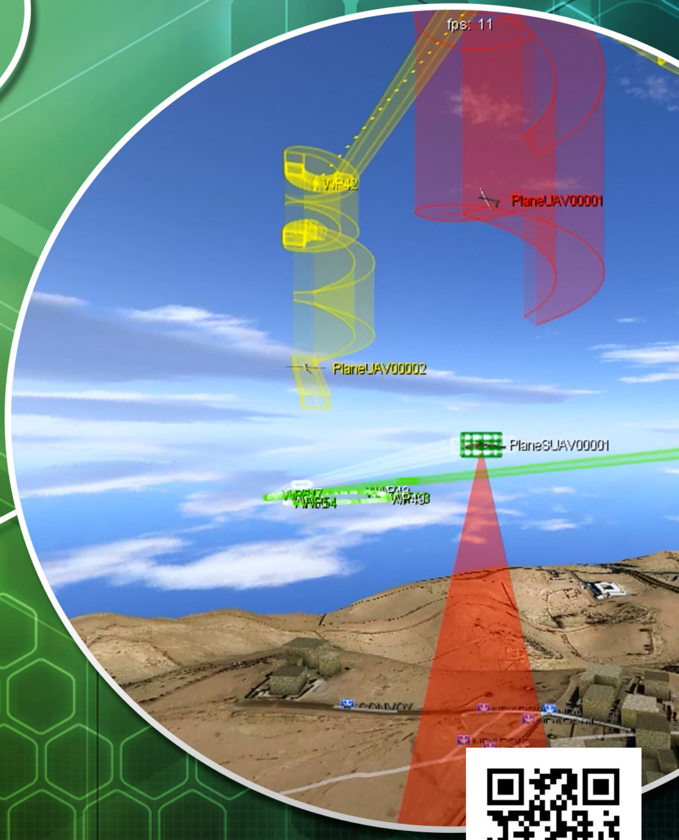
VOLUME 3 NUMBER 1
MARCH 2015

JOURNAL OF CYBER SECURITY & INFORMATION SYSTEMS

APPLYING MODELING & SIMULATION FOR DEFENSE

Information Dominance / Sensor Analysis & Development / Streamlining Acquisition



Achieving Information Dominance: Unleashing the Ozone Widget Framework

By Ms. Patricia Diercks, Captain George Galdorisi (U.S. Navy – Retired), Ms. Amanda George, Mr. Brent Brockman, Ms. Wanda Lam, Ms. Analiza Lozano, Ms. Rita Painter, and Mr. Glenn Tolentino

> "The continued development and proliferation of information technologies will substantially change the conduct of military operations. These changes in the information environment make information superiority a key enabler of the transformation of the operational capabilities of the joint force and the evolution of joint command and control."
>
> *- US Joint Chiefs of Staff's Joint Vision 2020*

"The enemy's ships are coming out of port," a series of flag signals warned as the message was relayed from ship to ship until it arrived at the *HMS Victory*, the flag ship of Lord Nelson. This crucial piece of information was the catalyst of the naval battle at Trafalgar where the Royal Navy defeated the combined French and Spanish fleet and established the command of the British empire of the world's seas.

The importance of delivering the right information to the right individual is just as critical to military operations today as it was in Lord Nelson's time. In this age of instant information collection and dissemination, the ability for military forces to rapidly harness needed information to plan and execute can mean the difference between victory and defeat. Warfighters today need the ability to pull information from across all information domains to build an accurate picture of the operational battle space. As the Duke of Wellington once noted:

> All the business of war, and indeed all the business of life, is to endeavour to find out what you don't know by what you do; that's what I call guessing what's on the other side of the hill.[1]

The information revolution has made it possible to reduce the guess work as information technologies provide the ability to gather and share information from a wide variety of sources to build a complex view of one's environment. However, military command and control along with military planning are beset with the challenge of obtaining information efficiently and effectively between different security domains. Military planners need to not only receive all the information, no matter the security classification, but also to pass the information relevant to the plans of action to their action officers who may have different security classifications. Too frequently information is "siloed" by its classification system, with necessary data residing on one or all of these networks: unclassified Nonsecure Internet Protocol Router Network (NIPR), classified Secret Internet Protocol Router Network (SIPR), or TOPSECRET Joint Worldwide Intelligence Communications System (JWICS). While this challenge is rampant within a single service, it becomes even more difficult when the planned mission needs to incorporate more than one service or more than one nation.

The Primacy of Information

"The joint force must be able to take advantage of superior knowledge to achieve 'decision superiority'—better decisions arrived at and implemented faster than an opponent can react…,"[2] notes the *Joint Vision 2020*. A key component of achieving "decision superiority" is the ability to access the right information at the right time—particularly in a future operating environment characterized by complexity and uncertainty. The *Capstone Concept for Joint Operations* notes that the future joint force must be able to engage in globally integrated operations:

> [Globally integrated operations] require a globally postured Joint Force to quickly combine capabilities with itself and mission partners across domains, echelons, geographic boundaries, and organizational affiliations. These networks of forces and partners will form, evolve, dissolve, and reform in different arrangements in time and space with significantly greater fluidity than today's Joint Force.[3]

Given the need to operate in a networked operational environment—one that calls for integration with joint, coalition, and National mission partners—it has become even more important that information be gathered appropriately from all sources, all classifications, and combined into a cohesive and useful data set that can be shared. Providing a framework to sift, organize, and swiftly share information received is vital if everyone in the military organization is to achieve the ability to make efficient and timely decisions. As the U.S. Joint Chiefs of Staff state, "decision superiority does not automatically result from information superiority. Organizational and doctrinal adaptation, relevant training and experience, and the proper command and control mechanisms and tools are equally necessary."[4]

The U.S. Navy has made information a "main battery" of its arsenal to enable effective maritime superiority and maintain global maritime awareness. Information, when networked across joint, allied, and coalition forces enables commanders with the ability to create a cooperatively created common operating picture—to better able to see what is over the horizon faster than the adversary. As noted in the *U.S. Navy's 2010 Vision for Information Dominance*, "[t]o be successful at 21st century warfare, the Navy will create a fully integrated C2, information, intelligence, cyberspace, environmental awareness, and networks operations capability and wield it as a weapon and instrument of influence."[5] Enhancing its proficiency at operating within the information domain will also allow the U.S. Navy to better respond to a rapidly changing battlespace as it takes advantage of advanced IT and networks; develop a global enterprise through network centric operations and command and control (C2); and elevating the use of information as a main weapon alongside traditional weapons.

The *U.S. Navy's Information Dominance Roadmap* recognizes the issue of ensuring the U.S. Navy can "maintain essential network and data link services across secured segments of the electromagnetic spectrum in order to transport, share, store, protect and disseminate critical combat information."[6] The *U.S. Navy's Information Dominance Roadmap* states the importance of having a system that can reach across secured segments of U.S. Navy's networks; there is currently not a fielded system to address the problem. The U.S. Navy faces a number of unique challenges in passing information out to its deployed fleet, and back to headquarters commands. While work on this problem is progressing in other areas, the U.S. Navy's Space and Naval Warfare Systems Center Pacific (SSC Pacific) has brought its experience with command and control, as well as programing and networks, to bear on the problem.

Secure Web Integration Framework (SWIF)

SSC Pacific has grappled with the problem of moving information through different security domains in an innovative and agile framework. The use of SSC Pacific's open source and in-house technologies such as OZONE Widget Framework (OWF), the Secure Web Integration Framework (SWIF) Security Services, and the Data-Driven Documents JavaScript (D3JS) library, can provide a secure environment where mission planners and analysts can develop comprehensive target systems for effects-based planning. This tool will allow users to build comprehensive political, economic, and social graphical models in direct support of warfighter needs. Information normally residing in multiple classification enclaves, such as NIPRNET, SIPRNET, JWICS, and higher will be accessible and discoverable by mission planners and analysts with a need to know via these interactive graphical models. The web-based interactive analytic planning tool will allow planners to visualize adversary factors such as threat, economic support, and weapons production, in terms of graphical features such as color, shape, and thickness. Drilling down on graphical elements, planners with the appropriate security accesses will have access to detailed target information.

Current analytical tools do not have the security features to handle—and where necessary—harmonize information from disparate classified networks. As a result, planners and warfighters are typically relegated to using static Power Point slides on the high side—resulting in sub-optimal planning and execution. Consequently, key adversary information remains undiscovered and the planner is typically unable to explore alternative scenarios and courses of action. This often results in suboptimal mission planning and in a worst-case scenario, can result in mission failure. The SWIF Security Services provide an interactive analytic tool that allows joint operational planners to visualize and access critical adversary data from multi-domain spaces to produce effective, safe, and successful mission plans. Planners and intelligence analysts will use this tool to develop dynamic models that will answer the "What if"-type questions typically posed by senior leadership and will ultimately enable these leaders to make better decisions, faster, with fewer people and fewer mistakes.

The analytical planning tool will allow planners to dynamically manipulate analytical data on the high side. These planners will be able to collaborate with in-house analysts, analysts from other organizations, and subject matter experts from academia and other agencies to discover information on the target system without fear of compromising security or mission success. Planners will have more effective tools that are able to seamlessly leverage all-source intelligence. Hence, they will be better equipped to deliver timely, mission specific plans to the warfighter.

SWIF Mission

SWIF is a web-based framework that allows users to collaborate and share information in a secure environment. SWIF provides different layouts for lightweight applications, called widgets, via a web browser. Information residing in SWIF is available to users who are cleared for access, yet, restricted to those who are not. The Joint Staff Senior Leadership has endorsed SWIF as a potential solution to address the challenge faced by the Joint operational planning community: Information that was available to planners was not discovered and therefore not utilized – impeding the flow from data, to information, to knowledge, and typically leading to suboptimal results.

SWIF Architecture

SWIF was developed on top of the OWF. OWF provides a platform for the rapid development and deployment of web-based applications that have the ability to communicate with each other. OWF is a web-based application framework developed by the National Security Agency (NSA) for use in a secure environment. NSA has provided the framework to the open-source community to foster further development and integration. Developed as a secure framework, OWF implements Discretionary Access Control (DAC) at the widget-level. This allows users and groups of users to access specific widgets they are authorized for depending on their role and responsibility. This provides some multi-level security but does not specifically implement security for access to the underlying data that will be utilized by the widgets.

The SWIF development team created several components to add the Mandatory Access Control (MAC) capability to OWF. MAC, the strictest of all levels of control, controls access to the data that differs for all resource objects on the system. Thus, under MAC, each unit of data is assigned a different security level allowing access to be controlled based on the data. The addition of MAC on the data itself in a multi-level security framework, will provide the security to allow for its use in a variety of multi-institutional settings. The SWIF development team also created an Application Programming Interface (API) to allow any developer to create widgets that are 'MAC enabled.' The extension of the OWF's capability to enable security MAC enhances the sharing and coordination of multi-institutional activities and artifacts within different accesses and classifications.

SWIF Security Model

SWIF implements data access restriction by enforcing MAC on all of its data operations. A user can only access the data which he or she is cleared to view. MAC is implemented at multiple security levels and can be configured based on the security policy of the network on which the framework is deployed. SWIF also implements DAC inherited from OWF to manage permission of widgets based on a user's roles. For example, a user with the Planner role will be granted access to the Plan Editor widget, the Capability Service Provider role to the Concept of Execution widget; this same user would not be granted access to widgets that were restricted to other roles.

In order to use this construct, all data must be assigned security labels, either from its original source or by users' input. The system will verify the data labels against the user's security accesses upon retrieval and saving of data. This will ensure a user cannot view (read) or label (write) data that are classified above his or her clearance level. This security implementation of MAC at the row (or record) level supports an environment where multi-level data access is required.

SWIF provides a core set of secure web services via a set of Representational State Transfer (REST) APIs. Developers who want to develop SWIF widgets would use the SWIF JavaScript Services to allow their widget(s) to communicate with the database and other widgets to display appropriate security banners for its content.

SWIF Dynamic Search

SWIF provides a dynamic search functionality that filters results based on a user's security accesses. Users can perform searches based on attributes such as keywords, characteristics of the data, security labels, or clearance level, etc., depending on the type of data.

In a prototype developed for the experienced planners in fiscal year 2013, SWIF widgets with specific search requirements were implemented to aid the planners and intelligence analysts in target and capability selection. Depending on the type of information needed, users could dynamically pull information such as targets, capabilities, courses of action from a plan from the SWIF database based on their roles (via DAC) and clearance level (via MAC). The SWIF Search widgets allowed the planners to select target/capability matches based on fields such as expected effect and target type to incorporate into their plan. Results would only include those capabilities to which the planner had access thereby maintaining MAC.

The search algorithm used in the SWIF Search Capability Widget was a text-based search that could match on multiple fields of the target and capability. The prototype effort has demonstrated the viability of SWIF in the Joint planning community. Future plans to enhance the Capability Search function include cell-level MAC and an ontological hierarchy to normalize capability descriptions.

Widget developers utilize the SWIF built-in search services via the SWIF REST APIs in two forms: searching and querying. The Search API provides the ability to request exact matches explicitly for one or more fields within the collection. The Query API accepts a string of terms and returns results that match one or more terms, along with a score for each result, based on the total sum of occurrences of all terms in all indexed fields.

SWIF Widgets

SWIF widget core capabilities act in concert to support all aspects of mission planning from target selection to concept of operations development. Target widgets focus on providing planners and analysts the ability to diagram and analyze government, economic, and social entities' relationships in support of target and capability selection. Planning widgets allow the user to develop multiple courses of action (COAs) and visualize events within the context of the overall plan. Most importantly, third parties are allowed to use SWIF as a framework for developing, as well as hosting, widgets to enrich core capabilities. Existing non-SWIF widgets can be rapidly adapted to integrate into SWIF. However, all widgets within SWIF must undergo the SWIF Governance Process for certification and accreditation (C&A) prior to deployment.

