Carnegie Mellon University
Software Engineering Institute

2020

YEAR IN REVIEW

The Software Engineering Institute (SEI) is a federally funded research and development center (FFRDC) sponsored by the U.S. Department of Defense and operated by Carnegie Mellon University.

The SEI's mission is to support the nation's defense by advancing the science, technologies, and practices needed to acquire, develop, operate, and sustain software systems that are innovative, affordable, trustworthy, and enduring.

The *2020 SEI Year in Review* highlights the work of the institute undertaken during the fiscal year spanning October 1, 2019, to September 30, 2020.

A Message from the Director and Chief Executive Officer

Radio operators use the expression *five by five* to indicate that signal strength and quality are loud and clear. Organizations send signals as well, in the form of direct requests, implied needs, or even yet-unrecognized issues. The SEI listens and probes intently to learn our sponsor's needs, so that our work provides a path to solving critical artificial intelligence (AI), software engineering, and cybersecurity issues.

In 2020, through the global COVID-19 pandemic, the SEI persisted in our mission to advance software as a strategic advantage for national security. We delivered excellence to our work sponsors by adapting ways to share our expertise and by safely meeting at our customers' sites, when in-person meetings were the best way to accomplish their aims.

In this *SEI Year in Review*, you'll read of some prominent 2020 results that express our loud and clear response:

- With funding and support by the Office of the Director of National Intelligence, the SEI is fostering a community to develop a discipline for AI engineering, to assure that AI-enabled systems are scalable, robust and secure, and human-centered.
- Having been at the forefront of software engineering technologies and practices for decades, we have launched an effort to build and lead a community that will form a national agenda to architect the future of software engineering and articulate a research roadmap.
- Continuing to bring together government and industry, we introduced the CERT/CC Vulnerability Information and Coordination Environment (VINCE) to increase the level of direct collaboration between vulnerability reporters, coordinators, and software vendors.

We are also loud and clear in our commitment to diversity, equity, and inclusion (DE&I) in our workforce and our workplace. We established an office to coordinate and advance our efforts to be a workplace where all employees have the opportunity to do their best work; be assured of fair treatment, access, opportunity, and advancement; and know how what they do matters to our organization and beyond.

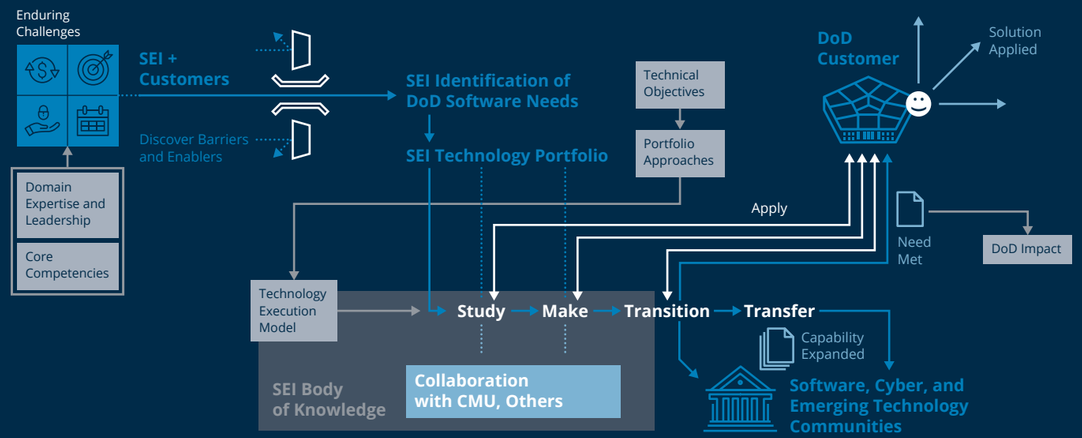
For our people and sponsors, we show that we receive their messages five by five and that our response is loud and clear.

Paul Nielsen

Execution Strategy

The SEI facilitates the transfer of research results to practice in Department of Defense (DoD) programs, the Office of the Secretary of Defense's science and technology initiatives, and non-DoD U.S. government organizations where improvements will also benefit the DoD. In doing so, we gain deeper insight into mission needs, insight that forms the basis for new research. In addition, we transition matured technologies more broadly to Defense Industrial Base organizations and others in the DoD software supply chain.

Through ongoing research and development and communication with customers, the SEI identifies priority areas for further research and development. Through our *study* approach, we generate academic and theoretical reports, presentations, and books on gaps or issues in those areas. We *make* software tools, processes, datasets, analytic approaches, and training materials to mitigate those gaps or issues. We combine our *body of knowledge* with external material and systems engineering to deliver, through *transition* and *transfer* activities, quantitative impact to a U.S. government organization, DoD organization, or DoD end user.



Funding Sources

In FY 2020, the SEI received funding from a variety of sources in the Department of Defense, civil agencies, and industry.

Table of Contents

Briefs

Researchers **Art Manion, Emily Sarneso, Jonathan Woytek**

CERT/CC's VINCE Platform Enables Collaboration on Software Vulnerabilities

The SEI's CERT Coordination Center (CERT/CC) debuted a web-based collaboration platform for coordinated vulnerability disclosure called the Vulnerability Information and Coordination Environment (VINCE) in June.

Sponsored primarily by the Department of Homeland Security Cybersecurity and Infrastructure Security Agency (CISA), CERT/CC is a hub for the discovery, reporting, disclosure, and mitigation of software vulnerabilities, especially those affecting safety, critical or internet infrastructure, or national security.

CERT/CC staff used to use encrypted email to distribute all communications manually among vulnerability reporters, researchers, and vendors. VINCE's peer-based interaction model uses a central, web-based platform so all stakeholders can collaborate directly with CERT/CC and each other.

With far fewer emails to shuffle, CERT/CC staff can concentrate on coordinating complex multi-vendor cases, analyzing vulnerabilities, and influencing standards and policy. "Finding, fixing, patching, and defending against vulnerabilities—we're trying to help others do it faster and better while lowering risk and cost," said Art Manion, the SEI's Vulnerability Analysis technical manager.

*As of early 2021, almost **400 vendors** and **1,000 users** had used VINCE to coordinate nearly **100 vulnerability cases.***

As of early 2021, almost 400 vendors and 1,000 users had used VINCE to coordinate nearly 100 vulnerability cases. CERT/CC is now working to enable communication universally among many such vulnerability coordination platforms.

To learn more about VINCE, visit **kb.cert.org/vince/**.

Researchers **Andrew Hoover, Gavin Jurecko, Katie Stewart, David Rossell**

CMMC Model and Guides Strengthen DoD Supply Chain Cybersecurity

In early 2020, the SEI and partner Johns Hopkins University Applied Physics Laboratory (APL), a university affiliated research center, released the initial version of the cybersecurity maturity model at the heart of the Cybersecurity Maturity Model Certification (CMMC) program. CMMC provides the Department of Defense (DoD) Office of the Under Secretary of Defense for Acquisition and Sustainment (OUSD(A&S)) with a powerful tool to improve risk-informed decisions and contractor security in the Defense Industrial Base (DIB) supply chain.

Over the following months, the SEI and APL developed the first two *CMMC Assessment Guides*, which the DoD released in late 2020. The guides' detailed discussions and references are intended to assist both supplier organizations and assessors in their certification preparation and review.

To learn more about the CMMC, visit **acq.osd.mil/cmmc/**.

Researcher **Matt Kaar**

SEI Supports Second Annual Cybersecurity Competition for Federal Workforce

The Department of Homeland Security Cybersecurity and Infrastructure Security Agency (CISA) selected the SEI to orchestrate the second annual President's Cup Cybersecurity Competition. The contest identifies, challenges, and recognizes talented cybersecurity professionals in the federal workforce.

The 2020 President's Cup attracted more than 1,400 individuals and nearly 250 teams from 19 departments and agencies.

The SEI grew the competition challenges and delivery software platform that it had developed for the 2019 competition. The 2020 open source challenges are available to all participants and the public for adaptation into cyber workforce instructional materials.

The 2020 President's Cup finals were held in February 2021. The winning team of cyberspace capability engineers from the 780th Military Intelligence Brigade scored the highest across both days of the teams competition and nearly fully solved all five final challenge scenarios.

Learn more at **cisa.gov/presidentscup**.

Photo: U.S. Army

Researchers **James Wessel, Michael Gagliardi, Daniel Plakosh**

Missile Defense Agency Appoints SEI to Technical Direction Agent

During 2020, the SEI was appointed to the Missile Defense Agency's (MDA) Technical Direction Agent (TDA), a group composed of representatives from multiple federally funded research and development centers that provide strategic MDA mission support. Because of the SEI's unique mission and an SEI team's past success in supporting the MDA's Ground-based Midcourse Defense (GMD) program, the agency named the SEI as the TDA GMD program lead for software engineering and cybersecurity. The appointment came after the SEI GMD Quality Attribute Workshop (QAW), whose final report was issued in February 2020. The QAW provided insights into the GMD software architecture.

As MDA GMD works to modernize its software development approach, the SEI is providing architecture, software, and cybersecurity support, including digital engineering and DevSecOps assistance, which incorporates advice regarding approach, infrastructure, procedures, and metrics.

Researcher **Scott McMillan**

Linear Algebra Graph Algorithms Approach C++ Standardization

A project headed by the SEI's Scott McMillan took a step in 2020 toward standardizing graph algorithm application development in C++.

The GraphBLAS, Basic Linear Algebra Subprograms for Graphs, is a community-driven, open programming specification for graph analysis. The specification makes the development of high-performance graph algorithms simpler and hardware agnostic by defining the algorithms in terms of higher-level linear algebraic operations.

"Graph computations are fundamental to many important defense and national security applications," said Matt Gaston, director of the SEI's Emerging Technology Center. These applications include logistics, intelligence, and mission planning. "GraphBLAS enables standardized and scalable development of graph applications as well as the ready adoption of future advanced computing capabilities."

In summer 2020, the SEI released version 3.0 of the GraphBLAS Template Library (GBTL), which adds functionality to the implementation of GraphBLAS in C++, one of the most common high-performance programming languages.

Originally intended to facilitate graph analysis, GraphBLAS has many potential applications thanks to its ability to perform a large class of linear algebra operations. The complexities of these operations, coupled with different matrix storage types, make the proposed GraphBLAS application programming interface (API) especially suited for efficient and maintainable implementation in C++.

