Carnegie Mellon University
Software Engineering Institute

2021 YEAR IN REVIEW

Always focused on the future, the Software Engineering Institute (SEI) advances software as a strategic advantage for national security. We lead research and direct transition of software engineering, cybersecurity, and artificial intelligence technologies at the intersection of academia, industry, and government. We serve the nation as a federally funded research and development center (FFRDC) sponsored by the U.S. Department of Defense (DoD) and are based at Carnegie Mellon University, a global research university annually rated among the best for its programs in computer science and engineering.

The *2021 SEI Year in Review* highlights the work of the institute undertaken during the fiscal year spanning October 1, 2020, to September 30, 2021.

"Driven by our organizational values, we work collaboratively within the SEI, with researchers at CMU and other leading universities, and with stakeholders in government and industry."

A Message from the Director and Chief Executive Officer

Management consultants and human resources leaders have been describing COVID-driven alterations to how we work as our new normal. Organizations have adapted to the virus's deadly effects by operating with enhanced telework rules, vaccination requirements, and greater awareness of workplace safety.

Many interpret the phrase *new normal* to mean that things will never be as they were before the pandemic. That may be in some respects.

The Carnegie Mellon University Software Engineering Institute has also adapted how we work in the pandemic. But *what* we do is very much the same. We continue to advance software as a strategic advantage for national security.

In 2021, for instance, we gathered a panel of world-renowned experts to develop a roadmap for software engineering research to enable future systems. We also coalesced years of applying artificial intelligence for national defense and security missions into a new AI Division. This technical organization will enhance our leadership of a national initiative to form an essential engineering discipline for AI.

We have been able to take these and other significant strides in an uncertain time for several reasons. Driven by our organizational values, we work collaboratively within the SEI, with researchers at CMU and other leading universities, and with stakeholders in government and industry.

Our collaborative approach rests on our organization's commitment to diversity, equity, and inclusion. Those outcomes enable our people to blend skills in areas such as computer science, accounting, data science, acquisition, and technical communications to serve the needs of our work sponsors.

In addition, CMU leadership has provided common-sense guidance to employee health and safety since the onset of the pandemic, giving the SEI a sure foundation on which to continue creating and delivering solutions for the most critical software issues.

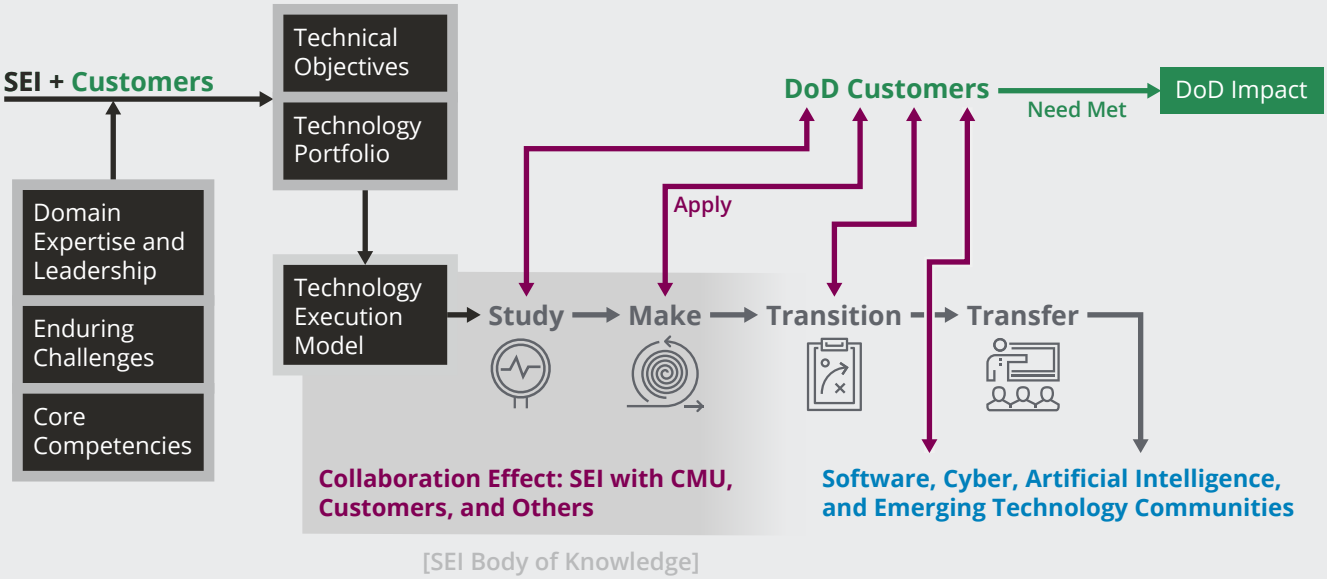
For us at the SEI, the *new normal* continues to be full of anticipation for a future in which our national security collaborators, sponsors, and stakeholders will gain dominance through unsurpassed software engineering, cybersecurity, and AI.

Paul Nielsen

Execution Strategy

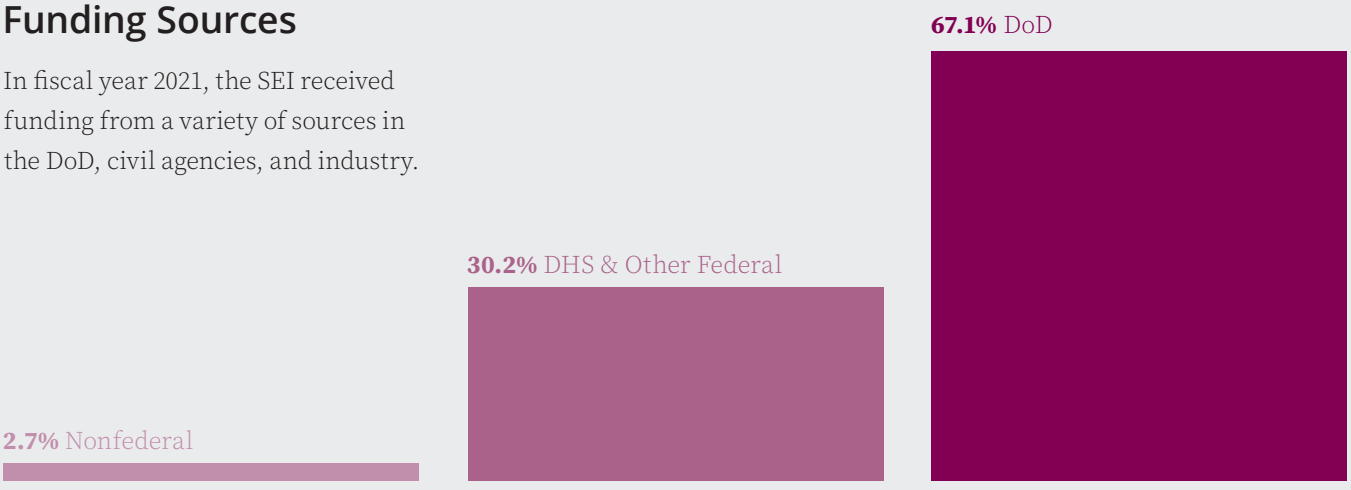
The SEI facilitates the transfer of research results to practice in Department of Defense (DoD) programs, the Office of the Secretary of Defense's science and technology initiatives, and non-DoD U.S. government organizations where improvements will also benefit the DoD. In doing so, we gain deeper insight 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.

We collaborate at the nexus of government, industry, and academia to integrate research in artificial intelligence, software, and cybersecurity to develop and pilot prototype tools, build and transition innovative solutions, and provide input for our sponsor's policy decisions about software and related technologies. 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 fiscal year 2021, the SEI received funding from a variety of sources in the DoD, civil agencies, and industry.



Contents

News Briefs

Greg Touhill Takes Helm of CERT Division

The SEI appointed Gregory J. Touhill as director of the SEI's CERT Division in spring 2021.

The CERT Division is known for innovations in cybersecurity. Under Touhill's leadership, the CERT Division has expanded its efforts in zero trust, data integrity, and strategic engagement.

Touhill is an author and a retired U.S. Air Force brigadier general. He was the first chief information security officer (CISO) of the U.S. federal government and a senior cybersecurity leader in the Department of Homeland Security. Most recently, he was president of Appgate Federal Group, a government-facing cybersecurity services firm.

"Throughout my professional career, I have been fortunate to be a member of some amazing teams that have contributed to protecting national security and national prosperity," said Touhill. "I am honored to have been selected as the director of the CERT Division to pursue the mission of assuring our nation's cyber defense."

> **"I am honored to have been selected as the director of the CERT Division to pursue the mission of assuring our nation's cyber defense."**
>
> **GREG TOUHILL,** SEI CERT Division Director

"[Avionics organizations] need a rich set of modeling and analysis capabilities that AADL uniquely delivers."

JEROME HUGUES, Senior Researcher, SEI Software Solutions Division

SEI Leads Development of New SAE AADL Version

In 2021, the SEI collaborated with the AADL community to develop version 2.3 of the Architecture Analysis and Design Language (AADL), an SAE International standard, to be released in 2022. The SEI leads the AADL standardization committee. New features include multicore support, enhanced graphical editor and analysis capabilities, and a workflow layer expected to extend the tool set's adoption by practitioners.

Avionics organizations use AADL to express the designs of their evolving platforms. "They need a rich set of modeling and analysis capabilities that AADL uniquely delivers," said senior SEI researcher Jerome Hugues.

The U.S. Army has adopted AADL to support projects such as the Joint Multi Role Mission Systems Architecture Demonstrations (JMR MSAD). From 2013–2020, the JMR MSAD exercised and matured the AADL language, tools, and processes, proving it effective in the modeling and analysis of complex, safety-critical embedded computing systems. More multicore processors on safety-critical embedded systems require understanding of potential hazards with shared resources. The AADL language now supports modeling and analysis of multicore processors for insights into safety- and time-critical systems.

Photo (Above) Alice de Casanove

Applying AADL Expertise to Future Vertical Lift Modeling

The Department of Defense Digital Engineering Strategy seeks to formalize the development, integration, and use of models to inform enterprise and program decisions. Recent SEI work for the U.S. Army's Future Vertical Lift (FVL) program closes the gap between making architectural software models and ensuring that the software systems conform to them.

The SEI developed Architecture Analysis and Design Language (AADL) models of helicopter avionics embedded in mission systems, the approach to translate the models into executing system code, and code for specific avionics applications, and then loaded it all onto a mission system computer. SEI partner Innovative Defense Technologies validated the property values of the executing system against an analysis of the AADL models performed with the SEI's Open Source AADL Tool Environment (OSATE).

Photos U.S. Army, Bell

The approach assembled a tool chain to seamlessly transition from a formal model to an executing system and verify the system from recorded data. The solution enables quick modification and analysis of test posture, ensures conformance to model specifications, and ensures that system requirements are met.

Operationalizing Responsible Artificial Intelligence

While artificial intelligence (AI) has leapt ahead, guidance on its responsible use has not kept up. The technology's constant evolution, trust and transparency challenges, and unpredictable operational contexts have made it difficult to develop practical heuristics for creating and maintaining ethical AI systems.