SWIF Widget Governance Process

The SWIF goal is to foster innovation rapidly to field relevant capabilities in order to meet existing and emerging collaborative needs amongst all branches of the military and from disparate security access levels. Currently, new capabilities are subjected to lengthy testing and C&A processes. This necessary, but lengthy, process may take as long as nine months to complete in which time crisis planning needs may be unmet. The SWIF architecture allows for a decoupling of the hosting web-based infrastructure and the widgets where functionality resides. The infrastructure consisting of OWF, SWIF Security Services, and the SWIF database would be subject to the full gamut of C&A review. However, once the infrastructure was certified and accredited, it will only undergo C&A for upgrades—not when new widgets are added. Widgets, on the other hand, would undergo a governance process that would streamline the C&A process based on their capabilities, complexity, and security boundaries.

Widgets are characterized as simple or medium based on their capabilities, complexity and security risk posture in relation to the networks in which they operate and the applications with which they interface. Table 1 delineates the difference between a simple and medium widget category type in SWIF:

Table 1: SWIF Widget Category

Widget Type	Renders Data from the SWIF Database	Saves Data to the SWIF Database	Inter-widget Communication
Simple	Yes	Yes	No
Medium	Yes	Yes	Yes

Widget approval is dependent upon the residual risks the widget poses to the network in which it operates and the systems it supports. These residual risks are then weighed against mission efficiencies, accuracies and overall improvements the widget creates in specific mission execution.

The widget governance process is streamlined into workflows dependent upon the widget's profile. The Widget Submission Package of medium widgets will undergo a workflow with more rigorous testing and review as compared to the governance workflow for simple widgets. Both the Simple and Medium Widget Governance Workflows can be seen in Figure 2 with color-coded roles. The Developer role (in blue) is responsible for ensuring the Widget Submission Package is complete and submitted appropriately according to the Widget Submission Package Checklist. The SWIF Project Team/Approval Board role (in light red) is responsible for: reviewing the Widget Submission Package for completeness, functional testing, integration testing, and final approval. Finally, the Security role (in light green) confirms that all Information Assurance (IA) testing is performed appropriately for the widget type. This governance process ensures that widgets are tested properly but without the unnecessary waste of time and effort.

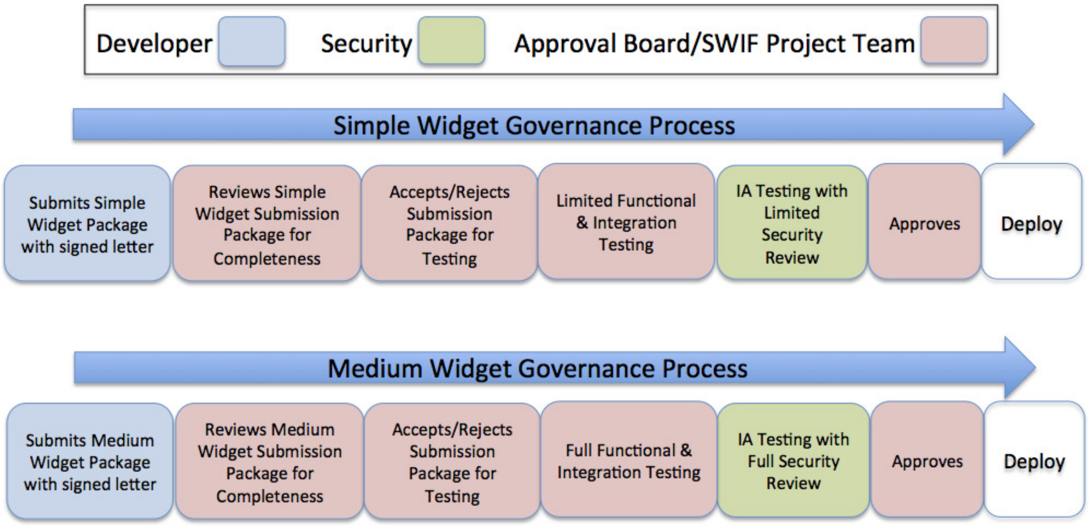

Developer
Security
Approval Board/SWIF Project Team
Simple Widget Governance Process
Submits Simple Widget Package with signed letter
Reviews Simple Widget Submission Package for Completeness
Accepts/Rejects Submission Package for Testing
Limited Functional & Integration Testing
IA Testing with Limited Security Review
Approves
Deploy
Medium Widget Governance Process
Submits Medium Widget Package with signed letter
Reviews Medium Widget Submission Package for Completeness
Accepts/Rejects Submission Package for Testing
Full Functional & Integration Testing
IA Testing with Full Security Review
Approves
Deploy

Figure 2: Widget Governance Process Workflow

SWIF Components

There are a variety of components that make up the SWIF construct. These components include an unstructured database, secure web services, APIs, and banner service.

NoSQL Database

For data storage, SWIF uses a NoSQL database. The main feature of the NoSQL database that SWIF utilizes is the capability to provide a dynamic schema. Standard relational databases require all field information to be defined ahead of time before data can be entered into the table. Having a dynamic schema allows the operator to insert data into a collection (table in relational database terms) with different fields for the same collection. In other words, a collection is created to which data is entered, but fields are not defined within a collection. This allows a widget to be installed without having to initialize a database to define tables. The simplification of a widget installation enhances the accreditation process because the core system does not have to be changed to install a widget.

SWIF Secure Web Services

Based on the Representational State Transfer architectural style (REST), the SWIF secure web services are provided to give access to MAC data stored in the SWIF NoSQL database. The services include standard methods that allow a developer to retrieve, save, update, delete, search, and label a particular data entity. Widget developers are also allowed to insert any fields into a collection as needed. The only requirement with MAC data in the NoSQL database is that every entity inserted into a collection has a security label with the required system security attributes and the user must have the required security accesses to the label. REST services are url-based and are problematic for widgets when urls are modified. To address this, a JavaScript library was incorporated into SWIF to handle the communication with the secure web services.

SWIF JavaScript API

The SWIF JavaScript API allows the widget to communicate with the SWIF secure web services by executing JavaScript methods from within the widget. This greatly simplifies the process of creating a secure widget by abstracting the complexity of knowing which URLs to call from a widget.

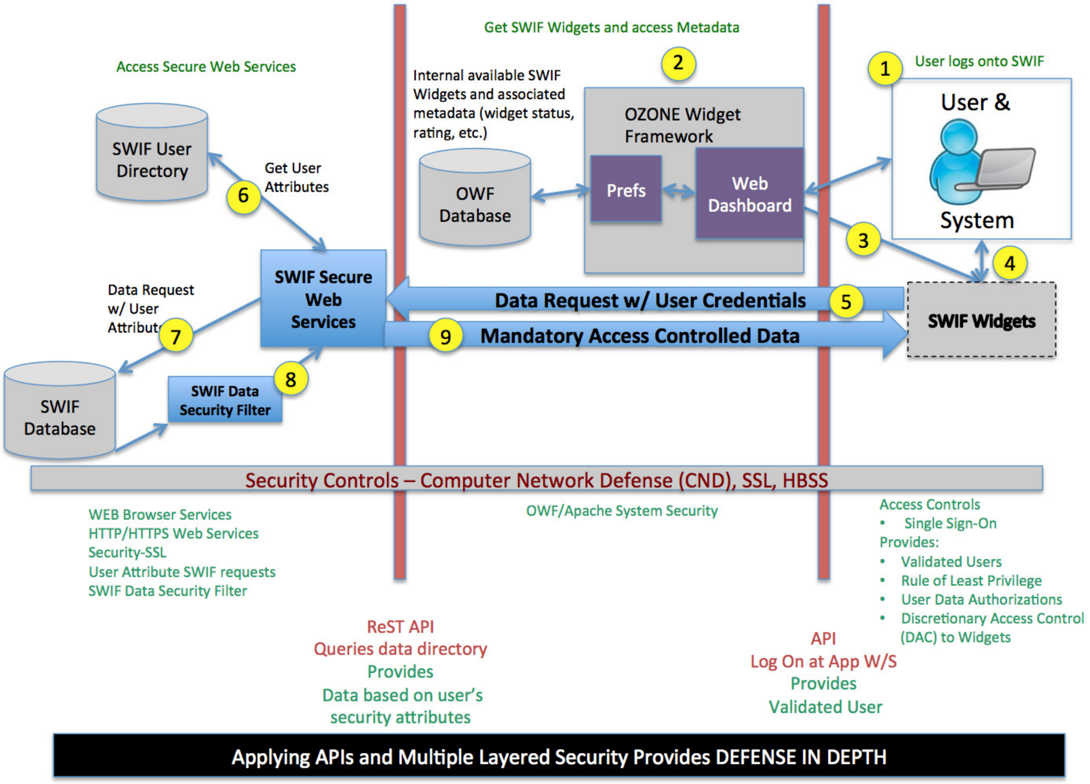
Banner service

SWIF contains a banner service that displays the current security information for all data inside a particular widget.

The banner is updated by the JavaScript library whenever data is changed in the widget. This keeps the user knowledgeable of the security of a data residing in a widget. The SWIF banner service also creates a banner at the top of the browser window that is a union of all security labels for all widgets on the dashboard. All banners are always in sync with the data that is contained under them.

SWIF Widget Lifecycle

The SWIF widget lifecycle describes how all of the SWIF components work together. Figure 3 shows the process of the SWIF Widget Lifecycle.



Access Secure Web Services
Get SWIF Widgets and access Metadata
User logs onto SWIF
Internal available SWIF Widgets and associated metadata (widget status, rating, etc.)
OZONE Widget Framework
SWIF User Directory
Get User Attributes
OWF Database
Prefs
Web Dashboard
User &
System
1
2
3
4
5
6
7
8
9
SWIF Secure Web Services
Data Request w/ User Attribut
Data Request w/ User Credentials
Mandatory Access Controlled Data
SWIF Widgets
SWIF Database
SWIF Data Security Filter
Security Controls – Computer Network Defense (CND), SSL, HBSS
WEB Browser Services
HTTP/HTTPS Web Services
Security-SSL
User Attribute SWIF requests
SWIF Data Security Filter
OWF/Apache System Security
Access Controls
• Single Sign-On
Provides:
• Validated Users
• Rule of Least Privilege
• User Data Authorizations
• Discretionary Access Control (DAC) to Widgets
ReST API
Queries data directory
Provides
Data based on user's security attributes
API
Log On at App W/S
Provides
Validated User
Applying APIs and Multiple Layered Security Provides DEFENSE IN DEPTH

Figure 3: SWIF Widget Lifecycle

1. User logs onto OWF via a web browser.
2. OWF retrieves the user's preferences and displays the user's OWF Dashboard that contains the widgets the user has selected to view.
3. User-selected, MAC-enabled, SWIF widgets are loaded onto the dashboard.
4. User interacts with the SWIF widgets that make calls to the secure database.
5. Data requests from SWIF widgets use the Central Authentication Service (CAS) Single Sign-on to pass along the user's credentials with each request.
6. SWIF Services receive all security attributes from the user account.
7. SWIF Services queries the secure database with the user's security attributes. Since the queries contain restraints using the user attributes, no data is returned from the database that the user should not see.
8. For additional security, SWIF services processes the data to ensure user's security attributes match data's security attributes.
9. Requested MAC data returned to the SWIF widget.

Exercise and Usability Testing

After the development of the SWIF prototype, in January 2013, a three-day event was held at SSC Pacific to explore—with the planning community—the usefulness of SWIF in accomplishing their planning mission. It allowed the demonstration of SWIF as a proof of concept enabling users to actively use the prototype as part of their planning process. The event focused on capturing user community input on SWIF features as well as its operational impact. The participants included policy support personnel, experienced Combatant Command planners, Naval Postgraduate students, observers from Johns Hopkins University Applied Physics Laboratory, and developers from SSC Pacific.

The productive three days provided SSC Pacific with a set of improvements to SWIF. Stakeholders identified attributes that will help SWIF evolve to a refined planning system:

- Ability to identify or search for capabilities to achieve desired effects outside of the current system

- Ability to pull planning and intelligence data from other domains that can easily be manipulated and presented
- Ability to pull all related planning data from a cloud source to the current system
- Improve capabilities by allowing SWIF types of applications with inherited MAC and DAC into a cloud-based secure mail application, similar to Google, Amazon, and Yahoo
- Customer off-the-shelf products that users would like to see integrated with SWIF to include Google earth, Google Docs, Tablets, and Gmail

The event provided a means for users to align their work with SWIF and validate the usefulness of SWIF with its MAC and DAC implementation. Attendees saw the value of SWIF to provide key functionality to their planning mission, as well as the integration of COTS related products.

Operational Impact

The operational SWIF user receives many benefits from using the SWIF architecture including increase productivity, faster functionality, and even cost savings. Increased productivity for the users stems from SWIF enabling the user to get the right information more quickly. In particular the increased operational functionality of the SWIF to include double-blind matching web-based applications improves the user's ability to match data in the database. Additionally, the interoperability of the SWIF widgets across different domains and networks allows different users to utilize the shared services, significantly decreasing the possibility of missing information due to differing classification levels.

The widget governance process also provides for faster delivery of functionality to SWIF users. The SWIF widget process uses a streamlined governance process, which embeds certification and accreditation, to shorten the delivery time. Small compact widgets, that don't impact the underlying data for the PoR, in particular have a very quick accreditation process. Even the larger widgets have a smoothly planned process for integrating into the SWIF. This decrease in delivery time allows the user to benefit from new tools and updated tools in a timely manner.

Not only does SWIF and its widgets increase productivity and deploy new tools in a smaller time frame, it also offers significant cost savings for industry, academia, and the Department of Defense. The OWF that SWIF and its widgets are based on is an open source framework allowing anyone to build their own widgets for their own specific challenges. The widgets would still go through the governance process, but the use of the open source framework significantly reduces the barriers to entry in creating widgets. Additionally, the integration of the testing and accreditation into the widget process will reduce the maintenance needed on deployed widgets; the widgets are thoroughly tested before they are deployed, thereby reducing the errors and vulnerabilities once deployed.

SWIF may serve as a key technology is in command and control (C2). One of the driving forces of command and control is having access to a number of C2 capabilities and data sources in order to accomplish the mission. Current C2 systems and data sources are often independent of each other, limiting the commander's ability to seamlessly reach across different systems and data sources to build the needed operational picture due to sensitivity, need to know, classification restrictions, or technology constraints. Even if the commander is given access to the information and capabilities, there exist some latency issues which may prevent the commander from getting the information in a timely manner.

