



2013 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 advance the technologies and practices needed to acquire, develop, operate, and sustain software systems that are innovative, affordable, trustworthy, and enduring.

CONTENTS

2	Message from the Director
3	Strategy
4	Areas of Work
5	Funding
6	Advanced Mobile Systems Team Probes the Public Safety Value of Social Media
8	Collaboration Group Spurs Knowledge Sharing Among DoD and Government Agile Users
9	Real-World Agile: Bulletins from the Front Lines
10	SEI and STEM: Encouraging the Software Engineers of Tomorrow
11	SEI's Independent Program Assessment Demonstrates Utility for Large-Scale Systems
12	Making Sense of DoD Software Program Data
14	Cadence Design Systems Nets Improvement from TSP Pilot
15	SEI Team Lends Know-How to National Science Foundation's XSEDE Project
16	Addressing Challenges in Cloud Computing at the Tactical Edge
18	Checkpoint Diagnostic Pilot Illuminates Business Value of Process Improvement
19	TSP-PACE Leverages Data to Measure Software Development Performance Effectiveness
20	Digital Forensics Tools Speed Investigations
22	Insider Threat Center Breaks New Ground on Unintentional Insider Threat
23	Cyber Resilience Reviews Provide DHS a Comprehensive Set of Performance Data, Create Snapshot of Critical Infrastructure Practices
24	New STEPfwd Training Platform Helps U.S. Department of Defense and Its Partners to Train as They Fight
25	Mead Named SEI Fellow
26	To Encourage More Robust Development Practices, CERT Maps Solutions to Microsoft's Simplified Security Development Lifecycle
27	ISO Standard, New Books Among Secure Coding 2013 Highlights
28	Understanding the State of Cyber Intelligence
30	Architecting Systems of the Future
32	Transition
33	Leadership
34	Board of Visitors
35	SEI Organizational Chart
36	Publications
40	SEI Staff and Other Contributors

MESSAGE FROM THE DIRECTOR



Software and cybersecurity challenges are now inseparable, a reality that the Carnegie Mellon University Software Engineering Institute (SEI) has recognized, and acted on, for several years.

In 2013, we realigned the SEI to enable greater impact on solving our nation's toughest software and cybersecurity problems. We pursue our technical agenda through an organization focused on research and development in software solutions, cybersecurity, and emerging technology. In those areas, our strengthened organization delivers value effectively across a spectrum from conducting research, to building and demonstrating prototypes, to transitioning innovative technologies to the U.S. Department of Defense (DoD) and the Defense Industrial Base.

We also welcomed a new Chief Technology Officer, [Dr. Kevin Fall](#). Immediately on joining the organization, Kevin made and implemented strategic decisions to boost the already considerable mission relevance of our technical research plan. In this year, our researchers unveiled, for instance, a prototype tool that automates the malware analysis of suspicious files. Working with researchers at Carnegie Mellon University, we also developed a reference architecture to exploit "cloudlets" that soldiers in the field can access from their mobile devices. In addition, our work with 30 government and industry organizations culminated in frameworks for cyber intelligence tradecraft.

Those achievements, among many others, provide enhanced, ongoing value to our DoD sponsor as well as a significant impact for our defense,

federal, and industry clients—despite a fiscal environment characterized by sequestration and constrained budgets.

At the SEI, however, we are more than merely the sum of our accomplishments. The knowledge, skills, and experience of our men and women have earned our organization a global reputation for quality and innovation. This year, in recognition of her career-long excellence, we named [Dr. Nancy Mead](#) as our newest SEI Fellow. Nancy, who is already an IEEE Fellow, is especially well known for leadership in making software engineering an accepted curriculum and for outstanding contributions to fashioning a model curriculum for software assurance.

Indeed, the passion and dedication of our entire staff resonate through our mission to advance the technologies and practices needed to acquire, develop, operate, and sustain software systems that are innovative, affordable, trustworthy, and enduring.

A handwritten signature in black ink, reading "Paul D. Nielsen". The signature is fluid and cursive, with a long horizontal stroke at the end.

Paul D. Nielsen
Director and CEO

STRATEGY

The SEI achieves its goals through technology innovation and transition. The SEI creates usable technologies, applies them to real problems, and amplifies their impact by accelerating broad adoption.

Create

The SEI addresses significant and pervasive software engineering and cybersecurity problems by

- motivating research
- innovating new technologies
- identifying and adding value to emerging or underused technologies
- improving and adapting existing solutions

SEI technologies and solutions are suitable for application and transition to the software engineering and cybersecurity communities and to organizations that commission, build, use, or evolve systems that are dependent on software. The SEI partners with innovators and researchers to implement these activities.

Apply

The SEI applies and validates new and improved technologies and solutions in real-world government and commercial contexts. Application and validation are required to prove effectiveness, applicability, and transition potential. Solutions and technologies are refined and extended as an intrinsic part of the application activities.

Government and commercial organizations directly benefit from these engagements. In addition, the experience gained by the SEI informs

- the “Create” activities about real-world problems and further adjustments, technologies, and solutions that are needed
- the “Amplify” activities about needed transition artifacts and strategies

The SEI works with early adopters to implement the “Apply” activities.

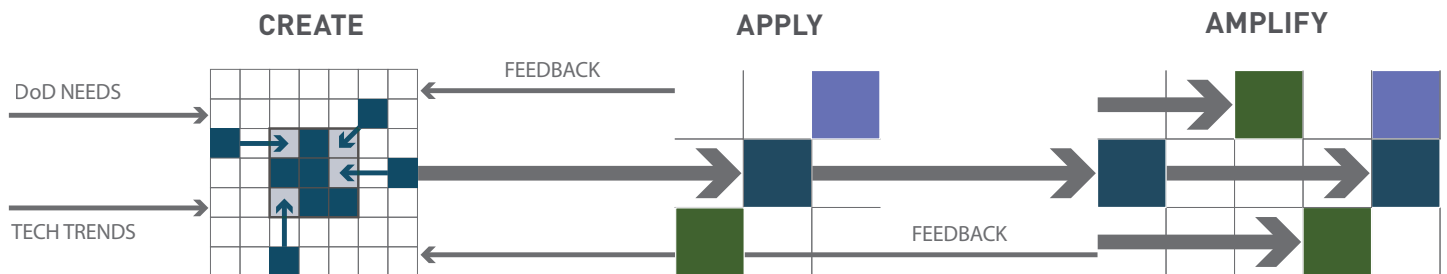
Amplify

The SEI works through the software engineering and cybersecurity communities and organizations dependent on software to encourage and support the widespread adoption of new and improved technologies and solutions through

- advocacy
- books and publications
- courses
- leadership in professional organizations
- licenses for use and delivery
- web-based communication and dissemination

The SEI accelerates the adoption and impact of software engineering and cybersecurity improvements.

The SEI engages directly with the community and through its partners to amplify its work.



AREAS OF WORK

Software is critical to the system capabilities the Department of Defense (DoD) needs to achieve its mission. The pace of innovation in information technology (IT) is unmatched by any other technology crucial to the DoD's mission readiness and success. The expectations placed on software and IT have only increased. If the DoD is to acquire and deploy trustworthy software-enabled capabilities, it must address systems engineering, cybersecurity, and software engineering together from conception to sustainment.

Since 1984, the Carnegie Mellon University Software Engineering Institute (SEI) has served the nation as a federally funded research and development center sponsored by the DoD. The SEI helps organizations improve their ability in order to acquire, develop, operate, and sustain software systems that are innovative, affordable, enduring, and trustworthy.

To support these objectives, the SEI is focusing on several technical directions in the following major areas:

- software engineering, including issues of software system acquisition, design, development, integration, testing, and sustainment
- cybersecurity, including activities related to the security of networks and computers, with a strong focus on deployable tools, methods, and workforce development
- assurance, comprising a combination of techniques in software engineering and security that focus on a “designed-in” approach throughout the software lifecycle
- DoD critical component capabilities, such as cyber-physical systems, high performance computing and parallel algorithms, mobile applications, networking, and autonomous operations

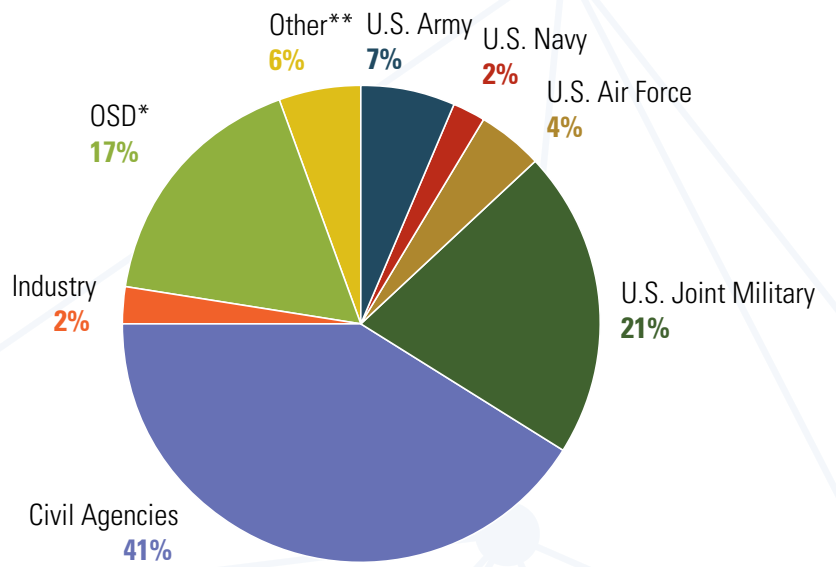
The SEI conducts research and development and publishes findings in these areas, and works together with partners and collaborators in industry, academia, and government. The SEI also undertakes pilot programs to refine best practices and inform our future technical direction. The SEI disseminates mature and proven solutions through software tools, training courses, licensing, and publication of best practices.

FUNDING

In FY 2013, the SEI received funding from a variety of sources in the Department of Defense, civil agencies, and industry.

*funding provided by the Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics—the SEI's primary DoD sponsor—to execute the SEI technical program

**course fees, conference fees, and other recovered costs



ADVANCED MOBILE SYSTEMS TEAM PROBES THE PUBLIC SAFETY VALUE OF SOCIAL MEDIA

As director of the Huntingdon County, Pennsylvania, Emergency Management Agency, Adam Miller must oversee public safety for one of the largest outdoor music festivals in the United States. Each year, the event attracts more than 50,000 attendees, most of whom camp on the festival site's 600 acres.

Miller is ever on the lookout for ways to make this enormous challenge more manageable. In February 2013, his search led him to the Joint Interagency Field Exploration ([JIFX](#)), an event that promotes innovation and collaboration among the Department of Defense, government agencies, industry, universities, and first responders. At JIFX, Miller viewed a demonstration of tools developed by the SEI's [Advanced Mobile Systems Team](#), and he knew that he and the SEI team needed to talk.

"I'm looking at technology paths that can help support the broader prevention and response in mission spaces for the responder community," said Miller. "And, as we talked, I realized the SEI folks were knowledgeable about this mission space."

Miller and the SEI team saw the festival as an opportunity to field test the team's tools and ideas. Specifically, the SEI would test tools that gather and analyze social media data in ways that might support public safety activities.

"Studies have been published that show social media users can respond faster to some natural disaster incidents than even first responders," said the SEI's [Jeff Boleng](#). "People on site immediately communicate information on social media that can be valuable to first responders."

"The challenge for us is cognitive overload resulting from the amount of information available to us in the social media space," noted Miller. "For us to be effective in basing actionable decisions on this broad piece of intelligence, we have to apply business rules to condense it into something that can be acted upon reasonably."

- sentiment analysis: an aggregate gauge of crowd sentiment determined by analysis of individual Tweets
- topic modeling: the categorization of Tweets by content
- entity identification: a natural language analysis to determine nouns and noun phrases in a Tweet



"We had real validation from people directly at the tactical edge that this area of research—the large gathering of people challenge—is captivating."

— Bill Anderson

The SEI team took just six weeks to produce a tool ready for field testing. Informed by social media data associated with the Boston Marathon bombings and Hurricane Sandy, the team's [Edge Analytics](#) tool was designed to produce four kinds of information:

- forensic information for post-incident analysis
- reactive information for near-real-time analysis
- predictive information for analyses that might be useful for alerting public safety officials to potential issues
- preventative information for use by public safety officials to head off problems before they have a chance to escalate

The Edge Analytics tool helped the team process raw festival data streams into more meaningful and potentially actionable information. Specifically, it produced

- keyword alerting: the ability for analysts to set alarms on specified terms

The SEI's [Bill Anderson](#) was encouraged: "We had real validation from people directly at the tactical edge that this area of research—the large gathering of people challenge—is captivating."

Joining Boleng and Anderson on this project were SEI colleagues Joe Seibel, Gene Cahill, Soumya Simanta, Ben Bradshaw, and Derrick Karimi.

Miller sees great promise in the work the team is doing. "It's a starting point, but we saw real-world examples of where efficiencies can be found. And this is only a small sample. Imagine if we were able to grow this thing."

For more information about the work of the Advanced Mobile Systems team, please visit <http://www.sei.cmu.edu/about/organization/softwareolutions/mobile-systems.cfm>.



Gene Cahill



Soumya Simanta

“We’re trying to keep people safe, to allow them to go about their business unobstructed from the challenges in the environment they may face. We want to empower them to make the right decisions.”

– Adam Miller, Director,
Huntingdon County Emergency Management Agency

COLLABORATION GROUP SPURS KNOWLEDGE SHARING AMONG DoD AND GOVERNMENT AGILE USERS

The SEI's leadership in exploring the application of [Agile](#) methods in large and complex systems continued to grow during 2013. Agile is an iterative approach to software development that emphasizes collaboration and a lightweight governance framework. It is designed to be cost effective, timely, and adaptable.

For the past several years, the SEI has led research into the appropriateness of applying Agile methods to the development of complex and large-scale software projects, such as those often pursued by the Department of Defense (DoD). From that effort has sprung a series of SEI technical notes on adapting Agile to DoD programs—and the development of the Agile Collaboration Group.

The SEI's [Mary Ann Lapham](#) has played a key role as the leader of one branch of the SEI's Agile efforts and is a founder of the group.

The Agile Collaboration Group grew from a handful of like-minded people interested in Agile in 2011. “We had about 15 members in the first year,” Lapham said, “growing past 100 in 2013.” The group now includes representatives from the DoD, the armed forces, industry, federal agencies, and academia.

The group provides a forum for sharing experience and knowledge about applying Agile in larger programs. By pooling members' Agile experiences and knowledge, the group saves members time and helps shortcut the learning curve for applying Agile methods, Lapham said.

“We're able to provide a map,” she added, noting that the Agile Collaboration Group comprises organizations with a range of experience—from those just starting with Agile to those with ongoing experience in using Agile methods daily.

For the DoD, the SEI's customer for Agile research and development, the Agile Collaboration Group has yielded a continuing stream of unbiased guidance on using Agile methods and has become a resource for “lessons learned” about applying Agile to larger-scale projects.

To read recent research completed with help from Agile Collaboration Group members, please visit: <http://resources.sei.cmu.edu/library/asset-view.cfm?assetid=77747>.

The Agile Collaboration Group provides a forum for sharing experience and knowledge about applying Agile in larger programs. By pooling members' Agile experiences and knowledge, the group saves members time and helps shortcut the learning curve for applying Agile methods.



REAL-WORLD AGILE: BULLETINS FROM THE FRONT LINES

The 10-Point Plan for IT Modernization released in 2012 by the Department of Defense (DoD) calls for streamlined processing by “Enabling Agile IT.” To help those who work in the DoD and other federal agencies understand and, where appropriate, adopt Agile, two members of the SEI technical staff have launched a series of podcasts exploring real-world experiences in Agile acquisition.

Each episode in the “[Agile in the DoD](#)” series features Mary Ann Lapham, a principal engineer, and [Suzanne Miller](#), a principal researcher, both of whom work with federal agencies adopting Agile. In each episode, Miller and Lapham discuss their real-world experiences applying each of the 12 principles behind the [Agile Manifesto](#),

which outlines a software development philosophy that stresses individuals and interactions over processes and tools; working software over comprehensive documentation; customer collaboration over contract negotiation; and responding to change over following a plan.