The Defense Innovation Unit (DIU), which accelerates adoption of commercial technology in the Department of Defense (DoD), saw that its own programs should be practicing the DoD's five ethical principles for AI. DIU collaborated with the SEI to operationalize these principles within DIU's commercial prototyping and acquisition programs. The lessons learned and cross-sector best practices culminated in DIU's fall 2021 report, *Responsible AI Guidelines in Practice*.

"As DIU fields and scales commercial technology, we are building on the DoD's commitment to responsible AI," explained DIU's AI and machine learning technical director, Jared Dunnmon. "The *Guidelines* facilitate agreements between DoD partners and commercial vendors, enabling DIU to stimulate, structure, and document a process of building AI capabilities that aligns with the DoD AI ethical principles on DIU programs."

Mitigating bias, misuse, abuse, and unintended consequences in AI capabilities requires understanding context and focusing on the humans that interact with the system. Human-centered AI is one of the SEI's proposed three pillars of AI engineering. "Human-centered AI is now recognized as important to successful AI systems, but guidance is needed for how to implement it," said the SEI's Carol Smith, a co-author of the DIU report. "The *Responsible AI Guidelines* provide the government with actionable guidance to do this important work."

The guidelines concretize ethical concepts into actionable practices across the AI workflow. SEI researcher Alex Van Deusen, another report co-author, said, "Our goal was to establish a process that is reliable, replicable, and scalable across the DIU and expandable to other DoD organizations."

For help making human-centered, responsible AI, contact the SEI AI Division at info@sei.cmu.edu.

> **"Our goal was to establish a process that is reliable, replicable, and scalable across the DIU and expandable to other DoD organizations."**
>
> **ALEX VAN DEUSEN,** Assistant Design Researcher, SEI AI Division

Quantifying Uncertainty in Mission-Critical AI Systems

The Department of Defense (DoD) and the intelligence community are adopting more artificial intelligence (AI) technology. However, many machine learning (ML) models within AI applications cannot accurately estimate or communicate the certainty of their inferences about real-world data. Downstream AI components and human users may make decisions about inferences they cannot know are bad.

The SEI is leveraging experience in human-computer interaction, enterprise-level infrastructure, and AI to develop new techniques and tools to quantify, identify, and rectify uncertainty in ML models. Improving ML uncertainty estimation supports the robust-and-secure pillar of AI engineering, a field spearheaded by the SEI.

Quantifying uncertainty is first. According to SEI senior research scientist Eric Heim, deep neural network models tend toward overconfidence and require calibration, but current calibration methods are error prone and often yield poor confidence estimations.

In 2021, Heim and his colleagues developed metrics to evaluate the calibration of ML models against mission context. Better calibrated ML models can supply more accurate, context-sensitive estimates of confidence. This ability could help an intelligence operator, for example, decide when to trust an ML system's identification of a vehicle from satellite photos. Heim and his colleagues will release the calibration metrics, and the evaluation code that produced them, on the SEI's GitHub site.

Calibration evaluation is the first step toward detecting ML model uncertainty, determining its cause, and mitigating it. To achieve these challenging goals, Heim's team works with Carnegie Mellon University ML experts Aarti Singh and Zachary Lipton. "We intend our methods, metrics, visualizations, and algorithms to be matured and eventually equip practitioners with tools to build more robust ML models," said Heim. Such tools could make mission-critical AI systems more reliable and transparent, safer, and faster to update and deploy in DoD and intelligence operational environments.

"We intend our methods, metrics, visualizations, and algorithms to be matured and eventually equip practitioners with tools to build more robust ML models."

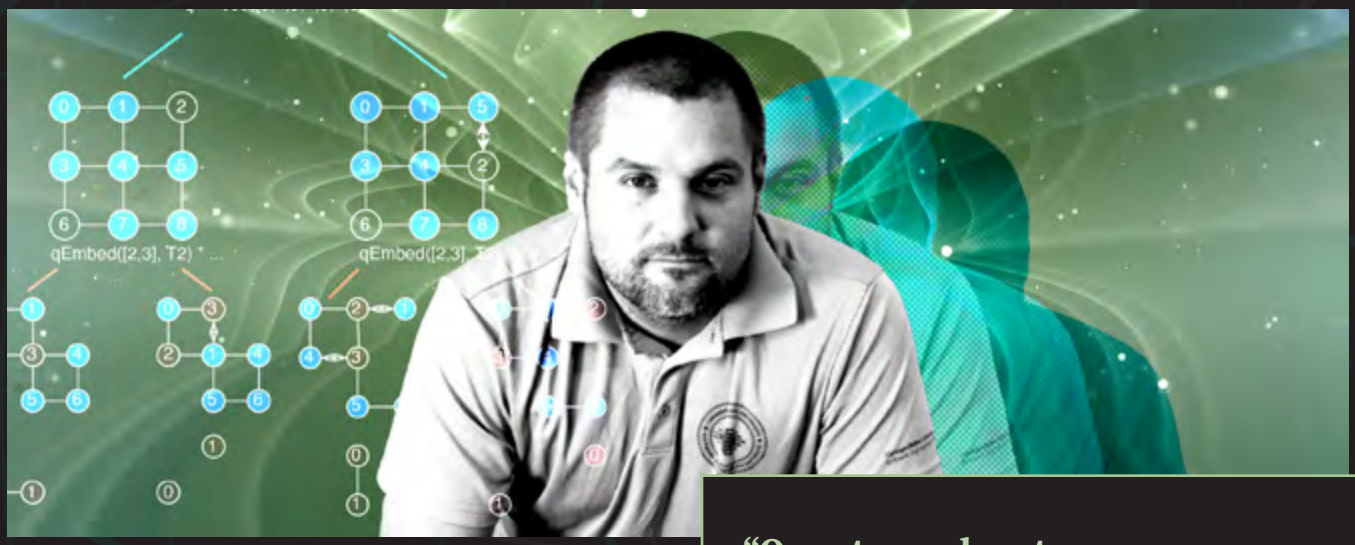
ERIC HEIM, Senior Machine Learning Researcher, SEI AI Division

Building the Quantum Advantage Evaluation Framework

Quantum computing offers a possible solution for hard computing problems in the Department of Defense (DoD), such as materials science and combinatorial optimization. But this nascent technology requires significant, targeted investment. To help guide the DoD's research and development, the SEI developed the Quantum Advantage Evaluation Framework (QAEF), which will be used to predict the computing applications that will show quantum advantage in the next one to three years.

"Quantum advantage occurs when quantum computing can solve some practical DoD problem faster, or create a higher quality of solution, or both, than alternatives like classical state-of-the-art computing," said Jason Larkin, an SEI senior researcher leading the QAEF project.

The SEI has expertise in the algorithms and software engineering of both quantum and classical computers. The SEI collaborated with QuantumHub at Carnegie Mellon University (CMU); CMU researchers; government organizations, such as the research laboratories of the Air Force, Army, and Navy; and the Pittsburgh Supercomputing Center. The SEI also recently became part of the IBM Quantum Network and in the past year has transitioned its fundamental research into customer contexts.



QAEF will compare application benchmarks on both quantum and classical state-of-the-art computing to determine quantum advantage. QAEF will be able to benchmark any DoD-relevant applications and algorithms by executing them on real and simulated quantum devices. "That's challenging because to get optimal performance, as in classical computing, you've got to optimize for quantum computing across the full stack, which is currently under development," Larkin said. Though stack development may take years, Larkin and his team have already begun comparing application benchmarks.

"Quantum advantage occurs when quantum computing can solve some practical DoD problem faster, or create a higher quality of solution, or both, than alternatives like classical state-of-the-art computing."

JASON LARKIN, Senior Researcher, SEI AI Division





AI and Open Source Software Contribution

The SEI has a long history of developing tools and platforms and releasing them as open source software to further research and practice. As of late 2021, the SEI had more than 100 open source software project repositories on its GitHub site and main website.

In fiscal year 2021, the SEI released several new tools and updated a number of existing open source projects.

Kaiju Malware Analysis Tool Suite

Building on the CERT Division's Pharos advanced binary code analysis framework, Kaiju extends the U.S. National Security Agency's Ghidra reverse engineering platform with several powerful new analysis tools. Kaiju brings a variety of improvements to Ghidra's disassembler and decompiler, including powerful code comparison tools, an advanced capability for reasoning about program behavior, and improved support for decompiling C++ programs.

Foundry Appliance

In partnership with the Cybersecurity and Infrastructure Security Agency (CISA), the SEI's CERT Division developed the Foundry Appliance, which seamlessly integrates numerous SEI open source applications used to put on the annual President's Cup Cybersecurity Competition. Users can leverage this virtual appliance to build cyber laboratories, challenges, and competitions.

NetSA Tool Suite

The NetSA tool suite includes YAF (Yet Another Flow Sensor), the Mothra security analysis platform, and Super Mediator, among other tools. In 2021, the CERT Division updated the YAF and Super Mediator products.

Crucible Framework

The CERT Division's Crucible is an open source, cyber-simulation application framework enabling everything from small-scale virtual-environment labs and cyber challenges to large-scale multi-team exercises sponsored by the U.S. Marine Corps, Army, Air Force, Cyber Command, Indo-Pacific Command, Special Operations Command, Department of the Treasury, and others.

Juneberry

The AI Division's Juneberry tool improves the experience of machine learning experimentation by providing a framework for automating the training, evaluation, and comparison of multiple models against multiple datasets, reducing errors and improving reproducibility.

> **See more of the SEI's GitHub projects at cmu-sei.github.io and the NetSA tool suite at tools.netsa.cert.org.**

Agile Virtual Schoolhouse Enables Vital Distance Learning

Though many Department of Defense (DoD) software developers shifted to working from home in 2020 due to the COVID-19 pandemic, they still needed to develop skills in iterative development approaches such as Agile. The SEI responded by offering the Agile Virtual Schoolhouse platform.

The FY18 National Defense Authorization Act and the Defense Innovation Board Software Acquisition and Practices study indicated that the DoD needs to develop organic expertise in Agile and other iterative development methods. The SEI's years of experience with Agile and the government setting have helped it develop and continually evolve multiple Agile classroom courses, which it adapted to the online format in 2021.

Throughout that year, about 250 learners from five DoD program offices used the Agile Virtual Schoolhouse platform to access a tailored sequence of learning packages, each of which includes a custom self-study assignment of curated learning resources and a live, online lecture and discussion session. Topics in the learning packages focus on DoD concerns, such as Agile in the DoD landscape, oversight and insight in Agile government settings, Agile and requirements, and Agile and testing.

"The real-world examples the instructors share add depth and background to the topics, rather than the purely academic description that could have been given," said one participant.

"Our intent from the beginning has been to remain customer centered," said the SEI's Crisanne Nolan, one of the platform development leads. "We built the Virtual Schoolhouse to be modular. We refashion our learning packages to always provide a rich experience relevant to the highly regulated environments in which our customers work."