SWIF allows for sharing of applications and information seamlessly with the DAC and MAC SWIF technical capabilities. It allows for a framework in which users are able to confidently and securely store information as well as share information on a need to know basis. It is a mechanism allowing for proprietary information from various classification levels to be shared in order to accomplish the mission. In addition, SWIF allows for the quick integration of widgets that allows planners and operators to be able to use the information in a secure manner without jeopardizing information that a specific person does not have the need to know.

Way Forward

Integration of the SWIF technology on two separate networks (high and low) will help meet the need to bridge the gap between highly classified networks and external networks, while maintaining security within a multi-level secure environment. SWIF's open architecture framework will allow for rapid deployment of analytic planning and visualization applications for the planning community, while enforcing a MAC and DAC connection to a database. In addition, development of planning widgets that can retrieve row- and cell-level data from a MAC-enabled database will allow for a more granular MAC labeling that will support planning at multiple security levels.

As the Department of Defense moves to implement the Joint Integrated Environment (JIE), the demand for multi-level security access, when only a select sub-group should have access to the information or the coordination of activities across agencies will significantly increase. The JIE will be a single joint enterprise IT platform that can be leveraged for all DoD missions.[7] In this case, the importance of enabling all partners to maintain control of access to their organization's data while conducting coordination and operating in a shared network space will be even more important.

Outside of the military, there are other communities that could also benefit from an environment with a security MAC-based framework, enabling the coordination of activities, and sharing of select company proprietary information with select partners while protecting the rest of their intellectual property from disclosure. This is especially important for institutions that are responsible for the integration of information in a single repository allowing various permutations of information sharing between organizations. It will allow different types of data to include business proprietary, educational research, and Government for official use only to be shared amongst each other or groups of people. An example of the usefulness for a non-military entity is Federal Emergency Management Agency's (FEMA) desire to improve the whole of community response to disasters. In this case, multiple federal, state and local authorities, as well as formal and informal non-governmental organizations would need to coordinate activities. Each organization has laws, rules, regulations, mandates or operating principles that dictate the use and sharing of information. This makes it impractical for the organizations to operate in a single, shared-information space; however a distributed architecture framework such as envisioned by SWIF would facilitate this coordination, allowing organizations to share information while controlling its distribution and access. SWIF provides the needed framework to enhance the sharing of different types of information seamlessly into one system to accomplish a goal or mission.

Endnotes

[1] Duke of Wellington, cited in Louis J. Jennings, ed., *The Correspondence and Diaries of the Late Right Honourable John Wilson Croker, Secretary to the Admiralty from 1809 to 1830 (London: John Murray, Albemarle Street, 1885), p. 276.*

[2] United States Joint Chiefs of Staff, *Joint Vision 2020 (Washington, D.C.: United States Joint Chiefs of Staff, 2000, p. 8.*

[3] United States Joint Chiefs of Staff, *Capstone Concept for Joint Operations: Joint Force 2020 (Washington, D.C.: United States Joint Chiefs of Staff, 2012), p. 4.*

[4] United States Chairman of the Joint Chiefs of Staff. *Joint Vision 2020. Department of Defense. 2000. Pg. 8.*

[5] United States Navy, *The U.S. Navy's Vision for Information Dominance, (Washington, D.C.: United States Navy, 2010), p. 3.*

[6] United States Chairman of the Joint Chiefs of Staff. *Joint Vision 2020. Department of Defense. 2000. Pg. ii.*

[7] Enabling the Joint Information Environment (JIE), (Ft. Meade, Maryland: Defense Information Systems Agency, 2014) p. 2.

About the Authors

Brent Brockman is a Software Architect and Software Development Lead for SPAWAR Systems Center Pacific. He has over 15 years of experience in Software Engineering with comprehensive experience in all levels of the software development life cycle. Brent has led technical teams mainly utilizing web technologies. He has focused the last several years on applications implementing Mandatory Access Control. He is experienced employing agile methodologies for his projects and is a Certified ScrumMaster. Mr. Brockman has a Bachelor of Science Degree in Computer Science from San Diego State University.

Patricia Diercks is a Senior Systems Engineer for the Command and Control Department at Space and Naval Warfare (SPAWAR) Systems Center Pacific (SSC PAC) located in San Diego, CA. Ms. Diercks has worked in the field of Command, Control, Communications, Computers, and Intelligence (C4I) and Crisis Management for over 25 years with emphasis on software design, development, and integration for Decision Support Systems in the area of logistical and mission planning tools. She is currently leading an effort to develop secure planning applications in a multi-level secure environment. She received her Master of Science Degree in Applied Mathematics (1987) from San Diego State University.

George Galdorisi is Director of the Corporate Strategy Group at SPAWAR Systems Center Pacific where he helps direct the Center's efforts in strategic planning and corporate communications. Prior to joining SSC Pacific, he completed a 30-year career as a naval aviator, culminating in 14 years of consecutive experience as executive officer, commanding officer, commodore, and chief of staff; including command of HSL-43, the Navy's first operational LAMPS Mk III squadron, HSL-41, the LAMPS Mk III Fleet Replacement Squadron, USS Cleveland (LPD-7), and Amphibious Squadron Seven. His last operational assignment spanned five years as Chief of Staff for Cruiser-Destroyer Group Three, during which he made combat deployments to the Western Pacific and Arabian Gulf embarked in the USS Carl Vinson and USS Abraham Lincoln. He is a 1970 graduate of the United States Naval Academy and holds a Masters Degree in Oceanography from the Naval Postgraduate School and a Masters Degree in International Relations from the University of San Diego.

Amanda George is a strategic analyst for SPAWAR Systems Center Pacific (SSC Pacific). Working with SSC Pacific's Corporate Strategy Group, Amanda supports SSC Pacific's programs in command and control, ballistic missile defense, widgets and apps, and agile software development. Amanda joined SSC Pacific in 2010. She recently received her Master's Degree in Pacific International Affairs from the University of California, San Diego with a dual concentration in International Politics and Economics. Prior to pursuing her Master's Degree, she founded and operated a tutoring company in San Diego's North County. She graduated magna cum laude from the University of California, San Diego with a Bachelor's Degree in Political Science with a focus on International Relations.

Wanda Lam is currently a senior systems engineer at Space and Naval Warfare (SPAWAR) Systems Center – Pacific (SSC-PAC). She has over 23 years of technical and management experience in joint distributed network systems with the last 6 years focusing on enterprise web-based architecture framework. Her knowledge and expertise focus in Command, Control, Communications, Computers, and Intelligence (C4I) and Crisis Management. She has led multiple technical teams to provide architectural design, software development and integration support to Intelligence Community customers, DOD agencies such as DARPA, ONR, and NSA, as well as non-DOD agencies such as ONDCP, NIH, and NASA. Ms. Lam holds a Bachelor of Science degree in Computer Science (1992) from San Diego State University.

Analiza Lozano is a Program Manager and a Branch Supervisor for the Command and Control Department at Space and Naval Warfare Systems Center Pacific, located in San Diego, CA. She has years of experience working with test and evaluation, afloat installations, project/program management, and personnel management. She holds a Bachelor of Science Degree in Information Decision Systems from San Diego State University and a Masters of Applied Science in Architecture-based Enterprise Systems Engineering from University of California, San Diego. She is currently the Deputy Program Manager for a C4I program.

Glenn Tolentino is a Senior Systems Engineer for the Command and Control Department at Space and Naval Warfare Systems Center Pacific located in San Diego, CA. He holds a Bachelor of Science Degree in Applied Mathematics with an emphasis in Computer Science from San Diego State University. He has also earned a Masters of Science Degree in Software Engineering from Southern Methodist University. He has over 20 years experience working with joint systems installation, design, development, integration, and deployment in the area of Command, Control, Computers, and Intelligence (C4I) programs for a variety of Department of Defense and Intelligence Community customers with focus on Systems Design, Information Operations, Decision Support Systems, and Computer Network Operations. He is currently a Systems Architect/Chief Engineer for a C4I program.

Rita Painter Wos serves as a SSC Pacific Liaison and embedded employee at the Naval Postgraduate School (NPS), Monterey California for the last 14 years. She facilitates and advises on collaborative research and sponsored programs between SSC Pacific and NPS to include marketing, proposal development, planning, financial management and delivery of research products to Navy and DOD funding sponsors. She also identifies and promotes collaborative research opportunities between SPAWAR, NPS, NSA, other DOD agencies, private sector laboratories, and private/state universities. Prior to her position at the NPS, she held positions at the National Security Agency for 11 years and was a consultant with Booz Allen and Hamilton for five years. She has a BA degree from the University of the State of New York, Albany and is working towards a MS degree in Information Systems Management.

Sensor Life Cycle Acquisition and Training with Modeling & Simulation

By Susan Harkrider, Dr. Keith Krapels, Andrew Krug, and Lana McGlynn

The U.S. Army's Night Vision and Electronic Sensors Directorate (NVESD) Modeling and Simulation Division (MSD) provides sensors acquisition engineering and analytical support and an extensive set of Government-owned Models and Simulations (M&S) to several Army Program Executive Offices/Project and Program Managers (PEO/PMs), supporting numerous Army acquisition programs across their life cycle. The MSD is organized to support sensor analysis, development, experimentation, testing, fielding, training and operations by: 1) providing sensor performance modeling, 2) refining models through field and laboratory measurements of developed sensors, and 3) developing models and simulations using physics-based algorithms of actual sensor performance or platforms. The M&S includes electro-optic, infrared, acoustic, magnetic, seismic, synthetic aperture and ground penetrating radar sensors, as well as certain munition effects related to the sensors' capabilities.

The NVESD MSD uses M&S to improve systems acquisition processes by reducing time, risk and resources while increasing utility and supportability. This paper will explain how the MSD has successfully utilized M&S throughout the acquisition life cycle of several programs, to include the Long Range Scout Surveillance System (LRAS3). Additionally, the paper provides a description of the development of the New Equipment Training (NET) simulation systems and their transition to a fielded, sustained simulator training solution.

Defense Acquistion Management System

The Defense Acquisition System exists to manage the nation's investments in technologies, programs, and product support necessary to achieve the National Security Strategy and support the United States Armed Forces. DoD Acquisition Policy is articulated in two principal documents: DoD Directive 5000.01 which describes management principles and overarching policy, and Interim DoD Instruction 5000.02 which describes the operation of the Defense Acquisition Management System. The Defense Acquisition Management System is an event-based process, and is commonly referred to as the acquisition life cycle. The generic model for this process is illustrated in Figure 1. PMs are authorized to tailor this model using discretion and prudent business judgment to structure an innovative, responsive program.

The life cycle process consists of periods of time, called phases, separated by decision points called milestones (MS). Some phases are divided into two efforts separated by program reviews. These milestones and other decision points provide both the PM and milestone decision authorities (MDAs) the framework with which to review acquisition programs, monitor and administer progress, identify problems, and make corrections.

Modeling and Simulation can be used to support the life cycle process from determination of mission needs; research; development; production; deployment; support; upgrade; and finally, demilitarization and disposal. When

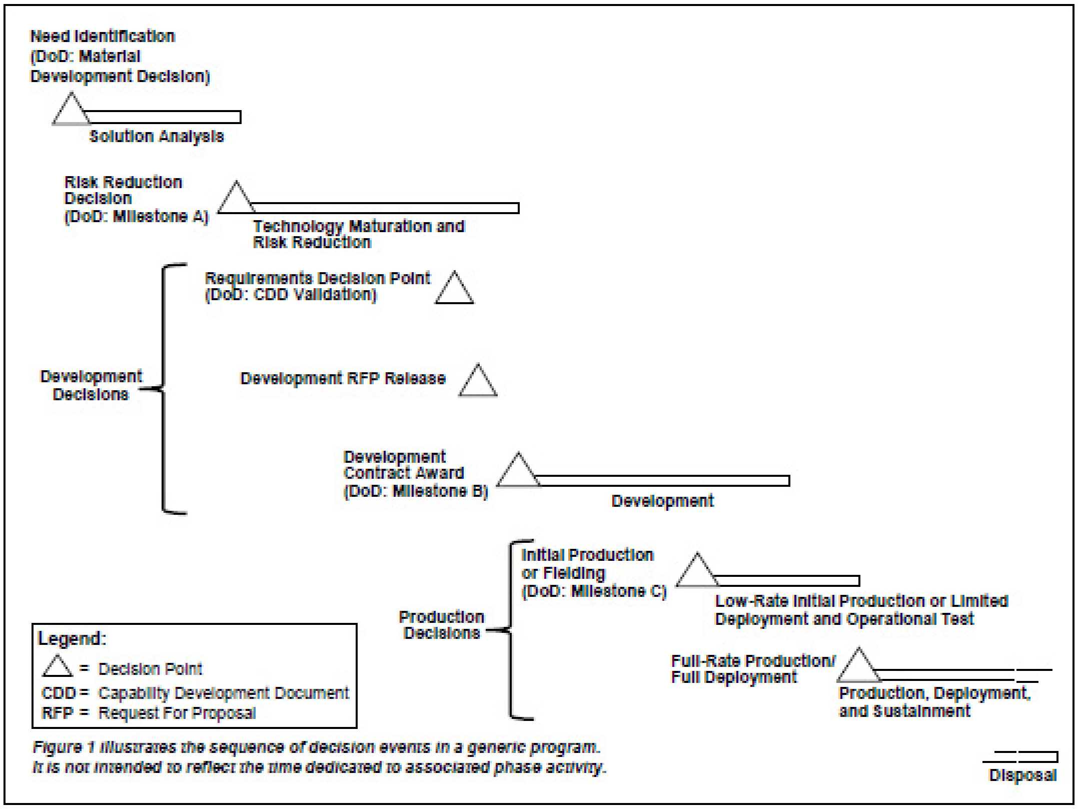


Figure 1 illustrates the sequence of decision events in a generic program. It is not intended to reflect the time dedicated to associated phase activity.

Figure 1: DOD Acquisition Process

used properly, M&S can help reduce costs, accelerate development, support test and evaluation, and better inform decision makers.

