



G2 Ops Press Hits

CHIPS
THE CENTER FOR THE U.S. CYBER INTELLIGENCE ECOSYSTEM

A new cyber-resilient approach for warfighting platforms
By Tracy Gregorio - January 18, 2023

Our military critical warfighting assets, such as **Adapt, Build, Operate, Sustain** (ABOS) and the **ABOS** Support System (ABOS), are being pushed to their operational limits. They are operating at the edge of their capabilities, and the risk of mission failure is increasing. The challenge is to ensure that these assets are resilient enough to survive in a world of increasing cyber threats.

Commanders need these systems to have the capability to detect, identify, and respond to cyber threats in real time. This is a challenge because these systems are often designed for a specific mission and are not designed to be resilient to cyber threats. The challenge is to ensure that these assets are resilient enough to survive in a world of increasing cyber threats.

1. Their systems and subsystems consistently face multiple concurrent threats. With increasing networked systems, the threat landscape is becoming more complex. The threat is no longer just a single point of entry, but a multi-point attack that can target multiple systems simultaneously.

2. Cyber threat actors are becoming more sophisticated. The threat actors are becoming more sophisticated and are using advanced techniques to penetrate defenses and gain access to critical systems.

3. Degraded platforms are not static. Many platforms for the warfighting force (WFF) have limited time to be in the field. This means that they are often operating at the edge of their capabilities, and the risk of mission failure is increasing.

There is, however, an approach available to optimizing cyber risk across the most critical assets. Our experience has been working through a range of Small Business Innovation Research (SBIR) programs to develop and test a new approach to cyber resilience. This approach is based on the concept of "Cyber Resilience by Design" (CRbD). CRbD is a process of designing systems to be resilient to cyber threats from the start. This approach is based on the concept of "Cyber Resilience by Design" (CRbD). CRbD is a process of designing systems to be resilient to cyber threats from the start.

1. Reduce the baseline. The first step involves creating a digital twin of the complete SBIR program. This involves creating a digital twin of the complete SBIR program. This involves creating a digital twin of the complete SBIR program.

Defense One

How Digital Twinning Is Helping Improve Submarine Communications
Lessons from the challenging world of undersea operations ought to be applied across the military.

By Tracy Gregorio

The world's most advanced submarine communication system, the **Adapt, Build, Operate, Sustain** (ABOS) program, is helping to improve submarine communications. The program is helping to improve submarine communications. The program is helping to improve submarine communications.

IDEAS
How Digital Twinning Is Helping Improve Submarine Communications
Lessons from the challenging world of undersea operations ought to be applied across the military.

TRACY GREGORIO | JANUARY 18, 2023

COMMENTARY | NAVY | INDUSTRY | LEAD

One thing slowing down the upgrade cycles of weapons is the painstaking effort it takes to predict the reliability, maintainability, and availability, or RMAA,

ARS & STRIPES

HISTORY | LIVING | SPORTS | MULTIMEDIA | COMMUNITIES

more modern-day cyber

Tracy Gregorio - CEO Creates Waves in...

Watch later | Share

STEVE SPONSOR

Category Archives for "Podcast"

Using the Small Business Innovation Research (SBIR) Program to Grow your Business - Tracy Gregorio

TECH LEADER TALK

Listen on **Apple Podcasts** | **Google Podcasts** | **Spotify**

Did you know that the SBIR program can help your small business grow by solving particular problems defined by public sector organizations?

On this episode, I am talking with Tracy Gregorio. Tracy is the CEO of G2 Ops, which is an IT engineering and cybersecurity company.



Contents

Summary	3
Highlights	5
Byline articles	8

Summary



34

Pieces of Coverage

Total number of online and social clips



32.9K

Estimated Views

Prediction of lifetime views of coverage, based on audience reach & engagement rate on social



3.87M

Audience

Combined total of publication-wide audience figures for all outlets featuring coverage



209

Engagements

Combined total of likes, comments and shares on social media platforms



55

Avg. Domain Authority

A 0-100 measure of the authority of the site coverage appears on. Provided by Moz

Highlights

Defense One
How Digital Twinning Is Helping Improve Submarine Communications

3.92K 693K 49

CHIPS
A new cyber-resilient approach for warfighting platforms

47 13.5K 0

Steve Spenseller
Using the Small Business Innovation Research (SBIR) Program to Grow your Business - Tracy Gregorio

0

Lady Empire Podcast
Tracy Gregorio - CEO Creates Waves in Cybersecurity

1 9 -

Washington Technology
Why cyber resiliency might be your best cloud sales pitch

397 42.8K 3

Stars and Stripes
The need for more modern-day cyber warriors

3.48K 838K 0

Washington Technology

TOP 100
Introducing the 2023 Washington Technology Top 100

GSA launches recomputer of OASIS professional services vehicle


INSIDER EXCLUSIVE: How DUJ funnels commercial tech to end users

Top 100 Q&A: Stu Shea and the future of Piratun

Population tech maker fetches \$13M from Lockheed's venture arm, other investors

New Government & Education Data Cloud Smalls Down Barriers to Data Driven Decision-Making

Is model-based systems engineering right for you?



