 people attended the tutorials prior to the

Antelope Valley High School Robotics Team Members 'The Robolopes' receives a check in the amount of $3500 from Mr. Douglas Hoffelt



Major General Eichhorn and ITEA Antelope Valley Chapter President, Tim Chalfant

Mr. Douglas Hoffelt presenting a check for $2500 to math teacher, Ms. Mary Hanes and Mr. Nat Adams, principal at Desert High School for the purchase of TI-84 Graphing Calculators



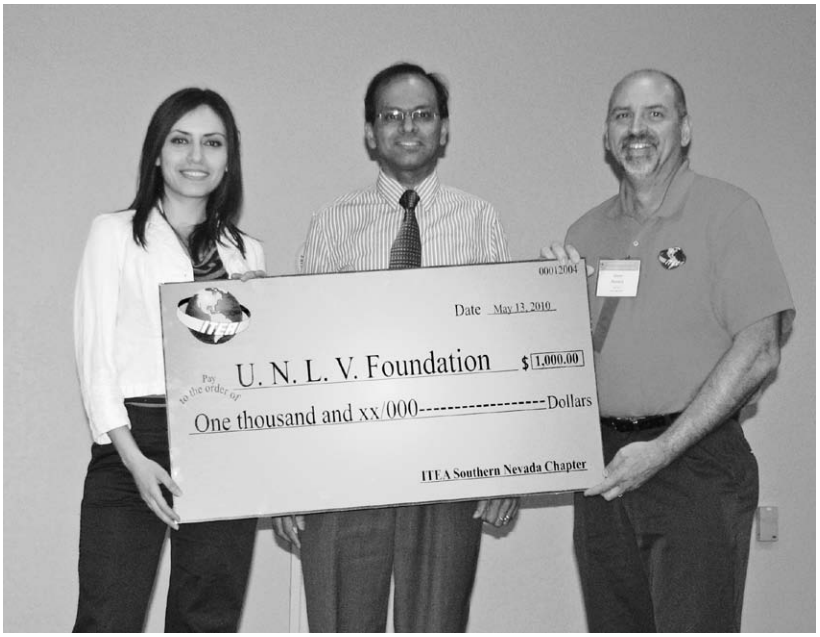
Mr. Jeremy Pontius, teacher and primary faculty advisor at Joe Walker Middle School receives a check from Mr. Douglas Hoffelt in the amount of $2500 for the Joe Walker Science Jets Team

start of the workshop. There were also more exhibitors this year.

"We have grown in attendance to almost 100 percent," AV Chapter President, **Mr. Tim Chalfant** said. "I'm happy with the tutorials which are a useful service for training attendees." The workshop kicked off on Monday, May 10 with tutorials and an annual golf tournament. The following day, the workshop convened with the ITEA President, **Russell "Rusty" Roberts** explaining what ITEA is all about and thanking Edwards Air Force Base Commander, **Major General David J. Eichhorn** and Nellis Air Force Base Commander, **Major General Stanley J. Kresge** for their continued support and for ways to provide a platform to do such presentations.

Major General Eichhorn kicked off the workshop as the first keynote speaker and set the tone for the technical sessions that followed that day. The following morning, **Mr. Derrick Hinton**, Principal Deputy Director Test Management Resource Center

Ms. Lauren Park, Eagle Robotics Club President from Lancaster High School accepts a check in the amount of $3500 for the Eagle Robotics Team 399 from Mr. Douglas Hoffelt



(From left to right) Electrical Engineering student Ph.D. Candidate, Neveem Shlayan and Dean Rama VenKat, Ph.D. accept a scholarship check in the amount of $1000 from Chapter president, Steve Moraca.

(TRMC), addressed the audience to provide the TRMC's perspective on a common vision for test and training infrastructure. The technical sessions that followed varied on topics from Science and Technology- Spectrum Efficiencies Technologies to Software Tools for T&E. Major General Kresge concluded the workshop by expressing their mission to "shape the way our force fights through operational testing, tactics development and advanced training in air, space and cyberspace at the operational and tactical levels."