Materiel Solution Analysis Phase

The purpose of the Materiel Solution Analysis phase is to conduct the analysis and other activities needed in order to choose the concept for the product that will be acquired and to begin translating validated capability gaps into system-specific requirements, including the Key Performance Parameters (KPPs) and Key System Attributes (KSAs). The process begins with Need Identification, called the Materiel Development Decision by DoD, and simply stated is the decision that a new product is needed. This decision directs execution of the Analysis of Alternatives (AoA), and authorizes the DoD Component to conduct the Materiel Solution Analysis phase. To achieve the best possible system solution, the Materiel Solution Analysis phase places emphasis on innovation and competition. The PM examines existing, commercial off-the-shelf and other solutions drawn from a diverse range of large and small businesses. An AoA and a technology development strategy are developed to help guide the efforts during the next phase, which is technology development. The lead Component recommends a materiel solution to the capability need identified in the initial requirements document (ICD). The Materiel Solution Analysis phase concludes when the PM has completed assessing potential materiel solutions, and satisfying the entrance criteria for next milestone designated by the Milestone Decision Authorities (MDA).

NVESD is currently supporting an AoA for an Optical Augmentation Pre-Threat Detection system working with the Army's Maneuver Support Center of Excellence (MSCoE) Capability Development and Integration Directorate (CDID) at Fort Leonard Wood. NVESD will be using M&S to simulate the capability of the conceptual systems to determine the preferred attributes and their associated values with defensible analytic evidence. The objective of the analysis is to inform the MDA, currently PEO-Soldier, and to be used to help mitigate capability gaps identified while meeting affordability goals.

The Army's Combat Developers (CD) from Fort Leonard Wood previously utilized NVESD MSD expertise and M&S to assist in reaching a MS A decision for an Intelligent Munition System (IMS). Using the requirements provided by the CD via the ICD and draft Capability Development Document (CDD), NVESD modeled the IMS using the Night Vision Toolset's Comprehensive Munition and Sensor Server (CMS2). Working with the Army's Maneuver Battle Lab at Fort Knox to establish simulation scenarios, NVESD successfully analyzed measures of effectiveness and system performance parameters for the conceptual IMS. The results of the M&S efforts directly influenced the MDA as part of an AoA and helped satisfy the entrance criteria for the Technology Develop phase. The models developed during this phase were later refined to help the MDA through the down-select process. PM Scorpion was established to manage the IMS system that further leveraged NVESD MSD for use during the Engineering & Manufacturing Development phase to assess system performance in support of MS B and C decisions.

NVESD MSD also uses M&S to support the Material Solution Analyses phase and to design studies to identify the preferred solutions within future sensor systems. To support sensor analysis and development, the NVESD MSD develops and provides the Night Vision Integrated Performance Model (NV-IPM). This integrated set of sensor performance characteristics is based on physics research performed by the laboratory. The NV-IPM is a systems engineering tool that enables model-based engineering with a simple interface for trade studies. The sensor characteristics and modeled parameters can be provided as specifications to industry for actual development. The integrated model allows for a common baseline of performance specifications and scene conditions to enable prototype sensor systems development by industry. The NVESD MSD validated physics models enable the laboratory to compare many diverse sensor systems based on current research and/or potential development.

Sensor performance models are used both for data collection and analysis, and to support concept experiments and capabilities assessments. For example, the NVESD MSD used a virtual simulation to measure and determine the overall effectiveness of a virtual pointer (VP) targeting system, ultraviolet (UV) target marking system, and a system combining the two technologies during the Material Solution Analysis phase of the projects. The simulation also included a Soldier (human-in-the-loop) subjective survey that helped to identify the preferred solutions for pointer shapes, sizes, colors and reticle patterns within future optics systems. This subjective data was analyzed along with the sensor performance data to determine what factors led to the best target acquisition and identification times using the various targeting technologies. An example of a future optics design experiment is shown in Figure 2.

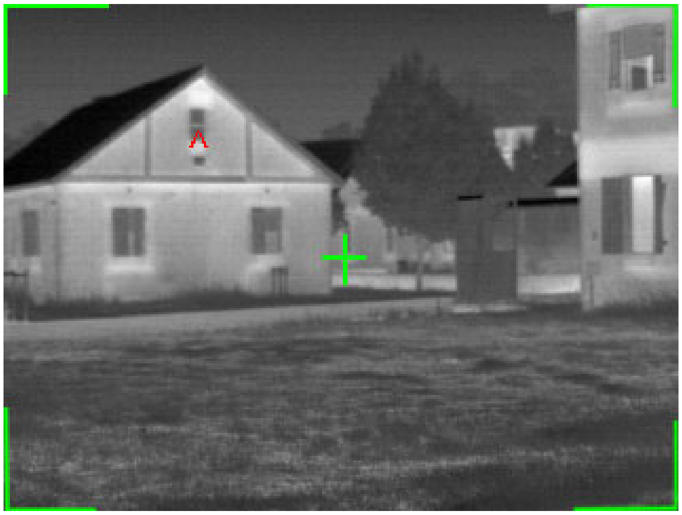


Figure 2: Future Optics Design Experiment

Technology Maturation and Risk Reduction Phase

The Technology Development Phase begins after the Milestone A decision has been reached. The ICD and Technology Development Strategy guide the work during the Technology Development phase. The purpose of this phase is to reduce technology risk, determine the appropriate set of technologies to be integrated into a full system, and complete a preliminary design. M&S is used to support competitive prototyping to reduce technical risk, validate designs and cost estimates, evaluate manufacturing processes, and refine requirements. The project exits the Technology Development phase when an affordable program or increment of militarily useful capability has been identified, the technology has been demonstrated in a relevant environment, manufacturing risks have been identified and assessed, a preliminary design review has been conducted for the solution, and a system or increment can be developed for production within a short timeframe (normally less than 5 years for weapon systems), or when the MDA decides to terminate the effort. At MS B, the MDA approves the acquisition strategy, the acquisition program baseline, the type of contract for the next phase, and authorizes entry into the engineering and manufacturing development phase.

The following paragraphs are examples of how NVESD MSD provides simulations and data collection to support business case reviews (BCR) leading to Milestone B decisions on whether to proceed with further development of new sensor systems.

To support the MS B decision for the future Family of Weapons Sights (FWS) capabilities, the MSD provided simulations support to PM Soldier Maneuver Sensors (SMS), under Project Manager Soldier Sensors and Lasers (PM SSL). The MSD planned, executed, and analyzed a series of data collection simulations comparing the FWS to the current Thermal Weapon Sights (TWS) capabilities, using Maneuver Battle Lab (MBL) approved scenarios with current Army Tactics, Techniques, and Procedures (TTPs). The data collected was used to support a BCR that led to the decision to proceed with further development of the new sensor system.

Following the analysis PM SMS, in developing the Family of Weapon Sights - Individual (FWS-I) for Rapid Target Acquisition (RTA), wanted to determine the most effective and desirable user interface (UI) for the FWS-I. The NVESD MSD was tasked by PM SMS to create a series of simulation exercises, using a simulated FWS-I and human in-the-loop exercises, to determine the best UI configuration based on measurable analytical data and subjective Soldier feedback gathered via surveys. This study also analyzed items such as the RTA reticle attributes, response times, and the preferred menuing and overlay options for the system. Trends were identified to determine what features of the FWS-I UI should be considered as requirements for the system and were incorporated into a report to PM SMS. The MSD continues to support FWS analyses and tests as development proceeds.

In addition, PM SMS wanted to gather subjective feedback on a design for a remote switch for the FWS-I system. The proposed design of the remote switch has a different hardware configuration than previous remote operating switches used with similar sensor platforms. NVESD MSD created a physical prototype (see Figure 3) using a 3-D printer based on the design for the FWS-I remote switch. NVESD integrated a $10, commercial, off the shelf (COTS) game controller board providing the button layout and functionality of the switch. This prototype interacted with the NVESD MSD simulation of the FWS-I sensor enabling subjective feedback from Soldiers and civilians on form, fit, and functionality. The feedback was gathered via surveys and conversations with the test subjects and used to inform the MDA for a MS B decision.

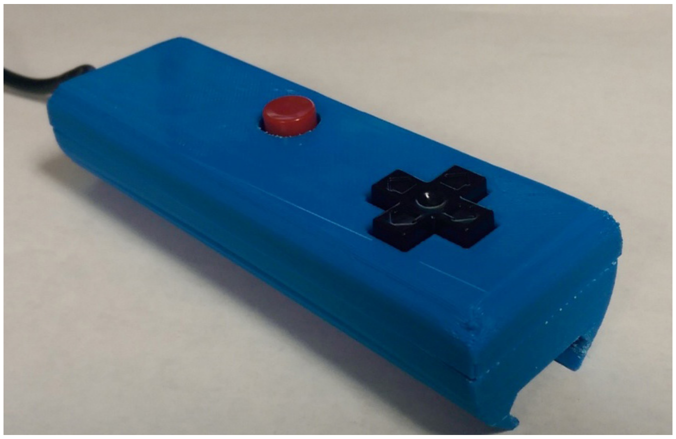


Figure 3: 3-D Printed Prototype FWS-I Remote Switch

Sensor performance models and simulations are continually improved as industry prototypes and systems are tested during field and bench tests. The refined M&S are used for sensor testing, fielding, training and operations. The Program Manager Close Combat Systems (PM CCS) Scorpion system used a verified and validated NVESD MSD physics-based model to provide munitions effectiveness and system performance estimates prior to live testing. NVESD MSD created a real time casualty assessment (RTCA) tool that intercepted a munition launch message, carried out the RTCA, and notified the human operator of whether their target had been killed or not. By using these M&S capabilities, PM CCS was able to determine weaknesses of their detection, and fusion algorithms and suggest corrections to the prime contractor before the problems were exposed in live testing. PM CCS was able to realize cost and schedule efficiencies by planning risk mitigation in advance, and eliminating the need for expensive and repetitious live field testing requiring the acquisition of expensive live targets with robotic controls.

Engineering and Manufacturing Development Phase

Entry into Engineering and Manufacturing Development phase is a significant milestone because it represents formal program initiation. The primary purpose of Systems Engineering in this phase is the reduction of system-level risk. During the Systems Engineering portion the following key activities are conducted: develop a system or an increment of capability; complete full-system integration; develop an affordable and executable manufacturing process; ensure operational supportability, with particular attention to minimizing the logistics footprint; implement human systems integration (HSI); design for producibility; ensure affordability; protect critical program information by implementing appropriate techniques such as anti-tamper; and demonstrate system integration, interoperability safety, and utility.

The second part of this phase typically contains two efforts: integrated systems design and system capability and manufacturing process demonstration. A post-critical design review (CDR) assessment by the MDA takes place to authorize entry into system capability and manufacturing process demonstration.

During the EMD phase of the Intelligent Munition System, PM Scorpion leveraged M&S to support and inform the MS C MDA. NVESD MSD Subject Matter Experts (SMEs) and M&S were used to verify system performance whenever modifications to the threat detection and engagement algorithms were made. To do so, NVESD MSD recorded meta-data from various developmental testing (DT) and operational test (OT) events involving prototype systems and live threat targets. The collected data enabled NVESD MSD to replay the live events using constructive simulation to assess the different outcomes based on changes to the algorithms.

In addition, live simulation was used to perform real-time casualty assessment (RTCA) against actual threat targets. Targets were outfitted with GPS transceivers, with their ground truth being received by the NVESD MSD simulation in real-time. The NVESD MSD simulation also operated on the tactical network to intercept live system launch messages. Once intercepted, the live launch messages caused the NVESD MSD simulated system to launch a virtual munition. The virtual munition executed its engagement algorithm against a threat based on the live ground truth received and performed the RTCA. The outcome of the RTCA was relayed to the threat vehicle wirelessly, and the operator was notified via a red strobe light in the event of a causality.

Production & Deployment Phase

The fourth phase of the life cycle is the Production & Deployment phase. It consists of two efforts; Low Rate Initial Production (LRIP) and Full Rate Production and Deployment (FRP&D), separated by a Full Rate Production Decision Review (FRPDR). It begins after a successful Milestone C review. The key activities of this phase are: Intensive testing; DT, full-up system level Live Fire Test and Evaluation (LFT&E), Initial Operational Test and Evaluation (IOT&E) and interoperability testing. The purpose of this phase is to achieve an operational capability that satisfies the mission need.

In September 2014, the current systems being supported have not reached the Production & Deployment phase, therefore no examples are available.

Operations & Support Phase

The Operations & Support phase consists of two efforts, Life-Cycle Sustainment and Disposal. The phase is not initiated by a formal milestone, but instead begins with the deployment of the first system to the field, an act that initiates the Life-Cycle Sustainment effort of this phase. The purpose of this phase is to: maintain readiness and operational capability of deployed system(s); execute operational support plans; conduct modifications and upgrades to hardware and software; and measure customer confidence. The Life-Cycle Sustainment effort overlaps the Full Rate Production and Deployment (FRP&D) effort of the Production & Deployment phase. Life Cycle Sustainment starts immediately upon fielding or deployment and seamlessly spans a system's entire life cycle, starting with the Materiel solution analysis, to disposal.

As a follow-on effort to the previous LRAS3 work performed to develop simulation models to test the system performance in a laboratory environment for specification adherence, this same simulator, and its underlying models, was then further developed for use with the NET simulation system (see Figure 4). All functionality of the physical system was incorporated into the simulation. The total savings to PM FLIR by reusing the Government models was several millions of dollars. This savings was passed on to the LRAS3 program, which allowed the program to develop two sets of mobile training environments that support both operator and maintenance training. To date, the LRAS3 NET teams have used a combination of classroom instruction, simulator training and hands-on training to train over 2000 soldiers on the LRAS3 system. In addition to the cost savings, using the simulator has increased the amount of system training time from approximately thirty minutes per soldier on the actual system to over eight hours on the simulator. As the NET is transitioning to sustained schoolhouse training, the Government Furnished Equipment (GFE) training and maintenance simulators are being transitioned to Fort Lee, VA, and to Fort Benning, GA, to be incorporated into their training programs of instruction.