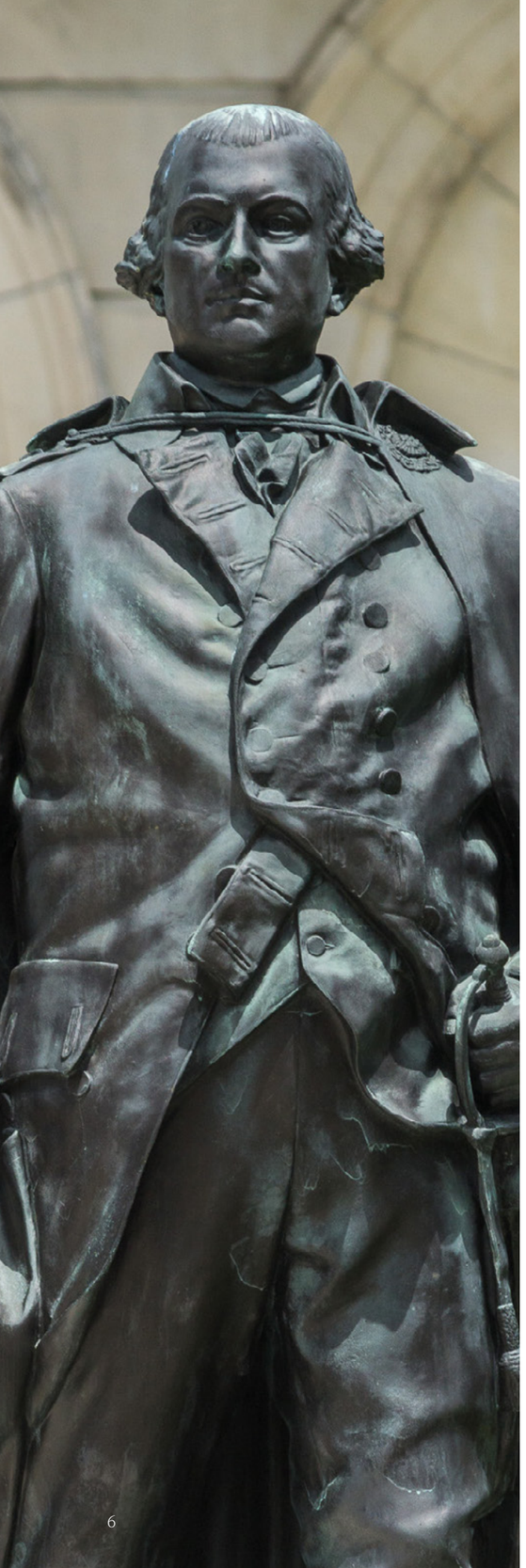
To learn more about GraphBLAS, visit **resources.sei.cmu.edu/library/asset-view.cfm?assetid=644365**.

Researchers **Julie Cohen, Shane Ficorilli, Forrest Shull**

SEI Research Contributes to DoD's Software Acquisition Pathway

The SEI reached a major milestone in its multiyear engagement with the Office of Acquisition Enablers within the Office of the Secretary of Defense when Ellen Lord, undersecretary of defense for acquisition and sustainment, signed Department of Defense (DoD) Instruction 5000.87, the formal issuance of the Software Acquisition Pathway on October 2, 2020. In support of the Deputy Assistant Secretary of Defense for Acquisition Enablers (DASD(AE)), the SEI's Forrest Shull, Shane Ficorilli, and Julie Cohen lent their expertise in evidence-based research to the development, piloting, testing, and updating of the policy. Their contributions helped speed delivery of the policy, which was released one year in advance of the deadline stipulated by Congress. "The team may have set a new acquisition policy conceptualization-to-publication record," said Lord in a media briefing.

The new policy aims to help the DoD acquire software with modern software practices, including Agile and DevSecOps, embracing innovative software solutions and delivering capabilities with a speed that matches the Department's dynamic mission needs. "Our goal with this pathway is to simplify the acquisition model to enable continuous integration and delivery of software capabilities to support the warfighter," said Lord in prepared remarks announcing the launch.



Editorial **Tom Longstaff**

An Integrated Vision of Software Engineering

SEI chief technology officer Tom Longstaff proposes a holistic future for software engineering.

"Logistics is the stuff that if you don't have enough of, the war will not be won as soon as." That quote from Nathanael Greene, major general of the Continental Army, is as true today as it was during the American Revolutionary War. Today's U.S. military relies ever more on software systems to protect our nation and our allies.

The software in the F-35 Lightning II fighter, to pick just one example, contains more than 8 million lines of code. While that software is just as vital to the aircraft as its propulsion system or integrated airframe, it is inherently different from those hardware components: more malleable and adaptable to new capabilities.

Software moves fast. The vital logistics that have supplied warfighters long before even Nathanael Greene's time must now account for digital materiel whose development, defense, and capabilities evolve more quickly than any other asset.

As the only federally funded research and development center dedicated to software, the SEI has long sought to make software a strategic advantage for national security. The nation's adversaries are pushing to erode that advantage. To stay ahead, we must stay at the forefront. Today, the SEI works at three leading edges of research:

- modernizing software development and acquisition
- attaining autonomous cyber operations and resilience
- realizing computational and algorithmic advantage

But software moves fast. In the next 5 to 10 years, even the meaningful attainment of these three objectives may not provide sufficiently responsive software systems. The warfighters in the Department of Defense (DoD) need their software-intensive tools to adapt to an ever-widening variety of operational scenarios and environments, including the mercurial terrain of cyber warfare.

The answer is not just more invention. The SEI must be the place that integrates model-based software engineering, modern acquisition, autonomous cyber resilience, and artificial intelligence—and areas yet to be explored. These all should be part of the way we develop, maintain, and sustain future software systems.

I envision a time in which formal modeling and resilient code work with all forms of rigorously engineered AI, in offensive- and defensive-cyber-operational environments, to operate and adapt faster than the adversary in every engagement. In this vision of a cyclical software pipeline, the models interpret telemetry on the dynamic landscape, needs, and events. The feedback updates the model to generate new environment code and data, execute within the tactical environment, gather more telemetry on the effectiveness of that execution, and give developers the chance to interpret this information and feed it back into the system. Autonomous environments, especially autonomous cyber environments, will enable repeatable empirical assessment of cyber mission readiness and capability.

Some DoD software programs are heading in a more agile direction. The Army Futures Command has been implementing the Architecture Analysis and Design Language (AADL) and associated tools in its Future Vertical Lift (FVL) programs, to reduce the costs of reimplementing theoretical concepts and retraining engineers, as well as to detect defects early.

Imagine if the FVL programs incorporated a cyclical, semi-automated software pipeline. Prototypes could be fielded, telemetry on system performance could gather data on performance weaknesses, and software updates could be quickly incorporated into the next iteration. We are not done until a missile in flight updates its software on the way to the target.

Integrating the strands of software, cybersecurity, and AI engineering will not be easy. Each strand is its own complex, robust domain that must be trustworthy, capable, affordable, and timely—the same four enduring challenges laid down by the DoD at the SEI's founding in 1984. The SEI has the expertise and the relationships with government, academia, and industry to forge this path.

Software moves fast. The SEI seeks partners who will make that next move with us, to merge today's best research into transformative systems that will make software a strategic advantage for national security.

Photo: U.S. Air Force

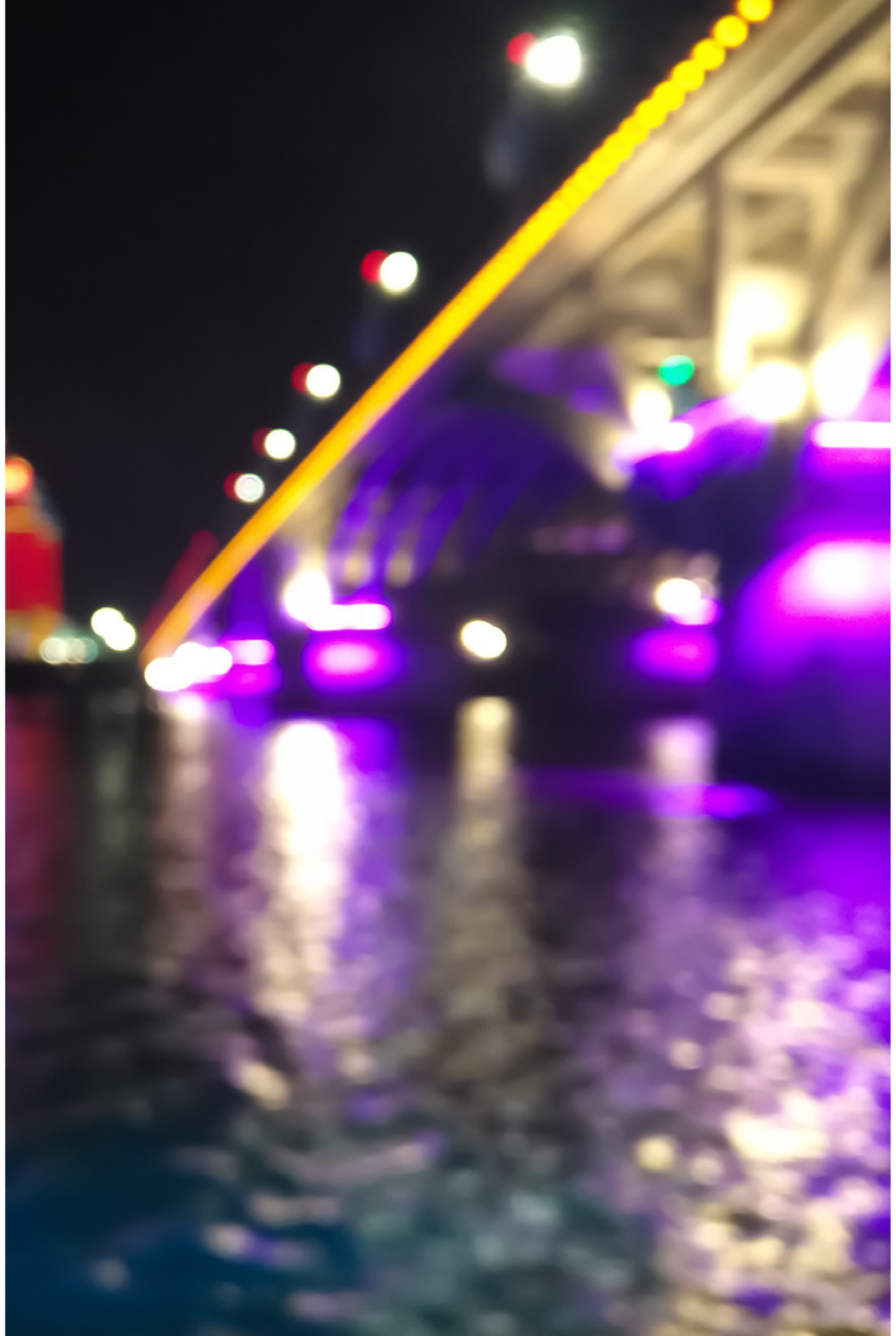
Researchers **Matt Gaston, Tanisha Smith, Frank Redner, Hollen Barmer, Alex Van Deusen, John Wohlbier, Jay Palat, Carol Smith, Rachel Dzombak, Tina Sciullo-Schade**

National Initiative Forges the Path to an Engineering Discipline for AI

In the global rush to harness the transformative potential of artificial intelligence (AI), most research and development has been devoted to creating capabilities. Little progress has been made in the engineering of those capabilities to ensure that they are safe and reliable. Current AI solutions, which are often speedily deployed and difficult to replicate, verify, and validate, could lead to unintended negative consequences.