> **U.S. government organizations interested in the Agile Virtual Schoolhouse should contact the SEI at course-info@sei.cmu.edu.**

> **"We refashion our learning packages to always provide a rich experience relevant to the highly regulated environments in which our customers work."**
>
> **CRISANNE NOLAN,** Transition Program Coordinator, SEI Software Solutions Division

Building a Roadmap for System Cybersecurity Improvement

System developers often consider security engineering a separate activity from software and systems engineering. They either address security inadequately or defer it until late in the engineering lifecycle or after deployment. Consequently, organizations operate software-reliant systems with high residual cyber risk. Operating software-reliant systems in system-of-systems environments compounds these problems. Systems engineering organizations need a roadmap to building security in, rather than bolting it on.

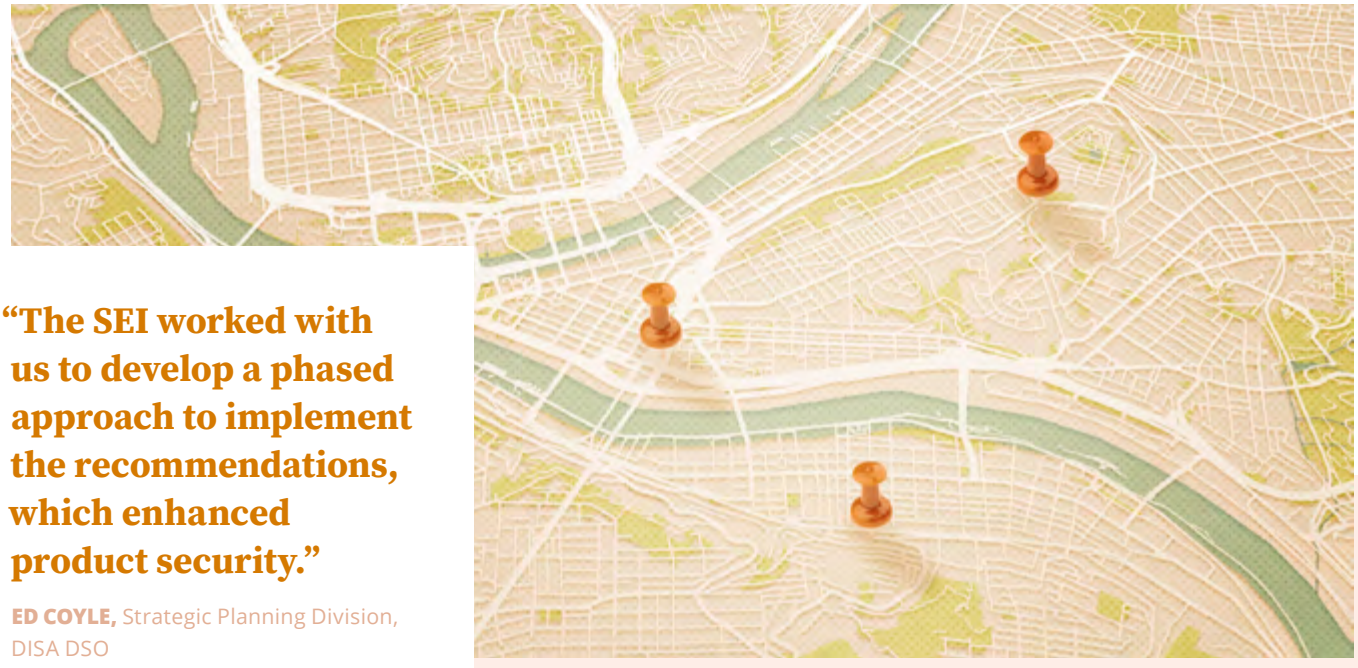
The SEI created such a roadmap: the Cybersecurity Engineering Review (CSER), an innovative assessment based on the SEI's history in developing practice frameworks and models for acquisition, software engineering, and operational resilience.

The CSER documents leading cybersecurity engineering practices across the lifecycle and supply chain. It assesses a program's integration of cybersecurity with software and systems engineering practices. The CSER shows programs how to bake security into their processes when acquiring and engineering highly complex software-reliant systems designed to operate in system-of-systems environments.

The SEI completed two CSER pilots in 2021: one for an Air Force Foreign Military Sales (FMS) program and a second for the Defense Information Systems Agency (DISA) Defense Spectrum Organization (DSO). The CSER identified gaps in both programs' cyber practices and recommended improvements.

"The CSER conducted document reviews and interviewed key personnel associated with our program," said Ed Coyle of DSO. "It provided recommendations focused on unique aspects of our program. The SEI worked with us to develop a phased approach to implement the recommendations, which enhanced product security. The CSER also provided recommendations for comprehensively integrating security across the program, increasing the security posture."

The SEI plans to conduct more pilots and describe the CSER process in a technical paper. As organizations better merge cybersecurity engineering with systems and software engineering, the Department of Defense can have greater confidence in the security and resilience of deployed software-reliant systems.



"The SEI worked with us to develop a phased approach to implement the recommendations, which enhanced product security."

ED COYLE, Strategic Planning Division, DISA DSO

A Vision and Roadmap for Software Engineering Research and Development

Software systems continue to grow and extend their reach, delivering an expansive array of new capabilities in environments as familiar as our homes and as exotic as outer space. They are rapidly becoming more interconnected, are increasingly utilizing artificial intelligence (AI), must be considerably more resilient, and must be updated almost continuously. Software systems constitute a vital component of our national competitiveness and national security.

Software weaknesses reflect the inadequate state of the art and practice of software engineering, and systems are growing in size, complexity, and ubiquity. Significant investment in software engineering research and development is needed now to develop the foundations and tool support for a reconceived notion of the software engineering development lifecycle for continuously assuring rapidly evolving Department of Defense (DoD) systems.

To scout the future of this ever-more-complex field, the SEI led a major study producing a multiyear research and development roadmap for engineering next-generation software-reliant systems, and it recently published its results in the book *Architecting the Future of Software Engineering: A National Agenda for Software Engineering Research & Development*.

"To guide this work, we leveraged our relationships across the public and private sectors," said Anita Carleton, director of the SEI's Software Solutions Division and study lead. "We formed an advisory board comprising visionaries and thought leaders in industry, academia, research labs, the DoD, and technology companies."

Carleton said they imagined future development of software-intensive systems less as a manual refining of specifications and code and more as a technical conversation between humans and computers.

"The guiding vision we articulated replaces the current notion of the software development pipeline with one where humans and AI are trustworthy collaborators that rapidly evolve systems based on programmer intent," said Carleton. "People and computers will each do what they do best."

"To achieve this vision, the field of software engineering needs new development and architectural paradigms, founded on new areas of research mapped out in our study." The research roadmap includes six focus areas:

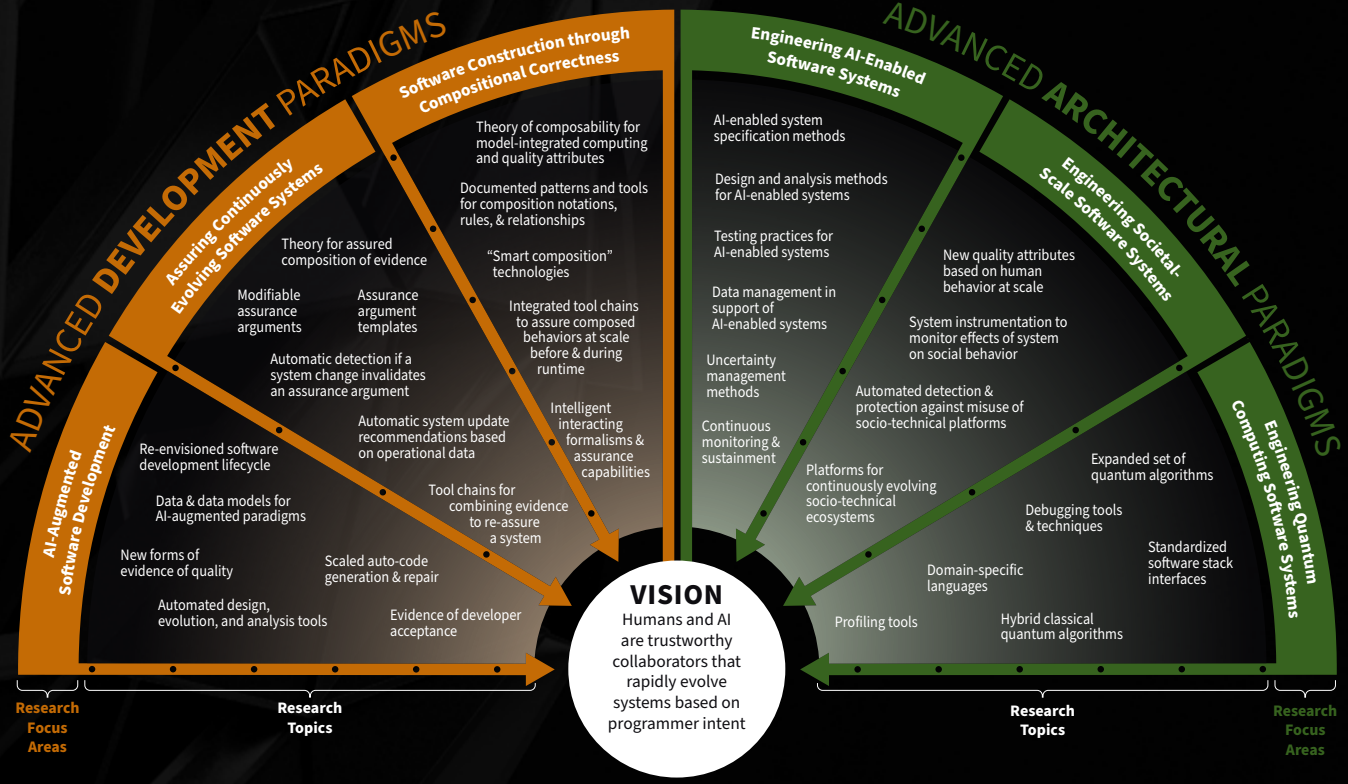
- **AI-Augmented Software Development:** Re-envision the entire software development process with increased AI and automation tool support for developers.
- **Assuring Continuously Evolving Software Systems:** Develop a theory and practice of rapid and assured software evolution that enables efficient and bounded re-assurance of continuously evolving systems.

> **"The guiding vision we articulated replaces the current notion of the software development pipeline with one where humans and AI are trustworthy collaborators that rapidly evolve systems based on programmer intent. "**
>
> **ANITA CARLETON,** Director, SEI Software Solutions Division

- **Software Construction through Compositional Correctness:** Create methods and tools that enable the specification and enforcement of composition rules that allow the creation and assurance of required behaviors.
- **Engineering AI-Enabled Software Systems:** Explore which existing software engineering practices can reliably support the development of AI systems and identify and augment software engineering techniques for the development and sustainment of systems with AI components.
- **Engineering Societal-Scale Software Systems:** Leverage insights from the social sciences to build and evolve societal-scale software systems that consider qualities such as bias and influence.
- **Engineering Quantum Computing Software Systems:** Enable easier and more reliable programming of current quantum computers, then enable increasing abstraction as larger, fully fault-tolerant quantum computing systems become available.