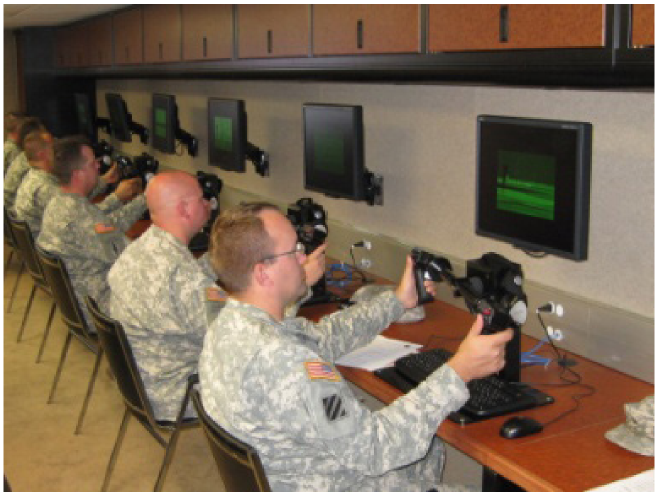
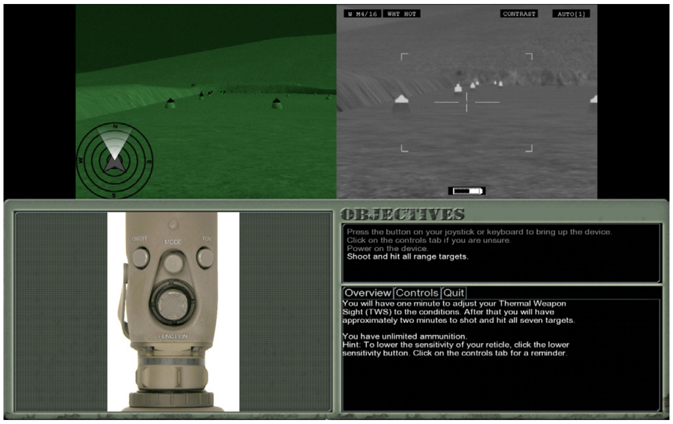


Figure 4: Long-Range Advanced Scout Surveillance System (LRAS3) Trainer



Press the button on your joystick or keyboard to bring up the device.
Click on the controls tab if you are unsure.
Power on the device.
Shoot and hit all range targets.

You will have one minute to adjust your Thermal Weapon Sight (TWS) to the conditions. After that you will have approximately two minutes to shot and hit all seven targets.

You have unlimited ammunition.
Hint: To lower the sensitivity of your reticle, click the lower sensitivity button. Click on the controls tab for a reminder.

Figure 5: PEO Soldier Sensor Trainer

Rapid Fielding Initatives

In support of Rapid Fielding Initiatives and subsequent program development of base defense sensor systems, the NVESD MSD has developed visual, acoustic and other sensor models that replicate all current sensors and those under consideration for the Base Expeditionary Targeting and Surveillance System–Combined (BETSS-C). These models were used for test development of the individual BETSS-C sensors and their integration into the system. The BETSS-C sensor models were adapted to desk-top training simulations and are used by PM Night Vision Reconnaissance Surveillance Targeting and Acquisition (PM NV RSTA) for NET to deploying units. Figure 6 shows the actual laboratory of the BETSS-C system. The models are also being used for testing of the Sensor Ground Station (SGS). The SGS is a common ground station for the BETSS-C system. In addition, the models continue to be used for testing new SGS software and BETSS-C capabilities in live field events in support of Program Executive Office Intelligence Electronic Warfare and Sensors (PEO IEW&S). The use of these NVESD MSD M&S models and tools has been critical to BETSS-C employment in Theater as the new sensor systems and SGS are unavailable for home station training. The NVESD MSD has provided M&S solutions throughout BETSS-C development and acquisition processes.

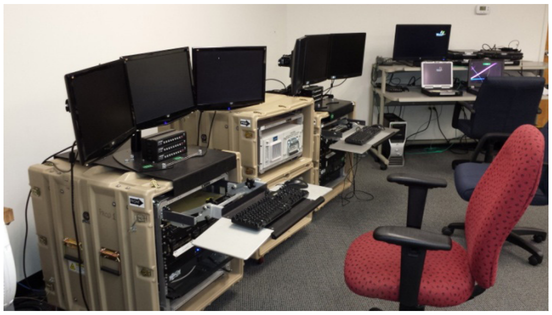


Figure 6: BETSS-C Sensors Integration Laboratory

Conclusion

This paper covers just a few of the many examples of how NVESD MSD provides critical information to the PM during the acquisition life cycle to positively affect cost, schedule and performance. The cost benefits when M&S is used at the very early stages of acquisition life cycle are compounded by reducing the cost of development, reusing models, and the ability to change system performance as the program matures. The NVESD MSD continues to provide M&S support to sensor PMs, and to other PMs using sensor technologies in their systems. The NVESD MSD offers Government-owned M&S models, algorithms, simulations and simulator solutions to improve development and realistic training for electro-optic, infrared, acoustic, magnetic, seismic, and ground penetrating radar systems.

References

Department of Defense, (2007). DOD 5000.01: *The Defense Acquisition System*. Washington, DC: Under Secretary of Defense for Acquisition Technology.

Department of Defense, (2013). DOD 5000.02: *Operation of the Defense Acquisition System*. Washington, DC: Under Secretary of Defense for Acquisition Technology.

Defense Acquisition University (n.d.). *Defense Acquisition Guidebook*. Retrieved from https://dag.dau.mil/Pages/Default.aspx

Department of Defense. (2011). *Army Acquisition Policy* (Army Regulation 70-1, pp 4, 44). Headquarters, Department of the Army, Washington, DC

Harkrider, S., May, C., Anderson, D. & Krug, A., (2014). U.S. *Army Sensors Life Cycle Acquisition With Modeling and Simulation. M&S Journal, Winter 2013-2014*, pages 15-21.

About the Authors

Ms. Susan Harkrider is the Deputy Director of the Modeling and Simulation Division (MSD) at the CERDEC Night Vision and Electronic Sensors Directorate (NVESD). She has over 20 years of experience supporting M&S, training and systems engineering efforts for the DoD. She has served on the Simulation Interoperability Standards Organization (SISO) Executive Committee and Standards Activity Committee. Ms. Harkrider is currently the chairperson of the RDECOM M&S Senior Working Group (SWG), which facilitates collaboration of M&S efforts between RDECOM laboratories in support of PEOs and PMs. She holds a BSE and MSE from the University of Central Florida.

Dr. Keith Krapels received a B.S. in math, B.A. in history, M.S. and Ph.D. degrees in electrical engineering from the Univ. of Memphis. Since 2008, he has been Director of the Modeling, Simulation & Netted Sensor Div. at the Army Night Vision Lab. He is a Captain in the Navy Reserve and was deployed to Afghanistan to the NATO Training Mission in 2012. From 2001-2008 he was the EO/IR Sensor Technology program officer in the Office of Naval Research's C4ISR Dept. In 2003, he deployed for Operation Iraqi Freedom. From 1999-2001, he was in the Sensor Performance Model Development Branch at the Army Night Vision Lab. From 1996-98 he was Special Programs Officer at the Naval Research Lab's Tactical Electronic Warfare Div. From 1990-96, he was an Electronic Counter Measures Officer in Navy EA-6Bs and flew 53 combat missions. From 1987-89, he was an EO-IR sensor analyst for Martin Marietta Orlando Aerospace, a Research Fellow at the USAF Arnold Engineering Development Center, and a Research Associate at the University of Memphis. He is a Fellow of the SPIE, the International Society of Optics and Photonics.

Mr. Andrew Krug is a certified Project Management Professional (PMP), simulations and information technology specialist with more than fifteen years of experience in managing day-to-day operations of projects and programs. Mr. Krug currently works at the US Army's NVESD MSD at Fort Belvoir, VA. His experience includes planning, integrating, and executing live-virtual-constructive (LVC) simulation experiments supporting milestone decision authorities through data analysis. He also manages sensors simulations design and testing used for research and development with a focus on IR sensors and active lasers.

Lana E. McGlynn, founder of McGlynn Consulting Group (MCG), has over 40 years of hands-on experience in technical and leadership positions. She offers comprehensive consulting in the fields of modeling and simulation (M&S), testing, logistics, acquisition, and studies and analyses. Ms McGlynn has lead various domestic and international working groups and task forces, to include serving as the Vice Chair of the NATO Modeling and Simulation Group. Prior to retirement from federal service, she served as the Special Assistant to the Deputy Under Secretary of the Army for Operations Research (DUSA (OR)) for Modeling and Simulation (M&S). She is a member of the Army Acquisition Corps and was certified as an Acquisition Professional, Level III, in the functional specialty of Program Management.

She is a graduate of Harvard's JFK School of Government Senior Executive Fellows Program April 2001, the Federal Executive Institute's Leadership for a Democratic Society Program August 1996, and the resident course at U.S. Army War College June 1993.

A Probability of 1

By Dr. Barbara Endicott-Popovsky

Note: The following information is presented for those who struggle communicating what we see and know with our senior leadership.

If you protect a luscious, valuable, amazingly tempting data object, the probability of its being stolen is 1. It's as sure as death and taxes. It's only a matter of an attacker's time and resources before its gone; these are no obstacles to determined adversaries like nation states and organized crime. So why don't our corporate leaders 'get' this certainty? Why are so many, like Target, caught off guard?

This question has bugged me ever since I attended a professional conference that featured a panel of top executives from the Fortune 500 congratulating themselves on their unbreakable perimeter defenses that 'no attacker could penetrate.' As I listened I had images of the Titanic going down and couldn't help raising my hand to ask if any had considered how to defend against other kinds of exploits that avoid firewall penetration, like Stuxnet (which I briefly explained). Why bother when compromising humans is so easy? Or as a colleague is fond of saying, 'there is no firewall for stupid!' [1]

There was stunned silence from the speaker and then a mumbled 'we probably need to explore other scenarios.' One of the panelists under his breath muttered, 'we just installed a USB port in….' and proceeded to describe a sensitive installation that would be a delightful target for the ill-intended.

How did we get here? How are so many aspects of society so blind when the consequences or cyber theft and compromise are so stark?

Lagging behind in the Information Age

I think you can agree that we all struggle to stay current with technology and often don't grasp the unintended consequences of the shiny new innovations that we embrace. We're transitioning to the Information Age, watching the Industrial Age fade in the rear view mirror. According to Covey [2, 3], this transforms our way of living in profound ways--how we advance in the world, how we work, our sense of time, how we problem solve, how we learn.

To gain appreciation for the enormity of what we've done to ourselves with our embrasure of technology, I've been reflecting on the table below, imagining myself in each age, visualizing my life in every detail. I marvel at the unintended consequences I've discovered as a result, and I work in this field!

I'm not suggesting we become luddites and live by candlelight; I am suggesting that we consider where we've come from and where we're now living. Morris Massey's training seminar called '*What You Are Is Where You Were When*' makes the case that our values are fixed in the paradigm existing when we turned age 10 [4]. From then on, we interpret what we see and weigh our decisions through that lens. Where were you at 10?

I invite you to take quiet time and contemplate this question. While you may be among the enlightened, technically, way ahead of most in 'getting' technology, ask yourself how likely is it that those who are leading us politically and economically really do understand the impacts of the transformation we are still in the

Table 1. Transformative Paradigms Source: Adapted from [2]

Attribute	Agricultural Age	Industrial Age	Information Age
Wealth	Land	Capital	Knowledge
Advancement	Conquest	Invention	Paradigm Shifts
Time	Sun/Seasons	Factory Whistle	Time Zones
Workplace	Farm	Capital equipment	Networks
Organization Structure	Family	Corporation	Collaborations
Tools	Plow	Machines	Networked Computers
Problem-solving	Self	Delegation	Integration
Knowledge	Generalized	Specialized	Interdisciplinary
Learning	Self-taught	Classroom	Online

middle of accomplishing. An exercise such as this might help you gain insight into why cybersecurity is something those at the top rarely grasp. Most likely, when they were 10, they were in the heart of the Industrial Age developing their world view from that paradigm. Is it any surprise they need extra help in thinking through cyber risk?

Surrounded by Oceans and 'Soft' Countries

At the heart of this transformation is our symbiotic relationship with the Internet. Table 2, brings home its pervasiveness; and we're only at the beginning! With only 25% of the world's population surfing the Net today, think how our lives will change as saturation increases and we move increasingly online. Further, consider the continued effects of the clash of cultures as radically different countries become side-by-side neighbors online.

In this country we have had the luxury of two oceans on either side, left and right, with two 'soft' countries above and below us that are basically cooperative and 'like us.' This can inure us to what we have done by becoming virtual next door neighbors with all of our friends online in the Table below. I'm fond of telling my students that my mother named six kids that I was absolutely to avoid like the plague when I was growing up. I still remember the name of the boy at the top of the list. These were perennial troublemakers in the neighborhood; if you hung around them, you were assured of no-good. (I can attest to it, having smashed a church window, by accident, playing softball with a couple of them!)

Now we are side-by-side with cultures and countries radically different from our own, with very different world views about IP (Intellectual Property), freedom, ethics, etc. (Read The Lure [5].) Why do we expect them to behave like us? Why should they?

Table 2: World Internet Usage (Source: Internet World Stats: http://www.internetworldstats.com/stats.htm) [3]

World Regions	Population (2012 Est.)	Internet Users Dec. 31, 2000	Internet Users Latest Data	Penetration (% Population)	Growth 2000-2012	Users % of Table
Africa	1,073,380,925	4,514,400	167,335,676	15.6 %	3,606.7%	7.0 %
Asia	3,922,066,987	114,304,000	1,076,681,059	27.5 %	841.9 %	44.8%
Europe	820,918,446	105,096,093	518,512,109	63.2 %	393.4 %	21.5%
Middle East	223,608,203	3,284,800	90,000,455	40.2 %	2,639.9%	3.7 %
North America	348,280,154	108,096,800	273,785,413	78.6 %	153.3 %	11.4%
Latin America/ Caribbean	593,688,638	18,068,919	254,915,745	42.9 %	1,310.8%	10.6%
Oceania / Australia	35,903,569	7,620,480	24,287,919	67.6 %	218.7 %	1.0 %
WORLD TOTAL	7,017,846,922	360,985,492	**2,405,518,376**	34.3%	566.4 %	100.0%

As we smash Industrial Age infrastructure, replacing it with Information Age interconnectedness, unintended consequences will continue to unfold: online fraud, illegal downloads, continuing threats to security and privacy, wrongful prosecution for misunderstood Internet crimes, and on and on [4,5,6,7]. Like Mickey Mouse, as the Sorceror's Apprentice in Fantasia, we have assumed the wizard's powers without anticipating the risks [8]!