“This is an ongoing part of the SEI’s mission to serve as an honest broker of information to our stakeholders,” said Miller, who spearheaded the series. The episodes are published as part of the SEI Podcast Series, which was launched in September 2012 and features research in the fields of acquisition, service-oriented architecture, software architecture, measurement, and other areas.

In each podcast, researchers interview other researchers to ensure that discussions cover topics relevant to practitioners in government, industry, and academia.

The SEI Podcast Series is available on the SEI website. Listeners may subscribe to these podcasts on Carnegie Mellon University’s iTunes U site. A new episode is added to the SEI Podcast Series every two weeks.

To listen to installments of the “Agile in the DoD” podcast series, please visit <http://www.sei.cmu.edu/podcasts/agile-in-the-dod/index.cfm>.

“This is an ongoing part of the SEI’s mission to serve as an honest broker of information to our stakeholders.”

– Suzanne Miller



Suzanne Miller and Mary Ann Lapham



SEI AND STEM: ENCOURAGING THE SOFTWARE ENGINEERS OF TOMORROW

A workforce knowledgeable in science, technology, engineering, and mathematics (STEM) is vital if the United States is to remain competitive on the global stage. These disciplines are also essential to ensuring the nation's defense in an ever-more-complex strategic environment. Unfortunately, the number of U.S. college students seeking a degree in one of the STEM disciplines has remained flat for more than 10 years. Leaders in both industry and government have expressed concern over a widening "skills gap" in which native talent is insufficient to meet the growing demand for STEM expertise. This is why the SEI's sponsor, the Office of the

Secretary of Defense (OSD), has made one of its mission goals the promotion of a workforce qualified to take on the toughest technological challenges confronting national defense.

Recognizing the serious dilemmas posed by the skills gap, educators and practicing professionals have undertaken a variety of programs to raise awareness and encourage young people to investigate the exciting possibilities available in STEM careers. In 2013, the SEI joined the effort by launching its own STEM initiative. "For years, SEI volunteers have been participating on their own in local and national STEM efforts to develop the

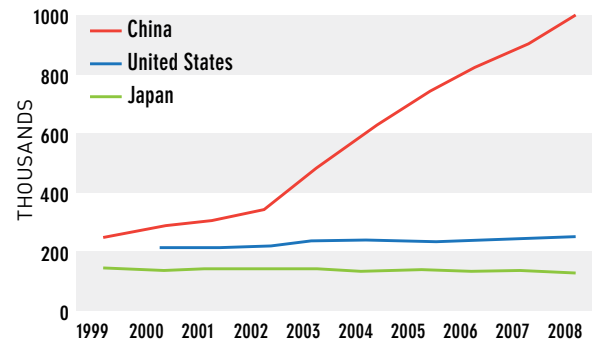
technology workforce the United States needs for the future," said the SEI's [Gail Newton](#), senior project manager and STEM Forum chairperson. "The short-term goal of the SEI's STEM initiative is to establish a framework for our staff to better promote STEM opportunities and provide them a toolkit for success." Newton added that the long-term goal of the SEI STEM effort is to effectively match SEI personnel and resources to STEM opportunities and requests arising from schools, students, and other organizations.



"The short-term goal of the SEI's STEM initiative is to establish a framework for our staff to better promote STEM opportunities and provide them a toolkit for success."

– Gail Newton

STEM COLLEGE DEGREES ATTAINED



Source: National Science Foundation, National Science Board



Photo: USACE

SEI'S INDEPENDENT PROGRAM ASSESSMENT DEMONSTRATES UTILITY FOR LARGE-SCALE SYSTEMS

Since 1998, the SEI has conducted independent technical assessments (ITAs) of more than 100 software-intensive programs for the Department of Defense and other government organizations. The institute has developed a reputation as an unbiased honest broker in conducting these analyses, and the results are used to inform critical leadership decisions about the future course of complex and costly programs.

In 2013, the SEI completed one of the largest and most comprehensive of these studies: an independent program assessment of Pennsylvania's Unemployment Compensation Modernization System (UCMS) project. The Commonwealth had made a substantial investment in a comprehensive and complex effort to replace legacy information systems, as well as add new capabilities, to enable the administration of the unemployment insurance program for Pennsylvania

citizens applying for benefits and the Commonwealth's employers who pay unemployment taxes.

In 2012, with the UCMS project significantly behind schedule and over budget, the Pennsylvania Department of Labor and Industry (DLI) engaged the SEI to conduct a comprehensive assessment of the UCMS program to better understand the problems besetting the UCMS project and to help inform future decisions. The SEI is scheduled to provide technical assistance into 2014.

"This was not a typical ITA, but rather a lifecycle program assessment," noted Michael McLendon, who led the assessment for the SEI. "The scope of the effort was comprehensive in addressing the programmatic and technical aspects of the UCMS lifecycle, from the original procurement solicitation and source selection to contract and project execution, then to plans for system sustainment."

The governor of Pennsylvania and the secretary of the DLI released the SEI's comprehensive report to the public in July and announced their decision to terminate the contract. This result generated significant media interest and discussion about the management of large, government-funded technical programs.

"The decision by the Commonwealth does not end our relationship with DLI," added McLendon. "We will continue to work with the Commonwealth in 2014 to provide a range of technical assistance to enhance their technical capabilities."

To read the SEI's report to the Commonwealth of Pennsylvania Department of Labor and Industry, please visit <http://www.portal.state.pa.us/portal/server.pt?open=18&objID=1351417&mode=2>.





SOFTWARE SOLUTIONS

MAKING SENSE OF DoD SOFTWARE PROGRAM DATA



“DoD programs are constantly running into software-development problems in terms of schedule, size, performance, and cost. Anything that can help them get a handle on that is something we see as valuable.”

– Jim McCurley

The DoD Cost Assessment and Program Evaluation (CAPE) Directorate provides independent analytical advice to the Secretary of Defense on all aspects of Major Defense Acquisition Programs (MDAPs). DoD contractors for MDAPs are required to submit to CAPE a significant amount of data about software development in a Software Resources Data Report (SRDR). This reporting requirement provides initial baseline estimates of time and effort by phase, code size, programming language, and other information about the planned software development. When the project is complete, contractors must also report actual results about the software development.

Together, these reports provide a set of planned and actual data with great potential for informing policy, decision making, and cost estimation. Unfortunately, no standards govern the way in which this data is collected and formatted, making potentially fruitful analysis difficult if not impossible. A team of SEI researchers set about tackling this problem in 2013.

In aggregate, SRDRs represent an unprecedented research opportunity for understanding the state of software development in DoD programs. “The fact that they’ve been collecting data from contractors for 10 years now without deriving much analytical value out of it is really the crux of why we’re working with this data,” says Brad Clark, a visiting scientist at the SEI. Unlocking the information in SRDRs provides a quantitative lens into software development as it occurs within major defense programs.

The process for reporting SRDRs makes analyzing it challenging. Flexibility is intentionally provided in the submission process. However, this makes aggregating the data for analysis impossible without considerable effort. Currently, the information is stored in a hierarchy of files and directories that organize the submissions, rather than in a database that can easily be accessed for analytical purposes. Further, many fields allow the submitters to use their own local definitions and measures. While allowing contractors to use their own formats and data definitions provides flexibility, this flexibility places a burden on those wanting to analyze the data, particularly across programs.

To address this problem, the SEI developed methods to extract the data from disparate SRDR sources and store it in the Software Cost Analysis Repository (SCAR) to facilitate research. “With data scraping,” says Clark, “we pull this information out of individual SRDRs and put it into a regular, accessible format that can be queried: a database. We then use the data to do research on software development practices related to duration, effort, size, and cost of projects.”

One output of the SCAR is a *DoD Software Factbook* aimed at decision makers in the DoD. The SEI team released an initial version of the *Factbook* in January 2014. The *Factbook* provides descriptive statistics on the DoD software portfolio as it is reflected in the SRDR data. In addition to descriptive information on the DoD software portfolio, it also provides analyses of the following three questions:

- Is there a difference in the amount of effort required to produce different types of software? If so, what are the differences and what types are most and least expensive?
- What is the relationship between effort and schedule? To what extent can additional effort be used to realize a shorter development schedule?
- For different types of software, what is the distribution of performance in terms of effort and schedule for projects of a given size?

Answers to questions such as these will help policy and acquisition decision makers to better understand, in a quantitative manner, the performance of those developing software for the DoD as well as the characteristics of the portfolio overall.

The initial *Factbook* is based on a subset of the reported information. The SEI team is currently working to extract the data from the submitted forms, check its quality and integrity, and migrate it to a database. Once the team completes the scraping and migration, it plans to produce additional editions of the *Factbook* and expand its analyses to focus on current policy and acquisition issues. These could include questions about the impact of reuse on productivity and whether concurrent development delivers systems faster.

“SRDRs are a valuable data asset that has been very much underutilized,” says [Jim McCurley](#), a senior member of the SEI technical staff. “DoD programs are constantly running into software development problems in terms of schedule, size, technical performance, and cost. SRDR data analysis to inform decision makers would be a valuable contribution.”

CADENCE DESIGN SYSTEMS NETS IMPROVEMENT FROM TSP PILOT

Cadence Design Systems, Inc., a leading provider of electronic design automation and semiconductor intellectual property, recently conducted a two-year pilot study of the Team Software Process (TSP). Cadence turned to TSP as part of its ongoing mission to improve developer productivity and product quality, and to remain competitive. In 2013, it conducted a study to measure the effectiveness of its TSP pilot and reported its findings at the 2013 TSP Symposium. The study employed data, such as the number of lines of code added or modified, and other change request data. In short, the results were good.

“Our early pilot team has been able to show a significant improvement in the quality of software released,” said Elias Fallon, engineering director for the Cadence development team piloting TSP. “The team was able to use the data to effect meaningful change on their own processes, with quantifiable results.”



Jim McHale

“When Cadence completes rollout of TSP in the 2017-2018 timeframe, the company will likely be the largest single user of TSP with well over 2,000 developers worldwide.”

– Jim McHale

The pilot study revealed a shift away from time spent on unit testing and toward code review. A related measure indicated that defect removal shifted away from the late-stage unit testing and, again, toward the earlier code review and code inspection stages of development. (Identifying defects

not higher” than before it began using TSP, according to Fallon. “The team clearly believes in TSP, and believes it is improving the overall quality of the code, reducing our overall software debt.”

“Our early pilot team has been able to show a significant improvement in the quality of software released.”

– Elias Fallon, Cadence Design Systems, Inc.

earlier in the lifecycle has been shown to improve efficiency and reduce cost.)

The study also showed a decrease in incoming change request bugs over time, as well as a decreasing number of defects per thousand lines of code. Total time on task remained the same under TSP, and the team’s productivity (in terms of functionality delivered) remained “just as high if

The report “Experience Report: Applying and Introducing TSP to Electronic Design Automation,” authored by Fallon and Lee Gazlay of Cadence, is part of the TSP Symposium Proceedings: <http://resources.sei.cmu.edu/library/author.cfm?authorid=28506>.

SEI TEAM LENDS KNOW-HOW TO NATIONAL SCIENCE FOUNDATION'S XSEDE PROJECT

In 2011, Carnegie Mellon University (CMU) joined 16 other organizations selected by the National Science Foundation (NSF) to collaborate on the Extreme Science and Engineering Discovery Environment (XSEDE) project, a five-year, \$130 million effort. XSEDE builds on the TeraGrid supercomputing network and provides researchers open access to state-of-the-art computational tools and digital resources.

As part of the CMU team, the SEI has played a significant role. “The SEI has been an enormously beneficial partner to the project in helping XSEDE to understand formal software and systems engineering practice and to adapt that practice to the very non-traditional context of XSEDE,” said John Towns, XSEDE principal investigator and project director.

To bring formal practice to the NSF community, the SEI developed a twofold approach, first establishing sound engineering practices to enable systematic, measured improvement in products and services. It is also introducing novel engineering practices to address unique challenges arising from XSEDE’s status as a highly distributed NSF/Office of Cyberinfrastructure (OCI) socio-technical ecosystem.

SEI staff members [Felix Bachmann](#), [Kurt Wallnau](#), [Linda Northrop](#), [Michael Konrad](#), [Scott Hissam](#), and [Rhonda Brown](#) worked with XSEDE to refine and document software engineering processes to enable effective iterative and incremental development. They further collaborated to define and institutionalize use-case development and active design review—a technique that advances effective communication

during software design. The team also conducted an initial study to identify engineering practices for engineering ecosystems.

Bachmann explains, “XSEDE exemplifies a software development ecosystem that many development organizations face or are about to embrace, where social science plays a major role alongside software engineering practices.”

Plans are in place to build on XSEDE’s success in adopting architecture-centric engineering and other SEI approaches. The goal is to transition them to practices more viable for conducting engineering at ecosystem scale.

For more information about the XSEDE project, please visit <https://www.xsede.org/>.



“The SEI has been an enormously beneficial partner to the project in helping XSEDE to understand formal software and systems engineering practice and to adapt that practice to the very non-traditional context of XSEDE.”

— John Towns, XSEDE principal investigator and project director



Felix Bachmann



Kurt Wallnau



Linda Northrop



John Towns

ADDRESSING CHALLENGES IN CLOUD COMPUTING AT THE TACTICAL EDGE

At the Armed Forces Communications and Electronics Association ([AFCEA](#)) International [2011 Joint Warfighting Conference](#), Colonel Timothy Hill, director of the Futures Directorate of the Army Intelligence and Security Command, said that “the cloud is one of the top 25 initiatives” for the Department of Defense (DoD) Chief Information Officer. During a panel that discussed the question “How Do We Provide Assured Comms to the Warfighter?” Hill stressed the importance of “cloud technology for the flexibility that it provides” and “the power that it provides to handle the data that our operators or analysts expect to see.”

In an attempt to move cloud computing benefits closer to soldiers in the field, first responders, and disaster-relief workers, the SEI’s [Advanced Mobile Systems Initiative](#), led by [Edwin Morris](#) and [Grace Lewis](#), has developed a software solution that enables the quick deployment of “tactical cloudlets.” These are discoverable, localized, stateless servers running one or more virtual machines on which soldiers can offload heavy, resource-intensive computations from their mobile devices.

[Cloudlets](#) are in single-hop proximity to the mobile devices they serve, such as in a tactical operations center, a vehicle on the ground, or an unmanned aerial vehicle flying overhead. This proximity decreases latency, improves network resilience, and potentially lowers battery consumption. The virtual-machine technology in

cloudlets provides greater flexibility in the type and platform of applications, reduces setup and administration time, and enables live migration, which is critical for systems in the field. [Dr. Mahadev Satyanarayanan](#) and Kiryong Ha of the Carnegie Mellon School of Computer Science collaborated on this work.

Colonel Hill also encouraged industry to use open standards for cloud computing. “We need to have private clouds offered in a nonproprietary, open architecture that allows us to leverage the entire commercial market,” Hill said. Although delivering an enterprise cloud is an important IT initiative for the DoD, Hill stated that the DoD lacks guidance on which standards will best support the different technologies that it uses.

Many in the cloud-computing community believe that the lack of interoperability hinders adoption. “Industry, civil agencies, and the DoD have similar interests in cloud interoperability,” Lewis said. “They all want to avoid vendor lock-in.” Vendor lock-in is the inability to move resources from one cloud provider to another if a relationship with a provider is not working. Portability, the ability to move a system from one platform to another, is thus a key quality attribute for cloud services.