"The purpose of a workshop like this is to interface and tie communities together, where they aren't normally tied together," Chalfant added. "It is easy for testers and trainers to get stuck where they are at. This workshop allows participants to step back and see the bigger picture, resulting in collaborations, cost-efficiency, and direct customer relationships."

The AV Chapter at Edwards and the China Lake Chapter in Ridgecrest have a thriving scholarship program and each year they provide scholarship checks to deserving students in the field of science and engineering as they continue to support the future workforce of T&E. Scholarship checks were presented by **Mr. Douglas Hoffelt**, ITEA AV Chapter Scholarship Chair, to the Antelope Valley High School Robotics team; the Desert High School Math Department; the Joe Walker Middle School; and the Lancaster High School Robotics club. This year, the two chapters mentored the newly established Southern Nevada Chapter and because of the success of this workshop and the dedication of the volunteers who planned and executed this event, Southern Nevada Chapter president, **Mr. Steve Moraca** was pleased to present the University of Las Vegas (UNLV) Engineering Department, **Dean Rama VenKat, Ph.D.** and Electrical Engineering student and Ph.D. Candidate, **Neveem Shlayan** with a scholarship check in the amount of $1000. "As a chapter, we are focused on sparking student interest in the T&E profession and making the student body at UNLV aware of

great networking opportunities ITEA brings to their engineers." Southern Nevada ITEA Chapter President Steve Moraca said.

The UNLV Engineering Department currently houses 1,500 undergraduates, 60 Master of Arts students, and 10 doctoral students. According to Ven Kat, UNLV is ranked in civil and mechanical engineering. "We hope that the Department of Defense comes to UNLV and hires our students," Interim Dean Ven Kat said. "We have a lot of DOD-related projects."

As we celebrate 15 years hosting the annual Test Instrumentation Workshop in 2011, we will look to Las Vegas as the city and the Tuscany Suites as the venue. The three chapters will once again work together to provide its audience with the latest information including recognizable experts; senior level policy makers; exhibitors demonstrating their products and services; and educational sessions on test instrumentation.

We are in the process of accepting abstracts for the 2011 program, *Test and Training: Converging Solutions in a New Millennium* scheduled for May 9-12 and encourage you to contact us if you are interested in participating. The deadline for abstracts is January 31. Please visit *www.itea.org* for more information.

■ ■ ■

Association News

2010 ITEA Annual Technology Review
By Mark D.J. Brown, Ph.D.

The ITEA Annual Technology Review has increased in popularity within the T&E community and this year's program was once again, a tremendous success. One-hundred and eighty participants gathered in sunny (and hot) Charleston, South Carolina, on July 20-22, 2010 for two full days of a technical conference. The conference captured the latest information on new technologies that impact T&E through featured speakers, panel discussions, and technical tracks, while a half day was dedicated to those wanting to attend stimulating tutorials on a variety of topics.

Since we held this conference in the Southeast, I feel obligated to draw an analogy to NASCAR. Compared to other Technology Reviews, we were a little slow at the starting line, but quickly caught up with the pack and took the checkered flag in a dazzling photo finish! When we decided to go to Charleston, we knew it would be different; we had at that time, no ITEA chapter in the area for support and no local ITEA presence. Conference planning started in the capable hands of ITEA Board Member, **Mr. John Wiley** with his choice of two superb Technical Co-Chairs, **Mr. Michael Greco** and **Mr. David Smoak** and his selection of a dedicated team of volunteers. John transferred the role of Program Chair to me, and I picked up a well-defined program that was already on its way to success. During the planning process, a new Chapter was formed in the Charleston area. The Charleston Chapter, also known as the Low Country Chapter, quickly became active and took over planning and execution of the first golf tournament associated with this event. I would be remiss if I didn't recognize the entire committee for their hard work: **Tiffany Crosby**, **Teresa Lucchesi**, **Art Titus**, **Dot Buckanin**, **Roy Maines**, **Tom Sweet**, **Suzie Townsend**, **Jeff King**, **Kathryn Mensch**, **Sabrina Keys**, **Jennifer Salmorin**, and **Phil Sobolewski**.