As the Department of Defense (DoD) invests in this rapidly evolving field, it is prioritizing safe, ethical, and secure solutions that consider AI's characteristics and complexities. In 2020, DoD leadership tasked the Defense Innovation Board (DIB) with proposing principles to support this intent. The DIB set forth recommendations for AI practices that integrate ethics, help shape international norms, and mitigate potential harms as part of the DoD vision.

To further this vision, the Software Engineering Institute (SEI) will lead a National AI Engineering Initiative with funding and guidance from the Office of the Director of National Intelligence (ODNI). "We are leading a movement to advance this discipline in support of defense and national security," said Matt Gaston, the director of the SEI's Emerging Technology Center. "Our effort with ODNI will bring together organizations and experts working in AI engineering to achieve the goals of scalable, robust and secure, and human-centered AI." AI must be *scalable* so it can be adapted to a variety of problems and sizes of problems; *robust* and *secure* so that it behaves as expected and is difficult for adversaries to manipulate; and *human-centered* to account for ethics and the needs of human users.



This work grew out of an earlier effort to define AI engineering. In 2019, in response to a growing call for an engineering discipline for AI, the SEI convened the first workshop on AI Engineering for Defense and National Security. This event laid a foundation for identifying challenges and opportunities for future initiatives. Findings from the workshop, along with needs identified by the DoD in its AI Strategy and in the DIB principles, informed the goals of the SEI–ODNI national initiative.

Discussing AI at the SEI 2020 Research Review, Joint AI Center director Lt. Gen. Michael Groen stated, "This is a transformation that's coming. We've got the great academic base, the great industrial base for creative thinking and data engineering and AI application. This is our superpower as a nation. Let's leverage it and get out in front of the wave."

"This is a transformation that's coming. We've got the great academic base, the great industrial base for creative thinking and data engineering and AI application. This is our superpower as a nation. Let's leverage it and get out in front of the wave."

— Lt. Gen. Michael Groen, director, DoD Joint AI Center

The SEI plans to stay out front. It will engage organizations and experts working in AI engineering and will include research and development activities such as creating tools, practices, processes, and methods. It will capture lessons from the experiences of industry, academic, and defense researchers, developers, and implementers to promote the engineering of AI capabilities that can meet the needs and challenges of defense and national security.

Thirty years ago, Mary Shaw, a founder of the SEI and its former chief scientist, wrote in her SEI technical report *Prospects for an Engineering Discipline of Software* that the problems of current practice often stimulate the development of a corresponding science. "There are good grounds to expect that there will eventually be an engineering discipline of software." AI's prospects appear similarly strong on its path to a more disciplined maturity.

To learn more, visit **sei.cmu.edu/our-work/artificial-intelligence-engineering**.

Researcher **Rotem Guttman**

Game-Based Design Improves AI Support of Human Decision Making

Even the most advanced artificial intelligence (AI) system can fail if it does not meet the needs of its human operators. After observing several deployed AI decision support systems within federal and state governments and the Department of Defense (DoD), Rotem Guttman, a senior cybersecurity researcher at the SEI, noticed a common issue. “Humans make poor choices when deciding to rely on or ignore existing AI decision support systems,” he said. “In some cases, these systems are being wholly abandoned despite the fact that the underlying model was operating as designed.”

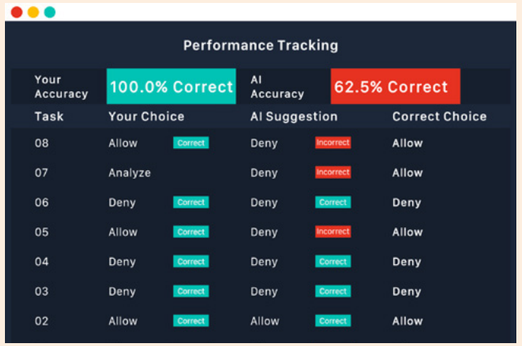
Perceiving that these systems failed to enable end users to intuitively understand and complete tasks, Guttman’s team worked to develop the Human-AI Decision Evaluation System (HADES), a test harness allowing researchers to collect human decision-making data on large sets of possible AI interfaces.

The team’s initial research indicated numerous factors that could be affecting AI system usability. They suspected that a failure to communicate model output meaningfully for the user could be contributing to poor decision making. The team identified more than 400 possible categories of interface design based on a set of candidate design elements. They needed a mechanism to determine which design practices would most affect decision making. Their goal was to develop a system for collecting data on real human decision making within a chosen domain and determine the appropriate best practices for AI system interface design for that domain.

To collect this data, a human would need to make the same type of decision over and over again with slightly different available information. “The problem is that humans aren’t machines and will very quickly tire of such a monotonous task,” noted Guttman.

The team realized that repeated decision making is a common characteristic of games, so they used game-based design techniques to reduce task fatigue and lack of interest. By opening up the HADES interface to game designers to allow integration with game environments, the system was able to collect players’ decision-making data in response to a variety of AI system advice.

As a test case, the SEI’s collaborators at Carnegie Mellon University’s Entertainment Technology Center developed a game that put approximately 350 players in the role of a system administrator making decisions about what software should be added to a software safelist. Depending on their assigned experimental condition, players received the AI’s recommendation in a simple summary or more detailed output. The system tracked what information the users chose to review, how long they spent on each element, and whether their final decision was correct or incorrect.



“Humans make poor choices when deciding to rely on or ignore existing AI decision support systems. In some cases, these systems are being wholly abandoned despite the fact that the underlying model was operating as designed.”

— Rotem Guttman, senior cybersecurity researcher, SEI CERT Division

One finding was that players trusted AI recommendations more when the stakes of the decision were higher, unless they were also given information about the AI’s degree of confidence. This kind of feedback on the quality of users’ decisions can be mapped back to the users’ recorded interactions with the system to determine what elements are promoting or preventing optimal decision making. Once a system design is selected and built, HADES can verify and validate that the system operates as intended when used by a human in the field.

HADES builds on previous SEI research that frames the entire AI system development process with a focus on the human. HADES can slot in an actual AI-enabled decision support system or simulate one, supporting multiple experimental designs to find the most intuitive one for end users prior to building the system. This key capability allows software acquirers to draft their system requirements with great accuracy. The same HADES harness can be connected to the delivered system to assure that it meets the specified design criteria, saving resources on both ends of the development cycle.

For now, HADES remains a prototype, but it could open a path for building government and DoD AI decision support systems that truly take the human into account.

To play the game yourself, go to **https://hades.cmusei.dev/**.

Researchers **Eric Heim, Jonathan Hoyle, Jacob Oaks, Alex Van Deusen**

Navigation Demonstration Flips the Script on Machine Learning in Naturalistic Scenarios

Intelligence, surveillance, and reconnaissance (ISR) missions frequently analyze activity-based intelligence about routine patterns of life, such as the daily movement of personnel and vehicles. Automating this time-intensive task would enable the reallocation of human analysis. Training machine-learning (ML) agents to analyze even tightly defined slices of the real world requires massive input of rules from human trainers.

The SEI recently released a demonstration of an ML method that allows ML agents to learn the norms of naturalistic behavior on its own. This inverse reinforcement learning (IRL) method predicts behavior and detects anomalies in open-world, naturalistic scenarios.

A common way to train an ML agent to complete a task is with reinforcement learning. For example, a programmer might teach a virtual, ML skeleton to walk by supplying rewards for certain outcomes, such as for forward movement, and penalties for others, such as falling, but no examples of correct behaviors. The ML agent tries many different behavior policies, keeps the ones reinforced by rewards, and eventually learns to walk. Some tasks, like autonomous driving, have far too many reward conditions—staying in the lane, stopping for pedestrians, and so on—for the programmer to re-create.

Inverse reinforcement learning flips the reinforcement-learning approach: programmers give the agent a dataset of policies, but no reward or penalty conditions. The agent observes the policies and infers the underlying rewards and penalties. Those are then fed into a reinforcement learning scheme to teach the agent the rewarded policies. The agent can then act and react in similar situations and, crucially, generalize to novel scenarios, too.

The SEI's demonstration of IRL used trajectory data of ships approaching New York Harbor to train an ML agent to plot its own course from anywhere nearby. Any trajectory might be influenced by an indefinite number of rewards. To narrow the field, the SEI told the model to commit most to policies that match observed trajectories and assume the least about trajectories it has not observed. This principle of maximum causal entropy (MCE) helps to keep the agent from drowning in a sea of potential actions and allows the IRL problem to be solvable.

Senior machine learning research scientist Eric Heim and his colleagues at the SEI say the IRL and MCE combination is well-suited to other naturalistic scenarios, such as satellite surveillance of areas where normal behaviors are not known. An ML agent would use IRL to observe, for instance, the movement of vehicles, infer rewards for routine vehicle trajectories, predict future movements, and flag observed abnormal movements.