"In *Architecting the Future of Software Engineering*, we have articulated a set of recommendations, an analysis of the current state of the practice, emerging trends and technologies, and a set of research focus areas and milestones spanning the next 10-to-15-year period," said Carleton. "We encourage practitioners and leaders in the field to download a copy of the book and consider how you or your organization can help advance and evolve these research areas of software engineering in the coming years."

To download a copy of *Architecting the Future of Software Engineering: A National Agenda for Software Engineering Research & Development*, visit **sei.cmu.edu/go/national-agenda**.



Software Engineering Research Roadmap with Research Focus Areas and Research Objectives (10-to-15-Year Horizon)

New Artificial Intelligence Division to Advance the Discipline

In June 2021, the SEI established a new research division dedicated to applied artificial intelligence (AI) and named Matthew Gaston as the new division's director. The SEI is leading a national initiative to advance the professional discipline of AI engineering with partners in industry, government, and universities.

The AI Division researches the practical design and implementation of AI so that government customers have the confidence and knowledge to acquire, build, and deliver AI systems that address mission needs. Division experts build real-world, mission-scale AI capabilities and apply the lessons learned to the research and definition of processes, practices, and tools supporting AI system operationalization.

The division draws on work done by the SEI Emerging Technology Center (ETC), which initiated and nurtured AI engineering at the SEI under Gaston's direction.

"Carnegie Mellon University recognized early on the promise of AI to enable better, faster decisions at scale," said former CMU Vice President for Research J. Michael McQuade. "It is critical for the U.S. government to bring engineering discipline to AI as a key enabler for national security, and it is particularly fitting for the Software Engineering Institute to contribute to this discipline because of the university's long history of leadership in this area."

AI engineering is an emerging field of research and practice that combines the principles of systems engineering, software engineering, computer science, and human-centered design to create AI systems in accordance with human needs for mission outcomes. This discipline will help the Department of Defense (DoD) and other government agencies meet mission goals by growing the body of knowledge to design, develop, and implement AI that is scalable, robust and secure, and human centered—the three pillars of AI engineering.

The AI Division released the initial definitions of these three pillars in June 2021 after collaborating with thought leaders in the field. The pillars support the goals of the *2018 Department of Defense Artificial Intelligence Strategy* and inform the AI Division's research projects in AI training and verification, inverse reinforcement learning, machine-learning uncertainty, and trustworthy AI.

As the home of the National AI Engineering Initiative, the division has also formed a steering committee of research collaborators, co-funders, and advocates in government, industry, and academia. The SEI was also a sponsor of the 2021 AI World Government conference, where SEI experts

"It is critical for the U.S. government to bring engineering discipline to AI as a key enabler for national security, and it is particularly fitting for the Software Engineering Institute to contribute to this discipline because of the university's long history of leadership in this area."

J. MICHAEL MCQUADE,
former Vice President for Research,
Carnegie Mellon University

participated in panels and presentations and Gaston gave a keynote address.

Before joining the SEI in 2011, Gaston led research in industry and at the National Security Agency. Gaston has published in the fields of complex networks, machine learning, multi-agent systems, and operations research. He earned his bachelor's degree in mathematics from the University of Notre Dame and his M.S. and Ph.D. degrees in computer science from the University of Maryland Baltimore County.

"I am very excited to lead the new SEI AI Division and to scale the SEI's AI engineering capabilities in support of defense and national security," said Gaston. "Using our initial work in the Emerging Technology Center and across the SEI as a foundation, we plan to build on the strong legacy of software engineering research at the SEI, initiate exciting new projects, work closely with world-class AI researchers across Carnegie Mellon University, and build a community of collaborators throughout government, industry, and academia."

"The Department of Defense sponsored the SEI in 1984 to bring engineering discipline to the creation and acquisition of software," said Paul Nielsen, SEI director and CEO. "Our goal in forming and growing the SEI AI Division is similar—to transform the creation of AI systems from one-time, custom-crafted solutions into repeatable, scalable, and reliable programs and services that can help the DoD achieve mission success."

"By putting these pillars in place as AI system design and development starts, you're more likely to build systems that achieve mission outcomes."

RACHEL DZOMBAK, Digital Transformation Lead, SEI AI Division

AI Engineering: Building the Discipline and Growing an Ecosystem

Most artificial intelligence (AI) applications fail, sometimes spectacularly. The drive to achieve one-off capabilities precludes a broader, disciplined approach that would enable the rapid uptake of AI demanded by the Department of Defense (DoD).

To mature AI practices and help national defense and security agencies adopt AI, the SEI has begun formalizing the field of AI engineering, much as it did for software engineering in the 1980s. AI engineering is an emerging field of research and practice that combines the principles of systems engineering, software engineering, computer science, and human-centered design to create AI systems in accordance with human needs for mission outcomes.

In October 2020, the Office of the Director of National Intelligence sponsored the SEI to lead an AI engineering initiative to guide the development of a multiyear research and development roadmap and develop capabilities based on partners' core competencies. Bolstered by its recently formed AI Division, the SEI leverages its researchers' expertise in AI; its deep knowledge of the government technology space; its status as a trusted federally funded research and development center; and its relationships with government, the armed services, industry, and academia. In 2021, partners from these spheres collaborated with the SEI to develop three initial pillars of AI engineering: AI systems should be scalable, robust and secure, and human centered.

The SEI's government partners cited scalability challenges in the private sector, amplified by government-sector barriers, as particularly worrisome. Often, AI projects fail to move past the prototype phase. The scalability pillar of AI engineering includes three areas of focus:

- scalable management of data and models
- enterprise scalability of AI development and deployment
- scalable algorithms and infrastructure

Even highly scalable systems will not fulfill mission outcomes if they are not robust and secure. AI systems must be robust against real-world variations—those that the systems can reason about and those that they cannot. The pillar of robust and secure AI calls out three focus areas:

- improving the robustness of AI components and systems, including going beyond measuring accuracy to measuring mission outcome achievements
- development of processes and tools for testing, evaluating, and analyzing AI systems
- designing for security challenges in modern AI systems

While security is a must for AI implementations in the DoD, so is keeping humans at the center. The human-centered pillar of AI engineering is intended to ensure that AI systems are built in alignment with the ethical principles of the DoD and other government agencies. The pillar of human-centered AI engineering highlights these areas:

- the need for designers and systems to understand the context of use and sense changes over time
- developing tools, processes, and practices to scope and facilitate human-machine teaming
- methods, mechanisms, and mindsets to engage in critical oversight

The three pillars would lend AI systems more than just their namesake qualities, according to Rachel Dzombak, digital transformation lead at the SEI and a leader of the SEI's work in AI engineering. "By putting these pillars in place as AI system design and development starts," she said, "you're more likely to build systems that achieve mission outcomes."

The AI engineering initiative invites collaboration on research projects to advance the discipline and build a community. It is also developing symposia for 2022 to further evolve the state of the art; gather lessons learned, best practices, and workforce development needs; and foster critical relationships. "By creating an ecosystem around the discipline," said Dzombak, "we can coalesce insights and establish best practices around how we design, deploy, and maintain AI capabilities."

Modeling DevSecOps for Software Pipeline Assurance

At a conference in 2020, the SEI's Tim Chick was asked, "How do you assure DevSecOps pipelines?" Based on their experience in the field, Chick and his SEI colleagues concluded that most organizations were making indefensible assertions about their pipeline's assurance and what it would provide for product assurance. While one can assure a software product, the concept of a DevSecOps pipeline lacked enough definition and substance to be assured, or verified to behave as expected, and to have its cybersecurity risks quantified.

A few months later, bad actors exploited a supply chain flaw to deliver malware to thousands of systems running SolarWinds software. This attack validated the SEI's conclusions: Both the product and pipeline need to be assured.

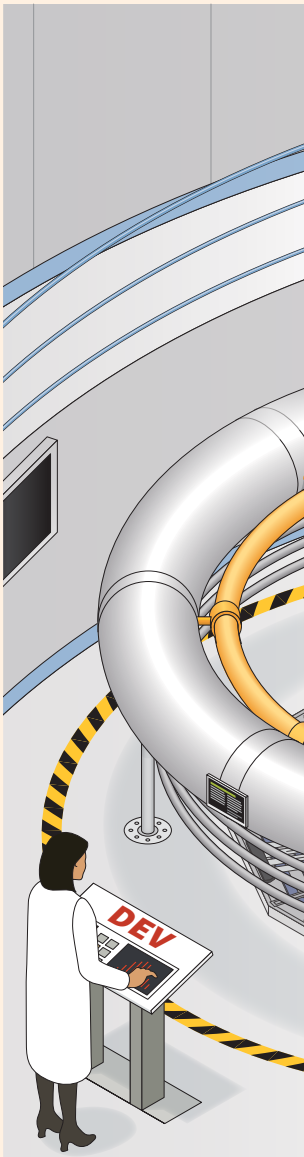
While there are many theories and tools for DevSecOps, there is no practical framework for its implementation and evaluation. "There's no holistic view of how you bring it all together," said Chick. Filling this gap is especially critical for major Department of Defense programs because they rely on the DevSecOps pipeline to repeatedly perform key assurance activities to address the scale and complexity of their software systems.