What was meant for good has ushered in unexpected troubling dislocations.

References

[1] Hamilton, M., CISO of the City of Seattle. (2013). Guest Lecture INFX571 Seminar on Information Assurance, University of Washington.

[2] Covey, S. (1989) *7 Habits of Highly Successful People*. New York: Free Press.

[3] Covey, S. (2005) *The 8th Habit: From Effectiveness to Greatness*. New York: Free Press.

[4] Massey, M. 'What You Are Is Where You Were When' Retrieved March 13, 2015 http://morrismassey.com/

[5] Schroeder, S. (2012). The Lure. Boston, MA: Course Technology.

About the Author

Barbara Endicott-Popovsky, Ph.D. CRISC (University of Washington), Executive Director Center for Information Assurance and Cybersecurity; Professor UW Institute of Technology Tacoma; Academic Director Masters in Infrastructure Planning and Management in Urban Planning; Fellow Aberyswyth University, Wales; Fellow of the American Academy of Forensic Scientists. Her 20-year career in industry encompassed executive and consulting positions in IT architecture and project management. Her research interests include enterprise-wide information systems security, forensic-readiness, secure coding practices. She earned her Ph.D. in Computer Science/Computer Security (University of Idaho, 2007); MS in Information Systems Engineering (Seattle Pacific University, 1987); MBA (University of Washington, 1985); BA (University of Pittsburgh).

How Does an Analyst Select M&S to Support the Entire DoD Acquisition Lifecycle Process?

Examine ARL's Executable Architecture Systems Engineering (EASE) Research Effort

By Christopher McGroarty, Christopher J. Metevier, Scott Gallant, Lana McGlynn, Joseph S. McDonnell, PhD

Modeling and Simulation (M&S) users who require complex M&S typically do not have a long lifecycle for an experiment, analysis initiative or simulation-based event. To reduce cost, they need to use well-established simulation architectures and robust models that are easy to integrate with other simulations. This desire for a short lead time for system design, development, integration, execution and data analysis forces the system definition and design to happen very quickly.

In addition to having limited time and financial resources, analysts are being forced to address ever increasingly multifaceted problems. These problems require resources far beyond the simple spreadsheets of the past. With the advent of multicore desktop computers, cloud architectures and data mining tools, analysts have the opportunity to leverage vast amounts of data in order to conduct their analyses. But manipulating output data is not the same as analyzing data. Truly analyzing data requires understanding the linkages among the input data, the design assumptions and the intricacies of the systems producing the data.

The United States (US) Army Research Laboratory (ARL) has developed tools and processes that will help M&S users with their goals of understanding the simulation capabilities that are available and executing complex M&S environments as needed rather than when technical staff is available. A description of the users' needs will provide the context of our efforts.

Needs of the User

The majority of analysts will agree that there never seems to be enough time when preparing for an experiment, test, analysis initiative or simulation-based event. A long planning cycle is a luxury they are not afforded. The analysts desire the ability to obtain key information in an effortless manner and to be able to employ tools that do not require a steep learning curve. Ultimately, the analysts want to spend more time examining the findings and less time learning to utilize the simulation tools.

There is seldom a single simulation that will accomplish the analysts' goals on its own; rather engineers will integrate multiple systems together. Each system represents specific aspects of the synthetic environment being used. These M&S users rely on standards and simulation developers to get the systems to communicate using the same syntax. This often works to instantiate a System of Systems (SoS) architecture [1] and to get models to share information. A SoS environment is an assembly of applications that together provide more capability than the sum of their individual capabilities. Within the M&S community, the applications assembled are each focused on representing a specific warfare function (or functions) based on data and models from an organization considered to be the center of excellence for that aspect of warfare. The SoS architecture provides many benefits when compared to executing a single monolithic model, including performance, model management and information transparency for analysis.

The United States Department of Defense (DoD) acquisition community is focused on creating viable materiel solutions. Figure 1 shows the DoD Acquisition Life Cycle [2]. While a formal Materiel Solutions Analysis occurs prior to Milestone A, a Project Manager (PM) can be faced with the challenge that the materiel solution they are developing is not meeting its required specification(s). However, this materiel may arguably be better than what is fielded for the same purpose. The challenge becomes how to make that case to senior acquisition decision makers who determine if a system is acquired or not.

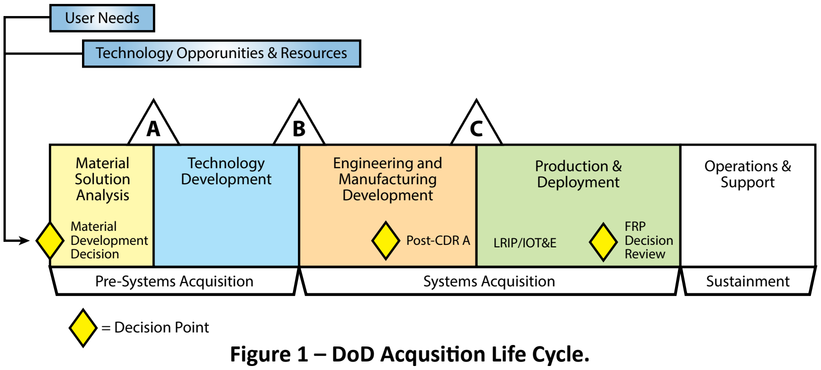


Figure 1 – DoD Acqusition Life Cycle.

The Technical Barriers to Robuse Use of Simulation

There are many obstacles for using M&S within the US DoD. This paper focuses on the technical barriers rather than the issues that relate to bureaucracy, financial resources or any other non-technical considerations. Those issues are very important and should not be overlooked, but our project, Executable Architecture Systems Engineering (EASE), is focused on technology solutions for bringing together distributed M&S for the appropriate purposes (hopefully despite many possible non-technical considerations).

The sheer breadth and depth of warfare to be represented adequately is massive. Understanding exactly what parts of warfare need to be represented is based on a detailed breakdown of the Measures of Performance (MoPs) and Measures of Effectiveness (MoEs) [3] for an event's goals. Once the modeling requirements are known though, it is impossible to know what exactly exists throughout US DoD in order to help. There have been efforts to catalogue the existing M&S assets but the information gathered is almost always limited to textual descriptions. Much work remains to be accomplished in order to understand whether the application fits the needs per fidelity, resolution and interoperability, along with many other factors.

A major problem with using multiple systems together is the interoperability among those systems. Interoperability among distributed M&S is complex, tedious and often difficult to evaluate. Integrating models that were developed for various purposes with disparate technologies and managed by independent organizations is often the goal. The effort required to meet this goal is frequently underestimated due to misunderstood commonalities between those applications. Common compliance with middleware architectures, modeling goals and object models gives a false impression of complete interoperability. There are numerous considerations when developing a distributed simulation environment. The event's objectives drive the necessary simulation functions but how those simulation functions interact needs to be meticulously designed for true interoperability. The semantics of the information transmitted, the behavior necessary across multiple applications and fidelity and resolution synchronization are only a subset of the systems engineering necessary for a coherent SoS.

Once the appropriate M&S applications have been procured, configured and integrated, there is a significant workforce requirement to learn how to use, setup, manage and execute the M&S applications for both the current event as well as future events. Reuse of M&S environments can provide cost avoidance, but retaining organizational knowledge is difficult with workforce turnover, particularly in this era of smaller budgets and shorter execution time periods. Once a M&S event concludes, we have often seen computers repurposed, configurations and software modifications completely lost and engineers moved on to other projects. It becomes impossible to build on the previous event with small changes so the organization must start almost from the beginning spending nearly the same resources as spent originally.

Towards this end, we have established a data-driven systems engineering infrastructure which allows SoS design encapsulation and connected an interview subsystem which allows a user to launch a distributed M&S execution based on functional and scenario choices. We have implemented generative programming techniques [4], which automatically generate executable computer programming artifacts from a higher level source, in order to quickly deploy a SoS architecture for military analysis. The flexibility required to implement our goal requires systems architecture qualities and objectives. This includes encapsulation of functionality into appropriately sized portions to be able to manipulate and construct larger capabilities, as needed, with as little engineering effort as possible. We aim towards an architecture that is fully compliant with US Army Verification and Validation guidance [5], and robust enough for decision-oriented analysis, while maintaining flexibility and quickness in order to save the DoD tremendous amounts of time and effort when constructing distributed M&S environments for various uses.

What Was: Modeling Architecture for Technology, Research, and Experimentation (MATREX)

To understand the impetus for solutions provided by the EASE research, it is important to understand where we have been. The Modeling Architecture for Technology, Research and EXperimentation (MATREX) program [6] had the mission to research and develop an M&S environment that included a collection of multi-fidelity models, simulations and tools which were integrated into an established architecture to conduct analyses, experimentation and technology trade-offs. The MATREX program was made up of many US Army Research, Development and Engineering Command (RDECOM) labs, centers and activities providing simulation solutions into the overall system architecture. A number of different customers used the simulation environment for varying purposes. Any particular instantiation of the MATREX system could be dramatically different than the next based on the user requirements and the subsequent model selections and system design choices made to satisfy the functional requirements. However, the flexibility of the system created a complex system design problem by allowing many different possible configurations.

The numerous and often generic potential uses of the system offered a difficult systems engineering challenge to link system requirements to detailed system design and technical dependencies. The MATREX Environment needed to retain the flexibility of the technical solution set while providing a rigorous and thorough systems engineering product set that could be used to design a system instantiation, provide technical design contracts and link low level data elements to high level user functional requirements. This need drove the initial creation of the System Design Description (SDD) [7], which is a data-driven systems engineering tool that linked operational and technical requirements to design decisions, allowing engineers to collaborate on system integration and provide traceability to event objectives. This tool was extended within the EASE project to support research goals as described in the next section.

Other tools developed within the MATREX project included tools to support rapid software development including a software library (ProtoCore) that abstracted away middleware details and allowed applications to run across different middleware protocols. It also included an over-the-wire testing tool (Advanced Testing Capability (ATC)) that provided stimulus and validated applications based on sequence diagrams that were imported from the systems engineering tool. These tools will be further explained in the upcoming Components section when extensions to support EASE research goals are described.

These tools enabled a more accurate and quicker process for developing and integrating M&S applications, applying systems engineering throughout development and testing. While useful, these tools still expected an M&S expert to employ them, leaving that expertise specialized and perishable. The next logical step was to build on that with automation by capturing additional details about the M&S environment, including how to install, configure, launch and capture data from those same applications. We could then orchestrate the execution of the M&S environment based on the same systems engineering data already used to ensure the correct warfare representation while accomplishing true interoperability. This next step is the EASE project.

What Is: Executable Architecture Systems Engineering

Background

The goal of EASE is to lower the barrier of entry to the use of M&S. EASE provides a single interface for systems engineers, software developers, information technology professionals and analysts to work together. These individuals define the simulation systems engineering data and execute the appropriate applications in order to support the M&S user's goals. EASE provides an interface to M&S users to select the capabilities they require and the scenario necessary to stimulate the appropriate warfare circumstances. The selection criteria are used to filter and display the most appropriate executions for the user to choose from. The user can then adjust configuration elements that have been exposed by the developers, select the number of runs they need to execute, schedule runs and hit the "Go" button to execute. The web-based interface provides a mechanism to launch potentially complex M&S in the cloud or on specific computing hardware. The systems engineers, developers and integrators can centrally manage all aspects of EASE and the execution of the proper M&S systems to achieve the M&S users' requirements. Having a data-driven and easy to use interface keeps the systems engineering technical information (i.e. interface specifications) current. In turn, each user can be assured that they're referencing and updating the latest information.

Needs Derivation

Simply learning which M&S and analytical tools exist within the DoD is challenging enough let alone actually obtaining them for use. Once users receive these systems, they still need to be trained and/or read lengthy and complicated user manuals on how to configure the systems and which execution options to use for a desired effect. This process is painful, time consuming and costly; so much so that users will opt for a simpler, but less effective solution. In order to ensure that the best tools DoD has to offer are used there is a need to quickly and easily find execution options for specific M&S needs.

After users become educated in the systems they use, that knowledge is generally not documented and remains only in their head. The complexity and nuances of running highly technical systems is if often too difficult or too time consuming for them to share the information with their peers. Each system is also delivered with its own types of documentation and few seem to follow existing standards when creating this documentation. There needs to be a method for capturing systems technical information in a common format for Systems Engineers (SEs). This method should connect functions across systems, understand the warfare capabilities of each element within the system and link the M&S solutions to experiment goals without adding more cost when compared to activities already being conducted to execute the experiment. In order to maximize the user's derived knowledge and time expended, there is a need to link systems engineering information with execution details.

Currently, the warfare functions of each M&S system are described through brochures, slides or user manuals in human readable text. This is only a precursor to what engineers and analysts need. Specifically, there needs to be more detailed information available and captured within a common systems engineering tool. Items, such as object model elements, middleware types, versions and execution options, need to be linked and the consequences of choosing each option understood as it relates to the warfare functions represented. For example, configuring a system to have the right resolution for the function under analysis is a configuration option and needs to be linked to the correct function. This requirement leads to the need to determine necessary technical systems, object models and middleware based on warfare functions required.

Knowing that two simulations represent warfare functions that seemingly compliment a larger analytical goal (e.g. a weather simulation and a chemical agent dispersion simulation to model a chemical release) does not necessarily imply that they will work together semantically. Even if two systems work on the same middleware and use the same object model, they still might not be interoperable when it comes to which data elements within the object model each system sends or receives. These important distinctions lead to the need to capture technical interface details to facilitate identification of integration gaps and understanding the data provided for analysis.

The semantics or reasons for systems communicating are also very important in order to determine that the two systems are indeed sharing the appropriate data. The M&S user needs the capability to easily capture these technical details and have better visibility to discover gaps for interoperability and how systems can be integrated. Providing a tool that assists users in integrating systems with true interoperability is the objective.

Software development schedules are often delayed. In turn, when multiple applications are designed to share data the development teams become reliant on others' schedules. This has major impacts to overall schedule and cost. Having the ability to quickly generate a surrogate application to replicate the functionality of a missing system allows the other systems to integrate into the distributed system and test their interfaces, timing and so on. This provides cost avoidance in those cases when a simulation system is unable to integrate. This leads to a requirement to create surrogates when key systems are delayed.