Mr James Ward and RADM Michael Bachmann

The conference began on Tuesday morning, with a Golf Tournament led by the Chapter Vice President, Roy Maines. The tournament was a huge hit and was won by Scientific Research Corporation's Antarctica Team. More importantly, it provided a strong start to the Charleston Chapter's scholarship fund. On Tuesday afternoon, we hosted three highly relevant tutorials to today's T&E technologies with over 40 students in attendance. The first tutorial covered Design of Experiments and was instructed by **Dr. Tom Donnelly; Mr. Gene Hudgins** led the second tutorial where he discussed the implementation of the Joint Mission Environment Test Capability (JMETC) and the Test and Training Enabling Architecture (TENA); and finally, the third tutorial discussed Redefining the Boundaries of Cyber Security with **Mr. Greg Vick**.

On Wednesday morning, the Technology Review began with its first plenary session and a welcome by **Mr. Rusty Roberts**, ITEA President. Following Rusty, we were greeted to the Charleston area by North Charleston Councilman **Mr. Kurt Taylor**. **Mr. James Ward,** Senior Vice President

Dr Charles Watt and Mr and Mrs James Ward

Integrated Systems and Solutions Division, SRC then introduced our Keynote Speaker, **RADM Michael Bachmann**, the Commander of the Space and Naval Warfare Systems Command (SPAWAR). RADM Bachmann presented an exceptional overview of SPAWAR and its test and evaluation capabilities. The plenary session concluded with a dynamic, interactive panel on Cyber Security and Data Fusion. This panel, led by **Mr. Steve Lariviere,** included **Mr. Mike Mulville**, **RADM David Crocker** (USN Ret), **Dr. Richard Brooks**, **Dr. Lance Hoffman**, and **Mr. Zal Azimi** – all notable cyber experts from the government, industry, and academia. Following brief opening comments by all of the panel members, there was a very lively question and answer session that was dealt with the current challenges the T&E community faces in developing the personnel skills, technologies, and policies needed to support cyber testing.

Wednesday afternoon consisted of the conference's first three tracks -- Cyber Security, T&E of Human System Technologies, and Data Fusion. Cyber Security, led by **Mr. Vince Van Houten** had excellent presentations by **Dr. Richard Brooks**, **Mr. Gene Wagenbreth**, **Mr. Ed Page**, **Mr. Tom McParland, Mr. Fred Wright**, and **Mr. Josh Davis**. The Human System track was led by **Mr. Michael Shumberger** with **Dr. Marianne Clark**, **Mr. David Bate**, and **Dr. Joshua Gomer** delivering exceptionally strong presentations. The Data Fusion track, led by the Director of the FAA William J Hughes Technical Center, **Dr. Wilson Felder,** included superb presentations by **Mr. Micheal Reil**, **Mr. Russ Neimy**, **Dr. James LaRue**, **Dr. Ke-Thia Yao**, **Mr. Dan Davis**, and **Mr. Terrance Westerfield**. All three tracks were well attended with over 130 participants listening to the technical presentations until the conclusion of the sessions. We concluded our Wednesday program with a reception hosted by Scientific Research Corporation where the attendees and participants gathered to network and socialize.