Washington Technology

Is model-based systems engineering right for you?

404 42.8K 9

Transitions Newsletter

Build-test-build Iterative Design Improves the Development Process for Small Businesses, Customers, Warfighters

By Jennifer Booth, Navy STP Managing Editor

Build-test-build, crawl-walk-run, spiral, fly-fix-fly: Iterative design has many different names. Iterative design is a user-centered process of refining and improving a product or design through repeated cycles of testing, feedback and revision during the development process. Based on feedback from the customer, designers can adjust and refine the technology and test it again, continuing this cycle until the design meets the customer's needs and expectations.

By testing and refining the design in an ongoing manner, designers can catch potential issues early on and realign before investing too much time or too many resources in the final product and help ensure designers and customers are on the same page. Several small businesses participating in the Navy SBIR Transition Program (Navy STP) use the process, saving time and money and delivering solutions that truly meet customers' needs.

"Continuous Solutions has long championed a build-test-build approach to design. Termed



Iterative design is a user-centered process of refining and improving a product or design through repeated cycles of testing, feedback and revision during the development process.

relatively low and on par with traditional design process," Marshall explained.

IMSAR, located in Springville, Utah, develops high-performance multi-mode airborne radar systems. To ensure high reliability, IMSAR uses a fly-fix-fly (FFF) method of development for the design

NavySTP Transitions Newsletter

Build-Test-Build Iterative Design Improves Development

542 981 0

Thursday, October 5, 2023

SEAPOWERS
The Official Publication of the Navy League of the United States

Home All Headlines Categories Advertising Subscribe About Seapower Contact Us

Systems Models Keep Submarines Mission Ready

Posted on October 3, 2023 by Seapower Staff

BY TRACY GREGG

An important, yet often underappreciated challenge for undersea warfare is keeping submarine systems well-maintained and available. Every command has a budget for reliability, maintainability, and availability (RMA), but those resources are limited and need to be carefully allocated to keep warfighting systems mission-ready.

For decades now, maintenance planning has been performed by seasoned engineers who understand how component lifecycles and failure rates can affect their systems. This process of expert-driven failure modes and effects analysis (FMEA) is time-consuming, expensive, and can take months to complete by veterans whose expertise is sorely needed elsewhere.

Additional time is also needed to evaluate changes using the Risk Management Framework (RMF), to identify cybersecurity vulnerabilities that may degrade system availability.

SEARCH

SUBSCRIBE TO OUR WEEKLY DIGITAL NEWSLETTER

Sign Up

Current Issue

Seapower

Systems Models Keep Submarines Mission Ready

244 23.5K 0

Byline articles

Exclusive bylines featuring Tracy Gregorio
thought leadership.



17 pieces



GovTech

Government Technology has IT articles for state, local and city government. Find government news...

81

Domain Authority

Provided by MOZ

172K

Unique Visits

Provided by SimilarWeb

December 16, 2022 • ONLINE

Digital Twins Key to Cyber Resilient Infrastructure

govtech.com/opinion/digital-twins-key-to-...



OPINION

Digital Twins Key to Cyber Resilient Infrastructure

Attack vectors in critical infrastructure are always changing, and agencies must move beyond just preventing cyber attacks and toward resiliency. Digital twin modeling can help governments prepare to work through any scenario.

December 16, 2022 • Tracy Gregorio, G2 Ops



Shutterstock/Yurchanka Siarhei

Deploying systems fully designed to sustain operations during and after a cyber attack is quickly becoming the most realistic method for keeping critical infrastructure online.

Critical infrastructures often comprise complex systems of systems (SoS) running through interrelated IT platforms, applications, operational technologies (OT) and human/machine interfaces. We depend on systems of systems to orchestrate transportation networks, protect citizens from terrorist attacks and sustain utility grids. The increasing convergence of IT and OT systems creates opportunities for exploitation that can have catastrophic consequences.

Most state and local government IT managers have recognized these vulnerabilities and responded by

Estimated Views

635 ✓

Estimated views calculated based on audience size and socia...

Engagements

13 ✓

Total number of social engagements



The Virginian-Pilot

The Virginian-Pilot: Your source for Virginia breaking news, sports, business, entertainment, weather an...

76

Domain Authority

Provided by MOZ

823K

Unique Visits

Provided by SimilarWeb

December 20, 2022 • ONLINE

Fixing the leaky pipeline for women in STEM | Expert column

pilotonline.com/2022/12/20/fixing-the-lea...

Estimated Views

5.02K

Estimated views calculated based on audience size and socia...

Engagements

0

Total number of social engagements

The Virginian-Pilot

Fixing the leaky pipeline for women in STEM [...]