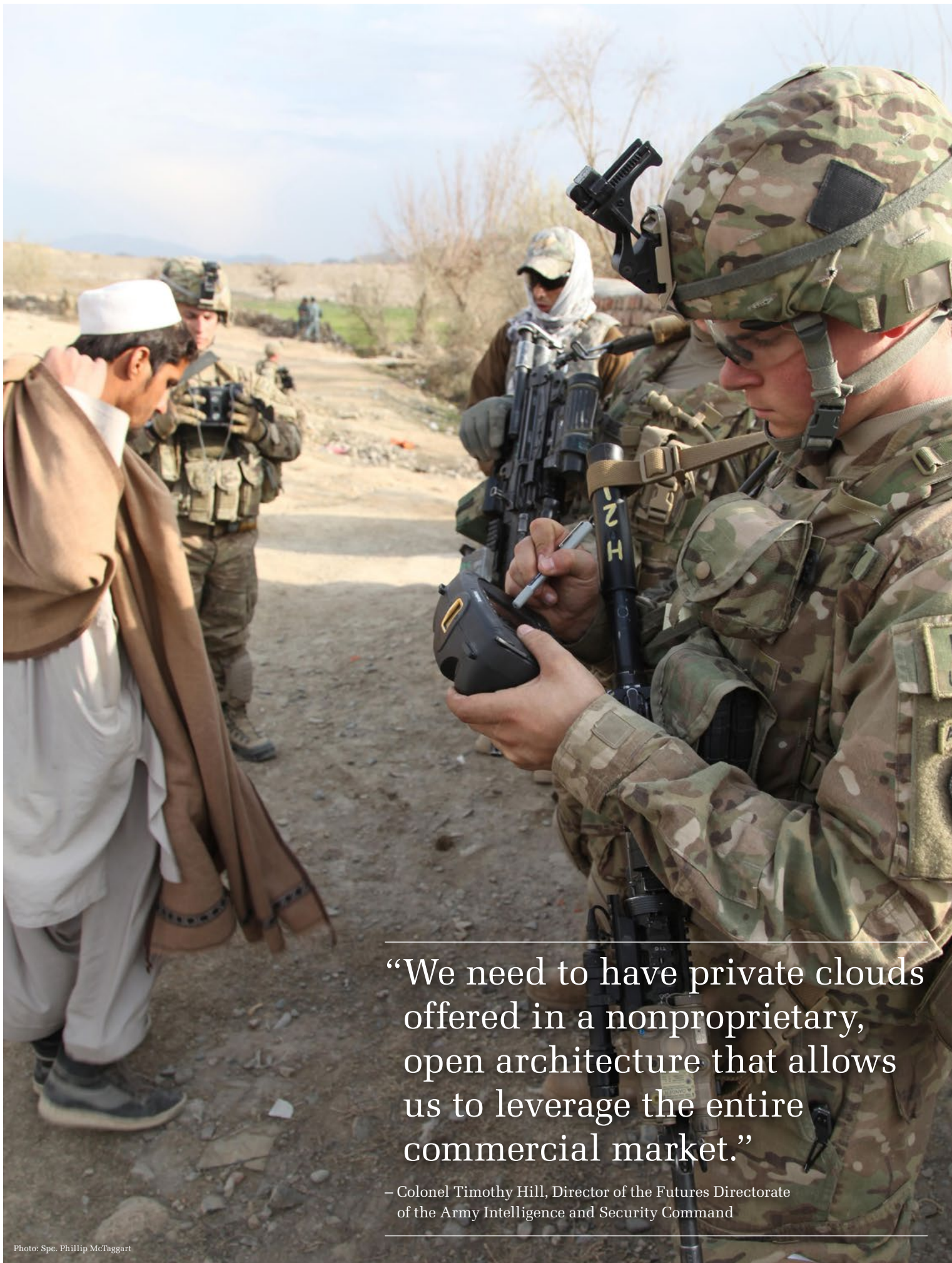
Using this quality attribute perspective, Lewis’s research has also explored the role of standards in cloud computing and offers recommendations for future standardization efforts, software

architects developing systems for the cloud, and organizations that are moving their computing needs to the cloud. As far as standards, Lewis recommends that standardization working groups initially focus on user authentication, workload migration, data migration, and workload management, which will serve as a starting point for the more dynamic use cases of the future. Workload migration, for example, would benefit greatly from standardized representations of virtual machine images that can be easily moved from one provider to another, or from public to private clouds and vice versa, or even to cloudlets at the edge.

To learn more about the SEI’s research on cloudlets and cloud computing, please visit <http://www.sei.cmu.edu/mobilecomputing/research/cyberforaging/index.cfm>.



Grace Lewis



“We need to have private clouds offered in a nonproprietary, open architecture that allows us to leverage the entire commercial market.”

– Colonel Timothy Hill, Director of the Futures Directorate of the Army Intelligence and Security Command

CHECKPOINT DIAGNOSTIC PILOT ILLUMINATES BUSINESS VALUE OF PROCESS IMPROVEMENT

One of the SEI's newest investigative approaches, the [Checkpoint Diagnostic](#), arose out of the SEI's 20 years of experience working with systems development organizations. A short, inexpensive diagnostic—as opposed to a full-blown appraisal—it maps a software development organization's business value against a best-practices model. By so doing, it provides organizations with actionable, performance-related information and analysis closely linked to business value. Using process models, data mapping, and quantitative analytics, the Checkpoint Diagnostic provides organizations

- qualitative process baselines: an analysis of project practices (against a best-practice model) and the associated artifacts, identification of key strengths and weaknesses, and process characterization

- quantitative performance baselines: project data and analysis designed to provide a performance baseline
- a benchmark performance comparison: SEI and benchmark data is used to compare the organization's performance to industry
- a prioritized list of improvement opportunities with estimated quantitative benefits and measurable improvement goals

In a 15-month pilot begun in May 2012 and concluded in July 2013, the SEI used the Checkpoint Diagnostic to establish the pilot organization's baseline performance. "We then rolled out the Team Software Process (TSP) throughout the organization," said the SEI's [Timothy Chick](#). "They released several versions of their software using the TSP methodology. We then conducted a second Checkpoint Diagnostic in July 2013 and compared the results against the baseline."

Chick and his colleagues observed that, within 15 months, TSP had resulted in a 43 percent reduction in defects reported by the pilot organization's customers and a 53 percent reduction in the number of defects found in verification and validation testing. "They also improved schedule delivery predictability while maintaining their productivity," noted Chick. This kind of improvement has a direct and positive impact on customer experience and demonstrates the business value of a TSP process improvement effort.

To view a webinar on the Checkpoint Diagnostic, please visit <http://resources.sei.cmu.edu/library/asset-view.cfm?assetid=59094>.



Timothy Chick

The Checkpoint Diagnostic uses process models, data mapping, and quantitative analytics to provide organizations with actionable, performance-related information and analysis closely linked to business value.

TSP-PACE LEVERAGES DATA TO MEASURE SOFTWARE DEVELOPMENT PERFORMANCE EFFECTIVENESS

In 2013, the SEI introduced the TSP Performance and Capability Evaluation ([TSP-PACE](#)). TSP-PACE provides an objective way to evaluate software development organizations by using the data collected by development projects employing [TSP](#). It includes a performance profile, which can be useful to organizations seeking to acquire software products from suppliers because it provides an independently and factually demonstrated evaluation of the organization's ability to develop and deliver software.

The TSP-PACE process can also be used to evaluate projects, programs, and organizations. Evidence can be used by management, software acquirers, or acquisition authorities as assurance that specific programs are correctly using sound methods and have successfully produced timely and high-quality work. Certification can also be used by software development and service organizations to distinguish themselves from their less capable competitors.

TSP is a disciplined development method that stresses realistic planning, process definition, disciplined execution of the process, commitment to quality, precise measurement, and individual commitment to continuous improvement. Organizations using TSP have reliably produced high-quality software at reasonable cost. Those organizations earning certification through TSP-PACE can readily demonstrate that

- the quality of their work is determined by the quality of the processes their people use
- the TSP process, when properly used, produces superior work outcomes
- organizations adopting TSP will do superior work

“There are some perceived limitations to conventional process- and compliance-based evaluations,” said the SEI's [Bill Nichols](#). “TSP-PACE goes a step beyond by measuring performance and outcomes. We ask, ‘What have they done? What were the results? And why do we think they can do it again?’ We can do

this because TSP developers keep their own personal engineering logs. They personally measure the results as they perform their work.”

Nichols noted these contemporaneous records are ideal for retrospective analyses. “We use summaries of their records to verify that they know what to do, they accurately record what they did, they can actually do it, and to determine how well it worked. We've done the analyses, and it works.”

Nichols and his colleagues have completed the initial pilots of PACE and are ready to provide PACE evaluations. They encourage organizations using TSP to consider an evaluation.

Interested organizations should contact info@sei.cmu.edu.



Bill Nichols

DIGITAL FORENSICS TOOLS SPEED INVESTIGATIONS

[Digital forensics](#) can be a complicated and time-consuming process. When law enforcement investigators confiscate a hard drive, they need to find out what's on it, and they need to know how any malicious or unfamiliar software behaves. These investigators often rely on far-flung experts who spend valuable investigation time on complex solutions that are costly and can add weeks or months to investigations. In many cases, basic triage can provide investigators with the information they seek. [Live View](#) and Malicious Code Automated Run-Time Analysis ([MCARTA](#)), two tools developed by the SEI, give investigators the ability to do their own triage quickly, affordably, and with minimal training.

A new version of Live View helps investigators gain a quick understanding of a confiscated computer's software and data. Using a disk image—a complete copy of all the software and data on a computer—Live View allows investigators to boot up a confiscated machine and interact with it in a safe and isolated environment, all while preserving the integrity of the evidence. Behind the scenes, Live View stores the original disk image on a read-only server; all interaction takes place in a virtual environment and is shown to the user in a web browser. Live View enables investigators to perform these operations with little training and in minutes. It also allows investigators to collaborate in a shared session.

“With Live View, anyone with minimal training can stand up a system, log in, and see what's going on to avoid lengthy investigations using lower-level tools,”

said Alex Corn, a member of the SEI technical staff working on Live View.

MCARTA provides a near-real-time system for analyzing malware. “MCARTA automates malware analysis, bringing together the best

doesn't require a specialized skill set, and it works quickly. “When you're in a mission context, you need fast results,” said Cois.

MCARTA is currently being used by 22 organizations, including a large



“MCARTA automates malware analysis, bringing together the best in class of commercially available tools, open source tools, and CERT tools all in one easy-to-use system.”

– C. Aaron Cois

in class of commercially available tools, open source tools, and CERT tools all in one easy-to-use system,” said the SEI's [C. Aaron Cois](#), software engineering team lead for MCARTA. Users access MCARTA through a web-based interface where they can submit suspicious files. In 4 to 7 minutes, MCARTA runs a file through a variety of tools, including 23 antivirus systems and a similarity search that compares pieces of malware based on their behavioral signatures. Based on this analysis, MCARTA produces a detailed report that tells the user what the file does and how it works.

MCARTA is useful for a wide variety of roles: law enforcement investigators, information security staff members, and even IT managers concerned about suspicious emails being sent to their employees. Like Live View, MCARTA

government agency. Live View has been deployed privately and will be available for wide release in 2014. “These tools allow just about anyone to log in and do some rudimentary work, which is sometimes all you need,” said Corn. “They lower the barrier to forensic analysis.”

To learn more about the SEI's work in digital intelligence and investigation, please visit <http://www.cert.org/digital-intelligence/>.



The SEI's Live View and Malicious Code Automated Run-Time Analysis (MCARTA) give investigators the ability to do their own triage quickly, affordably, and with minimal training.

INSIDER THREAT CENTER BREAKS NEW GROUND ON UNINTENTIONAL INSIDER THREAT

More than 40 percent of computer and organizational security professionals report that their greatest security concern is accidental employee error, such as lost devices or leaked data. This widespread concern spurred the [Insider Threat Center](#), part of the SEI's CERT Division, to undertake foundational research in 2013 on the problem of the unintentional insider threat (UIT).

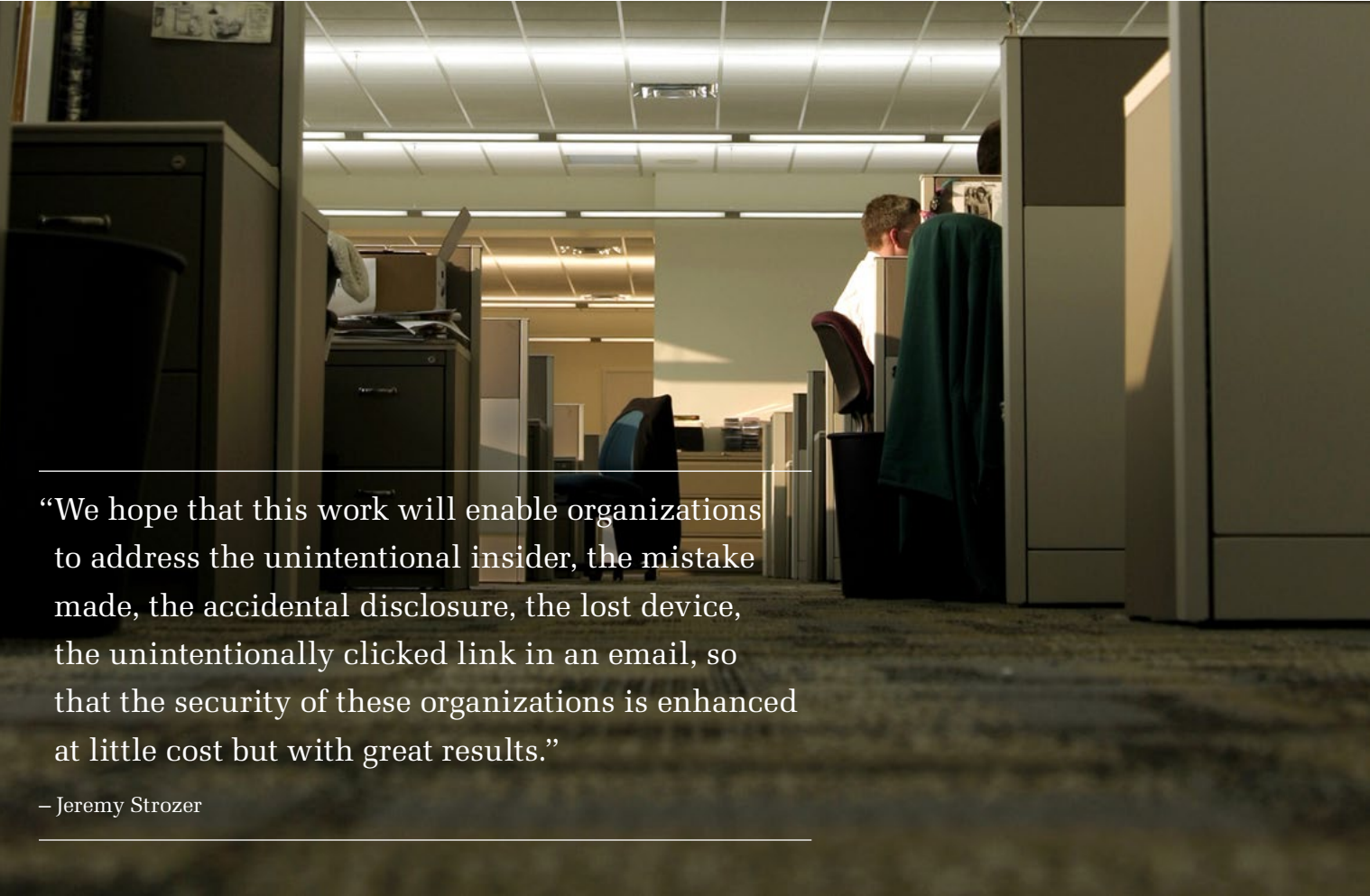
"A UIT is potentially more damaging to an organization than some other forms of insider threat," said Insider Threat Center researcher Jeremy Strozer. "An employee falling for a spear phishing campaign, for example, offers outsiders one of the best opportunities to infiltrate an organization's IT infrastructure without having to break through any firewalls."

The Insider Threat Center conducted foundational research on this previously unstudied topic to inform government and industry stakeholders about the problem and to steer research and development toward critical countermeasures. Researchers drew on relevant literature, public reports of UIT incidents, and a decade's worth of information in the Center's Insider Threat Database. Their work, documented in the technical notes [Unintentional Insider Threats: A Foundational Study](#) and [Unintentional Insider Threats: Social Engineering](#), produced an operational definition of UIT, its causes and contributing factors, examples and frequencies of different UIT case types, tools for sharing information about UIT incidents, groundwork for a UIT model,

and potential mitigation strategies and countermeasures.

Strozer said employers could use this information to train their employees on how to avoid becoming unwitting insider threats. "We hope that this work will enable organizations to address the unintentional insider, the mistake made, the accidental disclosure, the lost device, the unintentionally clicked link in an email, so that the security of these organizations is enhanced at little cost but with great results."

For more on the SEI's insider threat research, please visit <http://www.cert.org/insider-threat/>.



"We hope that this work will enable organizations to address the unintentional insider, the mistake made, the accidental disclosure, the lost device, the unintentionally clicked link in an email, so that the security of these organizations is enhanced at little cost but with great results."