Because IRL agents mimic the way people learn new patterns of behavior, Heim also believes IRL might be used to train computerized helpers. An ML agent might observe common ways users navigate and make choices in a computer application. Using IRL, the agent could determine the most likely outcome of any choice point and suggest it to beginner users, like having an expert at their side. "The benefit of using IRL for these tasks is that they're pretty robust," said Heim. "Even if they haven't seen the exact scenario before, these policies tend to generalize to a lot of different, maybe unseen tasks."

The adaptability of IRL opens ML to a range of applications.

> To learn more about IRL at the SEI, visit **sei.cmu.edu/our-work/projects/display.cfm?customel_datapageid_4050=201338**.

The SEI demo maps ship trajectories in New York Harbor.

Researchers **Grant Deffenbaugh, Shing-hon Lau, Chesleah Kribs, Brandon Marzik, Reggie Savoy, Alec Woods**

Network Simulations Evaluate AI-Powered Network Defense Products

The cybersecurity field is being challenged with attacks of ever-increasing number, speed, and scale. All the while, millions of cybersecurity positions needed to secure and monitor networks remain unfilled. To close this gap, organizations are turning to artificial intelligence (AI) to augment the cyber workforce and speed its response to attacks.

The growth of AI has produced a profitable industry of AI-powered network behavior analysis (NBA) products. Adoption of these devices is accelerating, with over 100 products now on the market. But threat actors know this too, and they are adapting their attack methods to evade AI-based defenses. Little research exists on evaluating how well AI-NBA devices really work. The SEI's Artificial Intelligence Defense Evaluation (AIDE) project, funded by the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency, is developing a rigorous, standardized methodology for testing AI defenses.

"A methodology for knowing if your system is secured as deployed is essential to secure operations," pointed out AIDE team co-lead Grant Deffenbaugh. "This is hard with AI systems because their state at any given moment is fluid, and the reasoning behind their conclusions is often opaque."

The AIDE team created a virtual environment that represented a typical corporate network, using an SEI-developed software framework called GHOSTS that simulates user behaviors to generate network traffic. This traffic was used to train two commercial AI-NBAs. The AIDE team performed baseline testing by emulating malicious activity, observing whether the AI-NBAs could detect it, without attempting to obfuscate that activity. Both AI-NBAs detected the malicious activity under the baseline conditions.

The team then made the test more difficult by obfuscating the malicious activity, altering the attack traffic patterns to match activities similar to the virtual users' job duties. Another test employed data poisoning, slowly introducing benign activities that generated traffic similar to that generated by the attack. This technique causes the AI-NBA to learn that attack traffic is normal traffic. Neither product was able to detect malicious activity in the presence of obfuscation or data poisoning. Results for both tests showed that a threat actor could use these methods to bypass detection on the network. AIDE team co-lead Shing-hon Lau surmised, "A sophisticated adversary could defeat the AI devices with a day or two of effort, and a state-level actor would have little trouble."

This method of testing an AI defense against an actual attack on a simulated network in operation is more realistic than presenting an AI-NBA with typical synthetic traffic. Lau said, "The big win of this project was testing a product as an organization would experience it, in the network it is protecting, while it is operating." Deffenbaugh added, "System administrators can use our approach to test a product in situ and verify that it behaves as expected."

"The big win of this project was testing a product as an organization would experience it, in the network it is protecting, while it is operating."

— Dr. Shing-hon Lau, senior cybersecurity researcher, SEI CERT Division

The results of this work could have broad applications. Using the methods developed in the SEI's AIDE project, the Department of Defense could evaluate AI defenses to determine their suitability for deployment on its networks or those of the Defense Industrial Base. Future work will include evaluating more AI-NBAs, types of attacks, and types of networks. The AIDE team seeks collaborators to meet those goals.

To learn more, watch a presentation about AIDE from the SEI 2020 Research Review at **resources.sei.cmu.edu/library/asset-view.cfm?assetid=651090**.

Photo: California Bureau of Land Management

Raw image Copyright 2019 Maxar/DigitalGlobe. Used under a Creative Commons Attribution-NonCommercial 4.0 license (CC BY-NC 4.0). Polygons added by Carnegie Mellon University Software Engineering Institute.

Researchers **Ritwik Gupta, Ricky Hosfelt, Eric Heim**

Wildfire Response Tests xView2 Damage Assessment Prototype

Assessing building damage is a critical first step when natural disasters strike. xView2, a machine-learning (ML) computer vision system, speeds this process by using satellite imagery to classify damage to structures. In a busy 2020 wildfire season, multiple disaster response agencies received an xView2 prototype for testing.

xView2 sprang from a Defense Innovation Unit (DIU) 2018 competition that focused on accelerating progress in four computer vision frontiers: reduce minimum resolution for detection, improve learning efficiency, enable discovery of more object classes, and improve detection of fine-grained classes. To build on this initial work, xView2 contestants built ML algorithms that scanned satellite photos of disaster-struck areas and classified building damage.

An SEI team worked with the DIU team to create the challenge, the baseline ML models, a building damage scale, and xBD, a database of satellite photos with human-labeled building damage, against which competitors' ML results would be judged. After the competition, the SEI packaged the best ML models into a prototype tool.

> *"Generally speaking, an analyst would take an entire day or two to clear a large fire area [...] xView could assess it in less than 10-20 minutes."*
>
> — Chief Manuel Villalba, intelligence analyst, California National Guard

In 2020, the California National Guard preliminarily tested the xView2 prototype during the massive August Complex fire and smaller Valley fire. "Generally speaking, an analyst would take an entire day or two to clear a large fire area containing hundreds of structures," said Chief Manuel Villalba, a California National Guard intelligence analyst specializing in wildfires. "According to our testing, it's possible xView could assess it in less than 10-20 minutes."

To learn more about xView2, visit **sei.cmu.edu/our-work/projects/display.cfm?customel_datapageid_4050=295280**.

Researchers **Philip Bianco, Michael Bandor, Mario Benitez, Jeff Boleng, Bryce Meyer, Timothy Morrow, Jake Tanenbaum**

Enabling the Advanced Battle Management System Vision through Architecture

The Air Force Advanced Battle Management System (ABMS) is the Air Force's approach to the Joint All Domain Command and Control (JADC2) effort to digitally connect different elements of U.S. military operations. ABMS aims to provide strategic advantage to the warfighter by enabling machine-to-machine data exchanges across systems and integrating existing systems, from sensors to shooters, with new technologies. All this must be done across all five warfighting domains: air, land, sea, space, and cyberspace. Software is central to achieving these goals.

Department of the Air Force ABMS efforts in 2020 involved more than 70 industry partners, 65 government teams, 33 platforms spanning 28 product lines, and hundreds of new and legacy systems and nodes managed across a large number of programs. ABMS is building out new capabilities and software infrastructure to deliver technical solutions in a way that balances diverse but critical qualities, such as resilience, predictability, and integrability. Managing this degree of complexity and coordination requires an effective architecture.

The SEI has demonstrated decades of leadership in software architecture, developing techniques that have been used across the DoD to remove ambiguities in architecturally significant requirements and design architectures that satisfy these requirements. The SEI was selected by the Department of the Air Force to help inform the ABMS architecture.

Top ABMS concerns include seamless communication across heterogenous software stacks and platforms throughout the Air Force and Space Force, and the need to integrate and process data across all five warfighting domains. These concerns will drive ABMS' most significant architecture requirements.

Photo: U.S. Air Force

Specifically, the SEI has been working on

- making mission goals, critical quality attributes, key enablers, and key capabilities explicit to enable consistent, informed reasoning about architectural trade-offs
- eliciting and prioritizing operational and developmental quality attribute requirements to guide architectural decisions for ABMS
- guiding ABMS stakeholders through the creation of key mission threads to clarify how ABMS products fit together for end-to-end capability and to guide creation of capability needs statements
- refining architecture views for an ABMS instance architecture to document allocation of responsibilities across product teams and enable analysis of duplication and gaps among product responsibilities
- identifying standards that promote interoperability and open architectures critical to enabling the ABMS vision of providing a military Internet of Things to the warfighters

The goal of these efforts is to help ABMS use architecture as a tool to

- iteratively refine the definition of ABMS itself to provide growing clarity to teams working across the ABMS ecosystem
- promote efficient collaboration and interoperation within the ABMS ecosystem
- analyze suitability of foundational decisions (e.g., common infrastructure) for long-term ABMS success, including operational and developmental perspectives
- make decisions that ease migration of existing systems into the ABMS ecosystem

"Proactive efforts to iteratively refine the ABMS architecture will help balance rapid capability delivery with long-term sustainability and broad adoption," said Philip Bianco, technical lead for the SEI's ABMS support.

Researchers **David Graham, Eric Heim, Jon Helland, Rob McCarthy, Hayden Moore, Jose Andre Morales, Jay Palat, Carol Smith, Alex Van Deusen, Jordan Widjaja, Oren Wright**

AI Collaboration Supports U.S. Army Operations

Artificial intelligence (AI) holds the potential to transform modern warfare through new methods of analyzing data. AI tools could analyze the datasets that U.S. Armed Forces collect from the battlefield, for example, to generate a game-changing perspective on the environment.

To develop these kinds of capabilities, the Army selected Carnegie Mellon University (CMU) to become the hub of the U.S. Army's Artificial Intelligence Task Force (AITF). CMU will help the Army develop technical solutions to improve its operations, as well as connect the Army to the AI community in both academia and industry. The SEI is positioned to play a key role in these efforts thanks to its close collaboration with CMU in the field of AI and its experience developing AI solutions for the Department of Defense (DoD).

In 2019, the SEI began to support the AITF in a number of projects. In one such project, the SEI is designing and carrying out experiments with novel system features to support and facilitate the development of a DoD-wide central platform called COEUS. The aim of COEUS is to enable the development and deployment of AI capabilities faster than previously possible. COEUS provides a way to collect usable data—often in real time as it comes in from the field—curate it, use it to effectively train AI models, and deploy them quickly as threats emerge.

In 2020, the SEI drafted the initial system design for COEUS and carried out proof-of-concept experiments that resulted in usable implementations of novel COEUS architectural and system features to inform the platform's further development.