BUSINESS

Fixing the leaky pipeline for women in STEM | Expert column



1 of 2
Tracy Gregorio

Pamela Manning/Courtesy photo



Yo



By TRACY GREGORIO and PILOT ONLINE

PUBLISHED: December 20, 2022 at 8:32 a.m. | UPDATED: December 23, 2022 at 1:38 p.m.



Listen to this article



Businesses in the Hampton Roads region and across the nation face a serious challenge getting and keeping employees in science, technology, engineering and math careers. Furthermore, the Center for Talent Innovation found that women leave STEM fields in droves, with 52% of highly qualified women working in the field abandoning their jobs. The result is a "leaky pipeline" for women in tech fields where we are already facing a severe shortfall.

Top
Cle
Dr. M



Defense One

Defense One provides news, analysis, and ideas about the future of national security to defense an...

75

Domain Authority

Provided by MOZ

693K

Unique Visits

Provided by SimilarWeb

January 18, 2023 • ONLINE

How Digital Twinning Is Helping Improve Submarine...

defenseone.com/ideas/2023/01/how-digit...

10th Anniversary
Defense One

US Woos Other Nations For Military-AI Ethics Pact

We Missed Social Media's Dark Side. Let's Be Smarter About The Metaverse

Can A New Information-Security Approach Save The Navy \$1B A Year?

China Gears Up To Shoot Down US Drones

Navy 'Setting The Pace' Among Services, Principal Cyber Advisor Says

SPONSOR CONTENT

How Data Empowers Coalition Partnerships At The Mission's Edge

The Seawolf-class fast-attack submarine USS Connecticut (SSN 22) and the Los Angeles-class fast-attack submarine USS Hartford (SSN 768) break through the ice in support of Ice Exercise (ICEX) 2018. U.S. NAVY / MASS COMMUNICATION 2ND CLASS MICHEAL H. LEE

IDEAS

How Digital Twinning Is Helping Improve Submarine Communications

Lessons from the challenging world of undersea operations ought to be applied across the military.

TRACY GREGORIO | JANUARY 18, 2023

COMMENTARY NAVY INDUSTRY C4ISR

f t in e

One thing slowing down the upgrade cycles of weapons is the painstaking effort it takes to predict the reliability, maintainability, and availability, or RMA,

Estimated Views

3.92K ✓

Estimated views calculated based on audience size and socia...

Engagements

49 ✓

Total number of social engagements



CHIPS

CHIPS is an official U.S. Navy website sponsored by the Department of the Navy (DON) Chief Informati...

88

Domain Authority

Provided by MOZ

13.5K

Unique Visits

Provided by SimilarWeb

January 20, 2024 • ONLINE

A new cyber-resilient approach for warfighting platforms

doncio.navy.mil/chips/ArticleDetails.aspx?...

CHIPS THE DEPARTMENT OF THE NAVY'S INFORMATION TECHNOLOGY MAGAZINE [Notify Me of New Issue](#)

CURRENT ISSUE BACK ISSUES AUTHOR INDEX BROWSE TAGS ABOUT CHIPS

A new cyber-resilient approach for warfighting platforms [Email](#)

By Tracy Gregorio - January-March 2023

Our nation's critical warfare assets, such as Arleigh Burke class destroyers (DDGs) and the AEGIS Weapons System (AWS), are uniquely difficult to protect from cyberattacks. They are examples of large Systems of Systems (SoS) running multiple concurrent mission threads, presenting vast numbers of threat surfaces that include complex integrated systems, satellite communications links, sensor fusion platforms and many human/machine interfaces.

Commands need those systems to have the resilience to stay on mission no matter what type of cyberattack they are subject to. While existing defensive cyber capabilities adequately monitor for vulnerabilities, it's been difficult, if not impossible, to identify which cyber threats pose the greatest threat to mission effectiveness. The resilience challenge is difficult because commands need to simultaneously grapple with three factors:

- 1. Their systems and subsystems continuously face multiple concurrent threats.** With vulnerability monitors flagging multiple threats, how should analysts prioritize which threats to focus on? Which could most impact their mission or missions? Analysts need to understand if and how those threats across information technology (IT) and operational technology (OT) systems might impact their ability to complete missions through denial of service, performance degradation or data loss.
- 2. Cyber threat actors relentlessly create new exploits.** Threats come in at such a pace that it's unrealistic to evaluate all potential threats and vulnerabilities, to know which might succeed, and which could compromise mission capability. A single vulnerability in a critical component could render a unit useless, while multiple vulnerabilities in another subsystem might mean cyberattacks can disrupt a series of operations, while the ability to execute mission-critical operations remains in full force.
- 3. Deployed platforms are not static.** Major platforms like the Arleigh Burke class DDG have useful lives across three decades or more, during which their IT and OT systems experience continuous spiral updates. A common byproduct of this, however, is that the platform drifts from its documented design baseline through poorly documented break/fix field workarounds, unplanned commercial-off-the-shelf (COTS) obsolescence refreshes and cumbersome configuration management processes.