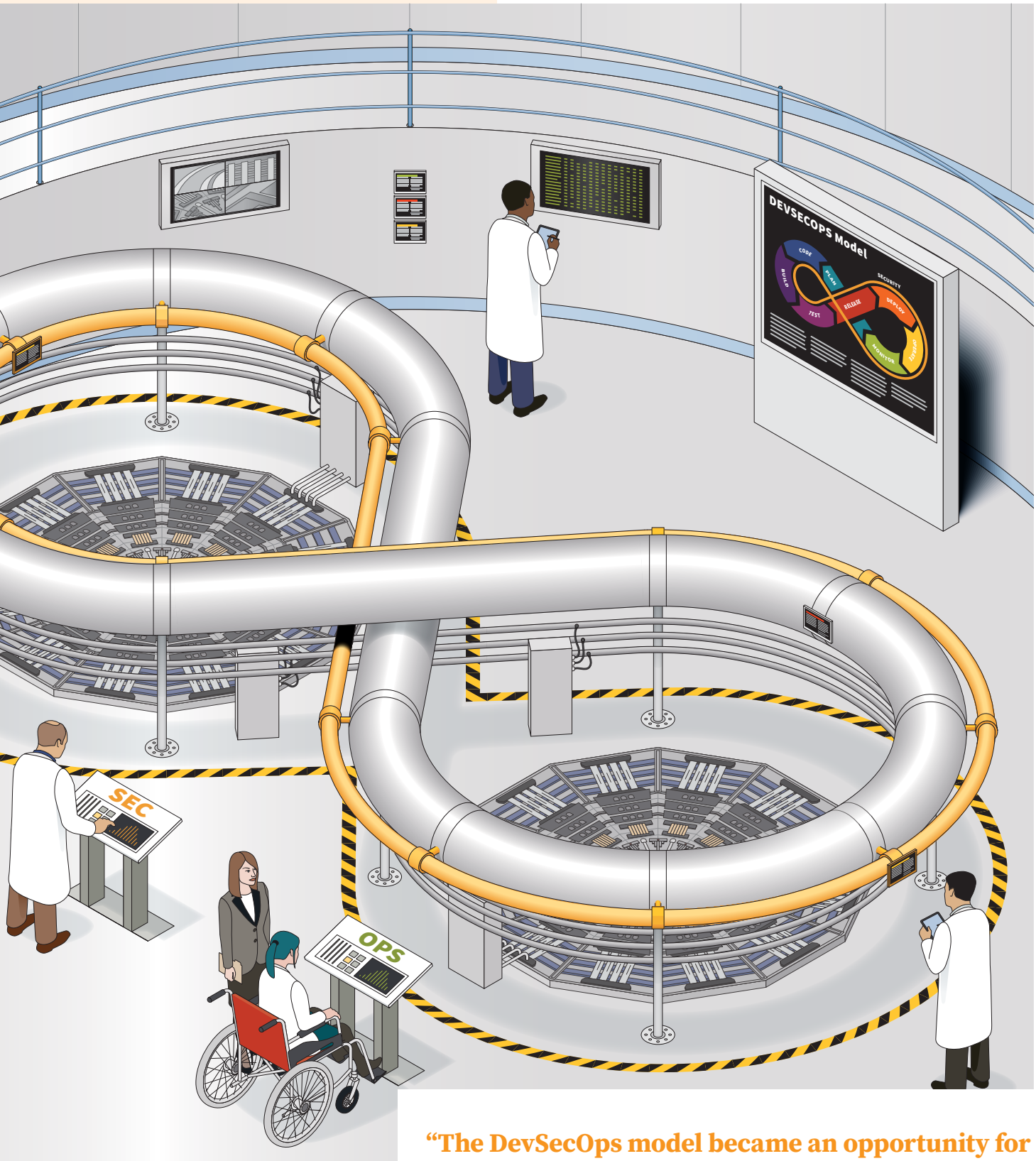
To bridge this gap between research and practice, the SEI developed a DevSecOps model. It includes 10 capability areas covering every stage of the DevSecOps lifecycle. Chick's team mapped requirements to capabilities and divided them into four levels. This structure enables organizations to quantifiably evaluate their DevSecOps capabilities, from planning to quality assurance. To fully encompass the socio-technical aspects of the pipeline, the model defines goals and measurements for the roles and responsibilities within the organization.

The model also maps out process flows required in building a secure and resilient DevSecOps pipeline, outlining the different data elements that impact the pipeline, building in security, and applying a measurement framework to allow model users to quantify the health of their DevSecOps pipeline through the development and operational lifecycles—all while reducing time to deployment.

Chick expects the model to be especially useful to government agencies and heavily regulated segments of industry, where implementing DevSecOps at scale can be challenging. The SEI brought decades of experience in developing maturity and capability models—such as the Capability Maturity Model Integration (CMMI), Smart Grid Maturity Model (SGMM), and CERT Resilience Management Model (CERT-RMM)—for just these kinds of organizations. "The DevSecOps model became an opportunity for different teams within the institute to bring all their knowledge and experience into a single resource," said Chick. "The model really represents the whole body of work of the institute."

The model should be released in early 2022, and the SEI seeks organizations to test it by implementing the model and adapting it to different scenarios; for example, in evaluating bids from DevSecOps contractors. Filling the DevSecOps definition gap is just the first step, though. The next phase of SEI research will apply current software assurance techniques to the pipeline and enhance or adapt those techniques to assure both the pipeline and the product, all while keeping pace with the rate of change in current Agile and DevSecOps environments.





"The DevSecOps model became an opportunity for different teams within the institute to bring all their knowledge and experience into a single resource."

TIM CHICK, Systems Team Technical Manager, SEI CERT Division

Enabling the Next Generation of U.S. Nuclear Deterrence

The U.S. Air Force (USAF) is replacing the 50-year-old Minuteman III intercontinental ballistic missile with its Ground Based Strategic Deterrent (GBSD) system. The GBSD will be the modernized land-based leg of the U.S. nuclear triad.

This modernization effort includes improving the infrastructure, technologies, and communication systems that support GBSD. To address the software assurance and cybersecurity of the effort, the SEI will help the GBSD program

- prioritize flexible, upgradeable, software-intensive solutions over hardware-based options
- adopt and implement modern Agile and DevSecOps methodologies
- leverage a shared, cross-program infrastructure
- establish a continuous authority to operate (ATO) with integrated cybersecurity monitoring
- architect a software-based, periodically refreshed nuclear surety environment

Leading with these priorities will allow the government to reliably and securely sustain GBSD against evolving threats for many decades to come.

In 2020, the USAF awarded Northrop Grumman Corporation (NGC) a $13.3 billion contract towards completion of the engineering phase of GBSD in FY29. The SEI's support requires a novel approach where teams from across the institute collaborate with NGC, teams from other federally funded research and development centers (FFRDCs), and the USAF to address issues, many of which have no methodological approaches. Carol Woody, cybersecurity lead of the SEI's GBSD effort, commented, "The SEI is researching solutions, and their integration across all aspects of the program's lifecycle is critical."

Photos U.S. Air Force, U.S. Navy, U.S. Department of Defense

To meet its requirements, GBSD must achieve four particularly challenging goals:

1. Modernize GBSD by applying a range of research areas, many of which are software centric.
2. Integrate these modernized aspects to meet the expansive program requirements while staying within cost and aggressive schedule projections.
3. Introduce precedents and shift mindsets concurrently in many government organizations and supporting vendors: a large-scale implementation of Agile methods to software development, business, and operations; a full DevSecOps pipeline; a hybrid (contractor and government) development team; and continuous ATO.
4. Integrate acquisition practices with cybersecurity and supply chain risk management practices.

SEI researchers are experienced in meeting challenges like these for the Department of Defense (DoD). They integrate SEI research in real-world situations, introduce technology and innovation to organizations, and collaborate with myriad research partners. SEI teams are supporting GBSD with research, risk analysis, and adoption planning.

GBSD is in its early stages. Key SEI contributions and early results include

- improving efficiency and productivity by establishing synchronization and communication at many levels of the GBSD program
- conducting Quantifying Uncertainty in Early Lifecycle Cost Estimation (QUELCE) workshops that identified and prioritized more than 130 significant program execution uncertainties, 20 percent of which materialized but were mitigated through advanced planning

As a key FFRDC partner, the SEI expects to continue its GBSD support for the next five to eight years. "This support represents a great opportunity for SEI longitudinal research in many technical areas, which, in turn, helps GBSD achieve its modernization mission," said Bob Stoddard, the SEI's GBSD lead.

Woody added, "This program also represents a tremendous opportunity for research collaborations between the SEI and GBSD, capitalizing on the trust and health of the customer relationship."

Reports from this modernization of one of the DoD's biggest and most critical programs have already been released to support other nuclear programs and cybersecurity efforts in the USAF. The GBSD promises to be an exemplar for cybersecurity and software assurance in DoD, U.S. government, and defense vendor organizations.

"The SEI is researching solutions, and their integration across all aspects of the program's lifecycle is critical."

CAROL WOODY, Principal Researcher, SEI CERT Division

"The ODE&I is an office, but it's one where everybody can say that they're a member."

PALMA BUTTLES-VALDEZ, Director, Office of Diversity, Equity, and Inclusion, SEI Director's Office

Supporting Innovation Through Diversity, Equity, and Inclusion

Innovating to overcome challenges is the backbone of the SEI's culture and drives the organization's vision of shaping the future of software for a better world. To support this vision, the SEI's Office of Diversity, Equity, and Inclusion (ODE&I) was established to help individuals and teams do their best work by seeking and cultivating diverse populations and perspectives and promoting equity and inclusion. SEI Director Paul Nielsen noted, "Our people are our greatest asset. Through a focus on DE&I, we hope to build a fertile ground for collaboration and innovation. We value different views, different backgrounds, and different approaches to solve the most complex problems in software engineering, cybersecurity, and artificial intelligence engineering."

In 2021, the SEI refreshed its organizational values. The ODE&I played a significant role by ensuring the process was inclusive and reflected the voices of staff members. The SEI's shared organizational values of leading, with integrity; building up people and fostering community; and collaborating to accelerate innovation reflect the ODE&I's guiding principles.

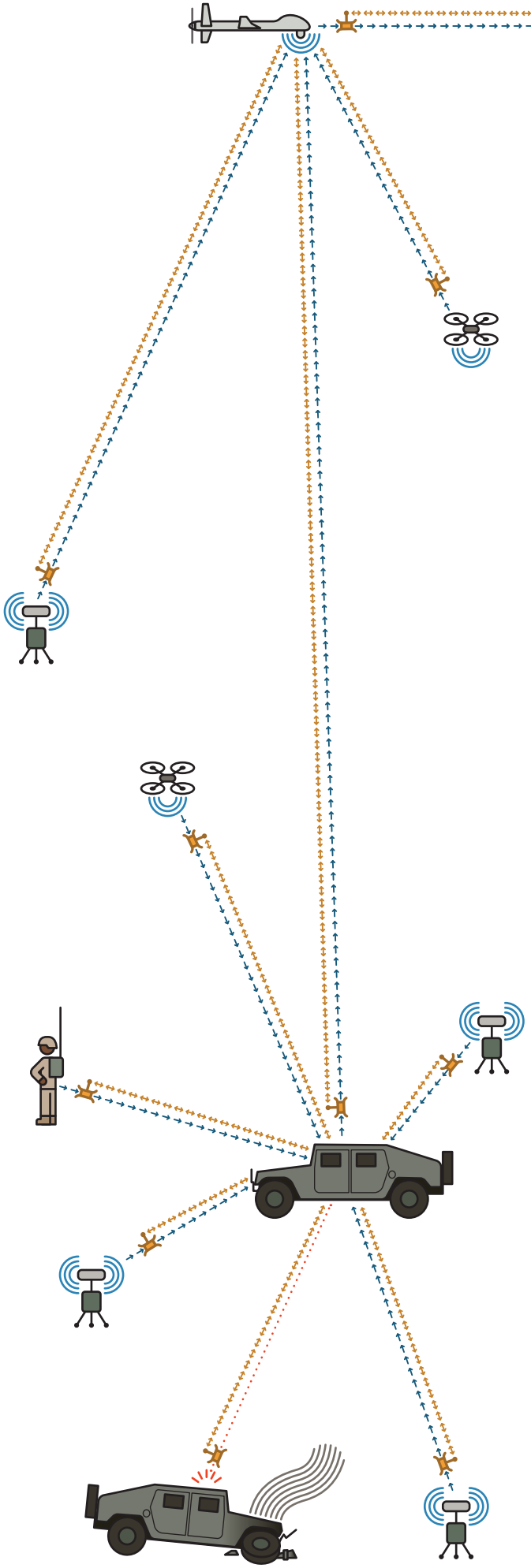
The ODE&I is part of the entire employee lifecycle, from recruiting to exit interviews, and works to ensure each employee feels welcomed and valued in the organization. "The Office of Diversity, Equity, and Inclusion supports employees by providing access to learning resources and opportunities to connect to and celebrate the unique backgrounds and cultures each of us brings to the SEI and our broader community," explained Palma Buttles-Valdez, the office's director.