The SEI is also supporting the AITF through a collaboration with CMU's National Robotics Engineering Center (NREC) on a team of autonomous air and ground vehicles that can sense threats in an area of interest to build situational awareness without exposing personnel to dangerous situations. The project enables sensorized vehicles to recognize important information from the data they collect, including the presence of possible threats and their location, all without intervention from the personnel operating the vehicles. To collect the sensor data needed to train the underlying AI models, the SEI helped to collect training data at several locations. After processing this data, the SEI trained the models and evaluated the system's object recognition algorithms.

SEI experts are exploring ways for the AITF's autonomous sensors to more rapidly update AI models in the field, without a reliance on high-bandwidth network connectivity. The goal is to replace the multi-week AI model updating and deployment process with a process that lasts one day or less. Additionally, the SEI is developing an interface that will make it more intuitive to go through the data and machine learning operations process, making it more streamlined and efficient.

Members of CMU's NREC set up equipment during a data collection event at Fort Hunter Liggett.

Photo: U.S. Army

> *"The SEI is a strategic partner and continues to grow its relationship with the Army Force Modernization Enterprise."*
>
> — AITF spokesperson

"The SEI is a strategic partner and continues to grow its relationship with the Army Force Modernization Enterprise," said an AITF spokesperson. "They fulfill a critical role with their ability to solve technical challenges in areas specific to the DoD and bridge developments that are not mature enough for industry but are more directed than generalizable basic research. This is critical with the rate of learning in many areas of application for AI technologies."

Researchers **Lori Flynn, Will Klieber, Matthew Churilla, Shane Ficorilli, Michael McCall, Ebonie McNeil, David Shepard, Matthew Sisk, Ryan Steele, David Svoboda, Joseph Yankel, Hasan Yasar**

Improving the Security of Software Code

Software vulnerabilities constitute a major threat to the Department of Defense's (DoD's) ability to secure its information and assure mission success. Today's software assurance tools and approaches cannot address the vulnerabilities in the DoD's huge volume of code, especially under-supported legacy software.

"The SEI's Secure Coding team has led the development of secure coding practices and standards," explained Bob Schiela, Cybersecurity Foundations technical manager, "as well as tools and practices for auditing software source code to identify and mitigate security flaws." This team's work includes improving the efficiency and efficacy of security flaw resolution. Two lines of research include automated code repair and improved static analysis result adjudication.

The Secure Coding team's automated code repair tools find and repair specific types of common security flaws in source code, avoiding painstaking verification and repair by human analysts and developers. Automated code repair is especially helpful for maintaining the security of legacy software.

The team wrapped up its Automated Code Repair to Ensure Memory Safety project in 2020. The tool they developed tracks the boundaries of allocated memory and checks that a pointer is within bounds before using it to access memory.

To evaluate the tool, the team used a software verification tool to compare code from Competition on Software Verification (SV-COMP) benchmarks before and after automated repairs were applied. Principal investigator Will Klieber explained, "Before the repairs, the tool couldn't verify any benchmarks as safe, and it found that over 90 percent were unsafe. After the repairs, the tool verified that more than 50 percent were safe, and it did not find any to be unsafe." The team then added an option to reduce the tool's overhead from 50 percent to 6 percent by repairing only lines flagged as problematic by a third-party tool. Software developers and sustainers could use these tools before building their software to eliminate critical memory-safety defects, which could allow an attacker to take control of a system.

In the second line of research, the SEI has been developing a machine-learning-based method to automatically classify and prioritize results from static analysis tools. This Rapid Adjudication of Static Analysis Alerts During Continuous Integration method helps auditors and coders address large volumes of results with less effort.

Different static analysis tools find different types of defects, and these tools miss defects, misidentify defects, or both. To increase their coverage, analysts generally use multiple tools. However, this approach typically produces more results than can be manually adjudicated. These results are often not analyzed, leaving defects that are not found and fixed. To address this problem, the Secure Coding team is using machine learning classifiers to increase the efficiency of adjudication. Using information from previous manual adjudications, the team trained the classifiers to automatically predict a confidence that new results are likely true or false. Analysts will be able to use this new confidence to prioritize their reviews and help ensure that likely defects are addressed.

"In 2020, we added design and implementation changes to the SEI's SCAIFE and SCALe tools to address challenges to using static analysis classifiers in continuous integration environments."

— Lori Flynn, senior software security engineer, SEI CERT Division

"In 2020, we added design and implementation changes to the SEI's SCAIFE [Source Code Analysis Integrated Framework Environment] and SCALe [Secure Code Analysis Lab] tools to address challenges to using static analysis classifiers in continuous integration environments," explained Lori Flynn, principal investigator of this research. For example, the SCAIFE and SCALe systems have been modified to enable external tools to automatically trigger evaluations and generate reports. In the coming year, the team will have SCAIFE integrated and running within a continuous integration environment.

The Secure Coding team is exploring how to incorporate both methods into the software development lifecycle to improve software assurance. With a large body of mission-critical software, including many legacy systems, the DoD stands to benefit from more accurate, thorough, and automated ways of addressing vulnerabilities. Schiela explained, "Combining automated code repair and machine learning classifiers to separate static analysis results into categories that support increased levels of automation promises to significantly improve the efficiency of fielding assured software."

To learn more about the SEI's work in secure development, visit **sei.cmu.edu/our-work/secure-development**.

Researchers **Jonathan Frederick, Brandon Grech, Nick Winski, Toby Meyer, William Reed, Alexander Corn, Robert Beveridge, Dennis Allen**

Virtual Exercise Trains Air Force Mission Defense Teams for Cyber Attacks

As interconnected systems of software and networks have brought the Air Force cutting-edge weapons systems, they have also introduced vulnerabilities to cyber attack. In 2016, to focus on the cybersecurity of some of the Air Force's most important missions, the Secretary of the Air Force and Chief of Staff of the Air Force directed the establishment of new cyber squadrons to provide mission assurance. The SEI capped its support for these Mission Defense Teams (MDTs) with 2020's Sentinel Reign IV, a globally distributed, multiparty cyber defense and correlation exercise.

MDTs proactively defend Air Force missions, networks, and weapons systems from cyber attacks. Over the past four years, the SEI's support of the Air Force Space Command and, later, the Air Combat Command (ACC) has prepared traditional communications squadrons for their new MDT responsibilities. ACC chose the SEI for its proven ability to meet delivery requirements and facilitate realistic war-gaming. SEI team lead Dennis Allen explained, "Our experience building complex virtual networks, instrumenting them with cyber tools, and rapidly transforming requirements into solutions makes us a valuable partner for the Air Force and other services."

The SEI's Cyberforce web-based training platform formed the backbone of the ACC's Sentinel Reign IV, conducted in August 2020. This coordinated cyber-defense exercise assembled MDTs, the ACC's Cyber Defense Correlation Cell (CDCC), Intelligence Support Squadrons, Operations Centers, and the Cyber Resiliency Office for Weapons Systems. Notional wing commanders and aircraft maintenance personnel were also used to refine workflows, develop incident handling procedures, and improve communication strategies. Training scenarios included nation-state adversaries targeting critical mission systems. Each scenario involved a complex set of threats designed to provide hands-on experience-building opportunities for MDTs.

1st Lt. Vaughn, 432nd ACMS MDT officer in charge, and 2nd Lt. Eric, 432nd ACMS MDT assistant officer in charge, review computer code together.

Photo: U.S. Air Force

Sentinel Reign IV was the culmination of years of SEI support for the MDT program. In 2017, the SEI developed an MDT training curriculum, consisting of courses, video-based training, knowledge-based assessments, and hands-on mission rehearsal exercises. The curriculum became a required part of the MDTs' Initial Qualification Training. Within 18 months, more than 2,300 Air Force MDT users had accessed this content and taken more than 70,000 hours of training. Over the next three years, the SEI grew the MDT mission rehearsal capabilities to incorporate a virtualized Air Force Cyberspace Vulnerability Assessment/Hunter (CVA/H) weapons system; notional F-22, F-16, and Airborne Warning and Control System aircraft simulators; and an Air Operations Center.

"The SEI has been extremely instrumental in providing high-speed and succinct development of virtual training environments and online applications to get our MDTs to mission-ready status," said Brig. Gen. Chad Raduege, director of cyberspace and information dominance and chief information officer at the Air Force's Headquarters ACC. "The simulated aircraft model used in the Sentinel Reign IV exercise to prove the effectiveness of the CDCC is very impressive and will allow wing commanders across ACC to improve cyber defense capabilities, increase overall wing cyber threat awareness, and let commanders make informed decisions about cyber defense."

"The SEI has been extremely instrumental in providing high-speed and succinct development of virtual training environments and online applications to get our MDTs to mission-ready status."

— Brigadier General Chad Raduege, director of cyberspace and information dominance & chief information officer, Air Force's Headquarters ACC

The web-based Cyberforce platform enabled five MDTs and other supporting groups, totaling more than 100 people across the globe, to participate and collaborate in the Sentinel Reign IV exercise virtually during COVID-19 travel restrictions. Post-exercise, MDTs can replay each threat scenario, on-demand, within Cyberforce.

The solutions the SEI built for the Air Force are available within Cyberforce for other Department of Defense (DoD) organizations. Many of the open source tools the SEI used to create and deliver these impactful solutions are available in the SEI's GitHub repository.

In future work, the SEI team plans to improve modeling and simulation prototypes, integrate different weapons systems, expand the threat inject library, and transition technologies that enable mission rehearsal exercises for the ACC and other DoD organizations.

- Explore the SEI's GitHub repository at **github.com/cmu-sei**.

Researchers **John Wohlbier, David Graham, Annika Horgan, John Kirchenbauer, Scott McMillan, Oren Wright**

Software-Defined Hardware Helps DARPA Reinvent Microelectronics Manufacturing

The Department of Defense (DoD) faces two crises in microelectronics: lack of American manufacturing capacity and hardware limitations for data-centric AI applications. Offshore manufacturing limits the United States' ability to make critical components for national defense, introduces supply chain issues, and increases the risk of vulnerabilities. Meanwhile, widening adoption of machine learning (ML) applications for analysis, logistics, intelligence, and other data-centric tasks is rapidly boosting the cost and complexity of microelectronics optimized for these computationally intensive applications.