— Jeremy Strozer

CYBER RESILIENCE REVIEWS PROVIDE DHS A COMPREHENSIVE SET OF PERFORMANCE DATA, CREATE SNAPSHOT OF CRITICAL INFRASTRUCTURE PRACTICES

In 2013, the SEI selected and analyzed results from 115 Cyber Resilience Reviews (CRRs) to produce valuable aggregate data about the performance of critical infrastructure organizations across the United States. The CRR, a derivative application of the CERT Resilience Management Model (CERT-RMM), contains 269 questions across 10 domains of capability to measure the cybersecurity strengths and weaknesses of the nation's most vital systems.

In collaboration with [Carnegie Mellon University's Machine Learning Department](#), the SEI analyzed the CRR data to determine trends and patterns in the cybersecurity practices of

critical infrastructure organizations. The resulting report provided the U.S. Department of Homeland Security (DHS) a comprehensive and detailed picture of operational resilience within the organizations.

This first snapshot of cybersecurity performance is an important milestone in the evolution of the CRR program. According to Matthew Butkovic, the SEI lead on the project, "In our view, having such expansive and precise information will help those responsible for protecting critical infrastructure target efforts to strengthen the cybersecurity capabilities of our nation's critical infrastructure organizations."

To date, the SEI has conducted more than 350 CRRs in support of DHS—the single largest use of CERT-RMM (or derivatives of the CERT-RMM method) in assessment. Data analysis is a key component of the CRR program and an emerging source of insights regarding the cybersecurity practices of critical infrastructure organizations for DHS.

Find out more about the SEI's work in cyber risk and resilience management: <http://www.cert.org/resilience/>.





Photo: U.S. Army Africa

CYBERSECURITY

NEW STEPfwd TRAINING PLATFORM HELPS U.S. DEPARTMENT OF DEFENSE AND ITS PARTNERS TO TRAIN AS THEY FIGHT

The Department of Defense (DoD) and its partner countries—the United Kingdom, Canada, Australia, and New Zealand—are using the SEI’s latest training and exercise platform to train their staff and evaluate their cyber mission readiness. The new platform, called the Simulation, Training, and Exercise Platform, or [STEPfwd](#), uniquely integrates the web-based delivery of captured video lectures and demonstrations, hands-on labs, team exercises, network models and simulations, and an easy-to-use learning management system that enables globally distributed workforces to train as they fight.

“SEI technology and services are foundational for DoD cyber exercises and online training,” said [Chris May](#), technical manager of the SEI’s Cyber Workforce Development Initiative. “Using STEPfwd, operationally deployed DoD units routinely participate in skill-sharpening, real-time cyber exercises from locations around the world.”

The platform was recently used for U.S. Cyber Command’s [Cyber Flag 14-1](#) joint exercise. STEPfwd modeled military networks and the internet, and it deployed more than 6,500 virtualized systems as well as thousands of very realistic simulated users. These simulated users type and send email, open attachments, click links, watch

“The DoD needed a convenient way to train and evaluate its geographically dispersed cyber workforce in a cost-effective and operationally realistic way. STEPfwd provides that,” said May.

To learn more about STEPfwd, please visit <https://stepfwd.cert.org>.



“Using STEPfwd, operationally deployed DoD units routinely participate in skill-sharpening, real-time cyber exercises from locations around the world.”

– Chris May

YouTube videos, etc. According to May, “End-user behavior represents a large portion of realized cyber threats today, so accurate user simulations that address this most common attack vector make DoD exercises much more realistic.”

MEAD NAMED SEI FELLOW

In 2013, [Nancy R. Mead](#), a principal researcher in the SEI's CERT Division, was named an SEI Fellow. Mead became the SEI's seventh fellow, a designation awarded to staff who have made outstanding contributions to the SEI and who continue to advise SEI leaders.

"It's an honor to be named an SEI Fellow and at the same time very humbling," said Mead. "I have been fortunate to have had wonderful support and mentoring from many people throughout my career."

Mead's research interests lie in the areas of software security, software requirements engineering, and

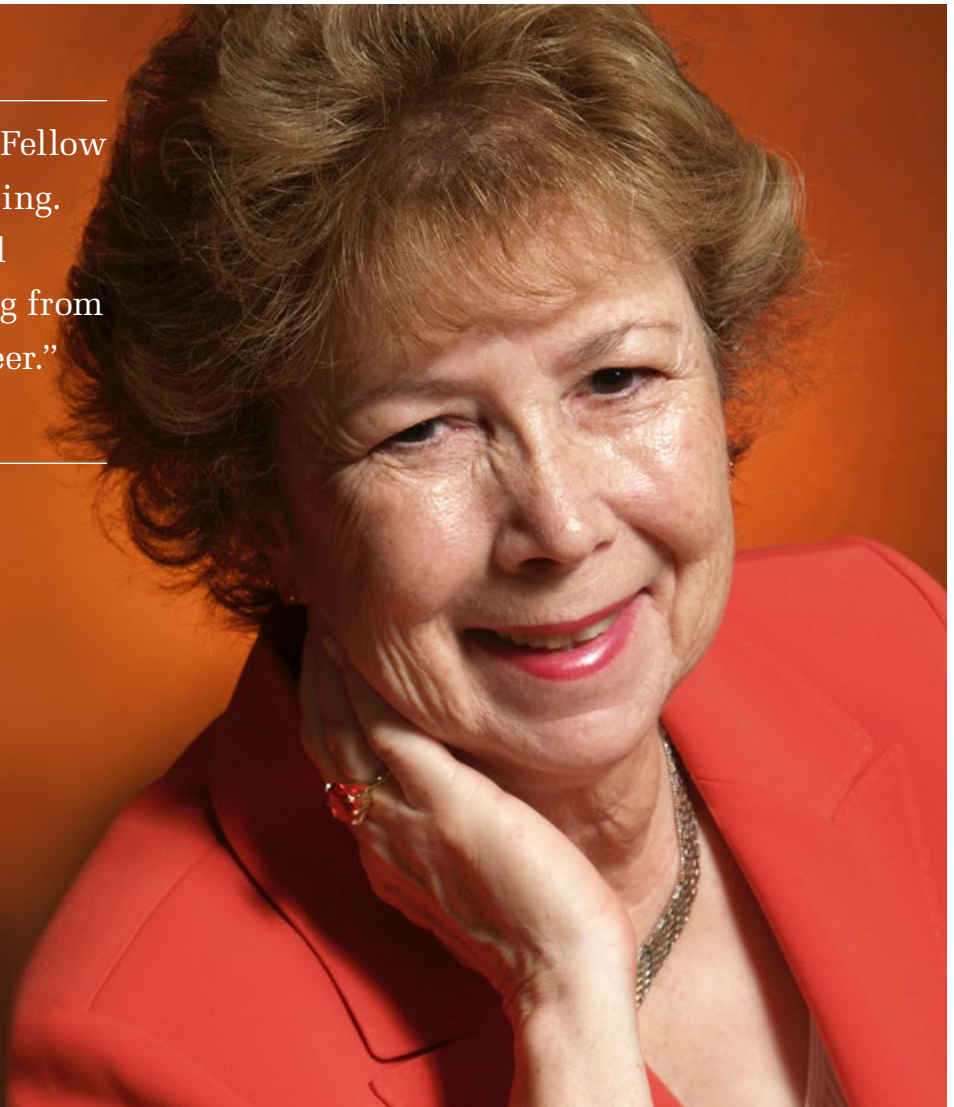
software architectures. Her current work involves the study of security requirements engineering and the development of software assurance curricula.

"Nancy has contributed significantly throughout her career," said Paul Nielsen, director and CEO of the SEI. "Her contributions have been many, but she is especially known for making software engineering an accepted curriculum." Nielsen also lauded Mead's work on a model curriculum for software assurance and her work in survivable systems analysis, a field in which she and her team broke new ground in understanding and assessing the survivability properties of systems.

Mead has authored more than 150 publications and invited presentations. She is a [Fellow of IEEE](#) and the IEEE Computer Society. Mead is also a [Distinguished Member of the Association for Computing Machinery](#) (ACM) and is a member of numerous advisory boards and committees. Prior to joining the SEI in 1990, Mead was a senior technical staff member at IBM Federal Systems, where she worked on the development and management of large real-time systems. Mead received her PhD in mathematics from the Polytechnic Institute of New York and received a BA and an MS in mathematics from New York University.

"It's an honor to be named an SEI Fellow and at the same time very humbling. I have been fortunate to have had wonderful support and mentoring from many people throughout my career."

– Nancy Mead



TO ENCOURAGE MORE ROBUST DEVELOPMENT PRACTICES, CERT MAPS SOLUTIONS TO MICROSOFT'S SIMPLIFIED SECURITY DEVELOPMENT LIFECYCLE

Developers often short-change software security until the last stages of development or even later, which can lead to expensive post-release fixes. To help address this problem, researchers in the SEI's CERT Division have mapped some of its software security solutions, such as its secure coding standards, Source Code Analysis Laboratory ([SCALE](#)), Security Quality Requirements Engineering ([SQUARE](#)), and the Survivability Analysis Framework, to a version of Microsoft's Security Development Lifecycle ([SDL](#)), a security assurance process that spans the software development lifecycle.

By connecting security solutions to the entire development lifecycle, the CERT-SDL mapping shows developers how to incorporate security from the beginning of a project, and it gives project managers tangible, credible evidence to justify these activities to their superiors. "It's how you can instantiate the SDL using SEI and CERT products," says [Robert C. Seacord](#), technical manager of the CERT Secure Coding Initiative. "It's a place to begin planning."

Microsoft has long used a customized SDL to reduce the number and severity of vulnerabilities in its own enterprise-scale software projects. [The Simplified Implementation of the Microsoft SDL](#), released by Microsoft in 2005, condenses the full SDL to 17 security practices across all stages of software development. Standards organizations, companies, and governments around

the world, such as the International Organization for Standardization (ISO) and the national government of India, have incorporated the SDL or its principles into their own software development work.

While Microsoft's Simplified SDL provides a recognized framework for security assurance, it does not provide usable solutions for implementing the recommended practices. In early 2013, Seacord mapped CERT secure coding solutions to the Simplified SDL. [Carol Woody](#), technical manager of the [CERT Cyber Security Engineering team](#), expanded the mapping to include products, tools, and services from across the CERT Division. "We're trying to capture the recognition that these pieces are tied together, and say how and why," said Woody.

The white paper "[Strengths in Security Solutions](#)," co-authored by Seacord, Woody, CERT technical staff member Allen Householder, and Microsoft's Arjuna Shunn, maps eight CERT tools, services, and processes to the Simplified SDL. At least one CERT solution—and often several—apply to all but one of the Simplified SDL's 17 practices. The paper describes each solution, its connection to the Simplified SDL, its value to security, and additional resources.

Woody hopes that the mapping will also start a larger conversation by connecting different sets of terminology. "We're mapping the language of security

"Microsoft appreciates CERT's views as an independent organization on secure development, as those diverse views often spark new lines of thinking and approaches."

– Arjuna Shunn, Microsoft

with the language of the development lifecycle," she said.

Meanwhile, the mapping provides the CERT Division with a structure to join many of its point solutions, and it provides Microsoft's SDL with the credibility of the CERT Division's expertise in software security. "Microsoft appreciates CERT's views as an independent organization on secure development," says Shunn, "as those diverse views often spark new lines of thinking and approaches."

The mapping covers just a small piece of the software-security big picture. But, says Woody, "until security is considered earlier in the lifecycle, we won't get the cost savings of building security in instead of trying to patch it on." Thanks to Microsoft and the CERT Division, developers now have a place to start.

ISO STANDARD, NEW BOOKS AMONG SECURE CODING 2013 HIGHLIGHTS

As part of the [ISO/IEC JTC1/SC22/WG14](#) working group, SEI Secure Coding team members, including David Keaton, Robert C. Seacord, and David Svoboda, worked to develop the technical specification ISO/IEC TS 17961:2013(E), [Information Technology—Programming Languages, Their Environments and System Software Interfaces—C Secure Coding Rules](#). This standard was published by the International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) in November 2013. The purpose of TS 17961 is to establish a baseline set of requirements for analyzers, including

static analysis tools and C language compilers, to be applied by vendors that wish to diagnose insecure code beyond the requirements of the language standard. The Secure Coding team's long experience in researching and developing secure coding practices for C and other programming languages positioned it well to contribute to this important work.

The Secure Coding team also published two books in 2013: Seacord's [Secure Coding in C and C++, Second Edition](#), identifies root causes of software vulnerabilities and promotes security best practices. [Java Coding Guidelines](#):

[75 Recommendations for Reliable and Secure Programs](#) by Fred Long, Dhruv Mohindra, Seacord, Dean F. Sutherland, and Svoboda offers updated techniques for protecting against deliberate attacks and other unexpected events and best practices for improving code reliability and clarity. In his introduction to [Java Coding Guidelines](#), James A. Gosling, known as the father of the Java programming language, calls the book "invaluable."

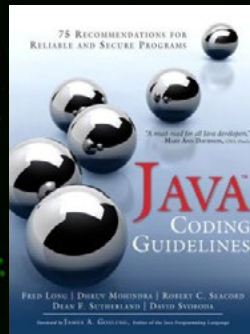
Learn more about the SEI's work in secure coding: <http://www.cert.org/secure-coding/>.



David Svoboda



Robert Seacord



"This set of Java™ coding guidelines, a follow-on to the earlier *CERT® Oracle Secure Coding Standard for Java™*, is invaluable."

—James A. Gosling, father of the Java programming language

UNDERSTANDING THE STATE OF CYBER INTELLIGENCE

Cyber intelligence—the acquisition and analysis of information to identify and predict cyber capabilities and intentions, and to enhance decision making—is a critical area of focus for government and industry. The Office of the Director of National Intelligence (ODNI), seeking a better understanding of how practitioners perform this work, sponsored work by the SEI Emerging Technology Center (ETC) to study the tradecraft that shapes organizations' cyber intelligence efforts.

The study began in June 2012. Its goal was to advance the cyber intelligence capabilities of organizations by examining their methodologies, processes, tools, and training. The ETC will use this research to prototype solutions to challenges faced throughout government and industry. The ETC will base these solutions on best practices and SEI expertise for challenges shared across government and industry.

To conduct the study, the ETC developed 35 assessment factors distributed among the five core functions it considered necessary for performing cyber intelligence: environment, data gathering, functional analysis, strategic analysis, and decision maker reporting and feedback. ETC members then collected information for these assessment factors from six government agencies and 24 organizations representing economic sectors such as energy, financial services, healthcare, defense contracting, and retail. Overall, the

data indicated that organizations used a diverse array of approaches to perform cyber intelligence. “While the data identified no universal standard for doing cyber intelligence work,” stated ETC member Jay McAllister, “we did find that successful organizations balanced the need to protect their network perimeters with the need to look beyond them for strategic insights.”

In January 2013, the ETC invited the study's participants to Pittsburgh for a workshop to present its initial findings and brainstorm with attendees on solutions for three challenge areas the study uncovered: data analytics, visualization, and training and education. Government and industry collaboration helped participants realize that looking beyond their own walls brought new solutions to problems across economic sectors.

ETC staff members developed multiple analytical products offering solutions to common challenges. They provided them to the ODNI, the study's participants, and the general public. Examples of these products include implementation frameworks that guide practitioners through three critical aspects of cyber intelligence tradecraft: threat prioritization, data collection management, and workforce development and management.

Leveraging participant feedback, the ETC also developed a white paper, *Cyber Intelligence Tradecraft Project: Summary of Key Findings*, identifying

the traits, core competencies, and skills of successful cyber intelligence analysts. A review of over 150 educational programs revealed that some addressed half of the skills identified, but no program addressed all of the necessary skills. ODNI integrated it into the government's discussion on developing a robust community of cyber intelligence practitioners. “We've also received very positive responses when presenting at conferences,” explains McAllister. “The general sentiment from those who have heard us present is that they're happy someone has finally done the research in this important area.”

To read the SEI white paper, *Cyber Intelligence Tradecraft Project: Summary of Key Findings*, please visit <http://www.sei.cmu.edu/about/organization/etc/cyber-intelligence.cfm>.

“Successful organizations balanced the need to protect their network perimeters with the need to look beyond them for strategic insights.”