The ODE&I's goal is to make diversity, equity, and inclusion part of the SEI's cultural DNA. As part of this effort, the ODE&I has been involved in developing bias-free communication guidance, providing opportunities to share and recognize employee pronouns, and adding more inclusive imagery throughout the SEI website.

This past year, the ODE&I has also engaged with the local community and with Carnegie Mellon University (CMU). In one example of a partnership with the local Pittsburgh community, Hill Community Development Corporation (Hill CDC) president and CEO Marimba Milliones gave a talk on community engagement and policy to SEI employees. This was the first in a series of ongoing activities with the Hill CDC, in which SEI employees were encouraged to participate in enrichment and volunteer opportunities.

CMU recently appointed Dr. Wanda Heading-Grant as the vice provost for diversity, equity, and inclusion and chief diversity officer to help build the foundation of DE&I at CMU. "Wanda has asked us to be part of a team that helps her to create a framework that we can all use at CMU," said Buttles-Valdez. Buttles-Valdez has started by sharing the resources that the SEI has created, such as SEI-developed guidance on bias-free language, with the DE&I team at CMU.

Deeply connected to building the best employee experience, the ODE&I is now working to understand how to factor inclusion into the SEI's return-to-office efforts, once staff can transition from the remote work posture brought on by the COVID-19 pandemic. Buttles-Valdez reflected that this effort is about ensuring that employees can do their best work. "I'd love to see DE&I be integrated as a part of everybody's day-to-day life and activities." She added, "The ODE&I is an office, but it's one where everybody can say that they're a member."



Getting the Jump on System Failures in AI-Powered Data Processing Pipelines

Up-to-date intelligence is essential to mission success, and data is essential to accurate and actionable intelligence. Data processing pipelines developed by the Department of Defense (DoD) employ artificial intelligence (AI) and other software capabilities to allow analysts to focus on more important analytical tasks.

These pipelines are complex and can suffer multiple problems. The ability of AI components to make inferences from data may degrade over time, software components might crash, hardware components might be compromised, or pipelines with overtaxed resources may suffer poor throughput. Such issues could impede analysts' ability to support assigned missions or, worse, give them inaccurate information for crucial decision making.

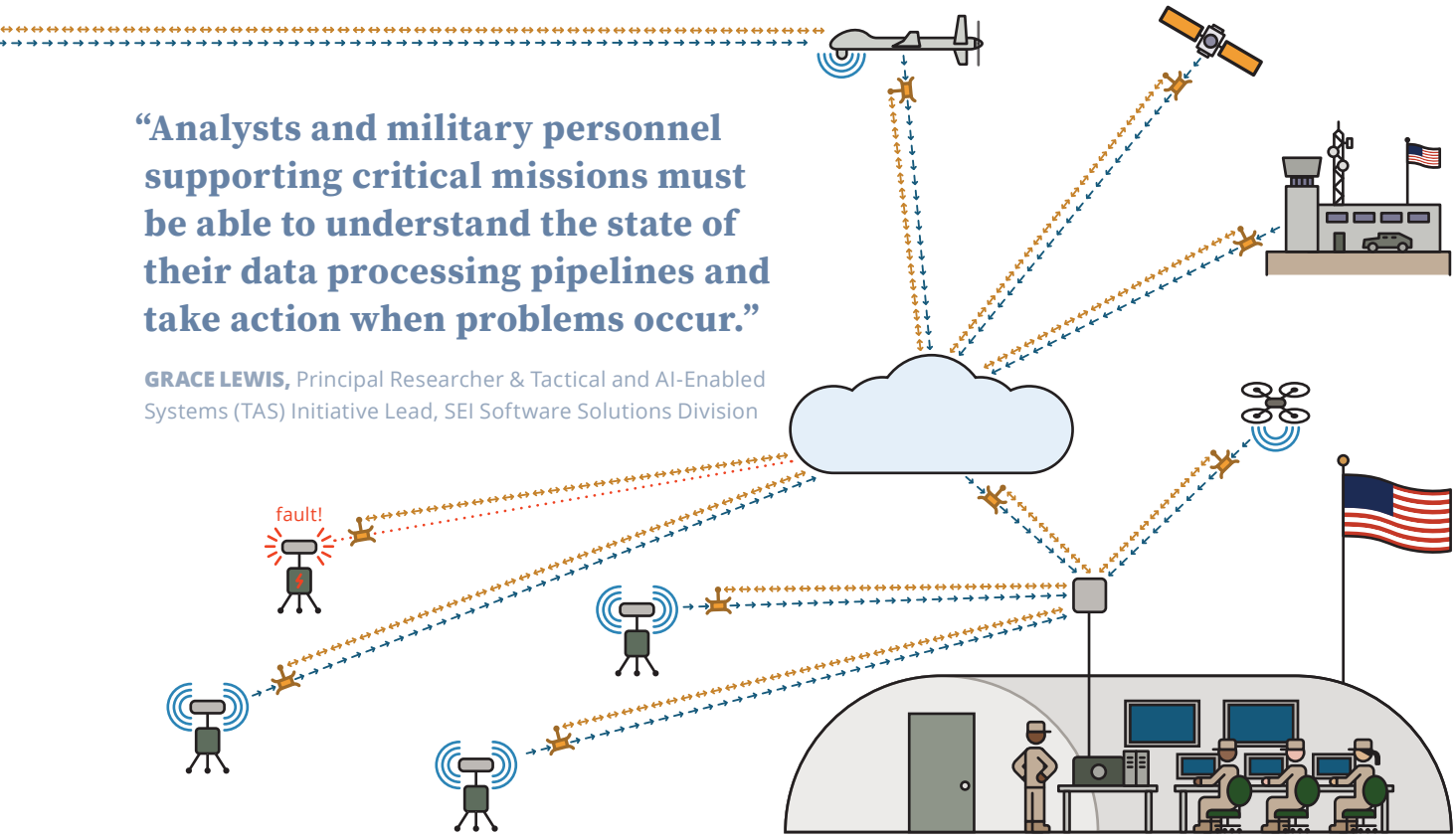
"Analysts and military personnel supporting critical missions must be able to understand the state of their data processing pipelines and take action when problems occur," said Grace Lewis, an SEI principal researcher. "System failures can be easy to detect. Detecting unreliable results of AI components is difficult because the system keeps producing results, but they're inaccurate."

To address this challenge, Lewis and her SEI colleagues are at work on AI End-to-End (AIE), a system for the development, deployment, and monitoring of data processing pipelines that may contain AI components. The goal of AIE, built on earlier SEI work on the Cornerstone resilient situational awareness system for the Office of the Under Secretary of Defense for Research and Engineering (OUSD(R&E)), is to monitor running pipelines and automatically reconstitute them when system or component failures are detected.

Monitoring becomes more complicated when data processing pipelines, especially those with AI

"Analysts and military personnel supporting critical missions must be able to understand the state of their data processing pipelines and take action when problems occur."

GRACE LEWIS, Principal Researcher & Tactical and AI-Enabled Systems (TAS) Initiative Lead, SEI Software Solutions Division



components, are distributed across multiple specialized nodes. "Field sensor data may be processed on a specialized edge device, with results pushed to the cloud for further processing and storage," said Lewis. "All these components might have been developed by different organizations. It's difficult to monitor different types of system elements, such as platforms, networks, software components, and, especially, AI components."

AIE data processing pipelines comprise services or containers with monitoring endpoints that expose component-specific metrics, including special metrics for AI services. During operation, AIE continuously polls these metrics and compares them against thresholds for component failure. If a component fails, AIE replaces the pipeline with an equivalent that can continue to meet mission needs.

Another challenge is continued pipeline operation on infrastructures that involve embedded, sometimes legacy, components, either commercial or developed by the DoD. These infrastructures demand new ways of measurement, modeling, and distributed management that are automated and adapt to a dynamic environment from the application to the physical layer.

The SEI's work on AIE has been integrated into a multi-organization demonstration of automatic reconstitution of an AI-enabled data processing pipeline. The next step is to support deployment and integration of services deployed on edge platforms. Lewis's team intends for AIE to automatically handle failures caused by the challenges of operating in tactical and edge environments, such as limited computing resources and network connectivity. This kind of technology supports robust and secure AI, one of the three pillars of the emerging discipline of AI engineering being led by the SEI.

AIE will enable large-scale automation of capabilities distributed between the cloud and embedded software infrastructures. The work will also allow more resilient, cost effective, and timely deployment of heterogeneous cloud infrastructure and provide a rich environment for fundamental research in system representation and analysis.

"Collaborative development across commercial, government, and DoD partners is critical for the software development and operations approach that allows assessment of the design, deployment, and maintenance phases of large-scale integrated systems," said Robert Bonneau, OUSD(R&E) director of software embedded systems and data analytics. "This approach enables rapid system reconfigurability as well as cost reduction."

Achieving Confidence in Multicore Processors to Enhance DoD Capabilities

Complex, cyber-physical Department of Defense (DoD) systems, such as aircraft, depend on software that does the right thing at the right time to properly and reliably execute crucial sensing, computing, and actuation functions. Timing failure can have disastrous consequences—a delay in translating sensor data into actuation, for instance, can cause system instability and loss of control.

The ever-growing complexity of DoD systems amplifies the need for precise software timing, which demands more processing power. Multicore processors, ubiquitous today, could supply it. But the DoD has been reluctant to take advantage of them because of timing concerns.

"Multicore processors share resources in the memory system," said SEI researcher Bjorn Andersson, "which makes it difficult to get correct timing of the software. Many practitioners disable all processor cores except one. This simplifies software timing verification but reduces the overall system capability." Disabled processor cores also represent unused computing capacity.

Andersson has been leading an effort to overcome obstacles to precise multicore processor timing. The research team brings decades of experience in this area, which the SEI first began investigating in the 1980s with research on rate-monotonic analysis for single-core systems. The team collaborates with Carnegie Mellon University's John Lehoczky and the University of California Riverside's Hyoseung Kim.

"Software systems used in warfighting are embedded computer systems with software that interacts with the physical world," said Andersson. "You have to satisfy

> **"Software systems used in warfighting are embedded computer systems with software that interacts with the physical world. You have to satisfy real-time requirements."**
>
> **BJORN ANDERSSON,** Principal Researcher, SEI Software Solutions Division

real-time requirements." Such critical software timing is determined by many shared resources in the memory system, including cache, memory banks, and memory bus, with complex arbitration mechanisms, some of which are undocumented.

The research team has been working on ways to enable software practitioners to use all processor cores while being confident about timing by providing real-time guarantees to software executing on undocumented multicore processors.

The SEI's approach involves reframing the problem. "Other academic works have modeled the resources in the memory system and developed analytic methods that compute an upper bound on the delay that software can experience," noted Andersson. "We take another view. Instead of modeling the hardware resource, we model the effect of hardware resources on the timing of software: how much software thread A slows down software thread B when A and B execute in parallel." This approach enables the team to analyze the timing of software executing on undocumented multicore processors.