"The performers in the DARPA ERI programs are of extremely high quality, in many cases the best in the world. We get the opportunity to help improve the technology not just from one group, but from several groups across several programs."

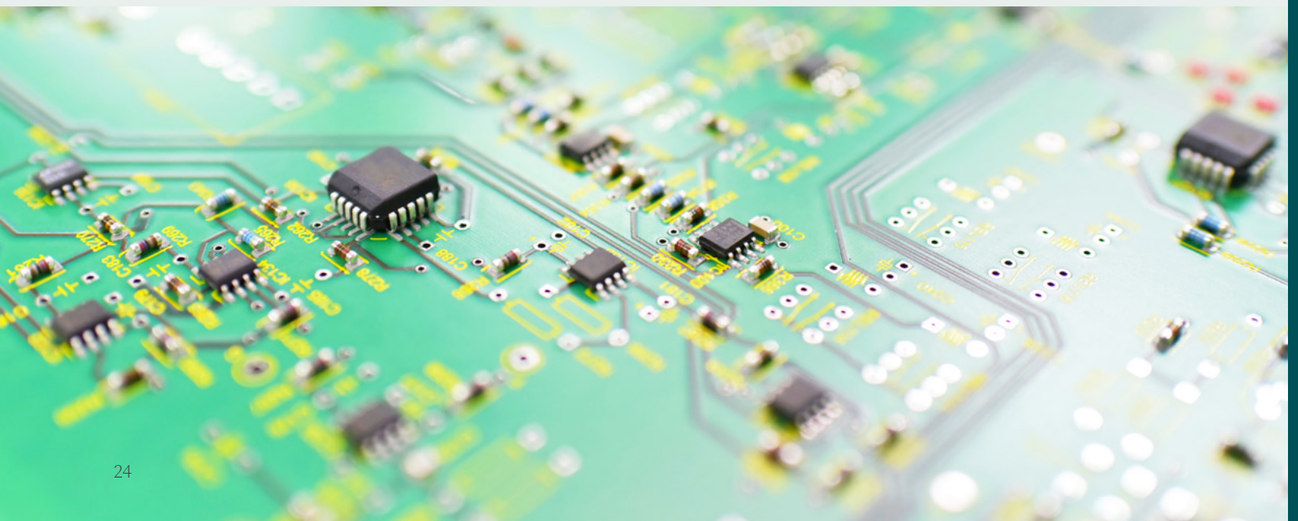
— John Wohlbier, senior research scientist, SEI Emerging Technology Center

The SEI joined with the Defense Advanced Research Projects Agency (DARPA) to tackle these two challenges. DARPA's Electronics Resurgence Initiative (ERI) is a 5-year, $1.5 billion initiative to revive microelectronics production in the United States, decrease hardware design and manufacturing costs, and optimize hardware for computationally intensive applications.

"The performers in the DARPA ERI programs are of extremely high quality, in many cases the best in the world," said John Wohlbier, a senior research scientist at the SEI. "We get the opportunity to help improve the technology not just from one group, but from several groups across several programs."

Researchers from the SEI are working on new methods to evaluate hardware-software codesigns for individual applications and entire operational domains. Hardware-software codesign involves concurrently designing the hardware and software components of electronic systems. This process optimizes their performance under given size, weight, and power (SWaP) constraints. While hardware-software codesign is not a new concept, it is getting a fresh look due to the high demands that AI systems make on hardware.

Contributing to the ERI programs requires knowledge and expertise across the entire technology stack, including algorithmic applications such as graph analytics and machine learning; high-level programming languages such as Python, C, and C++; and compiler technologies, including abstract syntax trees and intermediate representations. It also requires knowledge of low-level language concepts such as assembler and instruction set architectures, as well as hardware ideas such as cycle-level performance considerations and design tools. Most organizations cannot field a team with such a broad skill set.



"Hardware-software codesign is a critical concept in designing systems for machine learning to enable better performance at lower power," said DARPA's Tom Rondeau, program manager for DARPA ERI's Domain-Specific System on Chip (DSSoC) program. The SEI is helping DSSoC's test and evaluation team. DSSoC is developing a system-on-chip (SoC) to improve software performance within an operational domain. Applications within a domain have similar functional and system requirements. A processor tuned to the domain's requirements would run the domain's applications more efficiently than a general-purpose processor, without the difficulty and cost of building application-specific processors.

In contrast, the ERI's Software Defined Hardware (SDH) program targets applications, including graph analytics, graph neural networks, and convolutional neural networks. Participants in the SDH program codesign hardware and software systems that reconfigure themselves in real time as they process application workloads. This adaptability enables performance that is nearly as good as Application Specific Integrated Circuits (ASICs) while maintaining programmability for data-intensive algorithms.

The SEI's SDH team benchmarks DoD data-intensive mission workflows on a baseline platform. Team members evaluate the participants' hardware and software platforms to determine the best architecture to process complex, data-intensive applications. The team's results help DARPA decide which ERI software-defined hardware platforms to fund.

The SEI's feedback on DSSoC and SDH improves the tools used by DARPA ERI participants, leading to better designs. Its input drives DARPA's decisions about investments in future computing architectures.

To support this work, the SEI organized the Software-Hardware Codesign for Machine Learning Workloads workshop at MLSys 2020 in Austin, Texas. It featured talks from DARPA, startup companies for AI hardware, universities, national laboratories, and established chip vendors. "The timely hardware-software codesign workshop allowed us to communicate with an impressive list of speakers and attendees that will help us further expand our engagement with this community," said Rondeau.

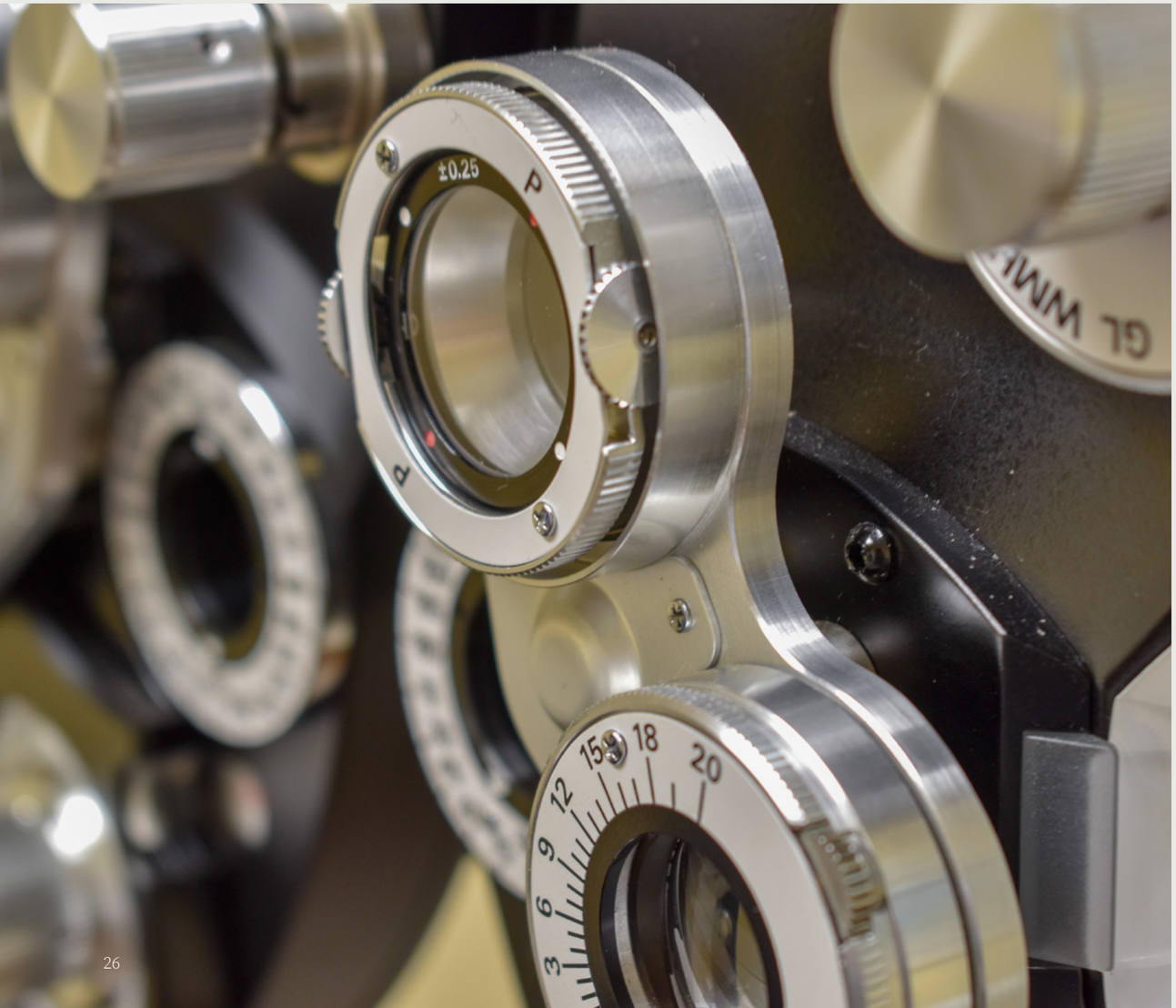
Researchers **Edwin Morris, Keegan Williams, Nathan West, Joseph Yankel, Jeffery Hansen, Rachel Brower-Sinning, Jeffrey Hamed**

SEI Lends Expertise to OSD Effort on Resilient Situational Awareness Systems

In today's environment, the Department of Defense (DoD) has access to more data than ever. But how can it quickly turn these huge volumes of data from numerous and diverse sources into verified, actionable intelligence useful to warfighters in the field? And how can it ensure the systems responsible for processing this data remain operative under adverse conditions?

The SEI is engaging in two efforts to increase DoD situational awareness. The first is an artificial intelligence (AI) engineering collaboration with the Defense Threat Reduction Agency (DTRA). The team produced a system called Cornerstone.

"Cornerstone uses AI to extract information from public data sources and transfer it to a system called the Biological Materials Information Program," explained Edwin Morris, a senior member of the SEI technical staff who leads part of the team supporting this effort. "That system contains information about facilities around the world that are using dangerous pathogens." For example, Cornerstone is capable of providing historical information about pathogens in laboratories and also providing near-real-time surveillance of disease outbreaks at locations around the world.