– Jay McAllister



Jay McAllister and Melissa Ludwick

ARCHITECTING SYSTEMS OF THE FUTURE

In June 2013, the [International Supercomputing Conference](#) published its [TOP500 Supercomputer Sites](#), the most powerful commercially available computer systems in existence.

One of the most powerful computers on the list serves the federal government: Titan, a Cray XK7 system installed at the U.S. Department of Energy's Oak Ridge National Laboratory. The Titan supercomputer contains thousands of graphics processing units (GPUs) that support its high-level computations. Systems like the Titan compute three-dimensional physics simulations, track network traffic data (netflow) through cyber domains, chart the spread of malware, and support logistics planning.

[Eric Werner](#), chief architect of the SEI's Emerging Technology Center (ETC), is leading a group of SEI researchers—including Jonathan Chu, Scott McMillan, and Alex Nicoll—in creating a software library that can exploit high-performance GPU computers such as the Titan. Their aim is to help developers create systems with more efficient computation and power consumption.

High-performance computing ([HPC](#)) is now central to federal government computational and network capabilities. Evidence of this trend, in industry and government, can also be seen in the shift from single-core and multi-core (homogenous) central processing units (CPUs) to many-core (heterogeneous) systems including CPUs and GPUs. This trend shows no sign of abating. The majority of computers (such as

smartphones and other mobile devices) now contain heterogeneous hardware with multi- and many-core chips.

Many-core systems pose a problem for developers, however, because software libraries, frameworks, and patterns were not developed for large-memory, many-core, heterogeneous computing environments. Complicating matters is the fact that software libraries for these many-core environments emphasize efficient and optimal computing over ease of use. As a result, these new hardware architectures aren't being used to their potential.

“Greater utilization of all of the resources in a system means faster computation and more efficiencies,” said Werner, adding that this research is a hallmark of the ETC, which aims to promote government knowledge of innovative technologies.

The team is using HPC architectures to simulate future computer architectures and develop software libraries, best practices, and patterns. Initially, the team limited its focus to graph analytics, which are widely used in government, science, and commerce to highlight relationships obscured by data.

As a reference, the team relied on the [Graph 500](#), an international benchmark similar to the TOP500 that rates how fast HPC systems test, traverse, and navigate a graph.

The team initially focused on reviewing patterns developed for heterogeneous systems as published in the computer

science literature. The team also reached out to collaborators in government, academia, and industry. Before developing a library of templates, the team will beta-test the library with software engineers who will use it to develop graph analytical code for advanced computing architectures.

The team has been collaborating with Indiana University's Extreme Scale Computing Lab, which developed the Parallel Boost Graph Library. In particular, it is working with [Andrew Lumsdaine](#), who serves with the Center for Research in Extreme Scale Technologies ([CREST](#)) and is considered a world leader in graph analytics.

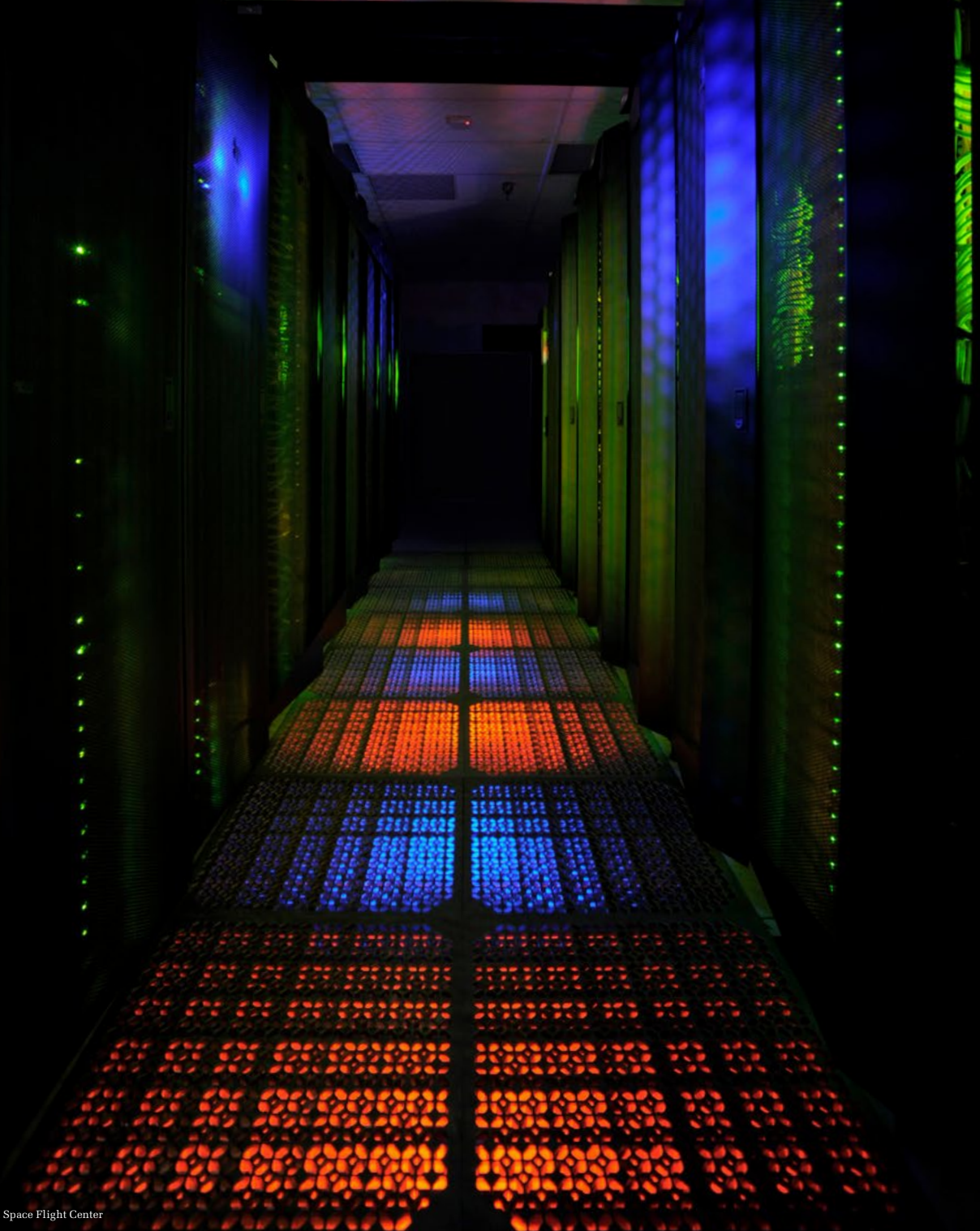
Future work will focus on other hardware platforms, including field-programmable gate arrays and other algorithmic domains.

For more on this topic, please visit <http://blog.sei.cmu.edu/archives.cfm/author/eric-werner>.



“Greater utilization of all of the resources in a system means faster computation and more efficiencies.”

– Eric Werner



TRANSITION

The SEI accelerates the impact of software and cybersecurity improvements by working to promote adoption of improved capabilities by the defense industrial base and the wider software and cybersecurity communities. The SEI does this by creating standards, prototypes and tools, technical guidance, and platforms for knowledge and skill acquisition.

Standards

The SEI develops standards that improve the software ecosystem on which the Department of Defense (DoD) relies. For instance, the CERT Secure Coding Initiative has been leading the community development of secure coding standards for common programming languages. Many of these proposed practices are in use by major participants in the supply chain for DoD software-reliant systems, including Cisco Systems and Oracle. The SEI has also worked to integrate several research technologies into the Architecture Analysis and Design Language standard, making it extensible and semantically well defined. Application of the standard promotes the virtual integration of system building and testing activities—an approach that supports DoD objectives of achieving integrated warfighting capabilities and delivering solutions sooner to warfighters.

Prototypes and Tools

SEI researchers develop software prototypes that test proposed solutions, like the smartphone app developed in collaboration with the Carnegie Mellon University Human-Computer Interaction Institute. Called the Edge Mission-Oriented Tactical App Generator (eMONTAGE), this software program for mobile devices enables warfighters to mash data from multiple sources and view the results on a unified display—all without writing code. SEI researchers have demonstrated an eMONTAGE

prototype at the U.S. Special Operations Command/Naval Postgraduate School (NPS) Tactical Network Testbed (August 2012) and at NPS's Joint Interagency Field Exploration (JIFX) (February 2013).

Tools

The SEI systematically builds software tools, especially those that address acute cybersecurity needs. Fuzz-testers and debuggers developed by the SEI's CERT Division, for example, can position military software engineers to meet requirements outlined in the 2013 National Defense Authorization Act for software assurance testing. Other SEI tools facilitate security analysis in large networks, enable analysts to rapidly query large sets of data traffic volumes, process packet data into bidirectional flow records, and simplify the building of analysis environments.

Technical Guidance, Workforce Development, and Knowledge Sharing

The SEI shares the progress and results of its research through a host of media avenues, including

- technical reports, blog entries, webinars, and podcasts available on its websites
- articles in prestigious professional journals and in publications geared to practitioners
- books in the SEI Series in Software Engineering published by Addison-Wesley

Those books often form the basis for education materials and training courses offered by the SEI and others. The SEI offers classroom and eLearning courses in software acquisition, network security, insider threat, software architecture, software product lines, software management, and other areas.

In 2012, the SEI introduced the CERT STEPfwd (Simulation, Training, and Exercise Platform) to help cybersecurity practitioners and their teams continually build knowledge, skills, and experience.

In addition, SEI researchers collaborated with educators from around the United States to develop the first curriculum for software assurance, the Master of Software Assurance (MSwA). The IEEE Computer Society and Association for Computing Machinery, as well as community leaders in curriculum development, formally recognized the MSwA Reference Curriculum as suitable for creating graduate programs or tracks in software assurance.

LEADERSHIP

CARNEGIE MELLON UNIVERSITY LEADERSHIP



[Subra Suresh](#)
President
Carnegie Mellon University



[Mark S. Kamlet](#)
Provost and Executive Vice President
Carnegie Mellon University

[SEI EXECUTIVE LEADERSHIP TEAM](#)



Seated: David Thompson, Chief Information Officer; Robert Behler, Deputy Director and Chief Operating Officer; Kevin Fall, Deputy Director and Chief Technology Officer; Mary Catherine Ward, Chief Strategy Officer

Standing: Matthew E. Gaston, Director, SEI Emerging Technology Center; Peter Menniti, Chief Financial Officer; Paul Nielsen, Director and Chief Executive Officer; Richard Pethia, Director, CERT Division; John Bramer, Chief of Staff; Edward Deets, Director, Software Solutions Division

BOARD OF VISITORS

The SEI Board of Visitors advises the Carnegie Mellon University president and provost and the 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 W. Boehm

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

Claude M. Bolton

Executive-in-Residence, Defense Acquisition University; Former Assistant Secretary of the Army for Acquisition, Logistics, and Technology

William Bowes

Aerospace Consultant; Vice Admiral, USN (Ret.); Former Commander, Naval Air Systems Command, and Principal Deputy Assistant Secretary of the Navy for Research, Development, and Acquisition

Christine Davis

Consultant; Former Executive Vice President, Raytheon Systems Company

Gilbert F. Decker

Consultant; Former President and CEO, Penn Central Federal Systems Company; Former President and CEO of Acurex Corporation; Former Assistant Secretary of the Army/Research, Development, and Acquisition