There is, however, an approach suitable for optimizing cyber risks across the most sophisticated SoSs. Our engineering team has been working through a pair of Small Business Innovation Research (SBIR) programs to better protect parts of some of the Navy's most important warfighting platforms and weapons system programs. These solutions involve four elements that can be readily extended to other platforms:

- 1. Model the baseline.** The first step involves creating a digital twin of the complete SoS including every subsystem, interface, data flow and mission thread. Model based system engineering (MBSE) captures the architectural and functional characteristics of each and every system interface via a high-fidelity digital twin model. This enables all potential cyberattack surfaces to be captured via a disciplined and standardized engineering approach. These digital models represent the architecture and operational behaviors through Systems Modeling Language (SysML) diagrams spanning from the mission threads down to the IT and OT Configuration Item (CI) levels. Each digital twin is created to represent the real-world as-is state of the platform. Baseline management and change management changes can then be automated to deal with design volatility, rapid refresh/insertion rates and ensure commonality between platform variants.
- 2. Connect intelligence repositories.** The next step in the approach is to cross-reference the digital twin against the latest threat intelligence databases. Automated processes are set up to ingest, aggregate and correlate threat data from open as well as classified sources and map

Tracy Gregorio

Related CHIPS Articles

- Naval Postgraduate School partners With Qualcomm to advance technological solutions
- U.S., South Korean agencies partner to #StopRansomware threat from DPRK
- Army using Europe and Pacific operational landscapes as 'laboratories' to enhance network resiliency
- NATO Cyber Defence Center taps the Defense Information Systems Agency as U.S. team lead for intense cyberattack challenge
- MCTSSA Hosts "Industry Day" at Camp Pendleton

Related DON CIO News

- Listen to: "Live from AFCEA West - Navy CIO's Game-Changing Tech for Enabling Information Superiority"
- DON IT Conference, West Coast 2023 Final Details
- Leader Challenge: Drive Competitive Advantage with Innovation
- Department of the Navy CIO Announces Campaign Plan to Further Information Security
- ALNAV: January is Operations Security Awareness Month

Estimated Views

47

Estimated views calculated based on audience size and socia...

Engagements

0

Total number of social engagements



Washington Technology

Latest news and information on the business of delivering technology and services to government...

59

Domain Authority

Provided by MOZ

42.8K

Unique Visits

Provided by SimilarWeb

April 27, 2023 • ONLINE

Why cyber resiliency might be your best cloud sales pitch

washingtontechnology.com/opinion/2023...

- TOP 100**
Introducing the 2023 Washington Technology Top 100
- GSA launches**
recompete of OASIS professional services vehicle
- EXCLUSIVE**
INSIDER EXCLUSIVE: How DIU funnels commercial tech to end users
- Top 100 Q&A: Stu Shea**
and the future of Peraton
- Propulsion tech maker**
fetches \$13M from Lockheed's venture arm, other investors
- SPONSOR CONTENT**
New Government & Education Data Cloud Breaks Down Barriers to Data-Driven Decision-Making

Why cyber resiliency might be your best cloud sales pitch



GETTYIMAGES.COM/THAPANA ONPHALAI

By **TRACY GREGORIO** // APRIL 27, 2023

Many government agencies still don't feel a compelling reason to migrate to the cloud but a focus on cybersecurity might be the lever you need to unlock that business.

COMMENTARY



Despite the Cloud First directive of 2010 and Cloud Smart in 2019, it's been a slow process migrating Federal systems to the cloud. It's not for lack of capacity: providers such as Microsoft, Amazon Web Services, Google, and Oracle have all invested to create federal-compliant cloud capacity far beyond demand.

But, while Cloud Smart provides strong guidelines on how to migrate, many agencies haven't felt a compelling motivation for such a move. Federal contractors can unlock cloud migration business opportunities by educating agency CIOs on how cloud platforms can enhance their

Estimated Views

397 ✓

Estimated views calculated based on audience size and socia...

Engagements

3 ✓

Total number of social engagements



Stars and Stripes

U.S. military news organization providing independent news and information to the military...

80

Domain Authority

Provided by MOZ

838K

Unique Visits

Provided by SimilarWeb

June 06, 2023 • ONLINE

The need for more modern-day cyber warriors

[strips.com/opinion/2023-06-06/modern-...](https://www.strips.com/opinion/2023-06-06/modern-...)

The screenshot shows the website's header with a navigation menu (THEATERS, BRANCHES, VETERANS, HISTORY, LIVING, SPORTS, MULTIMEDIA, COMMUNITIES), a search bar, and a 'SUBSCRIBE' button. The article title is 'The need for more modern-day cyber warriors' by Tracy Gregorio, dated June 6, 2023. Below the title is a photograph of a military uniform sleeve with a 'CYBER' patch and an 'AIR COMBAT COMMAND' patch.