The simulation community needs a rapid application development mechanism to quickly generate the software for connecting distributed simulations. This technology can be generic enough to be applicable across any model use case. Having the ability to generate source code will greatly reduce the software development cost of developing new models and integrating existing models into distributed environments. The generated code includes the ability to connect to the appropriate middleware, send and receive the right messages and even has software constructs that will simplify a modeler's learning curve into distributed simulation environments. This leads to the need to quickly, easily and more cost effectively modify a model to work within a distributed simulation environment.

Managing computers in a laboratory can be time consuming, redundant and tedious. Executing simulation systems across a laboratory can add to that burden. Launching a large distributed simulation environment can often take over an hour wherein the users have to manually script how the systems will be launched or even worse, walk around the lab and launch each system on each computing device manually. A system to manage the computers and launch applications according to the correct execution details and order is required.

This leads to the need to launch complex computing assets easily from a single point.

In laboratories that execute many simulation environments, each one can be slightly different from the previous one. Managing how each system needs to be modified for changing scenarios or even technical constraints like middleware or object model differences requires engineers to spend much of their time configuring and testing systems. This leads to the need to orchestrate the order and cooperation of systems as appropriate to the scenario and technical interoperability details.

Hardware requirements change depending on the applications, the scenarios they need to represent and the exercise architecture, among other things. Having to procure additional hardware can be expensive and unnecessary. Moreover, each computer in the lab has a finite useful life. Once the systems and scenarios grow, the hardware becomes unable to support the execution without upgrades. Having a cloud-based system to dynamically add and allocate processors, memory and network bandwidth will help alleviate the lab management of limited life time hardware. This leads to the need to flexibly allocate computing resources (memory and processors) to simulation systems based on scenarios, configurations and application-specific details.

Software integration with middleware specifications, such as the High Level Architecture (HLA) [8], can be complicated and error prone. Once integrated and tested, other software developers can reuse the software library for their own use. Making the software library generic to work across any object model and adding plug-ins to work across multiple middleware specifications allows this library to be reused across a wide spectrum of simulation systems. It additionally facilitates interoperating simulations which were not originally planned to work with other simulations. This leads to the need to abstract away technical middleware details from business logic to facilitate reuse and remove errors.

Requirements written in human readable text and provided to software developers can often be misinterpreted, especially if those requirements do not include enough detail or the semantics of the requirement. When system developers arrive to integrate their system for an analysis, any misinterpretation of the requirements will be discovered through trial and error. Another problem that occurs frequently is that system developers write their own simulation test procedures so any errors that they have in their minds will also be in their tests. These problems include erroneous encoding and decoding of simulation communication messages and middleware specification errors. Instead of discovering problems at the exercise site while personnel are on travel and using funds for hotel, per diem and other expenses, it would be useful if tests could be generated for the developers that properly test everything possible prior to developers traveling to the exercise site. These generated tests should test an application's middleware connection as well as the object model elements it needs to receive and send. This leads to the requirement to test systems prior to integration events based on an agreed upon system design.

The design of an analysis changes frequently as analytical goals are modified as well as between analyses that may leverage elements of the same simulations. Having to manually update test cases for simulations involved will lead to configuration management problems and be a time and cost driver. Being able to automatically update test cases based on a systems engineering tool that captures the methods and means of the analysis will save time and reduce errors. This creates a requirement to quickly update tests from design via automation and a data-driven export mechanism.

Components

EASE consists of the following components and associated software:

- Interview Component
- System Design Document
- Surrogate Generation Capability
- Deployment Management System
- ProtoCore
- Advanced Testing Capability

The Interview component of EASE is the interface for the M&S users, systems engineers, integrators and software developers to access and manage their respective areas of complex simulation. The user has the ability to search the system for scenarios that are applicable to their specific needs, configure those scenarios and execute the simulation environment on dedicated hardware assets by simply clicking on a button within the web browser. They can later return to the Interview interface to access the data artifacts that resulted from the scenario they previously executed. Systems Engineers enter into the framework what applications can perform what functionality, which then informs how scenarios can be created. Integrators create adjustable configuration fields for M&S users to configure complex simulation applications through an easy interface. This allows constraints to be put on the models, simulations and tools that ensure that the systems do not operate outside of their limits. Following the rules laid out by the systems engineers, the developers can upload, configure and approve their software for future execution within EASE.

The SDD is a systems engineering tool used by the systems engineer to capture the design details of a distributed computing environment. The SDD links high level requirements to subsystem specific details through Modeling Design Decisions that describe how the simulations will communicate, including sequence diagrams and architectural strategies. The SDD is a database driven tool which stores all of its information in the form of database fields with links across the database tables. This database driven approach allows the system to quickly generate systems engineering artifacts with database queries and templates for their output and subsequent use by the systems engineer. If a change is made to any of the systems engineering data, this artifact generation can be repeated automatically by the systems engineer. This ensures that systems engineering artifacts remain current with little effort, compared to most projects that need systems engineers to constantly update and configuration manage Microsoft Word, Excel or PowerPoint documents to ensure currency and consistency.

The Surrogate Generation Capability uses the SDD's ability to generate artifacts based on the SDD database. An SE can enter simulation business logic into the SDD and export a working software application that will execute within a distributed simulation environment based on the appropriate middleware and object model. This capability eliminates the need for the SEs generating a surrogate to: understand the simulation middleware details; know how to write interface details that are often repeated; or, know how to write a multi-threaded software application optimized for distributed simulation. The Surrogate Generation Capability includes an interface that is already filled in by the SDD based on which warfare function is to be surrogated. The correct events have already been included, with fields available for the user to manipulate and/or add their own simulation business logic. Once completed, the systems engineer can save their work back into the SDD, export the software application to their local desktop for further development or use and can have the surrogate they created automatically deployed to EASE for use by users in future executions.

The Deployment Management System component of EASE is responsible for the automated orchestration of simulation executions using dedicated hardware assets. In any distributed simulation environment, there is a specific order and configuration of the components for them to execute properly. This is often known only by a handful of integrators on each project. The Deployment Management System component captures this knowledge and automates it so that anyone can execute complex simulation environments. As a part of that orchestration, applications must be configured for the middleware, the application's performance data and for the specific scenario to implement, among other areas. Each component is executed in an emulated computing environment, known as a virtual machine, and via a virtual machine management interface. This allows EASE to dynamically partition processors and memory to each virtual machine, as appropriate, rather than be tied to the limitations of an existing piece of hardware with its associated operating system. Instead, each application gets the operating system and hardware required to properly execute. Those virtual machine executions can also be scheduled, repeated, started, stopped and monitored by the Deployment Management System component. A video stream is provided to the user to monitor each virtual machine while it runs, which is key to supporting Human-In-The-Loop (H-I-T-L) simulations [9]. After a simulation run has been completed, the data artifacts are gathered and exposed to the Interview component for the users to get data for their analysis. This implementation allows for easy scaling and management of hardware, software and their connection to requirements and goals of the simulation execution.

ProtoCore [10] is a software library developed to allow software developers to create simulations capable of communicating with other simulations in a distributed architecture without having to be experts on distributed simulation. Most distributed simulation middleware architectures have very similar concepts such as joining, subscribing, publishing and exiting. Distributed simulation environments also have some common simulation business logic, such as dead reckoning, time representation and coordinate conversions. These types of common concepts and utilities are included within ProtoCore so software developers do not have to write their own implementations. This saves developers time and it also helps ensure accurate implementation since the logic has been peer reviewed and used across many different simulations. An additional benefit of ProtoCore is its ability to provide these capabilities across a variety of middleware architectures due to its plug-in architecture. Plug-ins exist for HLA 1.3, HLA 1516, Distributed Interactive Simulation (DIS) [11] and Test and Training Enabling Architecture (TENA) [12] so a software developer using ProtoCore can write their code once and choose which middleware that it will use at run-time.

This allows software developers that support multiple projects on different middleware architecture to write their software once and allow it to work across several environments.

The Advanced Testing Capability [13] is a software tool that is used to test distributed simulation applications under controlled conditions without needing every simulation involved in a scenario. First, ATC is started along with any necessary middleware architecture components. Then, the simulation under test is started and connects to the middleware and ATC. ATC provides the stimuli to the application that is required for the scenario being tested and verifies the application's responses as sent over the middleware. This type of testing ensures that the application can properly join the middleware, transmit the data based on the middleware architecture's guidelines and publish and subscribe to the correct events. The ATC tests are presented as sequence diagrams where a tester can edit details, such as the events' attributes and the timing of each event. The ATC stores the test cases into an eXtensible Markup Language (XML) file called the Test Case Markup Language (TCML). The TCML file storage allows other tools to read, manage and export test cases. Additionally, the SDD can export TCML files based on system design information captured within its database.

Use Case

Beginning with a hypothetical problem, assume an acoustic sensor has a requirement to detect and discriminate targets, such as manned and unmanned ground vehicles, in urban environments with a specified false alarm rate [14]. During developmental testing, this acoustic sensor appears susceptible to background noise that could appear in some urban environments and, in turn, is not able to detect and discriminate targets in these environments with the required false alarm rate. It is, however, able to discriminate all required targets in non-urban environments, as well as a subset of urban environments that may be relevant to future operations, within the required false alarm rate. The current fielded acoustic sensor is significantly less reliable in the urban environments of interest. The PM wishes to make the argument that this new system should pass Milestone B due to the gains it provides to the force.

The analyst creates an experimental design that compares the current acoustic sensor to the one under development including operational scenarios in relevant urban environments. While he would like to use available empirical data, he is also interested in using physics-based models that replicate the acoustical phenomenology at hand and show how the sensors will perform as background noise is varied. The analyst logs in to EASE and sees that he already has models for the current system from when it was developed and fielded. Moreover, he has models of the system being developed from Pre-Milestone A. Using EASE, he modifies the scenario he had from Pre-Milestone A to reflect the operations in Milestone B and adds both sensors for comparison. He then modifies parameters within the simulations reflecting the background noise as input. Finally, he schedules multiple replications due to the stochastic nature of the physics-based models being used and hits the "Go" button. EASE then runs the simulations using available resources and provides the analyst with data when complete. Conveniently for this analyst, he was able to load his simulation post processors which modify the data for use as information after the runs are complete into the EASE system further automating the process. Through this analysis, he is able to show a comparison of the developmental system to the current system and operationally make the argument that there is utility to the developmental system. It is then up to the decision makers whether the operational utility outweighs the cost and sustainment footprint for a new system that is not meeting all requirements.

It should be stressed that there is no magic in this hypothetical situation. In our example, M&S professionals developed models that represented the acoustic sensors in question and systems engineers took the time to integrate them into EASE. Moreover, the analyst knew how he wanted to present the data and built post processors to facilitate the process. The key here was that as these models were developed, they were put into the EASE framework. In doing so, the constraints and capabilities were known as well as how to execute them. This allowed our analyst to take advantage of work done previously, possibly on an analysis of another weapon system for another PM, without having to call on the M&S experts or become an M&S expert himself. EASE also allowed the analyst to easily modify parameters, schedule runs and receive data. If the data looked incorrect, for whatever reason, the analyst could easily change the inputs and run again. Normally, this process is done by hand and is error prone, but the rigor of EASE ensures that this is not an issue. Should there be the need for a new model, the experts would then be called upon. Furthermore, should the question change from a comparison of acoustic sensors in environments for which the PM understood to a more SoS-like situation where the acoustic sensors had to interface with other operational systems, additional models may need to be entered into EASE. If these models were entered into EASE and a SoS question arose, various PMs would have the ability to leverage models from other PMs (presumably with some level of accreditation) to answer analytical questions that do not have just one PM. EASE provides that ease of use access to the M&S while facilitating re-use.

Mapping of Needs to Components

Table 1 – Mapping of Needs to Components of EASE.

Need	EASE Component
Quickly and easily find execution options for specific M&S needs	Interview
Link systems engineering information with execution details	Interview
Determine necessary technical systems, object models and middleware based on warfare functions required	Interview
Capture technical interface details to facilitate identification of integration gaps and understanding the data provided for analysis	SDD
Integrate systems with true interoperability	SDD
Create surrogates when key systems are delayed	Surrogate Generation Capability
Launch complex computing assets easily from a single point	Deployment Management System
Orchestrate the order and cooperation of systems as appropriate to the scenario and technical interoperability details	Deployment Management System
Flexibly allocate computing resources (memory and processors) to simulation systems based on scenarios, configurations and application-specific details	Deployment Management System
Quickly, easily and more cost effectively modify a model to work within a distributed simulation environment	ProtoCore
Abstract away technical middleware details from business logic to facilitate reuse and remove errors	ProtoCore
Test systems prior to integration events based on an agreed upon system design	ATC
Quickly update tests from design via automation and a data-driven export mechanism	ATC

What Should Be: Common Model Framework

While the M&S community works hard to produce solutions that support the needs of the analytical community, modelers and simulation developers often fall into the trap of focusing on their particular domain. They may or may not attempt to leverage existing representations of phenomena because they are so focused on what they need to model or simulate for the analyst. Reuse is always a hot topic, as is composability, but there are barriers to these two ideals that have kept them from becoming a reality.

The idea of a framework that brings models together as needed is not novel. Some might argue that various simulations have been defacto frameworks to that end. For example, we continue to develop specialized terrain to support the needs of simulations and recreate physical representations that support kinetic warfare. We do this because "our" particular simulation was not built to use "your" model, due to issues such as fidelity, format or data. Software programming, in general, relies on libraries that become canonical representations of their functions. These libraries can also be changed as necessary. Why aren't we using this approach for simulation development?

Imagine a paradigm where an analyst is able to pull together models that represented phenomena necessary to replicate the problem space being explored. These models would be produced by experts in those particular fields. This indeed would require some level of regulation and a serious Verification, Validation & Accreditation discussion, but we save that topic for a future paper. From the point of view of the analyst, if he is trying to have a fair comparison of two systems in a relevant operating environment, having a common source for models would be key. Furthermore, having the ability to pull together those same models for the next analysis, or being able to run updated models using the parameters of the original analysis and then performing a new analysis, would provide great analytic rigor. A potential solution might be a repository that literally houses these models and allows another analyst to leverage what was previously done, instead of the current perishable description of a model or simulation.