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

Tom Love

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

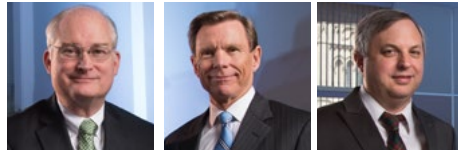
Alan J. McLaughlin

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

SEI ORGANIZATIONAL CHART



Paul D. Nielsen
Director and Chief Executive Officer

Robert Behler
Deputy Director and Chief Operating Officer

Kevin Fall
Deputy Director and Chief Technology Officer

Software Solutions Division



Edward Deets
Director

Anita Carleton
Deputy Director

Linda Northrop
Chief Scientist

CERT Division

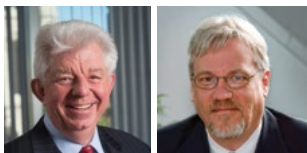


Richard Pethia
Director

Bill Wilson
Deputy Director

Greg Shannon
Chief Scientist

Office of Chief of Staff/ Office of Chief Information Officer



John Bramer
Chief of Staff

David Thompson
Chief Information Officer

Strategic Initiatives Office



Mary Catherine Ward
Chief Strategy Officer

Sally Cunningham
Deputy Director

Financial and Business Services



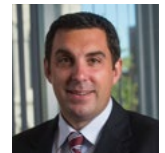
Peter Menniti
Chief Financial Officer

SEI Legal



Sandra Brown
SEI General Counsel

Emerging Technology Center



Matthew E. Gaston
Director

PUBLICATIONS

Articles

- Albarghouthi, Aws; Gurfinkel, Arie; Li, Yi; Chaki, Sagar & Chechik, Marsha. "UFO: Verification with interpolants and abstract interpretation." *Second Competition on Software Verification: 19th International Conference, TACAS 2013, Held as Part of the European Joint Conferences on Theory and Practice of Software, ETAPS 2013, Rome, Italy, March 16-24, 2013. Proceedings* (March 2013).
- Bachmann, Felix H.; Carballo, L.; McHale, James & Nord, Robert L. "Integrate End to End Early and Often." *IEEE Software* (July/August 2013).
- Bellomo, Stephany; Nord, Robert & Ozkaya, Ipek. "Study of Enabling Factors for Rapid Fielding: Combined Practices to Balance Speed and Stability." *Proceedings of ICSE 2013: 35th International Conference on Software Engineering* (May 2013).
- Carleton, Anita; Harper, Erin; Lapham, Mary Ann; Ozkaya, Ipek; Gates, Linda Parker & Schmidt, Doug. "What Will It Take to Achieve Agility at Scale?" *Cutter IT Journal* (November 2013).
- Cervantes, Humberto; Velasco-Elizondo, Perla & Kazman, Rick. "Principled Way to Use Frameworks in Architecture Design." *IEEE Software* (March/April 2013).
- Chaki, Sagar; Schallhart, Christian & Veith, Helmut. "Verification Across Intellectual Property Boundaries." *ACM Transactions on Software Engineering and Methodology (TOSEM)* (March 2013).
- Chaki, Sagar; Dolan, John M. & Giampapa, Joseph Andrew. "Toward A Quantitative Method for Assuring Coordinated Autonomy." *CMU-RI-TR-13-12, Robotics Institute, Carnegie Mellon University* (June, 2013).
- Chaki, Sagar & Giampapa, Joseph. "Probabilistic Verification of Coordinated Multi-Robot Missions." *Proceedings of the 20th International SPIN Symposium on Model Checking of Software (SPIN)* (July 2013).
- Chick, Timothy. "TSP: The Agile Way." *Proceedings of the CIISA, Congeso CIISA 2013*. (August 2013).
- Chrissis, Mary Beth; Konrad, Mike & Moss, Michele. "Ensuring Your Development Processes Meet Today's Cyber Challenges." *CrossTalk* (March/April 2013).
- de Oliveira, Raphael Pereira; Insfran, Emilio; Abrahão, Silvia; Gonzalez-Huerta, Javier; Blanes, David; Cohen, Sholom & de Almeida, Eduardo Santana. "A Feature-Driven Requirements Engineering Approach for Software Product Lines." *Proceedings of SBCARS 2013 - 7th Brazilian Symposium on Software Components, Architectures and Reuse* (October 2013).
- Eden, A.H.; Gasparis, E.; Nicholson, J. & Kazman, R. "Modeling and Visualizing Object-Oriented Programs with Codecharts." *Formal Methods in System Design* (January 2013).
- Giampapa, Joseph Andrew. "Test and Evaluation of Autonomous Multi-Robot Systems." *Proceedings of NDIA 16th Annual Systems Engineering Conference* (October 2013).
- Goodenough, John B.; Weinstock, Charles B. & Klein, Ari Z. "Eliminative Induction: A Basis for Arguing System Confidence." *Proceedings of ICSE 2013: 35th International Conference on Software Engineering* (May 2013).
- Hilburn, T.B. & Mead, N.R. "Building Security In: A Road to Competency." *IEEE Security & Privacy* (September/October 2013).
- Kasunic, Mark. "SEI Interactive Session: Empirical Study of Software Engineering Results." *Proceedings of TSP Symposium 2013* (September 2013).
- Klein, John & McGregor, John. "System-of-Systems Platform Scoping." *Proceedings of ICSE 2013: 35th International Conference on Software Engineering* (May 2013).
- Klein, John; Cohen, Sholom G. & Kazman, Rick. "Common Software Platforms in System-of-Systems Architectures: The State of the Practice." *Proceedings of the Eighth International Conference on System of Systems Engineering (SoSE)* (June 2013).
- Kruchten, Philippe; Nord, Robert L.; Ozkaya, Ipek & Falessi, Davide. "Technical Debt: Towards a Crisper Definition. Report on the 4th International Workshop on Managing Technical Debt." *ACM SIGSOFT Software Engineering Notes* (September 2013).
- Kruchten, Philippe; Nord, Robert L. & Ozkaya, Ipek. "Technical Debt: From Metaphor to Theory and Practice." *IEEE Software* (November/December 2012).
- Lago, Patricia; Kazman, Rick; Meyer, Niklaus; Morisio, Maurizio; Müller, Hausi A.; Paulisch, Frances; Scanniello, Giuseppe; Penzenstadler, Birgit & Zimmermann, Olaf. "Exploring Initial Challenges for Green Software Engineering: Summary of the First GREENS Workshop, at ICSE 2012." *ACM SIGSOFT Software Engineering Notes* (January 2013).
- Lago, Patricia; Lewis, Grace A.; Metzger, Andreas; Tomic, Vladimir; Bianculli, Domenico; Di Marco, Antiniscia; Polini, Andrea & Plebani, Pierluigi. "Report of the 4th International Workshop on Principles of Engineering Service-Oriented Systems (PESOS 2012): Internet of Services and the Quest for Case Studies." *ACM SIGSOFT Software Engineering Notes* (January 2013).
- Lewis, Grace A.; Nagappan, Nachiappan; Gray, Jeff; Rosenblum, David; Muccini, Henry & Shihab, Emad. "Report of the 2013 ICSE 1st International Workshop on Engineering Mobile-Enabled Systems (MOBS 2013)." *ACM SIGSOFT Software Engineering Notes* (September 2013).
- Mead, N.R.; Shoemaker, D. & Woody, C. "Principles and Measurement Models for Software Assurance." *International Journal of Secure Software Engineering* (January-March 2013).
- Mead, N.R. & Shoemaker, D. "The Software Assurance Competency Model: A Roadmap to Enhance Individual Professional Capability." *Proceedings of the Conference on Software Engineering Education & Training (CSEET)* (May 2013).
- Mead, N.R. "A History of the International Requirements Engineering Conference (RE)." *Proceedings of the International Requirements Engineering Conference (RE) 2013* (July 2013).
- Monteiro, Paula; MacHado, Ricardo J.; Kazman, Rick; Lima, Ana; Simões, Cláudia & Ribeiro, Pedro. "Mapping CMMI and RUP Process Frameworks for the Context of Elaborating Software Project Proposals." *Proceedings of Software Quality: Increasing Value in Software and Systems Development - 5th International Conference (SWQD 2013)* (January 2013).
- Nichols, William. "Toward a Quantified Reflection: Reflections on TSP Reflective Practice." *Proceedings of TSP Symposium 2013* (September 2013).
- Nord, Robert L. & McHale, James. "Integrate End-to-End Early and Often: Driving Out Technical Risk by Blending Architecture and Process Discipline." *Proceedings of the 25th Annual Software Technology Conference* (April 2013).
- Nord, Robert L.; Ozkaya, Ipek; Sangwan, Raghvinder S.; Delange, Julien; González, Marco & Kruchten, Philippe. "Limitations in Using Structural Metrics to Measure Architecture Modifiability Properties." *Proceedings of the 29th IEEE International Conference on Software Maintenance* (September 2013).
- Novakouski, Marc. "User-Centric Identity Management: A Future Vision for IdM." *CrossTalk* (September/October 2013).
- Over, James. "Advances in Conceptual Modeling." *Proceedings of ER 2012 Workshops: CMS, ECDM-NoCoDA, MoDIC, MORE-BI, RIGiM, SeCoGIS, WISM* (October 2012).
- Over, James. "Team Software Process Research Program at CMU SEI." *Proceedings of Current Issues in Conceptual Modeling (CICM)* (October 2012).
- Ozkaya, Ipek; Nord, Robert L.; Bellomo, Stephany & Brayer, Heidi. "Beyond Scrum + XP: Agile Architecture Practice." *Cutter IT Journal* (June 2013).

Ozkaya, Ipek; Gagliardi, Michael & Nord, Robert L. "Architecting for Large Scale Agile Software Development: A Risk-Driven Approach." *CrossTalk* (May/June 2013).

Porter, John F.; Cheung, Kawa; Giampapa, Joseph A. & Dolan, John M. "A Reliability Analysis Technique for Estimating Sequentially Coordinated Multirobot Mission Performance." *Proceedings of the 16th International Conference on the Principles and Practice of Multi-Agent Systems (PRIMA) 2013* (December 2013).

Raravi, Gurulingesh; Andersson, Björn & Bletsas, Konstantinos. "Assigning Real-Time Tasks on Heterogeneous Multiprocessors With Two Unrelated Types of Processors." *Real-Time Systems* (January 2013).

Shoemaker, D. & Mead, N.R. "Building a Body of Knowledge for ICT Supply Chain Risk Management." *CrossTalk* (March/April 2013).

Woody, Carol. "Mission Thread Security Analysis: A Tool for Systems Engineers to Characterize Operational Security Behavior." *INCOSE/INSIGHT* (July 2013).

Books and Book Chapters

Bass, Len; Clements, Paul & Kazman, Rick. *Software Architecture in Practice, 3rd ed.* Addison-Wesley Professional 2012 (ISBN-10: 0-321-81573-4).

Ionita, Anca Daniela; Litoiu, Marin & Lewis, Grace. *Migrating Legacy Applications: Challenges in Service Oriented Architecture and Cloud Computing Environments.* IGI Global 2012 (ISBN10: 1466624884).

Long, Fred; Mohindra, Dhruv; Seacord, Robert C.; Sutherland, Dean F. & Svoboda, David. *Java Coding Guidelines: 75 Recommendations for Reliable and Secure Programs.* Addison-Wesley Professional 2013 (ISBN-10: 032193315X).

Reinhartz-Berger, Iris; Sturm, Arnon; Clark, Tony; Cohen, Sholom & Bettin, Jorn (eds.). *Domain Engineering: Product Lines, Languages, and Conceptual Models.* Springer 2013 (ISBN-10: 3642366538).

Seacord, Robert C. *Secure Coding in C and C++, 2nd Edition.* Addison-Wesley Professional 2013 (ISBN-10: 0-321-82213-7).

Keynotes

Blanchette, Stephen. "New Tech in an Old Tech World." Software Challenges Workshop of the AIAA Aerospace Sciences Meeting (January 2013).

Feiler, Peter. "Challenges and Strategies for Safety-Critical Software-Reliant Systems." 6th International Workshop on Model-Based Architecting and Construction of Embedded Systems (September 2013).

Feiler, Peter. "Analytical Architecture Fault Models." Analytic Virtual Integration of Cyber-Physical Systems Workshop (AVICPS 2012), the 33rd IEEE Real-Time Systems Symposium (RTSS) (December 2012).

Gorton, Ian. "Tales from the (Scientific Software) Engineering Abyss." Twin Peaks Workshop Keynote, ICSE 2013: 35th International Conference on Software Engineering (May 2013).

Lewis, Grace. "Emerging Technologies for Software-Intensive Systems." First International Conference on Computer Systems Engineering (November 2012).

McHale, James. "Agile Meets CMMI... Again." TesTrek (November 2012).

Mead, N.R. "A Curriculum and Roadmap to Software Assurance Competency." 2nd International Conference on Software Process Improvement (CIMPS 2013) (October 2013).

Nichols, Bill. "The Quality Journey: If You Don't Know Where You Are, a Map Won't Help." ESELAW 2013: CibSE 2013: XVI Iberoamerican Conference on Software Engineering (April 2013).

Northrop, Linda. "Does Scale Really Matter? – Ultra-Large-Scale Systems Seven Years after the Study." International Conference on Software Engineering (May 2013).

Northrop, Linda. "Does Scale Really Matter? – Ultra-Large-Scale Systems Seven Years after the Study." Large-Scale Complex Software-Intensive Systems Symposium (June 2013).

Podcasts & Webinars

Bachmann, Felix & McHale, Jim. "Architecting a Financial System with TSP," (October 2012). <http://www.sei.cmu.edu/podcasts/index.cfm?getRecord=798090AD-D76B-2597-A7FBC05FC9096AC9&wtPodcast=ArchitectingaFinancialSystemwithTSP>

Bachmann, Felix. "Use of Architecture-Centric Engineering for Improving a Software System," (October 2012). <http://saturnnetwork.wordpress.com/2012/10/02/free-sei-webinar-1017-use-of-architecture-centric-engineering-for-improving-a-software-system/>

Bachmann, Felix. "Use of ACE for Improving a Software System," (November 2012). <http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=34136>

Bandor, Michael. "Technology Readiness Assessments," (February 2013). <http://www.sei.cmu.edu/podcasts/index.cfm?getRecord=3C3F3F1E-F444-6891-CF61C24EC97ADD38&wtPodcast=TechnologyReadinessAssessments>

Caralli, Richard & Allen, Julia. "Why Use Maturity Models to Improve Cybersecurity: Key Concepts, Principles, and Definitions," (August 2013). <http://www.cert.org/podcast/show20130827caralli.html>

Chick, Tim. "The Fundamentals of Agile," (January 2013). <http://www.sei.cmu.edu/podcasts/index.cfm?getRecord=2A79C795-026A-B03D-51D006D8AD15DBFB&wtPodcast=TheFundamentalsOfAgile>

Chick, Timothy A. & Miluk, Gene. "Checkpoint Diagnostic: Critical Element in a Performance Improvement Program," (August 2013). <http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=59094>

Clark, Brad & McCurley, Jim. "Software Cost Analysis Repository SEI Invitation-Only Webinar for DoD Personnel," (July 2013).

Edmondson, James; Gokhale, Aniruddha & Schmidt, Douglas. "Human-in-the-Loop Autonomy," (September 2013). <http://www.sei.cmu.edu/podcasts/index.cfm?getRecord=4B42D129-EA0B-174E882720690611E477&wtPodcast=Human-in-the-LoopAutonomy>

Elm, Joe. "The Business Case for Systems Engineering," (May 2013). <http://www.sei.cmu.edu/podcasts/index.cfm?getRecord=D1CB7A9A-94FC-CAF3-4BACF6CA8BAFAB0F&wtPodcast=TheBusinessCaseforSystemsEngineering>

Feiler, Peter & Delange, Julien. "The Latest Developments in AADL," (January 2013). <http://www.sei.cmu.edu/podcasts/index.cfm?getRecord=727E84DB-CDB0-5DE1-7AC24DADF26A5200&wtPodcast=TheLatestDevelopmentsinAADL>

Feiler, Peter. "What's New with Version 2 of the AADL Standard?" (March 2013). <http://www.sei.cmu.edu/podcasts/index.cfm?getRecord=FEC3F8C9-91DC-BF0A-32D580CBE933BAD3&wtPodcast=What%27sNewWithVersion2oftheAADLStandard?>

Feiler, Peter. "Reliability Validation and Improvement Framework," (May 2013). <http://www.sei.cmu.edu/podcasts/index.cfm?getRecord=EBAD1AD5-0079-1BAB-6EC010E85A4239F4&wtPodcast=ReliabilityValidationandImprovementFramework>

Firesmith, Donald. "Common Testing Problems: Pitfalls to Prevent and Mitigate," (July 2013). <http://www.sei.cmu.edu/podcasts/index.cfm?getRecord=F78D7189-9406-5EA6-CDC93C1604E8D8F5&wtPodcast=CommonTestingProblems:PitfallsToPreventandMitigate>

Gagliardi, Michael. "Uncovering Architectural Challenges in a System of Systems," (January 2013). <http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=48690>

Kim, Gene & Allen, Julia. "DevOps: Transform Development and Operations for Fast, Secure Deployments," (July 2013). <http://www.cert.org/podcast/show/20130730kim.html>

Lapham, Mary Ann & Miller, Suzanne M. "Applying Agile in the DoD: First Principle," (April 2013). <http://www.sei.cmu.edu/podcasts/index.cfm?getRecord=56FC4785-C59C-A419-B105D2D9E723C7EC&wtPodcast=ApplyingAgileintheDoD:FirstPrinciple>