OPINION

The need for more modern-day cyber warriors

By TRACY GREGORIO
SPECIAL TO STARS AND STRIPES • June 6, 2023



Airmen with 175th Cyber Operations, Maryland Air National Guard, train at Exercise Southern Strike at Camp Shelby, Mississippi, April 21, 2023. Southern Strike 2023 is a large-scale, joint multinational combat exercise hosted by the Mississippi National Guard that provides tactical level training for the full spectrum of conflict. (Renee Seruntine/U.S. Army National Guard)

Estimated Views

3.48K

Estimated views calculated based on audience size and socia...

Engagements

0

Total number of social engagements



Washington Technology

Latest news and information on the business of delivering technology and services to government...

59

Domain Authority

Provided by MOZ

42.8K

Unique Visits

Provided by SimilarWeb

June 21, 2023 • ONLINE

Is model-based systems engineering right for you?

washingtontechnology.com/opinion/2023...

Introducing the 2023 Washington Technology Top 100	GSA launches recompete of OASIS professional services vehicle	INSIDER EXCLUSIVE: How DIU funnels commercial tech to end users	Top 100 Q&A: Stu Shea and the future of Peraton	Propulsion tech maker fetches \$13M from Lockheed's venture arm, other investors	New Government & Education Data Cloud Breaks Down Barriers to Data-Driven Decision-Making

Is model-based systems engineering right for you?



GETTYIMAGES.COM/KRONGKAEW

By TRACY GREGORIO // JUNE 21, 2023

Model-based systems engineering is widely used when designing complex systems, but the question remains of when is it right for your project or system.

COMMENTARY EMERGING TECHNOLOGY



Model-based system engineering is widely used by developers of complex systems-of-systems at companies like Boeing, Ford, and Amazon Web Services. It is becoming increasingly important in next-generation military systems like the Columbia-class nuclear submarine.

U.S. military, other Federal agencies, and commercial enterprises are often intrigued by the idea of MBSE, but are unsure whether it's appropriate for them. The ideal MBSE user designs and develops complex systems and needs to increase the rigor of their system engineering.

Estimated Views

404

Estimated views calculated based on audience size and socia...

Engagements

9

Total number of social engagements



CHIPS

CHIPS is an official U.S. Navy website sponsored by the Department of the Navy (DON) Chief Informati...

88

Domain Authority

Provided by MOZ

33.9K

Unique Visits

Provided by SimilarWeb

August 01, 2023 • ONLINE

JAG's grueling but successful journey to Cloud First

doncio.navy.mil/CHIPS/ArticleDetails.aspx...

The screenshot shows the CHIPS website interface. At the top, there's a navigation bar with 'CURRENT ISSUE', 'BACK ISSUES', 'AUTHOR INDEX', 'BROWSE TAGS', and 'ABOUT CHIPS'. Below this is a search bar. The main content area features the article title 'JAG's grueling but successful journey to Cloud First' by Tracy Gregorio, dated July-September 2023. The article text discusses the challenges of cloud migration for the JAG Corps, including funding, skillsets, and RMF compliance. A sidebar on the right contains a portrait of Tracy Gregorio and a list of related articles such as 'PEO Digital stands up Neptune Cloud Management Office' and 'DISA launches OCONUS Cloud capability'.

Estimated Views

95

Estimated views calculated based on audience size and socia...

Engagements

0

Total number of social engagements



Washington Technology

Latest news and information on the business of delivering technology and services to government...

59

Domain Authority

Provided by MOZ

29.4K

Unique Visits

Provided by SimilarWeb

September 12, 2023 • ONLINE

Why model-based systems engineering is about more than...

washingtontechnology.com/opinion/2023...

GovTrite's top 20 contracts for September	Army developing next version of enterprise-wide payroll system	Booz Allen books \$630M Space Force engineering contract	KBR joint venture takes back lost NASA contract	Booz Allen stands alone in T4NG protest fight	How to secure systems without limiting innovation

Why model-based systems engineering is about more than just compliance



GETTYIMAGES.COM/ MR.COLE_PHOTOGRAPHER

By TRACY GREGORIO // SEPTEMBER 12, 2023

Known as MBSE, model-based systems engineering offers a way to standardize IT systems while increasing cyber resiliency.

COMMENTARY



Model-based systems engineering is quietly, but consistently, becoming an important part of the design, maintenance, and cybersecurity of the federal government's most complex IT platforms. MBSE supports the Department of Defense's push towards digital engineering, and helps designers create more effective and resilient systems of systems.

MBSE is now required in many new DoD contracts, and even skeptics are seeing benefits as MBSE helps projects complete time-intensive Risk Management Framework activities in days rather than weeks or months.

But it's a mistake to limit MBSE's impact to documenting RMF compliance

Estimated Views

242 ✓

Estimated views calculated based on audience size and social...

Engagements

1 ✓

Total number of social engagements



RealClearDefense

RealClearDefense (RCD) was created at the request of the Pentagon and Hill staff on the House Armed...