Under the hood, Cornerstone's natural-language processing (NLP) models are embedded in a flexible, SEI-developed architecture that makes it easy to change data sources, machine-learning (ML) algorithms, and data consumers. It also uses innovative self-monitoring that checks the ML algorithms and other system components for failures. The result is a situational awareness system that, by utilizing DevSecOps methodologies and containerization technologies, enables automated deployment and redeployment of the system.

The second SEI activity leverages Cornerstone's self-monitoring capability to make situational awareness systems more resilient to failures. This resilience engineering project is creating a prototype that ingests data about the state of system components, including ML algorithms, infrastructure, and cybersecurity status, and then uses that data along with a system model to reason about the state of the executing system.

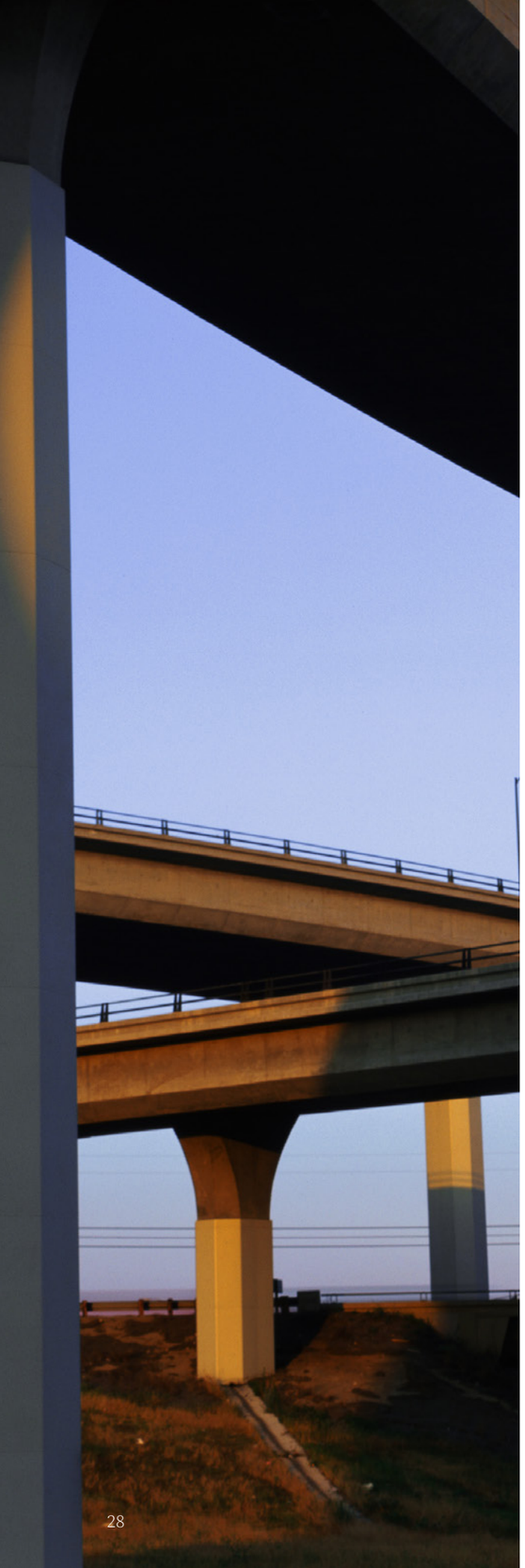
In ongoing work, the SEI team will use the system model and state to determine when the system is in danger of failing and automatically direct activities to restore the system, such as retraining ML algorithms or rebuilding and redeploying the system. To demonstrate the resilience capability, the SEI will enhance Cornerstone with additional self-monitoring capabilities, develop a system model that uses the resulting data to determine when intervention is necessary, and automate processing to restore the system to the necessary level of operation. If successful, the approach can be applied to ensure that situational awareness systems continue delivering critical intelligence to warfighters and other fielded DoD personnel, even in adverse conditions.

"The goal is to provide a simple way for others to construct resilient, ML-enabled systems using this pattern."

— Edwin Morris, senior member of technical staff, SEI Software Solutions Division

Morris hopes this resilience capability, as well as the flexible architecture developed for Cornerstone, can be used to improve other situational awareness systems. "The goal is to provide a simple way for others to construct resilient, ML-enabled systems using this pattern," he said.

To learn more about situational awareness work at the SEI, visit **sei.cmu.edu/our-work/situational-awareness/**.



Researchers **Hasan Yasar, Joseph Yankel, Shane Ficorilli**

DevSecOps Speeds Artificial Intelligence and Machine Learning Capability

The threat landscape for the Department of Defense (DoD) is constantly changing, as are the capabilities of the United States' adversaries. To keep pace and advance, the DoD must further modernize, automate, and secure its defense software engineering practices.

Hasan Yasar, SEI technical director, Continuous Deployment of Capability, and his team promote this effort, providing expertise for implementation of Development Security Operations (DevSecOps) in the DoD. Yasar works closely with Nicolas Chaillan, Air Force chief software officer and co-lead of the DoD Enterprise DevSecOps initiative. Applying this approach to harness the power of artificial intelligence (AI) and machine learning (ML) is a DoD priority. Air Force missions, in particular, sometimes depend on capturing and processing real-time data streams, a task well suited to AI/ML systems.

Traditional software projects involve writing, testing, and release of code into production. AI/ML projects present additional complexity. Among other challenges, they require collecting, ingesting, analyzing, and sanitizing data so that data scientists can train the model that will be used in the application production environment.

The industry currently holds heavy technical debt in AI/ML systems deployment, with a 75 percent failure rate. "While their model generation is working well, organizations are failing seriously in deploying to the production environment," said Yasar. "We have been starting to see successful deployment of ML systems along with the elevation and validation of the model, such as running Kubernetes-based AI components on U2 Dragon Lady Aircraft. DevSecOps is helping to speed model deployment; increase accuracy; enable reusability, traceability, and continuous feedback; and eliminate technical debt."

DevSecOps is an iterative, incremental approach using Agile methods. It emphasizes collaboration, eliminates process constraints to enable continuous workflow and delivery, and involves powerful tools working in an automated pipeline. Security is built into the process.

> *"DevSecOps is helping to speed model deployment; increase accuracy; enable reusability, traceability, and continuous feedback; and eliminate technical debt."*
>
> — Hasan Yasar, technical director, Continuous Deployment of Capability, SEI Software Solutions Division

The DevSecOps best practice of continuation technologies facilitates the AI/ML lifecycle. Continuous automated testing, monitoring, and validation enable continuous integration of developers' merged changes, automated release to production, and continuous automated deployment to the customer. The automated phases drastically reduce time to deployment, which is crucial to the DoD mission.

In 2020, the SEI contributed DevSecOps automation to multiple DoD AI/ML projects. In one of them, the SEI developed an AI/ML deployment pipeline in which DevSecOps significantly speeded data collection and generation as well as feedback collection from end users.

Another DoD priority alignment was between AI/ML system development and deployment methods and the DoD DevSecOps Enterprise framework. Yasar's team documented and formalized those methods and advanced the framework in the *Guide to Implementing DevSecOps for a System of Systems in Highly Regulated Environments*, a comprehensive roadmap to effective DevSecOps implementation. The team improved the guidelines for continuous authorization—the process that continually monitors the system to ensure compliance with requirements—by making it more secure and DevSecOps friendly.

To help determine an organization's fitness for adopting DevSecOps, Yasar's team developed two assessment instruments, to be released in 2021: the DevSecOps Assessment and the self-assessment version, *Software Assurance Guidance Evaluation (SAGE) Tool*. The SEI is the first federally funded research and development center (FFRDC) to offer such an assessment, which aids in setting an organization's expectations and detecting possible problems and impediments.

To learn more about DevSecOps, visit **sei.cmu.edu/our-work/devsecops**.

Researchers **Jerome Hugues, Anton Hristozov, John Hudak, Joseph Yankel**

TwinOps Combines Digital Twins and DevOps for Better Cyber-Physical Systems

Cyber-physical systems (CPS), which intertwine software and mechanical components, integrate computation, networking, physical objects and processes, and human proficiency. Multiple engineering, validation and verification (V&V), and testing challenges complicate every stage of CPS development, from capturing system requirements to building a solution that functions as designed and is fit for purpose.

"Currently, CPS engineering relies on models built in isolation, limiting in-depth unit and integration testing until the system is done," explained Jerome Hugues, senior architecture researcher at the SEI. "This isolation could produce imprecise characterizations of system behavior that may lead to accidents," he said, referring to recent failures in airliners and autonomous vehicles.

Hugues cites unmanned aerial vehicles (UAVs) as a modern CPS beset by complex development and testing challenges. Traditional modeling may not properly capture key issues such as sensor timing jitter or bias, or imprecise component behaviors that affect function, safety, and security. Issues could still appear late in testing—or even after the system has been deployed.

To improve CPS analysis and testing, Hugues and his colleagues combined the SEI's expertise in model-based engineering (MBE) and DevOps to efficiently deliver systems with increased quality. This solution, dubbed TwinOps, proposes a process that unifies MBE, digital twins, and DevOps practices in a uniform workflow.

MBE relies on models as first-class artifacts to analyze, simulate, and ultimately generate parts of a system. Creating digital twins simulates in software the operation of a physical system to streamline testing and iteration of novel technologies. DevOps focuses on software engineering activities, from early development to integration and improvement through the monitoring of the system at run time.

By combining these techniques with prior research on the Architectural Analysis Design Language (AADL), a standardized architecture description language, and the Open Source AADL Tool Environment (OSATE), the SEI was able to develop digital doppelgangers of systems to improve the CPS engineering process. "We combined DevOps and model-based engineering to ease the construction and deployment of simulation test benches and digital twins," said Hugues. "TwinOps combines system, software, and physical models to improve system understandings."

Hugues and his colleagues on the TwinOps project used AADL and the Architecture Centric Virtual Integration Process (ACVIP), along with SysML models, models of the environment, and an Internet-of-Things platform, to address both system and software concerns such as safety, security, performance, and code generation. "Analytical frameworks based on AADL were able to evaluate system integrability prior to actual integration testing, reducing the possibility of errors," noted Hugues.

"TwinOps combines system, software, and physical models to improve system understandings."