- Lapham, Mary Ann & Miller, Suzanne M. "Applying Agile in the DoD: Second Principle," (June 2013). <http://www.sei.cmu.edu/podcasts/index.cfm?getRecord=62688824-B1BC-D618-0107E097423E0E3F&wtPodcast=ApplyingAgileintheDoD:SecondPrinciple>
- Lapham, Mary Ann & Miller, Suzanne M. "Applying Agile in the DoD: Third Principle," (August 2013). <http://www.sei.cmu.edu/podcasts/index.cfm?getRecord=BB8F8208-001C-7AE9-2F558C0FA702AE7B&wtPodcast=ApplyingAgileintheDoD:ThirdPrinciple>
- Lewis, Grace. "Architecting Service-Oriented Systems," (December 2012). <http://www.sei.cmu.edu/podcasts/index.cfm?getRecord=770ED4B0-E817-AEF7-D637B139CE2D54EE&wtPodcast=ArchitectingService-OrientedSystems>
- Lewis, Grace. "Standards in Cloud Computing Interoperability," (February 2013). <http://www.sei.cmu.edu/podcasts/index.cfm?getRecord=019EDC08-C84D-AAC5-055DA1944DB31FA3&wtPodcast=StandardsinCloudComputingInteroperability>
- Lewis, Grace. "Part 1: Architecture and Design of Service-Oriented Systems," (March 2013). <http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=39580>
- Lewis, Grace. "Part 2: Architecture and Design of Service-Oriented Systems," (May 2013). <http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=48682>
- Lewis, Grace. "Application Virtualization as a Strategy for Cyber Foraging," (July 2013). <http://www.sei.cmu.edu/podcasts/index.cfm?getRecord=3A99461A-9B45-ABD9-4FFD6E1EF56FA827&wtPodcast=ApplicationVirtualizationasaStrategyforCyberForaging>
- Mayes, Joe & Allen, Julia. "Securing Mobile Devices aka BYOD," (March 2013). <http://www.cert.org/podcast/show/20130326mayes.html>
- McAllister, Jay; Townsend, Troy; Garcia-Miller, Suzanne. "The State of the Practice of Cyber Intelligence." <http://resources.sei.cmu.edu/library/asset-view.cfm?assetid=43858>
- McCurley, Jim & Stoddard, Robert. "Quantifying Uncertainty in Early Life-Cycle Cost Estimation," (November 2012). <http://www.sei.cmu.edu/podcasts/index.cfm?getRecord=BD60D188-AC6E-714B-10F420705985285B&wtPodcast=QuantifyingUncertaintyinEarlyLifeCycleCostEstimation>
- Mead, N.R. "Software Assurance Professional Competency," (February 2013). <https://www.brighttalk.com/webcast/574/63881>
- Mehravari, Nader & Allen, Julia. "Managing Disruptive Events: Making the Case for Operational Resilience," (December 2012). <http://www.cert.org/podcast/show/20121219mehravari.html>
- Mehravari, Nader & Allen, Julia. "Managing Disruptive Events: Demand for an Integrated Approach to Better Manage Risk," (January 2013). <http://www.cert.org/podcast/show/20130131mehravari.html>
- Mehravari, Nader & Allen, Julia. "Managing Disruptive Events: CERT-RMM Experience Reports," (June 2013). <http://www.cert.org/podcast/show/20130611mehravari.html>
- Morris, Edwin. "Software for Soldiers who Use Smartphones," (December 2012). <http://www.sei.cmu.edu/podcasts/index.cfm?getRecord=01F563EE-0491-803C-FD4135C8B347A1B2&wtPodcast=SoftwareforSoldierswhouseSmartphones>
- Mundie, David & Allen, Julia. "Using a Malware Ontology to Make Progress Towards a Science of Cybersecurity," (May 2013). <http://www.cert.org/podcast/show/20130509mundie.html>
- Novak, William; Moore, Andrew. "The Evolution of a Science Project," (April 2013). <http://www.sei.cmu.edu/podcasts/index.cfm?getRecord=32E3E4F2-F5E4-6A77-803D6ACF208118F3&wtPodcast=TheEvolutionofaScienceProject>
- Novak, William. "Joint Programs and Social Dilemmas," (June 2013). <http://www.sei.cmu.edu/podcasts/index.cfm?getRecord=A05F0216-E3F3-64AA-5D517EBC97BFA09D&wtPodcast=JointProgramsandSocialDilemmas>
- Novak, William. "Acquisition Archetypes," (September 2013). <http://www.sei.cmu.edu/podcasts/index.cfm?getRecord=93ABBF8C-9C9F-50CA-F7ACD96396B289AA&wtPodcast=AcquisitionArchetypes>
- Ozkaya, Ipek. "Achieving Agility and Stability in Large-Scale Software Development," (January 2013). <http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=48701>
- Silowash, George; Flynn, Lori & Allen, Julia. "Mitigating Insider Threat: New and Improved Practices Fourth Edition," (February 2013). <http://www.cert.org/podcast/show/20130228silowash.html>
- Whisnant, Austin; Faber, Sid; & Allen, Julia. "Using Network Flow Data to Profile Your Network and Reduce Vulnerabilities," (October 2012). <http://www.cert.org/podcast/show/20121023whisnant.html>
- Wojcik, Rob. "Eliciting and Specifying Quality Attribute Requirements," (January 2013). resources.sei.cmu.edu/library/asset-view.cfm?assetID=48695
- Woody, Carol. "Addressing Supply Chain Risk Management," (February 2013). <https://www.brighttalk.com/summit/softwareassurance>
- Zubrow, Dave. "The Importance of Data Quality," (October 2012). <http://www.sei.cmu.edu/podcasts/index.cfm?getRecord=2D20D3AC-9E21-AC54-D796FCD84E67A288&wtPodcast=TheImportanceofDataQuality>
- Workshops and Tutorials**
- Chick, Tim. "TSP: The Agile Way." Guadalajara, Mexico (August 2013).
- Donohoe, Pat. "Introduction to Software Product Lines." Florence, Italy (August 2013).
- Giampapa, Joseph Andrew. "Testing and Evaluating Autonomous System Coordination." Alexandria, VA (March 2013).
- Gorton, Ian & Klein, John. "Scalable Software and Data Architectures." Vancouver, BC, Canada (June 2013).
- Kruchten, Philippe; Nord, Robert L. & Ozkaya, Ipek. "Architecture and Release Planning." Minneapolis, MN (April 2013).
- Kruchten, Philippe; Nord, Robert L. & Ozkaya, Ipek. "4th International Workshop on Managing Technical Debt." San Francisco, CA (May 2013).
- Lapham, Mary Ann. "Ready & Fit: Understanding Agile Adoption Risks in DoD and Other Regulated Settings." Inter Agency SDLC Seminar (May 2013).
- Lewis, Grace. "T8: Architectural Implications of Cloud Computing." Minneapolis, MN (April 2013).
- Lewis, Grace; Gray, Jeff; Muccini, Henry; Nagappan, Nachiappan; Rosenblum, David & Shihab, Emad. "1st International Workshop on the Engineering of Mobile-Enabled Systems (MOBS 2013)." San Francisco, CA (May 2013).
- Nichols, W.R. "Navigating Your Quality Journey." Montevideo, Uruguay (April 2013).
- Nichols, W.R.; Chick, Tim A. & Miluk, Gene. "Navigating Your Quality Journey: How to Engineer Exceptional Quality Software." Dallas, TX (September 2013).
- Nord, Robert. "Strategic Management of Technical Debt." Vancouver, BC, Canada (June 2013).
- Woody, Carol. "Software Assurance Methods in Support of Cyber Security." Orlando, FL (December 2012).
- Woody, Carol. "Software Assurance for CISO Executive Program, Carnegie Mellon University Heinz School." Pittsburgh, PA (February 2013).
- Woody, Carol. "Introduction to Software Assurance." Online workshop (June 2013).

SEI Reports (Unlimited Distribution) Published October 1, 2012 – September 30, 2013

Allen, Julia H.; Curtis, Pamela D.; Mehravari, Nader; Moore, Andrew P.; Partridge, Kevin G.; Stoddard, Robert W. & Trzeciak, Randall F. *Analyzing Cases of Resilience Success and Failure—A Research Study.* <http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=34036>

- Andersson, Bjorn; Bellomo, Stephany; Brownsword, Lisa; Cai, Yuanfang (Drexel University); Chaki, Sagar; Claycomb, William R.; Cohen, Cory; Cohen, Julie B.; Feiler, Peter H.; Ferguson, Robert; Flynn, Lori; Gluch, David P.; Goldenson, Dennis R.; Gurfinkel, Arie; Havrilla, Jeff; Hines, Chuck; Hudak, John J.; Huth, Carly L.; Jin, Wesley; Kazman, Rick; Lapham, Mary Ann; McCurley, James; McGregor, John; McIntire, David; Nord, Robert; Ozkaya, Ipek; Phillips, Brittany; Stoddard, Robert W. & Zubrow, David. *Results of SEI Line-Funded Exploratory New Starts Projects*. <http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=57592>
- Bellomo, Stephany & Woody, Carol. *DoD Information Assurance and Agile: Challenges and Recommendations Gathered Through Interviews with Agile Program Managers and DoD Accreditation Reviewers*. <http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=34083>
- Brownsword, Lisa; Albert, Cecilia; Carney, David J.; Place, Patrick R.; Hammons, Charles (Bud) & Hudak, John J. *Isolating Patterns of Failure in Department of Defense Acquisition*. <http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=53252>
- CERT Insider Threat Team. *Unintentional Insider Threats: A Foundational Study*. <http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=58744>
- Chick, Timothy A. & Pomeroy-Huff, Marsha. *Team Software Process (TSP) Coach Certification Guidebook*. <http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=59127>
- Chick, Timothy A.; McHale, Jim; Nichols, William & Pomeroy-Huff, Marsha. *Team Software Process (TSP) Coach Mentoring Program Guidebook, Version 2.0*. <http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=59115>
- Collins, Matthew L.; Spooner, Derrick; Cappelli, Dawn; Moore, Andrew P. & Trzeciak, Randall F. *Spotlight On: Insider Theft of Intellectual Property Inside the United States Involving Foreign Governments or Organizations*. <http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=48668>
- Elm, Joseph P. *The Business Case for Systems Engineering Study: Assessing Project Performance from Sparse Data*. <http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=34055>
- Elm, Joseph P. & Goldenson, Dennis R. *The Business Case for Systems Engineering Study: Results of the Systems Engineering Effectiveness Survey*. <http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=34061>
- Feiler, Peter H.; Goodenough, John B.; Gurfinkel, Arie; Weinstock, Charles B. & Wrage, Lutz. *Reliability Improvement and Validation Framework*. <http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=34069>
- Flynn, Lori; Huth, Carly L.; Trzeciak, Randall F. & Buttles-Valdez, Palma. *Best Practices Against Insider Threats in All Nations*. <http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=59082>
- Goldenson, Dennis R. & Stoddard, Robert W. *Quantifying Uncertainty in Expert Judgment: Initial Results*. <http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=41102>
- Hansen, Jeffrey; Hissam, Scott; Meyers, B. Craig; Moreno, Gabriel; Plakosh, Daniel; Seibel, Joe & Wrage, Lutz. *Resource Allocation in Dynamic Environments*. <http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=28121>
- Hilburn, Thomas B. (Embry-Riddle Aeronautical University); Ardis, Mark A. (Stevens Institute of Technology); Johnson, Glenn ((ISC)2); Kornecki, Andrew J. (Embry-Riddle Aeronautical University) & Mead, Nancy R. *Software Assurance Competency Model*. <http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=47953>
- Hissam, Scott; Klein, Mark H. & Moreno, Gabriel. *Socio-Adaptive Systems Challenge Problems Workshop Report*. <http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=53242>
- Householder, Allen D. *Well There's Your Problem: Isolating the Crash-Inducing Bits in a Fuzzed File*. <http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=28043>
- Lewis, Grace. *The Role of Standards in Cloud-Computing Interoperability*. <http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=28017>
- Messinger, Dominik & Lewis, Grace. *Application Virtualization as a Strategy for Cyber Foraging in Resource-Constrained Environments*. <http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=53234>
- Moore, Andrew P.; McIntire, David; Mundie, Dave & Zubrow, David. *Justification of a Pattern for Detecting Intellectual Property Theft by Departing Insiders*. <http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=41110>
- Moreno, Silvana (Universidad de la República); Tasistro, Álvaro (Universidad ORT Uruguay); Vallespir, Diego (Universidad de la República); & Nichols, William. *PSP-VDC: An Adaptation of the PSP that Incorporates Verified Design by Contract*. <http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=47974>
- Mundie, Dave & McIntire, David. *The MAL: A Malware Analysis Lexicon*. <http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=40240>
- Nichols, William; Kasunic, Mark & Chick, Timothy A. *TSP Performance and Capability Evaluation (PACE): Customer Guide*. <http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=59407>
- Nichols, William; Kasunic, Mark; & Chick, Timothy A. *TSP Performance and Capability Evaluation (PACE): Team Preparedness Guide*. <http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=59393>
- Nichols, William; Tasistro, Álvaro (Universidad ORT Uruguay); Vallespir, Diego (Universidad de la República); Faria, João Pascoal (University of Porto); Raza, Mushtaq (University of Porto); Henriques, Pedro C. (Strongstep Innovation in Software Quality); Duarte, César (Strongstep Innovation in Software Quality); Fallon, Elias (Cadence Design Systems, Inc.); Gazlay, Lee (Cadence Design Systems, Inc.); Kusakabe, Shigeru (Kyushu University); Omori, Yoichi (Kyushu University); Araki, Keijiro (Kyushu University); Grazioli, Fernanda (Universidad de la República) & Moreno, Silvana (Universidad de la República). *TSP Symposium 2012 Proceedings*. <http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=34091>
- Silowash, George. *Insider Threat Attributes and Mitigation Strategies*. <http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=57586>
- Silowash, George; Lewellen, Todd; Burns, Joshua W. & Costa, Daniel L. *Detecting and Preventing Data Exfiltration through Encrypted Web Sessions via Traffic Inspection*. <http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=40224>
- Silowash, George & King, Christopher. *Insider Threat Control: Understanding Data Loss Prevention (DLP) and Detection by Correlating Events from Multiple Sources*. <http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=34008>
- Silowash, George & Lewellen, Todd. *Insider Threat Control: Using Universal Serial Bus (USB) Device Auditing to Detect Possible Data Exfiltration by Malicious Insiders*. <http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=35427>
- Silowash, George; Cappelli, Dawn; Moore, Andrew P.; Trzeciak, Randall F.; Shimeall, Timothy J. & Flynn, Lori. *Common Sense Guide to Mitigating Insider Threats, 4th Edition*. <http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=34017>
- Simanta, Soumya; Lewis, Grace; Morris, Edwin J.; Ha, Kiryong (Carnegie Mellon University School of Computer Science) & Satyanarayanan, Mahadev (Carnegie Mellon University School of Computer Science). *Cloud Computing at the Tactical Edge*. <http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=28021>

SEI STAFF AND OTHER CONTRIBUTORS

As of September 30, 2013

Full-Time & Part-Time Employees

Lisa M. Abel
John J. Ackley
Lorraine J. Adams
Steve Ader
Laura Aguera
Ilke L. Akin
Yoshihiro Akiyama
Cecilia Albert
Christopher J. Alberts
Michael J. Albrethsen
William T. Aldrich-Thorpe
Jared C. Allar
Dennis Allen
Julia H. Allen
Noelle Allon
Amanda K. Alvarez
Rogelio G. Alvarar
Kathryn M. Ambrose
Laura L. Anderson
Naomi M. Anderson
William B. Anderson
Bjorn A. Andersson
Archie Andrews
Eileen Angulo
John F. Antonucci
Luiz Antunes
Jeffrey J. Apolis
Melissa Argenziano
Leena Arora
Christopher A. Atwood
Brian J. Averi
Felix Bachmann
Marie A. Baker
Karen A. Balistreri
Vincent F. Balistreri
Aaron Ballman
Jeffrey Balmert
Ronald Bandes
Michael Bandor
Alex T. Bang
Richard E. Barbour
Michelle L. Barker
Hollen L. Barmer
Jeffrey J. Basista
Barbora Batokova
Roger A. Beard
Dwight S. Beaver
Stephen R. Beck
Robert F. Behler
Stephany Bellomo
Klaus Bellon
Jonathan Bender
Brian D. Benestelli
Kate Bennett
Constance M. Bennett
John K. Bergey
Anna M. Berta
Shawn D. Besselman
James E. Besterici
Robert W. Beveridge
Donald R. Beynon
Nicholas J. Bialaszewski
Philip Bianco
David Biber
Daniel R. Bidwa
Darlene R. Bigos
Tracy A. Bills
Adrienne N. Bishop
Stephen Blanchette

Jeffrey L. Boleng
Elaine W. Bolster
Joshua J. Bowen
Randall R. Bowser
Andrew D. Boyd
Diane I. Bradley
Ben W. Bradshaw
John Bramer
Kara Branby
Pamela Brandon
Heidi Brayer
Rex E. Brinker
Rita M. Briston
Rhonda M. Brown
Lisa L. Brownsword
Andrew M. Bunker
Matthew Butkovic
Tamara L. Butler
Palma J. Buttles-Valdez
Nickolas S. Byers
Gene M. Cahill
Anthony F. Calabrese
Rachel Callison
Kimberley S. Campbell
Linda M. Campbell
Linda Canon
Peter S. Capell
Richard A. Caralli
Anita D. Carleton
Cassandra L. Carricato
Ryan M. Casey
William Casey
Tracy M. Cassidy
Mary K. Cattrell
James Cebula
Anthony M. Cebzanov
Sagar J. Chaki
Gary J. Chastek
Mary Jo Chelosky
Timothy A. Chick
Leslie R. Chovan
Mary Beth Chrissis
Natalie Chronister
Jonathan Chu
Matthew T. Churilla
Jason W. Clark
Kathleen Clarke
William R. Claycomb
Michael R. Clement
Matthew F. Coates
Cory F. Cohen
Julie B. Cohen
Sanford (Sholom) G. Cohen
Constantine Aaron Cois
Mary Lou Cole
Matthew L. Collins
James Conley
Anne Marie Connell
Carol L. Connelly
John R. Connelly
James P. Conrad
Robert Conway
Christine Cooney
Stephen P. Cooney
Rebecca Lynn Cooper
Patricia A. Copelin
Stephanie Lynn Corbett
Alexander P. Corn
Daniel L. Costa
Jennifer Cowley
Randy Crawford

Rita C. Creel
Lucy M. Crocker
Stephanie D. Crowe
Larry J. Crowe
Michael E. Crowley
Natalie Cruz
Sally A. Cunningham
Pamela D. Curtis
Tenai J. Cutting
Jerome Czerwinski
Rebecca A. D'Acunto
Eugene T. Dailey
Roman Danyliw
Amanda H. Darcy
Rosemary J. Darr
Jeff Davenport
John M. Dayton
Dionisio De Niz
Edward H. Deets
Grant Deffenbaugh
Julien Delange
Nathan Dell
Kareem Demian
Matthew J. Desantis
Edward R. Desautels
Aaron M. Detwiler
Jill Diorio
John V. Diricco
Robert M. Ditmore
Mary Claire Dixon
Quintin A. Doles
George D. Doney
Patrick J. Donohoe
William A. Dormann
Audrey J. Dorofee
Joan P. Downing
Margie Ann Drazba
Elke Drennan
Michael W. Duggan
Evelyn Duncan
Catherine A. Duncan
Anthony C. Durante
Madelaine G. Dusseau
Ladonna Dutton
Karin Dwyer
Sean D. Easton
Sebastian Echeverria
James R. Edmondson
Danielle L. Edwards
Eileen A. Eicheldinger
Charles W. Eichholtz
Robin N. Eisenhart
Robert J. Ellison
Joseph P. Elm
Linda M. Elmer
Harold Ennulat
Lover Epps
Neil A. Ernst
Felicia L. Evans
Alan Evans
Sidney Faber
Michele E. Falce
Kevin R. Fall
Kimberly J. Farrah
Mariane Fazekas
Matthew A. Fazekas
Maureen Fechik
Jeffrey B. Federoff
Peter H. Feiler
Eric Ferguson
Robert W. Ferguson