The room was filled to capacity on Thursday morning as our first Keynote Speaker of the day, **Mr. Derrick Hinton**, Principal Deputy Director of the Test Resource Management Center, provided an overview of the Test and Evaluation/Science and Technology Program, including the Science, Technology, Engineering, and Mathematics (STEM) initiatives that they are currently pursuing to enhance the T&E workforce. Our second Keynote Speaker, **Mr. Robert Baker**, Deputy Director of Plans and Programs for Defense Research and Engineering (DDR&E), provided an overview of the defense research, development, test and evaluation budgets and how the new Quadrennial Defense Review may influence research initiatives. The morning continued with **Dr. Michael Drews** from Clemson University, who fascinated the audience with details on the technology behind the restoration efforts for the H.L. Hunley Civil War submarine. **Dr. Nicholas Rigas**, Clemson University, followed Dr. Drews and discussed the advancements in the testing of renewable energy sources. We concluded the plenary session with an outstanding panel on Unmanned Systems led by **Major General Stephen Sargeant**, Commander of the Air Force Operational Test and Evaluation Center. His panel was composed of **Mr. Derrick Hinton, Ms. Amy Markowich**, **Dr. Mark Swinson**, and **Mr. Ron Monroe** –senior government and industry leaders in the T&E community.

To follow the success of the previous afternoon, the conference concluded with three final technical tracks. The first was Unmanned Systems, led by **Mr. Ben Walsh,** where informative presentations covered technological advances and challenges in this area were provided by **Ms. Kristin Moore**, **Mr. Mark Pestana**, **Mr. Al Sciarretta**, **Mr. Vikram Manikonda**, **Mr. Joe Lougheed**, and **Mr. Steve George**. The second track covered a wide range of instrumentation technologies addressing many aspects of T&E was led by **Mr. Joe Bilodeau** with presentations by **Dr. Eddie Jennings**, **Mr. Steve Williams**, **Mr. Derek Strembicke**, **Mr. Jeffrey Schleher**, and **Mr. Roger Davis**. The final track on Real Time Hyper-Spectral Scene Generation was led by **Dr. Michael J. Barton**. This track also had exceptional presentations by **Dr. Jeff Sanders**, **Mr. Scott Brown**, **Mr. Al Curran**, **Mr. Stan Posey**, **Dr. Michael Stokes**, and **Dr. Robert Lucas.**

When a program cannot fit technical papers or presentations into the dedicated time allocations, we have the opportunity to still share that information with the audience by presenting 'Poster

Papers.' During this conference, we were pleased to showcase *Technology Challenges in the Development of LADAR Projectors for HWIL Testing* by **Mr. Hajin Him,** *Development of Compact Durable Medical Equipment for Battlefield and Domestic Applications* by **Mr. Matt Crum**, and *Sky Imager Mapping System* by **Mr. Phillip Janicki**. Because ITEA acknowledges those participating in the program that exceeded expectations, we presented **Ms. Sara Hanlin**, on behalf of Mr. Phillip Janicki, the award of Best Poster Paper for his paper, *Sky Imager Mapping System.*

At the conclusion of the program, we announced the recipient of the Best Paper award. A technical team comprised of several T&E leaders evaluated the submissions based on relevance to the T&E community and the novelty of the research involved to determine the winner. We were pleased to present the Best Paper award to Mr. Vikram Manikonda for his paper entitled *DCF® - A JANUS and TENA Compliant Agent-based Framework for Test and Evaluation of Unmanned Vehicles*.

I would like to extend our gratitude to our Platinum sponsors, Scientific Research Corporation and TASC; our Gold sponsors, American Systems, GTRI, and ITT; our Silver sponsors, Imagine One Technology & Management, SRA International; and our Bronze sponsor, Advanced Test Equipment Rentals. I also want to thank our exhibitors and once again our volunteers and the ITEA staff for their support and dedication. This was truly an incredible conference and that checkered flag photo finish is going to be a challenge to repeat.

Mark your calendar for the 2011 Technology Review Conference, July 19–21 in Annapolis, Maryland!

■ ■ ■

ITEA is pleased to welcome its new corporate members:

NetAcquire Corporation offers real-time telemetry and data acquisition products. Their proven COTS architecture creates a cost-effective environment for any mix of I/O signal, data format, and real-time data processing. Products include a range of network-centric distributed solutions that support low-latency, deterministic system operation common in airborne avionics and aerospace applications.