— Jerome Hugues, senior architecture researcher, SEI Software Solutions Division

This research's contributions are two-fold. First, it introduced ModDevOps as an innovative approach to bridging MBE and software engineering using DevOps concepts and code generation from models. ModDevOps smooths the transition from model-level V&V to software production. Second, the research developed TwinOps, a specific ModDevOps pipeline that equips system engineers with new analysis capabilities through the careful combinations of model artifacts as they are built. Adding a digital twin capability to ModDevOps could reduce cost and risk to Department of Defense programs requiring embedded software-hardware integration, such as the U.S. Army's Future Vertical Lift program.

TwinOps extends the SEI's research into improving both the state of the art and the state of the practice of designing and analyzing CPS. It builds on the SEI's expertise in DevOps and MBE by reusing and combining available tools in new ways, developing a pipeline to build better solutions.

To learn more about TwinOps, visit **resources.sei.cmu.edu/library/asset-view.cfm?assetid=651118**.

Researchers **Anita Carleton, John Robert, Mark Klein, Forrest Shull, Doug Schmidt, John Foreman, Charlie Holland, Jeff Boleng, Ipek Ozkaya**

Architecting the Future of Software Engineering

Software has become more complex, pervasive, and essential to the defense and national security of our nation. Individuals, organizations, entire industries, and governments depend on software almost as much as they do electricity, and today most new Department of Defense (DoD) capability is delivered through software. Our ever-growing dependence on software systems makes it imperative to maintain our nation's leadership and strategic advantage in software engineering.

To spur a national discussion that can inform the future direction of the field, the SEI is leading an effort to redefine how software is developed. "We're thinking about where the field of software engineering is headed and the new development and architectural paradigms it will take to get there," said Anita Carleton, director of the SEI's Software Solutions Division and head of the SEI's effort.

"We're thinking about where the field of software engineering is headed and the new development and architectural paradigms it will take to get there."

— Anita Carleton, director, SEI Software Solutions Division

Rapidly deploying software with confidence requires fundamental shifts in software engineering. How will these new types of systems push beyond the bounds of what current software engineering theories, tools, and practices can support? Based on where we are today, where will innovation take us in the next 5, 10, or 20 years? And what do we need to do to prepare for those futures?

The SEI has been engaging experts from across the entire software engineering ecosystem to answer these questions. One key event, which the SEI conducted in collaboration with DARPA, was the Software Engineering Grand Challenges and Future Visions Workshop. This event promoted a discussion among leading researchers, practitioners, and government stakeholders and promoted communication and collaboration within and across these communities. Its goal was to stimulate new thinking, articulate future needs, and discuss how emerging or disruptive software engineering technologies, methods, and tools can help address future challenges.

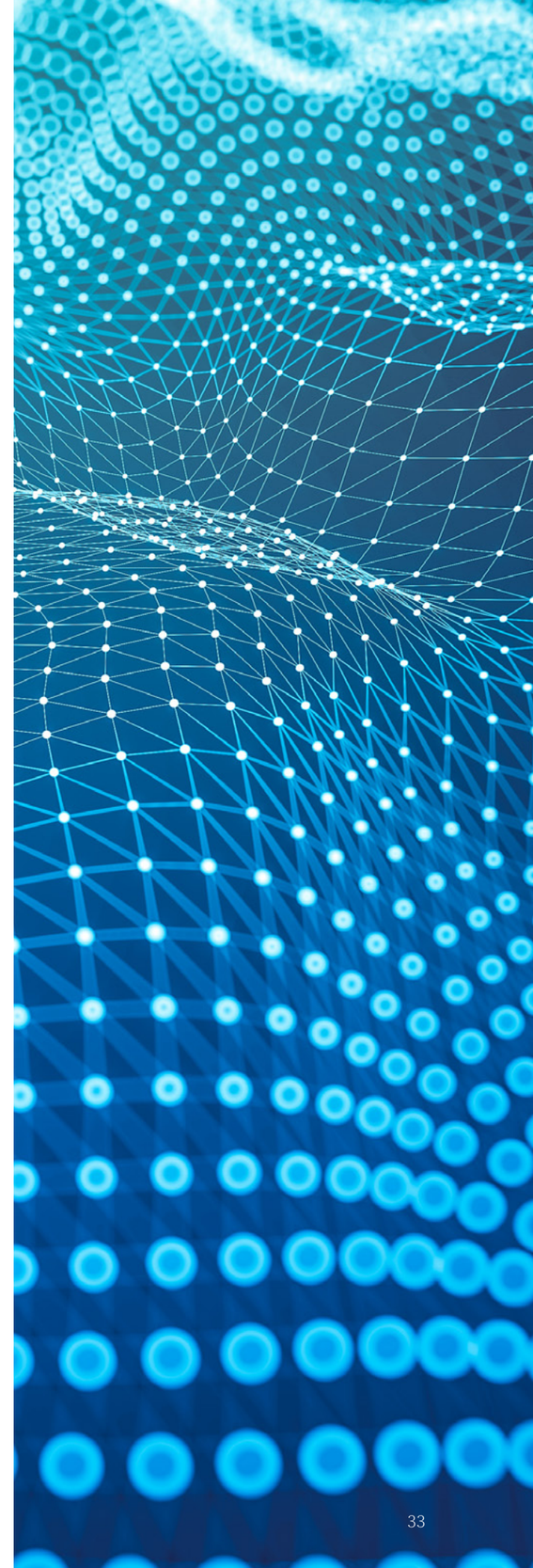
Five major themes emerged over the course of the workshop:

- **assuring continuously evolving systems:** Provide evidence and arguments that a system will behave as intended, considering both desired functionality and quality attributes, as it evolves continuously to incorporate new capability and dynamically self-adapts its operating configuration at runtime.
- **AI-augmented software development:** Augment each stage of software development with artificial intelligence (AI) to orchestrate continuous systems evolution, positioning for constant high-speed change.
- **engineering of AI-enabled software:** Develop empirically validated practices to support development and sustainment of next-generation AI-enabled software. Provide tools, verification methods, techniques, and practice to apply sound software engineering principles to AI engineering.
- **designing in ethics in software, systems, and societal-scale systems:** Build and evolve societal-scale software systems that enable transparency and mitigate risks of unethical influence on individuals, unrestrained social manipulation, or disruption of social epistemology.
- **composable software systems:** Provide a scientific and engineering basis for designing, building, analyzing, and assuring heterogeneous and composable software systems. Provide languages, tools, environments, and techniques to support these activities.

The SEI will combine these themes with input from other members of the software engineering community and our own research to produce a research roadmap and a strategy to

- catalyze the software engineering community to create a compelling multiyear vision, strategy, and roadmap for the research and development of next-generation software and software-reliant systems on which national security depend
- contribute to the development of an ecosystem for software engineering that engages academic, defense, and commercial communities to work together on solving future problems and developing critical abilities
- increase national security by informing future decisions, policies, and investments in software engineering

"Maintaining our nation's competitive advantage in defense, infrastructure, healthcare, commerce, and education means that we need the best engineers of software in the world," said Carleton. "Working with the best minds in the software engineering community, we are putting together a strategy to make software development a key part of the nation's security and prosperity, going forward."

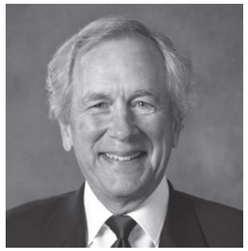


Board of Visitors

The SEI Board of Visitors advises the Carnegie Mellon University president, university provost, and SEI director on SEI plans and operations. The board monitors SEI activities, provides reports to the president and provost, and makes recommendations for improvement.

Barry Boehm
TRW Professor of Software Engineering, University of Southern California; Director, University of Southern California Center for Software Engineering

Russell Crockett
Managing Partner and CEO of Aztlán Chemical; Principal and Owner of RTC Energy LLC



Philip Dowd
Private investor; former Senior Vice President, SunGard Data Systems; Trustee, Carnegie Mellon University

John M. Gilligan
President, Gilligan Group; former Senior Vice President and Director, Defense Sector of SRA International; former CIO for the Department of Energy

Elizabeth A. Hight
Former Vice President of the Cybersecurity Solutions Group, Hewlett Packard Enterprise Services; former Rear Admiral, U.S. Navy; former Vice Director of the Defense Information Systems Agency

Tom Love
Chief Executive Officer, ShouldersCorp; Founder of Object Technology Group within IBM Consulting

Alan J. McLaughlin
Chair, Board of Visitors; Consultant; Former Assistant Director, MIT Lincoln Laboratory

Donald Stitzenberg
President, CBA Associates; Trustee, Carnegie Mellon University; former Executive Director of Clinical Biostatistics at Merck; Member, New Jersey Bar Association

Carnegie Mellon University Leadership

Farnam Jahanian
President

James H. Garrett, Jr.
Provost and Chief Academic Officer

J. Michael McQuade
Vice President, Research

SEI Executive Leadership

Paul Nielsen
Director and Chief Executive Officer

David Thompson
Dep. Director and Chief Operating Officer

Tom Longstaff
Chief Technology Officer

Anita Carleton
Director, Software Solutions Division

Bill Wilson
Director (Acting), CERT Division

Matt Gaston
Director, Emerging Technology Center

Heidi Magnelia
Chief Financial Officer

Mary Catherine Ward
Chief Strategy Officer

Sandra Brown
SEI General Counsel

DM21-0403

Credits

Manager, Communication Services
William Thomas

Manager, Corporate & Technical Communications
Janet Rex

Manager, Public Relations
Richard Lynch

Manager, Communication Design
Cat Zaccardi

Editor-in-Chief
Paul Ruggiero

Editorial
Ed Desautels
Claire Dixon
Patricia Flinn
Lope Lopez
Tamara Marshall-Keim
Gerald Miller
Sheela Nath
Nancy Ott
Sandy Shrum
Barbara White

Design
Christopher Baum

Digital Production
Mike Duda

SEI Pittsburgh, PA
4500 Fifth Avenue
Pittsburgh, PA 15213-2612

SEI Arlington, VA
NRECA Building, Suite 200
4301 Wilson Boulevard
Arlington, VA 22203

SEI Boston, MA
10 Maguire Road
Lexington, MA 02421

SEI Los Angeles, CA
2401 East El Segundo Boulevard
El Segundo, CA 90245