63

Domain Authority

Provided by MOZ

214K

Unique Visits

Provided by SimilarWeb

September 14, 2023 • ONLINE

DoD Managers Need to Share Cloud Resources

realcleardefense.com/articles/2023/09/12...

RealClear Defense

Articles Video Contact More

SIGN IN | SUBSCRIBE AD-FREE



NOW READING: DOD MANAGERS NEED TO SHARE CLOUD RESOURCES

UP NEXT:



DoD Managers Need to Share Cloud Resources

By Tracy Gregorio
September 12, 2023

U.S. Air Force photo by A1C Zachary Rufus

U.S. Air Force Maj. Nicholas Detloff, Course of Action Management product line manager from the 225th Air Defense Squadron, Washington Air National Guard, briefs fellow warfighters on the capabilities of the Advanced Battle Management System (ABMS) at the Shadow Operations Center at Nellis (ShOC-N). The ShOC-N is contributing to the development of ABMS via DevSecOps. (U.S. Air Force photo by A1C Zachary Rufus)

The Department of Defense (DoD) has been pushing digital engineering and cloud computing for the past five years, but many IT systems across the Services have yet to take advantage of either. System architects and program managers can help overcome the inertia and accelerate getting to the benefits of these new paradigms by sharing tools and foundational apps from one command to another.

Estimated Views

2.57K

Estimated views calculated based on audience size and socia...

Engagements

7

Total number of social engagements

NavySTP Transitions Newsletter

Now in its 23rd year, the Navy STP (SBIR/STTR Transition Program) has been a long-standing vehicle for connecting...

12

Domain Authority

Provided by
MOZ

717

Unique Visits

Provided by
SimilarWeb

September 14, 2023 •  ONLINE

Evaluating Cyber Risk: G2 Ops' Tools & Methodologies...

navystp.com/wp-content/uploads/2023/0...

Transitions Newsletter

Fall 2023

Evaluating Cyber Risk: G2 Ops' Tools and Methodologies Enhance Navy Capabilities

By Jennifer Reisch, Navy STP Managing Editor

“Collaboration is essential for Phase III transitions,” said Kevin Esser, chief business officer at G2 Ops. “Collaboration spanning the program office that needs the technology, the contracting organization—whether that’s NAVSEA, GSA, NAVAIR or another command, and the small business itself.” Esser has successfully transitioned two out of four Phase II SBIR technologies to the Navy. A third SBIR project, still in Phase II, has already transitioned portions of the technology. “A lot of companies don’t think about that collaborative requirement. It might be that they don’t have the resources or the know-how to collaborate with the Navy to construct a workable Phase III vehicle.”

G2 Ops uses model-based systems engineering (MBSE) to address systems engineering and cybersecurity challenges. The company develops and applies modeling tools and analytics to improve systems engineering and uncover cyber strengths and weaknesses in tactical system design.

The first technology G2 Ops transitioned to the Navy was Strategic Optics for Intelligent Analytics (SOFIA), a mission-based cyber risk assessment tool, developed in collaboration with PEO Integrated Warfare Systems (IWS) 1.0, the developers of AEGIS Combat Systems. “What made this so special was that we were already working

The name Sofia is derived from the Greek word for wisdom. “That’s what we’re providing here: insight into the cyber posture of a tactical platform and the impact of cyber vulnerabilities on mission-based risk.

Classical risk assessments focus on the component level, which does not give a true operational picture of where risk really resides. The beauty of this tool is that the systems modeling language models we create of the baseline architectures flow into a hierarchy that allocates components to the systems and missions they support. The digital engineering models give layered context to the way that a platform operates: not just its physical attributes, but its behavioral attributes—how they interrelate, downstream impact—and then risk-scored through an overlay against open-source intelligence data that we collect.”

For SOFIA, G2 Ops established a data pipeline encompassing over a dozen open-source intelligence databases. This pipeline provides cybersecurity engineers with ready access to data that is typically constrained due to concerns



Estimated Views

224 

Estimated views calculated based on audience size and socia...

Engagements

0 

Total number of social engagements



Seapower

Educating Congress and the American people about the activities, requirements and...

58

Domain Authority

Provided by MOZ

23.5K

Unique Visits

Provided by SimilarWeb

Thursday, October 5, 2023



SEAPOW

The Official Publication of the Navy League of the United States

Home All Headlines Categories Advertising Subscribe About Seapower Contact Us

Systems Models Keep Submarines Mission Ready

Posted on October 3, 2023 by Seapower Staff

BY TRACY GREGORIO

An important, yet often underappreciated challenge for undersea warfare is keeping submarine systems well-maintained and available. Every command has a budget for reliability, maintainability, and availability (RMA), but those resources are limited and need to be carefully allocated to keep warfighting systems mission-ready.

For decades now, maintenance planning has been performed by seasoned engineers who understand how component lifecycles and failure rates can affect their systems. This process of expert-driven failure modes and effects analysis (FMEA) is time consuming, expensive, and can take months to complete by veterans whose expertise is sorely needed elsewhere.