Qualis Corporation, founded in 1993 and headquartered in Huntsville, Alabama, is a woman-owned small business with proven performance supporting the U.S. Air Force, U.S. Army, U.S. Marine Corps, U.S. Navy, and NASA. Our skilled, diverse workforce in 16 states, Afghanistan, and Iraq has expertise spanning multiple disciplines including systems engineering, test and evaluation, logistics, and acquisition and program management.

RoundTable Defense, LLC (RTD LLC) is a Veteran-Owned Small Business founded by four partners with combined military and Department of Defense (DoD) acquisition experience of 100 years. RTD provides a seasoned, professional, and well rounded team with extensive experience in military operations, requirements analysis, test & evaluation, and acquisition management. RTD offers the Department of Defense and commercial defense vendors reliable, high-quality, experienced, and cost-effective support services. We are a systems engineering services company, specializing in Test & Evaluation, Operations Research and Systems Analysis, and Acquisition Management. RTD delivers a unique, well rounded team with expertise in both requirements analysis and operational test & evaluation. The "round table" in our name represents our belief in the equal importance of user requirements analysis, systems acquisition processes, and independent test and evaluation. To learn more visit www.roundtabledefense.com.

■ ■ ■

ITEA Corporate Members

A2LA—American Association for Laboratory Accreditation

ACRA CONTROL, Inc.

Advanced Sciences and Technologies

AEgis Technologies Group, Inc.

Agency for Defense Development

AI Signal Research

Alion Science and Technology

American Systems

AMPEX Data Systems Corp.

Applied Resources, Inc.

Arcata Associates, Inc.

Argon ST, Network Systems

ARINC Engineering Services, LLC

Astro-Med, Inc.

AVW Technologies

BAE SYSTEMS Technical Services

Battelle Memorial Institute

Boeing Company, The

CALCULEX, Inc.

Calspan Corporation

COLSA Corporation

CSC

Cubic Defense Applications Group

Defense Acquisition University

Department of Defence-RANTEAA

Dewetron, Inc.

DRS Defense Solutions LLC

Dynamic Science, Inc.

Epsilon Systems Solutions, Inc.

ERC, Inc.

EWA Government Systems, Inc.

Fabreeka International, Inc

General Dynamics C4 Systems

Georgia Tech Research Institute

Glacier Technologies, LLC

Herley Industries, Inc.

Image One Technology & Management, Ltd.

InDyne, Inc.

ITT Test & Support Systems

Jacobs Technology

Jacobs Technology Inc.

JT3 LLC

L-3 Telemetry-West

Life Cycle Engineering

MacAulay-Brown, Inc.

ManTech Systems Engineering Corporation

MEI Technologies, Inc.

MIL Corporation

NetAcquire Corporation

NewTec

NMSU/PSL, 21st Century Aerospace

Northrop Grumman Corporation

Photo-Sonics, Inc./IMC

PURVIS Systems Inc.

QineiQ North America-Systems Engineering Group

QUADELTA, Inc.

Qualis Corporation

Raytheon Missile Systems

Rockwell Collins, Inc.

RoundTable Defence, LLC

SAIC

Science Applications International Corporation

Sandia National Labs Interactive Systems Simulation & Assessment

Scientific Research Corporation

Sierra Lobo, Inc.

SPARTA, Inc.

Spiral Technology, Inc.

SRA International

Summit Instruments, Inc.

Summit Technical Solutions, LLC

SURVICE Engineering Company

SYMVIONICS, Inc.

System Development Center—CSIST

Syzygy Technologies, Inc.

Tactical Information Exchange Integration Office

TASC, Inc.

Trideum Corporation

U.S. Army Developmental Test Command

Weibel Scientific A/S

Westech International, Inc.

Windmill International, Inc.