The paradigm of distributed simulation in general arguably provides a level of reuse models and simulations; however, as discussed, taking a black box approach to simulation interactions leads to interoperability issues and does not support reuse of fundamental models. Part of the challenge lies in defining the primitives of what those fundamental models would be. There is additionally still a challenge in the breadth of uses of M&S to support acquisition. The types of models for a system-level analysis normally differ from the models used for a force-on-force analysis, but is that required? We need to derive environment representations from a canonical source without having data translation errors that plague terrain generation, simulation gateways, etc. This is an area for serious research and demonstration to prove where the state-of-the-art really is.

Furthermore, models and simulations are worth little without the data that drive them. There are numerous activities in the US and North Atlantic Treaty Organization (NATO) discussing data generation, collection and storage. What remains to be seen is how the M&S space can effectively tie in to these efforts, especially in context of taking advantage of the data as it emerges from the battlespace. Would a common framework for models better support this linkage and in turn, better support the lifecycle? Furthermore, while we have discussed the need for representing kinetics of warfare, research is needed to better support scenario development. The lack of standardization in scenario generation across simulation environments does not allow us to easily sketch out a mission for execution. Would a common model framework further improve this problem?

It is our belief that advancements in technology are beginning to solve the problems in computational power, data storage and distributed access to models and simulations. What remains is a concerted effort to define what capabilities an analyst would actually desire to do his job independent of the current methods and means used to produce and use M&S. Arguably, better defining how M&S could best support the acquisition lifecycle will allow us to move forward rather than continue a slow evolution.

Conclusions

While there remain challenges to enabling analysts to select M&S throughout the entire DoD Acquisition Lifecycle Process, by examining where we have been and where we are now we can make recommendations for where we should be. The challenges that we have identified with current methods will continue to be challenges as long as M&S is designed, developed and employed in the same way it has been. The EASE research project attempted to implement solutions to many of the challenges that we identified through our experience with the MATREX program and has found success in many. Unfortunately, while EASE can provide many benefits, it cannot fully enable true composability and reuse as long as M&S continues to be developed with disparate timelines and purposes. If the analysts define their ideal system, the Science and Technology community can demonstrate what technologies can achieve this vision driving towards a more useful paradigm in the future.

8.0 References

[1] M. Jamshidi. 2008. System of Systems Engineering. 1st ed. Wiley.

[2] Defense Acquisition University (DAU) ACQuipedia, 22 January 2008, “Acquisition Life Cycle” available via https://dap.dau.mil/acquipedia/Pages/ArticleDetails.aspx?aid=30c99fbf-d95f-4452-966c-500176b42688

[3] Roedler, Garry and Jones, Cheryl. Technical Measurement. A Collaborative Project of PSM, INCOSE, and Industry. 2005 INCOSE-TP-2003-020-01. (https://www.incose.org/ProductsPubs/pdf/TechMeasurementGuide_2005-1227.pdf)

[4] Czarnecki, K, 2000, “Generative Programming: Methods, Tools, and Applications”, Addison-Wesley Professional.

[5] Headquarters Department of the US Army, Army Regulation 5-11. Management of Army Modeling and Simulation. 2014. (http://www.apd.army.mil/pdffiles/r5_11.pdf)

[6] Metevier, Chris et al. Modeling Architecture for Technology Research and Experimentation (MATREX): M&S Tools and Resources Enabling Critical Analyses. 2009 Modeling and Simulation Information Analysis Center (MSIAC) Journal Summer 2009. (https://www.matrex.rdecom.army.mil/front/msiac_journal_july_2009.pdf)

[7] Beauchat, Tracey et al. A Collaborative Tool for Capturing the Design of a Distributed Simulation Architecture for Composable Execution. 2012. Fall Simulation Interoperability Workshop – Spring Conference.

[8] 1516-2010 IEEE Standard for Modeling and Simulation (M&S) High Level Architecture (HLA) – Framework and Rules. 2010. (http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?arnumber=5553440)

[9] Rothrock, Ling and Narayanan, S. Human-in-the-Loop Simulations: Methods and Practice. 2011. Springer.

[10] Keith Snively, Phil Grimm “ProtoCore: A Transport Independent Solution for Simulation Interoperability.” SISO Fall SIW 2006.

[11] 1278.1-2012 IEEE Standard for Distributed Interactive Simulation – Application Protocols. 2012. (http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=6387564)

[12] Powell, Edward and Noseworthy, Russell. The Test and Training Enabling Architecture (TENA). 2012. (https://www.tena-sda.org/download/attachments/6750/TENA-2012-Paper-Final.pdf)

[13] McCray, Paul and Snively, Keith. Functional Component Testing for Distributed Simulations. 2008. Simulation Interoperability Workshop Spring Conference, April 2008.

[14] Kaushik, B; Nance, Don; Ahuja, J, 23-25 May 2005, “A Review of the Role of Acoustic Sensors in the Modern Battlefield”, Proceedings of the 11th AIAA/CEAS Aeroacoustics Conference (26th AIAA Aeroacoustics Conference).

About the Authors

Christopher McGroarty (formerly Gaughan) is the Chief Engineer for Advanced Simulation and Deputy Technology Program Manager of the Modeling Architecture for Technology, Research and Experimentation (MATREX) program at the United States Army esearch Laboratory, Human Research and Engineering Directorate, Simulation and Training Technology Center (ARL HRED STTC). His research interests include distributed simulation, novel computing architectures, innovative methods for user-simulation interaction, methodologies for making simulation more accessible by non-simulation experts, service oriented architectures and future simulation frameworks. He manages and leads a variety of research efforts that mature, integrate and demonstrate these technologies in a relevant Army and Department of Defense context. He received his Master of Science and Bachelor of Science in Electrical Engineering from Drexel University in Philadelphia, Pennsylvania.

Christopher J. Metevier is the Chief of the Advanced Simulation Branch and Technology Program Manager of the Modeling Architecture for Technology, Research, and EXperimentation (MATREX) program at the United States Army Research Laboratory, Human Research and Engineering Directorate, Simulation and Training Technology Center (ARL HRED STTC). He has over 24 years of experience with the Army and Navy in the Modeling and Simulation (M&S) field. His M&S experience extends across the acquisition lifecycle and includes the research, development, adaptation, integration, experimentation, test and fielding of numerous simulation technologies and systems. He received his Master of Business Administration from Webster University and his Bachelor of Science in Electrical Engineering from the University of Central Florida.

Scott Gallant is a Systems Architect with Effective Applications Corporation. He has 20 years experience in distributed computing including United States Army Modeling & Simulation (M&S). Scott has led technical teams on distributed M&S programs for distributed software and federation design, development and execution management in support of technical assessments, data analysis and experimentation. He currently leads the technical team for the implementation of the Executable Architecture Systems Engineering (EASE) system and actively supports research activities of the Army Research Laboratory, Human Research and Engineering Directorate, Simulation and Training Technology Center (ARL HRED STTC) Advanced Simulation Branch.

Lana E. McGlynn, founder of McGlynn Consulting Group (MCG), has over 40 years of hands-on experience in technical and leadership positions. She offers comprehensive consulting in the fields of modeling and simulation (M&S), testing, logistics, acquisition, and studies and analyses. Ms McGlynn has lead various domestic and international working groups and task forces, to include serving as the Vice Chair of the NATO Modeling and Simulation Group. Prior to retirement from federal service, she served as the Special Assistant to the Deputy Under Secretary of the Army for Operations Research (DUSA (OR)) for Modeling and Simulation (M&S). She is a member of the Army Acquisition Corps and was certified as an Acquisition Professional, Level III, in the functional specialty of Program Management.

Joseph S. McDonnell, Ph.D. is a Principal Scientist and Director of Modeling and Simulation at Dynamic Animation Systems. Dr. McDonnell has over 20 years of experience providing senior level project and software development leadership, primarily in the area of advanced distributed simulation applications. He also gained experience in a staff position while supporting the RDECOM Modeling and Simulation Senior Advisory Group (SAG), overseeing the transition from a SAG to an RDECOM SOSI IPT. Dr. McDonnell is experienced in all facets of contract management and has led both small and large teams, as a subcontractor and as a prime. Dr. McDonnell is currently supporting the RDECOM ARL HRED STTC Advanced Simulation Branch (ASB) as Principal Scientist providing scientific and future planning support, as well as being the contractor research lead for the Executable Architecture Systems Engineering Distributed Modeling Framework (EASE DMF) project and the Distributed Soldier Representation (DSR) project. Prior to his current role, Dr. McDonnell was the contractor Technical Lead for the Modeling Architecture for Technology, Research and Experimentation STO. He has been the contract technical lead for programs for the Federal Emergency Management Agency's National Fire Academy in Emmitsburg, MD and at the Night Vision and Electronic Sensors Directorate at Ft. Belvoir. Dr. McDonnell holds a Ph.D. in Mathematics from the University of Virginia.

Article Submission Policy

The CSIAC Journal is a quarterly journal focusing on scientific and technical research & development, methods and processes, policies and standards, security, reliability, quality, and lessons learned case histories. CSIAC accepts articles submitted by the professional community for consideration. CSIAC will review articles and assist candidate authors in creating the final draft if the article is selected for publication. However, we cannot guarantee publication within a fixed time frame.

Note that CSIAC does not pay for articles published.

AUTHOR BIOS AND CONTACT INFORMATION

When you submit your article to CSIAC, you also need to submit a brief bio, which is printed at the end of your article. Additionally, CSIAC requests that you provide contact information (email and/or phone and/or web address), which is also published with your article so that readers may follow up with you. You also need to send CSIAC your preferred mailing address for receipt of the Journal in printed format. All authors receive 5 complementary copies of the Journal issue in which their article appears and are automatically registered to receive future issues of Journal

COPYRIGHT:

Submittal of an original and previously unpublished article constitutes a transfer of ownership for First Publication Rights for a period of ninety days following publication. After this ninety day period full copyright ownership returns to the author. CSIAC always grants permission to reprint or distribute the article once published, as long as attribution is provided for CSIAC as the publisher and the Journal issue in which the article appeared is cited. The primary reason for CSIAC holding the copyright is to insure that the same article is not published simultaneously in other trade journals. The Journal enjoys a reputation of outstanding quality and value. We distribute the Journal to more than 30,000 registered CSIAC patrons free of charge and we publish it on our website where thousands of viewers read the articles each week.

FOR INVITED AUTHORS:

CSIAC typically allocates the author one month to prepare an initial draft. Then, upon receipt of an initial draft, CSIAC reviews the article and works with the author to create a final draft; we allow 2 to 3 weeks for this process. CSIAC expects to have a final draft of the article ready for publication no later than 2 months after the author accepts our initial invitation.

PREFERRED FORMATS:

- Articles must be submitted electronically.
- MS-Word, or Open Office equivalent (something that can be edited by CSIAC)

SIZE GUIDELINES:

- Minimum of 1,500 – 2,000 words (3-4 typed pages using Times New Roman 12 pt font) Maximum of 12 pages
- Authors have latitude to adjust the size as necessary to communicate their message

IMAGES:

- Graphics and Images are encouraged.
- Print quality, 300 or better DPI. JPG or PNG format preferred

Note: Please embed the graphic images into your article to clarify where they should go but send the graphics as separate files when you submit the final draft of the article. This makes it easier should the graphics need to be changed or resized.

CONTACT INFORMATION:

CSIAC
100 Seymour Road Suite C102
Utica, NY 13502
Phone: (800) 214-7921
Fax: 315-351-4209

Michael Weir, CSIAC Director
John Dingman, Managing Editor
Email: info@csiac.org

CSIAC is a DoD sponsored Information Analysis Center (IAC), administratively managed by the Defense Technical Information Center (DTIC), technically managed by the Air Force Research Laboratory (AFRL) in Rome, NY and operated by Quanterion Solutions Incorporated, Utica, NY.

ABOUT THE JOURNAL OF CYBER SECURITY AND INFORMATION SYSTEMS

CSIAC JOURNAL EDITORIAL BOARD

Distribution Statement
Unclassified and Unlimited

CSIAC
100 Seymour Road
Utica, NY 13502-1348
Phone: 800-214-7921 • **Fax:** 315-732-3261
E-mail: info@csiac.org
URL: https://www.csiac.org/

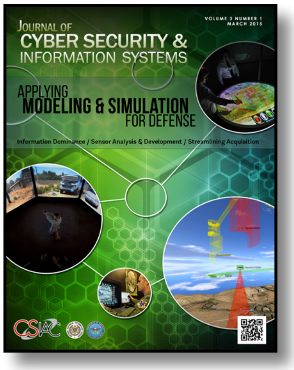
ABOUT THIS PUBLICATION

The Journal of Cyber Security and Information Systems is published quarterly by the Cyber Security and Information Systems Information Analysis Center (CSIAC). The CSIAC is a DoD sponsored Information Analysis Center (IAC), administratively managed by the Defense Technical Information Center (DTIC). The CSIAC is technically managed by Air Force Research Laboratory in Rome, NY and operated by Quanterion Solutions Incorporated in Utica, NY.

Reference herein to any specific commercial products, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or the CSIAC. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or the CSIAC, and shall not be used for advertising or product endorsement purposes.

COVER DESIGN

Shelley Howard
Graphic Designer
Quanterion Solutions, CSIAC



ARTICLE REPRODUCTION

Images and information presented in these articles may be reproduced as long as the following message is noted:

"This article was originally published in the Journal of Cyber Security and Information Systems Vol.III, No I"

In addition to this print message, we ask that you notify CSIAC regarding any document that references any article appearing in the *CSIAC Journal.*

Requests for copies of the referenced journal may be submitted to the following address:

Cyber Security and Information Systems
100 Seymour Road
Utica, NY 13502-1348

Phone: 800-214-7921
Fax: 315-732-3261
E-mail: info@csiac.org

An archive of past newsletters is available at **https://journal.csiac.org.**

Cyber Security and Information Systems
Information Analysis Center
100 Seymour Road
Suite C-102
Utica, NY 13502

Journal of Cyber Security and Information Systems – Volume III Number 1
Applying Modeling & Simulation for Defense

— IN THIS ISSUE —