Additional time is also needed to evaluate changes using the Risk Management Framework (RMF), to identify cybersecurity vulnerabilities that may degrade system availability.

Model-Based Approach.

To address this challenge, a model-based system engineering (MBSE) approach is starting to automate failure mode analysis, facilitating more efficient RMA planning. This shift provides additional time for design optimization, refinement of reliability predictions, and comprehensive analysis of casualty reporting. The result is better mission-readiness for our fleet, while consuming fewer resources.

Reliability analysis is important to ensure that a warfighting platform has no single point of failure across its many components. Between a ship's tight spaces and funding limitations, it's impossible to go to sea with spares for everything.

One organization using this new MBSE approach is the Undersea Communications & Integration Program Office, PEO C4I / Program Manager, Warfare (PMW 770). Their Program Manager, Captain David Kuhn explained, "If spares are not available, we have to plan for alternate ways of accomplishing a mission, even if it's less stealthily. To ensure we optimize our ability to change parts and/or have redundant paths for missions, we build forecasts based on how often parts are used. If a component fails early and there is no spare on board, it could be a mission kill."

The MBSE models enable program managers, like Kuhn, to create forecasts better and faster, while tying together different engineering disciplines and stakeholder communities. "Engineers specialized in systems design, cyber, and reliability each have their own approach," said Kuhn. "They need different views and have historically used different models. Now they use the same model, each getting the views they need, and enabling analysis that just couldn't be done before."

Confidence in Outcomes

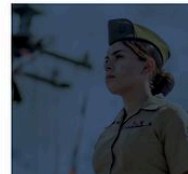
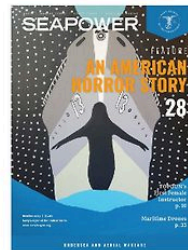
SEARCH

Search ...

SUBSCRIBE TO OUR WEEKLY DIGITAL NEWSLETTER

Sign Up

Current Issue



October 03, 2023 • ONLINE

Systems Models Keep Submarines Mission Ready

seapowermagazine.org/systems-models-...

Estimated Views

244

Estimated views calculated based on audience size and socia...

Engagements

0

Total number of social engagements



Efficient Plant

The Source For Reliability Solutions

39

Domain Authority

Provided by MOZ

5.84K

Unique Visits

Provided by SimilarWeb

Magazine ▾ Subscribe ▾ Events Resources ▾ Contact Us Advertise Staff

EFFICIENT PLANT

RELIABILITY ELECTRICAL ANALYSIS AUTOMATION EQUIPMENT LUBRICATION SAFETY SERVICES WORKFORCE

AUTOMATION | MAINTENANCE | RELIABILITY

Use MBSE to Optimize Systems

Gary Parr | November 30, 2023



MBSE models can be used to generate impact assessments that help decision makers understand the likelihood of system availability and to optimize maintenance schedules or plan for spares.

Model Based System Engineering advances enterprise reliability, availability, and maintainability.

By Tracy Gregorio, G2 Ops

As infrastructures increase in complexity to become integrated "systems of systems" that include components created and managed by different entities, ensuring their reliability, availability, and overall operational resilience becomes more challenging. The challenge is spreading across industry and public infrastructure with the arrival of autonomous vehicles, smart cities, and multi-directional power grids. The U.S. military

POPULAR CATEGORIES

- 1 Products
- 2 Management
- 3 Reliability
- 4 Maintenance
- 5 News
- 6 Automation
- 7 IIoT

FEATURED VIDEO



VIDEO: Pros And Cons Of Condition Monitoring Services

ABOUT THE AUTHOR

November 30, 2023 • ONLINE

Use MBSE to Optimize Systems

efficientplantmag.com/2023/11/use-mbse-...

Estimated Views

913

Estimated views calculated based on audience size and social...

Engagements

1

Total number of social engagements



Federal News Network

Federal News Network covers the latest issues and breaking stories within the U.S. government that...

68

Domain Authority

Provided by MOZ

439K

Unique Visits

Provided by SimilarWeb

December 11, 2023 • ONLINE

Managing the complex ecosystem of a new 5G DoD smar...

federalnewsnetwork.com/commentary/2...

Estimated Views

3.13K

Estimated views calculated based on audience size and socia...

Engagements

15

Total number of social engagements

On Air: Innovation in Government | TRENDING: 2024 pay raises by location / BoP retention pay ends / New rules for pay above grade | Email Alerts | Listen Live

FEDERAL NEWS NETWORK | TECHNOLOGY | DEFENSE | WORKFORCE/MANAGEMENT | PAY & BENEFITS | COMMENTARY | AUDIO | RESOURCES | SEARCH

COMMENTARY

Managing the complex ecosystem of a new 5G DoD smart warehouse

Tracy Gregorio
December 11, 2023 5:02 pm | 4 min read

5G technology enables many new applications across commercial sectors, government and our military. This latest wireless platform is expected to power autonomous vehicles, smart cities, remote healthcare, next-generation agriculture and more.