Wyle

Last updated: October 2010

THE ITEA JOURNAL
AD SALES

Ad Rates for 2011

THE ITEA JOURNAL AD SALES CONTACT

Bill Dallas
Ph: 703.631.6226
wdallas@itea.org
4400 Fair Lakes Court,
Suite 104
Fairfax, VA 22033
Fax: 703.631.6221

Journal Specifications

Trim Size: 8 1/2 x 11 inches. Journal trims 1/8 inch off top, bottom, and outside edge. Live matter should be a minimum of 1/2 inch inside the trimmed edges, and a minimum of 1/2 inch should be allowed for the bind.

Graphics should be a minimum of 350 dots per inch. Add 1/4 inch for bleeds.

Formats: We accept TIFF or EPS format for both Macintosh and PC Platforms. We also accept files in the following native application formats: Adobe Acrobat (.pdf), Adobe Photoshop (.psd), Macromedia FreeHand (.fh), Canvas (.cvs), InDesign (.id), QuarkXPress (.qxd), Illustrator, (.ai) CorelPoint (.cdr), PowerPoint (.ppt), and Pagemaker (.pmd).

***

Disclaimer: All claims for errors in advertisements must be made in writing and received within ten days of publication and will be considered only for the first insertion of the advertisement.

2011 Production Schedule

Issue	Space Reservation	Ad Material
March	1/12	1/25
June	4/12	4/25
September	7/12	7/25
December	10/12	10/25

AD Type	Rates Effective January 2011			Corporate Member/VIP Partner Discounted Rates		
	1x	2x	4x	1x	2x	4x
Cover 2	$3,000	$2700	$2500	$2500	$2200	$2000
Cover 3	$2,900	$2600	$2400	$2420	$2120	$1920
Cover 4	$3,300	$3000	$2800	$2740	$2440	$2240
	4-Color					
Full page	$2500	$2200	$2000	$2100	$1800	$1600
1/2 page	$2000	$1700	$1500	$1700	$1400	$1200
1/4 page	$1500	$1200	$1000	$1300	$1000	$ 800
2-page spread	$4000	$3700	$3500	$3300	$3000	$2800
	Black/White					
Full page	$1900	$1600	$1400	$1620	$1320	$1120
1/2 page	$1500	$1200	$1000	$1300	$1000	$ 800
1/4 page	$1000	$ 700	$ 500	$ 900	$ 600	$ 400
2-page spread	$3100	$2800	$2600	$2580	$2280	$2080

Coming Events

Visit www.itea.org or call 703.631.6220 for event details.

January 24-27, 2011
El Paso, Texas

Live-Virtual-Constructive Conference
Hosted by the ITEA White Sands Chapter

March 2, 2011
White Marsh, Maryland

One Day Forum
Hosted by the Francis Scott Key Chapter

March 22-24, 2011
Sierra Vista, Arizona

Joint Interoperability Conference
Hosted by the Huachuca ITEA and the Southern Arizona Armed Forces Communications-Electronics Association (AFCEA) Chapters

---

May 9-12, 2011
Las Vegas, Nevada

Test Instrumentation Workshop
Hosted by the China Lake, Antelope Valley and Southern Nevada Chapters

---

June 13-17, 2011
Huntsville, Alabama

Test Week
Tutorials hosted by ITEA and the Rocket City Chapter

July 19-21, 2011
Annapolis, Maryland

Technology Review Conference
Sponsored by ITEA

August 2-4, 2011
Albuquerque, New Mexico

Directed Energy Test and Evaluation Conference
Hosted by the Roadrunner Chapter and the Directed Energy Professional Society

---

September 12-15, 2011
Orlando, Florida

ITEA Annual Symposium
Fostering Partnerships in T&E and Acquisition
Sponsored by ITEA

The ITEA Vision: *To be recognized as the premier professional association for the international test and evaluation community.*

The ITEA Mission: *To advance the field of test and evaluation worldwide in government, industry, and academia.*

www.itea.org