Francis E. Finley
Kodiak Firesmith
Donald G. Firesmith
William L. Fithen
Robert W. Flooddeen
Lori Flynn
Jonathan M. Foote
Justin Forbes
John T. Foreman
Kunta Fossett
Arne Fostvedt
Summer Fowler
Tracey E. Fox
Jonathan Frederick
David French
Michelle Fried
Richard Friedberg
Jennifer R. Fritsch
Michael R. Fritz
Brent R. Frye
Michael J. Gagliardi
Brian W. Gardiner
Matthew E. Gaston
Linda Parker Gates
Jeffrey S. Gennari
Robert George
Joseph Giampapa
Ryan M. Gindhart
Dennis R. Goldenson
John B. Goodenough
Ian Gorton
Walter J. Goss
Bruce A. Grant
Douglas A. Gray
Michael D. Greenwood
David E. Gregg
Russell Griffin
Phillip A. Groce
Charlene C. Gross
Jon L. Gross
Jacqueline D. Grubbs
Rajasekhar Gudapati
Arie Gurfinkel
Rotem Guttman
David A. Guzik
Shannon Haas
Bart L. Hackemack
Nancy L. Hags
Alan W. Hall
John Haller
William Halpin
Jeffrey A. Hamed
Josh Hammerstein
Charles B. Hammons
Michael Hanley
Jeffery Hansen
Stephen D. Hardesty
Erin Harper
Gibbie Lu Hart
Eric Hatleback
Jeffrey S. Havrilla
Jason K. Hawk
John Hawrylak
William S. Hayes
Matthew A. Heckathorn
Stephanie L. Hedges
Jessica L. Hedges
Sharon Henley
Sandra Hepp
Christopher Herr
Kurt Hess

Charles Hines
Scott A. Hissam
Barbara J. Hoerr
Jonathan R. Holaday
Bryon J. Holdt
Lorraine M. Hollabaugh
Charles Holland
Andrew F. Hoover
Angela Horneman
Dan P. Horvath
Allen D. Householder
Joshua R. Howell
John W. Huber
John J. Hudak
Spencer Huff
Clifford C. Huff
Lyndsi A. Hughes
Alexa Huth
Jennifer Hykes
Chris Inacio
Terry A. Ireland
James Ivers
Jerry D. Jackson
Vanessa B. Jackson
Michael B. Jacobs
Carol A. Jarosz
Michael Jehn
Zachary Jensen
George M. Jones
Lawrence G. Jones
Jacob M. Joseph
Patricia Junker
Gavin T. Jurecko
Youngho Ka
Matthew Kaar
Stephen Kalinowski
Derrick H. Karimi
Rachel A. Kartch
Mark D. Kasunic
Harry P. Kaye
David Keaton
Tracey A. Kelly
Alexander Kem
Robert Kemerer
Brent Kennedy
Jennifer Kent
Carolyn M. Kernan
Kelly L. Kilgour
Christopher King
Kimberly D. King-Cortazzo
Mark H. Klein
Stacy Klein
John R. Klein
Mark Klepach
William E. Klieber
Dan J. Klinedinst
Georgeann L. Knorr
Andrew J. Kompanek
Michael D. Konrad
Keith A. Korzec
John J. Kostuch
Paul N. Krystosek
Robert E. Kubiak
Amy Kunkle
David S. Kyle
Michael L. Lambert
Joel Land
Debra J. Lange
Mary Ann Lapham
Frank Latino
Alyssa M. Le Sage

Bernadette Ledwich
Sung M. Lee
Ryan Lehman
Harry L. Levinson
Todd B. Lewellen
Darrell Lewis
Grace A. Lewis
Michele G. Ley
Alena Leybovich
Amy J. Leyland
Leanne M. Libert
Joshua B. Lindauer
Martin M. Lindner
Howard F. Lipson
Reed Little
Todd S. Loizes
Gregory Longo
Melissa Ludwick
Richard W. Lynch
Marlene T. MacDonald
Rudolph T. Maceyko
Vamsi Maddula
Lisa M. Makowski
Arthur A. Manion
Jay Marchetti
Attilio A. Marini
Tamara Marshall-Keim
Theodore F. Marz
Laura L. Mashione
Lola Mason
Michael D. Massa
Stephen M. Masters
Kelly B. Matrazzo
Joseph P. Matthews
Roxanne Matthews
Jeffrey Mattson
Christopher J. May
Joseph M. Mayes
John J. McAllister
Michael P. McCord
Jason D. McCormick
James McCurley
Kathleen McDonald
Patricia McDonald
Shane P. McGraw
James D. McHale
David M. McIntire
Bernadette McLaughlin
Michael McLendon
Joseph A. McLeod
Scott McMillan
Jason McNatt
Deborah McPherson
Nancy R. Mead
Ryan W. Meeuf
Nader Mehravari
Andrew O. Mellinger
Peter J. Menniti
Thomas J. Merendino
Jennifer C. Mersich
Leigh B. Metcalf
Toby Meyer
Bryce Meyer
Bertram C. Meyers
Amy Miller
Cassandra S. Miller
Gerald Miller
Suzanne M. Miller
Eugene E. Miluk
Marion V. Moeser
Soumyo Moitra
Elizabeth A. Monaco
Juan Montelibano
Austin Montgomery
Andrew P. Moore
Jose A. Morales

Damon Morda
Gabriel A. Moreno
John F. Morley
Steven Morley
Edwin J. Morris
Timothy B. Morrow
Anna Mosesso
Angela L. Mosqueda
Julia L. Mullaney
David A. Mundie
Robert Murawski
David J. Murphy
Michael P. Murray
Paul J. Murray
Mark Musolino
Lynne M. Naelitz
Melissa Neely
Cynthia L. Nesta
Gail L. Newton
John O. Nicholas
William Nichols
Alex Nicoll
Kenneth Nidiffer
Paul D. Nielsen
Crisanne Nolan
Robert Nord
Mika North
Linda M. Northrop
William E. Novak
Marc R. Novakouski
Kevin Nowicki
Ray Obenza
Patricia A. Oberndorf
Matthew O'Hanlon
Sharon R. Oliver
Michael F. Orlando
Jose Ortiz
Kristofer M. Ostergard
James W. Over
Ipek Ozkaya
Mari A. Palestra
Timothy Palko
K. C. Palmquist
M. S. Palmquist
Amanda Parente
Allison Parshall
Kevin G. Partridge
Nicole Pavetti
Carmal Payne
David J. Pekular
Kelwyn O. Pender
Brenda A. Penderville
Mary L. Penn
Samuel J. Perl
Sharon K. Perry
Linda H. Pesante
Richard D. Pethia
Thomas E. Petrus
David M. Phillips
Dewanne M. Phillips
Janet S. Philpot
Daniel Pipitone
Patrick Place
Daniel Plakosh
Michael J. Pochan
Alicia N. Poling
William Pollak
Stephanie R. Pomerantz
Mary E. Popeck
Douglass Post
Jerome J. Pottmeyer
John M. Prevost
Sean P. Provident
Kara Quinto
Traci M. Radzyniak
Angela Raible

James C. Ralston
Donald M. Ranta
Adam W. Rathbun
Michael Rattigan
Adam J. Rauf
Frank J. Redner
Aaron K. Reffett
Colleen Regan
David Reinoehl
Janet Rex
Clifford Rhoades
Louis A. Richards
Nathaniel Richmond
Michael A. Riley
Kimberly Ripple
John E. Robert
Lawrence R. Rogers
James D. Root
Steve W. Rosemergy
Robert Rosenstein
Sheila L. Rosenthal
Dominic A. Ross
Christian Royle
Bradley Rubbo
Daniel Ruef
Robin M. Ruefle
Paul Ruggiero
Kristopher Rush
Mary Lou Russo
Mary Lynn Russo
Charles J. Ryan
Venkatavijaya Samanthapudi
Thomas M. Sammons
Char Sample
Geoffrey T. Sanders
Concetta R. Sapienza
Emily E. Sarneso
Vijay S. Sarvepalli
Mark Satterfield
Jeff Savinda
Thomas Scanlon
Alfred R. Schenker
David A. Scherb
Robert B. Schiela
Andrew Schlackman
Steve Scholnick
Patricia Schreiber
Ryan W. Schroeder
James Schubert
Jonathon M. Schuler
Kenneth Schultz
Giuseppe Sciulli
Tina Sciuillo-Schade
Philip A. Scolieri
David M. Scott
Shirley M. Scott
William S. Scully
Robert C. Seacord
Martin Sebor
Joseph R. Seibel
James S. Semler
Lui Sha
Gregory E. Shannon
Sharon L. Shaw
Ryan Shaw
Sarah Sheard
David J. Shepard
Nataliya Shevchenko
Timothy J. Shimeall
Dongwan Shin
Yasutaka Shirai
Linda E. Shooer
Sandra L. Shrum
George J. Silowash
Soumya Simanta
Matthew P. Sisk

Lisa D. Sittler
Carol A. Sledge
Michelle A. Slusser
Holly Smith
Kenneth L. Smith
James Smith
Lenny D. Smith
Timur D. Snoko
Tara Sparacino
Debra A. Spear
James L. Spencer
Derrick Spooner
Jonathan Spring
Bryan Springer
Bryan D. Stake
Stephen B. Stancliff
Lauren M. Stanko
Jonathan Steele
Kate Steiner
Lizann Stelmach
Julie Stephenson
James F. Stevens
Katie C. Stewart
Robert Stoddard
John P. Stogoski
Michael P. Stone
Edward R. Stoner
Jeremy R. Strozer
Gregory Such
Siobhan Sullivan
Dean Sutherland
David M. Svoboda
Michael J. Szegegy
Lucille Tambellini
Joe Tammariello
Christopher Taschner
Brady Tello
Michael C. Theis
Marcia J. Theoret
Jeffrey E. Thieret
Kimberly E. Thiers
Alisa Thomas
William R. Thomas
Mark E. Thomas
David K. Thompson
Michele A. Tomasic
Barbara J. Tomchik
Carolyn Tomko
Brian M. Torbich
Troy L. Townsend
Helen Trautman
Peter J. Troxell
Donovan Truitt
Randall F. Trzeciak
Barbara A. Tyzenhaus
Laurie A. Tyzenhaus
David Ulicne
Jeanette Urbanek
Vijay Sai Vadlamudi
Michelle A. Valdez
Christine Van Tol
Marie Van Tyne
Kevin Vargo
Aaron M. Volkmann
Alexander Volynkin
Robert A. Vrtis
Todd Waits
Kurt C. Wallnau
Cynthia E. Walpole
Pennie B. Walters
Mary C. Ward
George W. Warnagiris
David Warren
Trina Washington
Andrea L. Wasick
Rhiannon Weaver

Michael S. Weber
Samuel M. Weber
Charles B. Weinstock
Eric B. Werner
James T. Wessel
Austin B. Whisnant
Barbara White
Amanda Wiehagen
Emerson R. Wiley
Jeffrey A. Wiley
Pamela J. Williams
William R. Wilson
Craig J. Wink
Brian D. Wisniewski
Robert M. Wojcik
William G. Wood
Carol S. Woody
Lutz Wrage
Michael A. Wright
Keith Wright
Evan Wright
Eileen O. Wrubel
Joseph D. Yankel
Charles G. Yarbrough
John W. Yarger
Hasan Yasar
Jamie L. Yoder
Lisa R. Young
Cat B. Zaccardi
Mark T. Zajicek
Marianne C. Zebrowski
John J. Zekany
Xiaobo Zhou
David Zubrow
Michael J. Zuccher

Other Contributors

Michael Appel
Max Blumenthal
Peter P. Chen
Randall Croker
Julie DeLorenzo
Larry Druffel
Ian Glasner
Andrew J. Holton
Ryan Howley
Kenneth Hsu
Lawrence Jackson
Wesley Jin
Frederick Kazman
Ari Zachary Klein
Nils Kresl
Justin Loo
Matthew Moses
Jennine Nash
Alexander Rodriguez
Laura Scherb
Doug Schmidt
Deana Shick
Eric Telmer
Joshua Thiry
Eric Wong
Xiao Yun Yang

Affiliates

Yoshihiro Akiyama
Michael R. Clement
Jose Ortiz
Mary Lynn Penn
Martin Sebor
Yasutaka Shirai

Copyrights

Copyright 2014 Carnegie Mellon University

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the United States Department of Defense.

References herein to any specific commercial product, process, or service by trade name, trade mark, manufacturer, or otherwise, do not necessarily constitute or imply its endorsement, recommendation, or favoring by Carnegie Mellon University or its Software Engineering Institute.

This material has been approved for public release and unlimited distribution except as restricted below.

Internal use:* Permission to reproduce this material and to prepare derivative works from this material for internal use is granted, provided the copyright and “No Warranty” statements are included with all reproductions and derivative works.

External use:* This material may be reproduced in its entirety, without modification, and freely distributed in written or electronic form without requesting formal permission. Permission is required for any other external and/or commercial use. Requests for permission should be directed to the Software Engineering Institute at permission@sei.cmu.edu.

* These restrictions do not apply to U.S. government entities.

No Warranty

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN “AS-IS” BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

Trademarks and Service Marks

Carnegie Mellon Software Engineering Institute (stylized), Carnegie Mellon Software Engineering Institute (and design), and the stylized hexagon are trademarks of Carnegie Mellon University.

Carnegie Mellon® and CERT® are registered marks of Carnegie Mellon University.

Team Software ProcessSM and TSPSM are service marks of Carnegie Mellon University.

For information and guidelines regarding the proper referential use of Carnegie Mellon University service marks and trademarks, see Trademarks and Service Marks at www.sei.cmu.edu/legal/marks/.

DM-0001088

The SEI Year in Review is produced by SEI Communication Services

Manager, Communication Services

William Thomas

Manager, Corporate & Technical Communications

Janet Rex

Manager, Public Relations

Richard Lynch

Editor-in-Chief

Ed Desautels

Editorial

Hollen Barmer

Heidi Brayer

Ed Desautels

Claire Dixon

Tamara L. Marshall-Keim

Gerald Miller

Paul Ruggiero

Pennie Walters

Design

Klaus Bellon

Illustration

Kurt Hess

Digital Production

Melissa Neely

Photography

Tim Kaulen, Photography and Graphic Services, Mellon Institute

Klaus Bellon

David Biber

TO DETERMINE HOW TO PUT THE SEI TO WORK FOR YOUR ORGANIZATION, CONTACT SEI CUSTOMER RELATIONS AT [INFO@SEI.CMU.EDU](mailto:info@sei.cmu.edu).

Work with the SEI

Congress established the SEI in 1984 because software is vital to the national interest. By working with the SEI, organizations benefit from more than two decades of government investment and participation from organizations worldwide in advancing the practice of software engineering.

The SEI creates, tests, refines, and disseminates a broad range of technologies, tools, and management techniques. These techniques enable organizations to improve the results of software projects, the quality and behavior of software systems, and the security and survivability of networked systems.

As an applied research and development center, the SEI brings immediate benefits to its research partners and long-term benefits to organizations that depend on software. The tools and methods developed by the SEI and its research partners are applied daily in organizations throughout the world.

How the SEI Works with Government and Industry

SEI staff members help the U.S. Department of Defense (DoD) and other government agencies solve software engineering and acquisition problems. SEI direct support is funded through task orders for government work. Engagements with the SEI are of particular benefit to government program managers, program executive officers, and senior acquisition executives, particularly those with long-range programs that will benefit from strategic improvements that the SEI fosters.

The SEI has a well-established process for contracting with government agencies and will work with an organization to meet its needs.

The SEI works with commercial organizations that want to develop a strategic advantage by rapidly applying improved software engineering technology.

The SEI works with organizations that want to combine their expertise with the SEI's expertise to mature new technology for the benefit of the entire software industry.

Customer Relations

Software Engineering Institute
Carnegie Mellon University
4500 Fifth Avenue
Pittsburgh, PA 15213-2612
1-888-201-4479 or +1-412-268-5800
info@sei.cmu.edu

SEI Employment

The SEI seeks candidates for its technical, business, and administrative staff divisions. Contact the SEI Human Resources department to learn about the benefits of working at the SEI: www.sei.cmu.edu/careers.