The work has achieved some important objectives:

- **verification**—a method for timing verification that does not depend directly on undocumented design qualities and quantities
- **parameter extraction**—a method for obtaining values for parameters in the model of a software system suited for timing verification
- **configuration**—a configuration procedure, such as assigning threads to processor cores or assigning priorities to threads, that takes a model as input and produces a configuration for which the verification will succeed, if such a configuration exists

SEI expertise on multicore processor timing has influenced the air vehicle certification and qualification guidance of the U.S. Air Force and U.S. Army Aviation and Missile Center (AvMC). Andersson and his colleagues have taught multicore timing techniques within AvMC and demonstrated multicore timing tools. The project's ultimate objective is to provide the DoD with a general-purpose technology that unlocks the capabilities of multicore processors in almost all warfighting systems.

Transitioning the DoD's Software Acquisition Pathway to Programs

Since the October 2020 issuance of Department of Defense Instruction 5000.87 (DoDI 5000.87), the DoD's first software-specific acquisition pathway, the SEI has been working with early adopters of the policy to test its efficacy and deliver capabilities to warfighters.

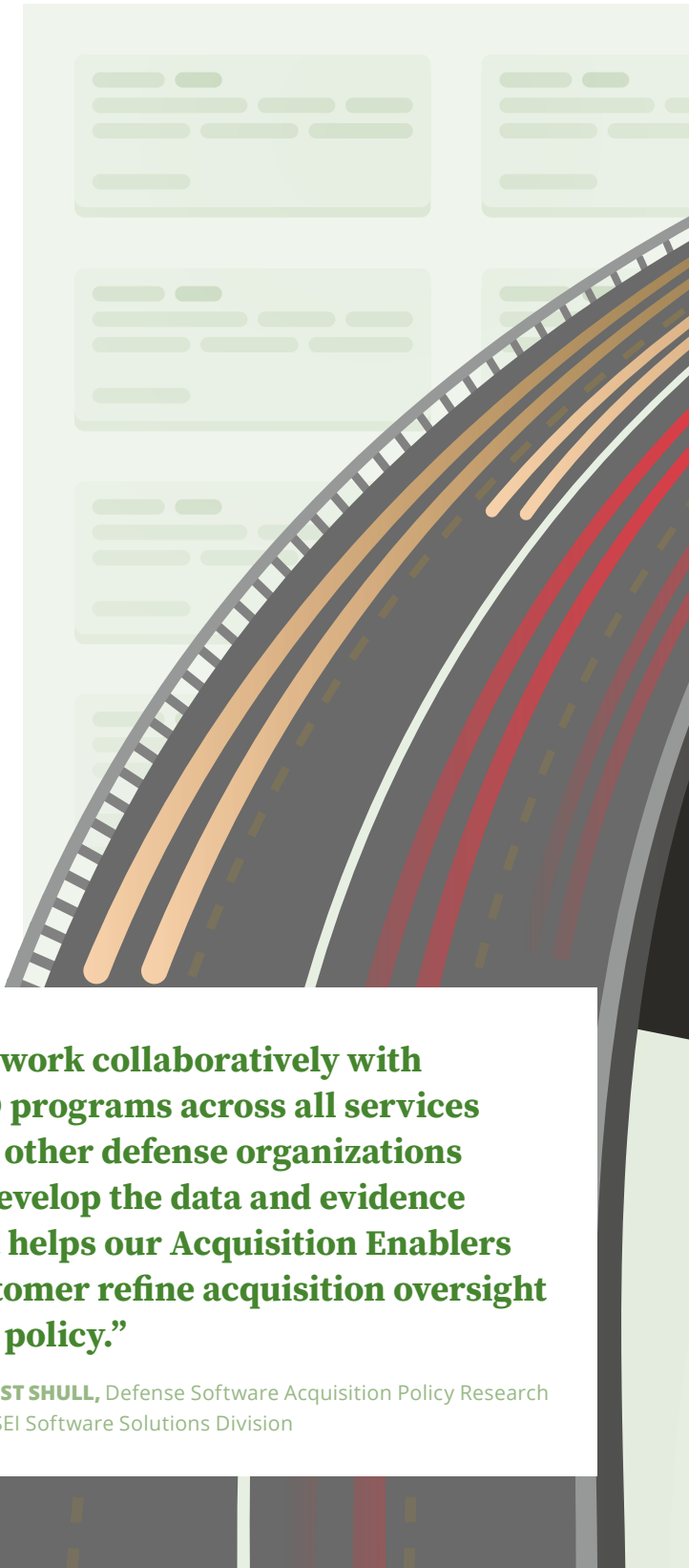
The purpose of DoDI 5000.87 is to enable agile, iterative software delivery to provide capabilities to the warfighter more rapidly. The new policy reflects the DoD's growing recognition that software acquisition for applications and embedded systems needs to be done differently to respond to operational needs.

The software acquisition pathway departs from decades of hardware-based acquisition regulations. The policy aims to help the DoD acquire software by applying modern software practices, including Agile and DevSecOps, to deliver software capabilities with a speed that matches the department's dynamic mission needs, in accordance with Section 800 of the FY20 National Defense Authorization Act (NDAA).

The software acquisition pathway focuses on human-centered design; active, committed user engagement and feedback; the use of enterprise services and platforms; rapid and iterative deliveries; and greater use of automated tools. The SEI team, led by Forrest Shull, lent their expertise in evidence-based research to the development, testing, and updating of the policy as well as to the foundational Defense Innovation Board study, *Software is Never Done*.

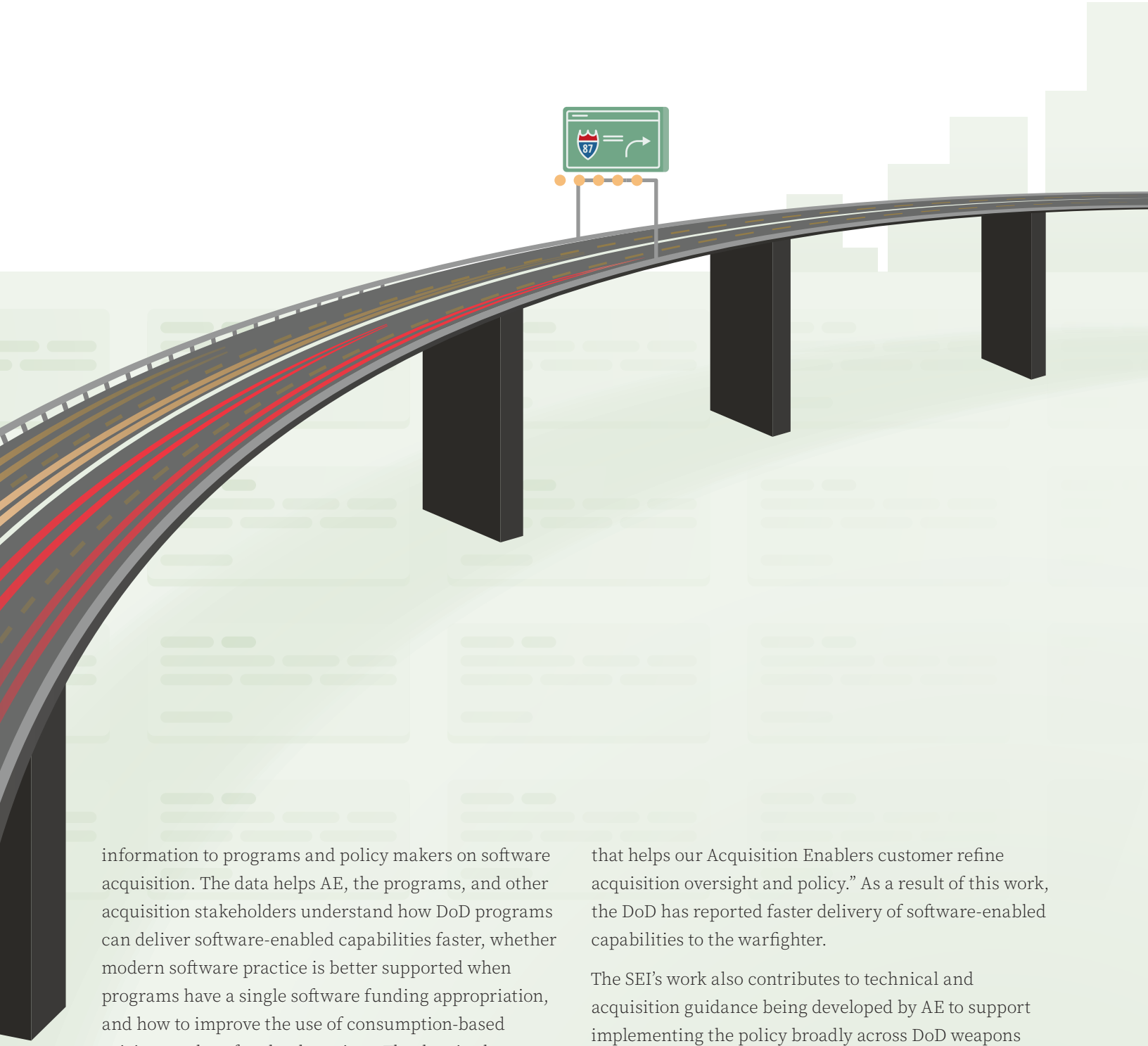
The number of programs adopting the software acquisition pathway continues to climb. These programs and the policy owners need data- and experience-based support adapting the existing policy for a given program's unique environment, as well as determining what changes to policy and guidance would better support the larger DoD enterprise.

The Office of the Deputy Assistant Secretary of Defense for Acquisition Enablers (AE) manages software acquisition policy. The SEI supports AE by designing and executing pilot programs to provide empirical



"We work collaboratively with DoD programs across all services and other defense organizations to develop the data and evidence that helps our Acquisition Enablers customer refine acquisition oversight and policy."

FORREST SHULL, Defense Software Acquisition Policy Research Lead, SEI Software Solutions Division



information to programs and policy makers on software acquisition. The data helps AE, the programs, and other acquisition stakeholders understand how DoD programs can deliver software-enabled capabilities faster, whether modern software practice is better supported when programs have a single software funding appropriation, and how to improve the use of consumption-based pricing, such as for cloud services. The data is also featured in reports to Congress on legal stipulations related to DoD software modernization.

"The SEI is strategically positioned to help programs transition to using the new policy and to help the department evolve it through the experience of programs," says Shull, the SEI's lead for defense software acquisition policy research. "We work collaboratively with DoD programs across all services and other defense organizations to develop the data and evidence that helps our Acquisition Enablers customer refine acquisition oversight and policy." As a result of this work, the DoD has reported faster delivery of software-enabled capabilities to the warfighter.

The SEI's work also contributes to technical and acquisition guidance being developed by AE to support implementing the policy broadly across DoD weapons programs. The SEI is leveraging its extensive research in Agile and Lean techniques, DevSecOps, and technical debt in a variety of DoD contexts.