The Defense Department's FutureG Office within the Office of the Under Secretary of Defense for Research and Engineering is working to develop a 5G smart warehouse for U.S. Naval Base Coronado. The project aims to solve some of the Navy's most complex logistics challenges while serving as a DoD testbed for multiple state-of-the-art technologies and applications. The smart warehouse project is intended to be a standard setter for how the DoD innovates with advanced technology. It fits into a broader set of initiatives to help improve the readiness of our fighting forces by circumventing human error to keep us all safer.

The smart warehouse

The 5G smart warehouse is expected to increase efficiencies across inventory management, storage, receiving, shipping and delivery. It is also expected to reduce lost, stolen or damaged materials while fulfilling orders faster and more accurately.

The 5G smart warehouse includes a private 5G network to provide reliable, high-performance and highly secure communications transport. The 5G network is designed to support multiple advanced technologies and applications, such as radio frequency identification, augmented reality, autonomous robots, and internet of things solutions.

— Join us Jan. 4 at 2 p.m. EST for a discussion with agency and industry leaders on how data strategy can improve agency mission outcomes, sponsored by LexisNexis. | CPE credit eligible

Interoperability, cybersecurity and operational resiliency across 5G network subsystems can be particularly challenging due to each subsystem technology's diversity, interdependence and rapid evolution. An essential resource to ensuring all those elements work smoothly together is model-based system engineering (MBSE).

MBSE has been around for years, but is relatively nascent within DoD. It has become

Register for FEDERAL INSIGHTS EVENTS

The latest in Government Events powered by: GovEvents

- 119 CES 2024
- 119 A Complimentary Webinar by Serving...
- 119 How to Do Business with NASA

View More Events | Post Your Event

RELATED STORIES

Pentagon eyes 5G, 'future G' to help warfighters

DEFENSE NEWS

O-RAN will transform wireless and enable 5G adoption

COMMENTARY

Navy charts massive transformation in shipboard IT as commercial 5G, satellite links join the fleet

ON DOD

TOP STORIES

First win in Europe: DoD employees get union representation at German military installation

TOP STORY

OFPP's acquisition workforce modernization effort to kick into gear in 2024

ACQUISITION

New direct hire authority aims to assist agencies with AI talent surge

ARTIFICIAL INTELLIGENCE

Path to modernization is well defined, now Air Force has to 'follow through'

AIR FORCE

NGA, DHS S&T's unique approaches to zero trust, cybersecurity

ASK THE CIO



CSO Online

CSO delivers the critical information about trends, practices, and products enterprise security leaders...

85

Domain Authority

Provided by MOZ

509K

Unique Visits

Provided by SimilarWeb

January 23, 2024 • ONLINE

Defend critical infrastructure from cyber threats like th...

csoonline.com/article/1297773/defend-cri...

Estimated Views

1.86K

Estimated views calculated based on audience size and socia...

Engagements

16

Total number of social engagements

CSO

Topics Events Newsletters Resources

Home • Security • Defend critical infrastructure from cyber threats like the US Navy protects ships



by Tracy Gregorio
CEO, G2 Ops

Defend critical infrastructure from cyber threats like the US Navy protects ships

Opinion

Jan 25, 2024 • 6 mins

Critical infrastructure Threat and Vulnerability Management

Smart cities, power grids, and other distributed critical infrastructure could learn from how the US Navy protects the mission-readiness of its deployed fleet.

in

X

▼



Credit: US Navy



Related co



Contract Management

The starting point for all things NCMA, the community for contract management, procuremen...

52

Domain Authority

Provided by MOZ

13.5K

Unique Visits

Provided by SimilarWeb

January 11, 2024 • ONLINE

Leveraging the Small Business Innovation Research Program

ncmahq.org/Web/Web/Resources/Contra...



Estimated Views

184 ✓

Estimated views calculated based on audience size and socia...

Engagements

1 ✓

Total number of social engagements



RealClearDefense

RealClearDefense (RCD) was created at the request of the Pentagon and Hill staff on the House Armed...

63

Domain Authority

Provided by MOZ

133K

Unique Visits

Provided by SimilarWeb

March 27, 2024 • ONLINE

Cybersecurity Analytics and Visualization for...

realcleardefense.com/articles/2024/03/27/cybersecurity-analytics-and-visualization-for-warfighting-advantage

Cybersecurity Analytics and Visualization for Warfighting Advantage

By Corren McCoy
March 27, 2024

Marine Corps Forces Cyberspace Command

The power balance in modern warfare increasingly hinges on which side has the greater information advantage, which makes cybersecurity an essential priority. Information advantage is best realized when warfighting systems can instantly communicate to orchestrate systems involving personnel and manned and unmanned weapon systems deployed across land, air, sea, and space. For simplicity, we call such Rubik's Cubes "multi-domain systems."

Estimated Views

1.84K

Estimated views calculated based on audience size and social media activity.

Engagements

31

Total number of social engagements