Accelerating New Capability Through Rapid Certifiable Trust (RCT)

In today's military, as in most sectors, the line between computer and mechanical device has blurred. For such cyber-physical systems (CPS), new and critical capabilities come mostly by way of software rather than hardware. Rapid delivery of new capabilities to CPS helps maintain our nation's strategic advantage. This demand for more rapid deployment, however, requires system verification techniques that can adapt to a faster deployment cadence.

CPS that are complex, involve unpredictable components such as machine learning, or are part of mission- and safety-critical systems can slow or stymie traditional verification techniques. Existing formal methods for verification do not scale to the level of assurance required, and existing testing methods are not reliable. "Department of Defense systems that interact with the physical world, like vehicles and weapons, need to be certified for safety-critical properties before they are deployed, and this certification process is complex and error prone," said Dio de Niz, the SEI's technical director of assuring CPS and lead of the project Rapid Certifiable Trust (RCT).

De Niz and his team are developing techniques to automatically verify critical properties of CPS using scalable formal verification. The team comprises world-class researchers in timing, logic, security, and

"Our solutions make formal methods scalable by ensuring that infrequent but catastrophic erroneous CPS behaviors are monitored and guarded against without compromising capability."

DIO DE NIZ, Technical Director, Assuring Cyber-Physical Systems, SEI Software Solutions Division

control verification and includes experts from Carnegie Mellon University, University of California Riverside, and Washington University in St. Louis. With help from these collaborators, the SEI developed an approach that leaves most of the software unverified and adds small pieces of verified code that enforce the safety-critical properties of interest. The system no longer needs to verify all the software code, only the enforcers.

"We created a new way to monitor and enforce the output of a system to evaluate whether the output is safe and, if not, replace it with a safe one," said de Niz. "Our solutions make formal methods scalable by ensuring that infrequent but catastrophic, erroneous CPS behaviors are monitored and guarded against without compromising capability."

Part of this effort is developing compositional verification techniques to allow operation of multiple enforced components, minimizing and automatically removing conflicting enforcer assumptions—for instance, reducing a plane's airspeed to avoid a crash while increasing airspeed to prevent stalling. These techniques will allow the Department of Defense (DoD) to assure full-scale systems, even if most of their functionality is implemented by unverified components.

The SEI team has presented this work in 17 academic and industrial publications and conferences. It has also produced two open source projects: a real-time mixed-trust computing framework and a verified hypervisor.

The goal of RCT is to reduce the deployment time of CPS by reducing the overall development and assurance times. The technique enables the use of unverified commodity software components, such as open source drone piloting software, guarded by verified enforcers that guarantee the containment of unsafe component behavior. The DoD has long relied on bespoke components, but RCT opens the door to commodity components as a way to improve the rapid deployment of critical capabilities.

Improving System Interoperability with a Data-Centric Universal C2 Language

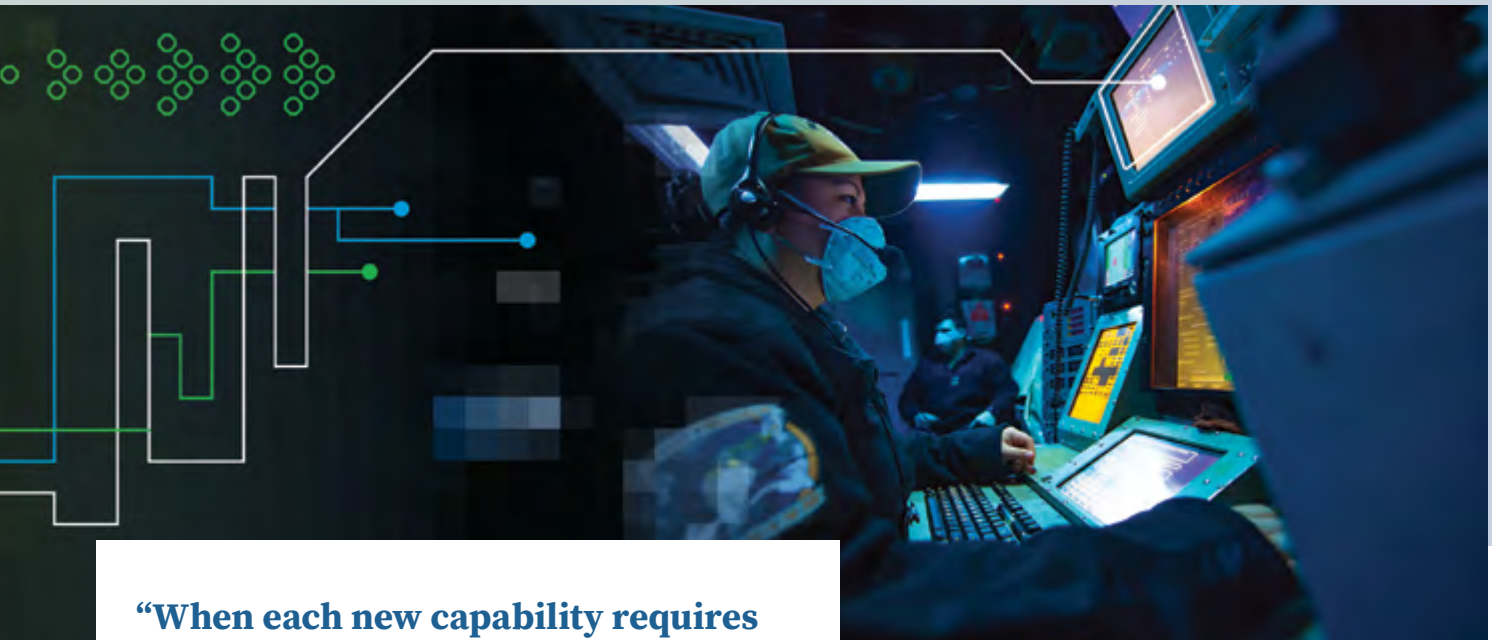
Many incompatible standards are in use for information exchange and storage, impeding Department of Defense (DoD) goals for interoperability and resilience across a range of mission, weapon, and command-and-control (C2) systems. Any solution must address essential variation, imposed by differences in application domains, while eliminating spurious variation due to independent development by vendors and programs. Variation makes everything harder, ultimately hindering interoperability and resilience.

Fully Networked Command, Control, and Communications (FNC3) is a modernization priority of the Office of the Under Secretary of Defense for Research and Engineering (OUSD(R&E)). To address longstanding issues of interoperability and resilience, FNC3 is investing to develop a standard for information exchange that builds on existing C2 protocols to eliminate spurious variation, enables the incorporation of essential variation, and evolves to add new information types and functionality while preserving backward compatibility. The program, called Universal Command and Control (UC2), applies data-centric principles that data should be self-describing and expressed in open source formats.

The UC2 program comprises a set of technical working groups led by a coalition of six federally funded research and development centers (FFRDCs) with representatives from the military. Together, FNC3 and the Aerospace Corporation, the Institute for Defense Analyses Systems and Analyses Center, the MIT Lincoln Laboratory, the MITRE National Security Engineering Center, the RAND National Defense Research Institute, and the SEI are developing a universal C2 language and standard. The SEI brings extensive experience in model-based engineering, C2 architectures, tactical networks, other DoD interoperability standards, and domain experience in air defense and special operations technology.

To be successful, UC2 must not degrade critical qualities, such as latency, message size, data rate, and computational burden. Compliance with the standard must not significantly increase costs compared to current C2 protocols and software architectures. Two main factors affect these costs: encoding method and message structure.

SEI team lead John Klein explained that UC2's data-centric approach is novel: "Many DoD standards define message-centered protocols, with a distinct type of message for each



Photos U.S. Air Force, U.S. Navy

> **"When each new capability requires new messages, that becomes hard to evolve."**
>
> **JOHN KLEIN,** Principal Member of the Technical Staff, SEI Software Solutions Division

type of information. When each new capability requires new messages, that becomes hard to evolve." Modern data-centric practice uses a small set of flexible message types, each carrying many types of information objects defined in a data model. Evolution adds information objects rather than new message types. The data model simplifies translation to and from other operational standards. It also helps engineers rapidly assess the cost of, and risks to, interoperability during an integration.

The UC2 data model carries forward the best approaches of the National Information Exchange Model, the Air Force's Unified Command and Control Initiative, the Army's Integrated Sensor Architecture, the Missile Defense Agency's Adaptable Toolkit for Open Message Service, and other operational standards. UC2 employs modern commercial standards like Efficient XML Interchange (EXI), whose variable-length encoding is more interoperable, evolvable, resilient, and efficient than the legacy formats used in many DoD systems. Klein said, "While some DoD protocols use variable-length encoding, most are customized formats. EXI allows us to participate in the mature ecosystem of XML technology."

UC2 will significantly increase interoperability between diverse DoD platforms while minimizing engineering and operational costs and constraints on system design. The DoD will benefit from easier component reuse and replacement at the system level, easier integration at the system-of-systems level, and improved C2 resilience for the enterprise.

Though development of UC2 continues, early implementations have validated the language and standard, and transition is accelerating. OUSD(R&E) acknowledges that the adoption of a standard like UC2 will be gradual as program offices recognize the benefits for their mission needs. Program offices and industry are invited to collaborate on UC2 system development through existing contractual relationships.

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; Trustee, Carnegie Mellon University

Philip Dowd
Private investor; former Senior Vice President, SunGard Data Systems; Emeritus 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; Emeritus Trustee, Carnegie Mellon University; former Executive Director of Clinical Biostatistics at Merck; Member, New Jersey Bar Association

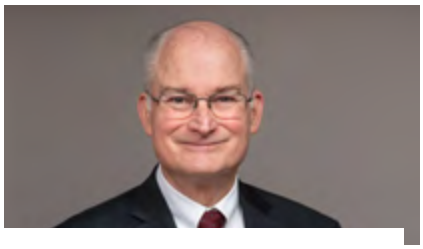
CMU Leadership

Farnam Jahanian
President

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

Daryl Weinert
Vice President for Operations and Interim Vice President for Research

SEI Executive Leadership



Paul Nielsen
Director and Chief Executive Officer

David Thompson
Deputy Director and Chief Operating Officer

Tom Longstaff
Chief Technology Officer

Anita Carleton
Director, Software Solutions Division

Gregory J. Touhill
Director, CERT Division

Matt Gaston
Director, Artificial Intelligence Division

Heidi Magnelia
Chief Financial Officer

Mary Catherine Ward
Chief Strategy Officer

Sandra Brown
General Counsel

SEI Research Teams

Copyright

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

DM22-0269

Credits

Manager, Communication Services
Janet Rex

Manager, Public Relations
Richard Lynch

Manager, Communication Design
Cat Zaccardi

Editor-in-Chief
Paul Ruggiero

Editorial
Ed Desautels
Claire Dixon
Patricia Flinn
Tamara Marshall-Keim
John Morley
Sheela Nath
Sandy Shrum
Barbara White

Design
Christopher Baum

Illustration
Christopher Baum
David Biber
Kurt Hess
Todd Loizes

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