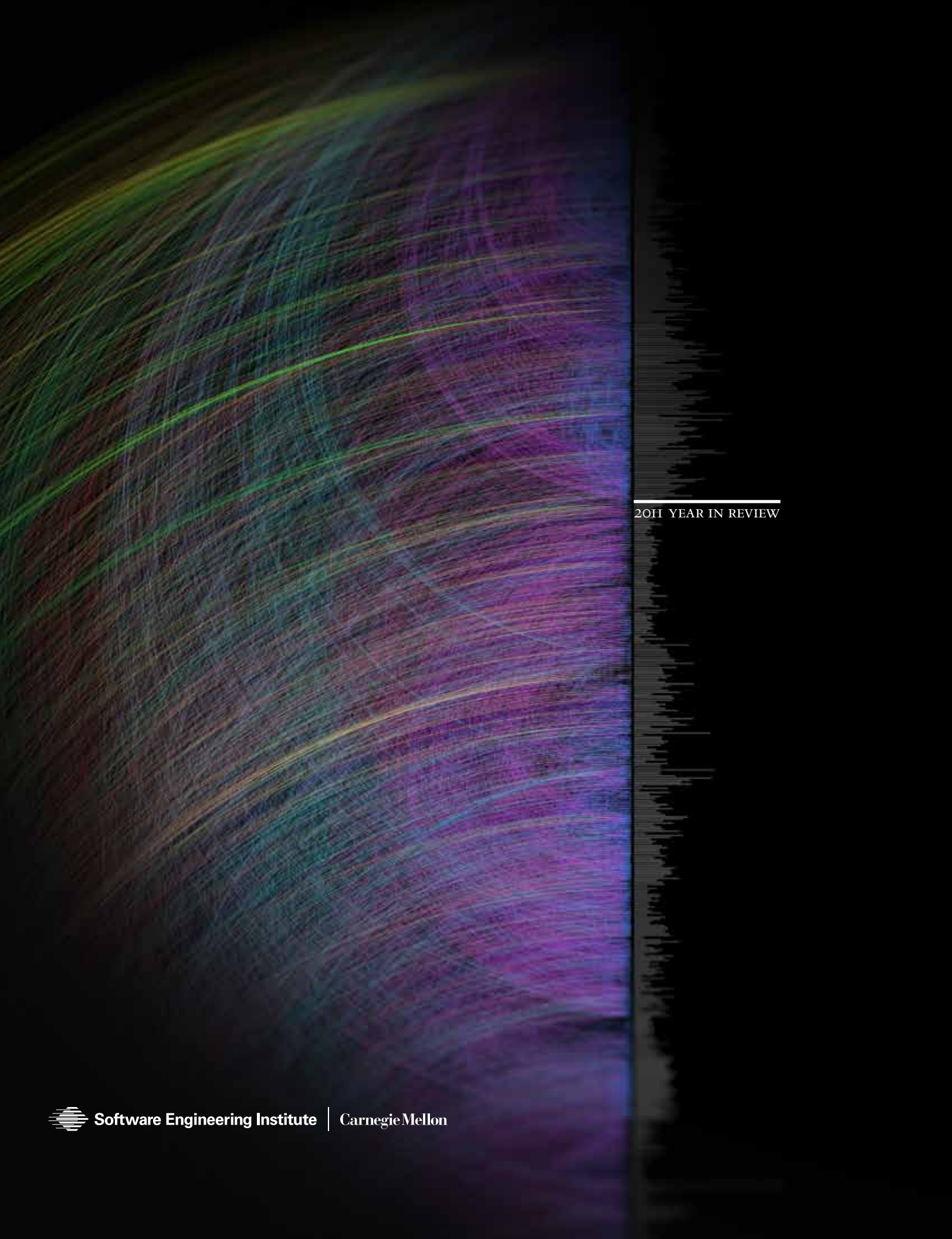


2011 YEAR IN REVIEW

Software Engineering Institute | Carnegie Mellon

Software Engineering Institute | Carnegie Mellon

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 mission is to advance software engineering and related disciplines to ensure systems with predictable and improved quality, cost, and schedule.

CONTENTS

MESSAGE FROM THE DIRECTOR

2011 was a record year for the SEI—a year of significant growth in our impact, in our influence, and in our initiative. Working with the Department of Defense (DoD), we sharpened the research focus of the Institute, added to our world-class staff, and received funding for the largest amount of new work the SEI has ever undertaken in one year. It was a year of leadership, excellence, and growth in software engineering.

The SEI's success is really the success of its men and women. Across the Institute, the SEI is fortunate to have a skilled, smart, and inquisitive staff—some 600 people dedicated to excellence and innovation.

That dedication was recognized in 2011 at the individual level with the naming of Linda Northrop as an SEI fellow, a designation awarded to people who have made especially significant career contributions to the SEI and the software engineering community—and who continue to chart the future on key issues. Northrop, director of the Research, Technology, and System Solutions Program, is the Institute's fifth SEI fellow. We congratulate her *(see page 26)*.

2011 was also, unfortunately, a year of departures. We marked the retirement in September of Clyde Chittister, a 26-year SEI employee who served the organization as deputy director for operations and chief operating officer. And, shortly after the end of the fiscal year, Doug Schmidt—our deputy director for research and chief technology officer—announced his decision to return to Vanderbilt University to teach and mentor the next generation of researchers.

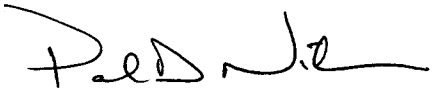
This report in many ways reflects the hard work and innovative thought of people such as Linda Northrop, Clyde Chittister, and Doug Schmidt, shared and amplified by our entire staff.

Among the many stories in these pages, here are glimpses of just a few:

- As the challenge to provide warfighters competitive advantage quickly has grown more acute, interest in Agile methods within the DoD acquisition community has also grown. In 2011, the SEI focused its investigation of Agile methods to develop guidance for DoD program managers, and plans to develop a companion contingency model in 2012 *(see page 8)*.
- Two senior members of the technical staff at the SEI collaborated on a "should-cost" analysis of the software used in the F-22 modernization program. The Air Force program was one of the first to use the new should-cost estimation process *(see page 7)*.
- Government and industry both want to know: "How can we improve, evaluate, and standardize the quality of data we use?" To begin to tackle this problem, SEI researchers collaborated with the Office of the Under Secretary of Defense (USD) for Acquisition, Technology, and Logistics (AT&L), Acquisition Visibility (AV). The team set out to evaluate statistical methods for improving on existing, manual methods of anomaly detection *(see page 25)*.
- The Accelerated Improvement Method (AIM), streamlines CMMI adoption through a tailored version of the Team Software Process and Six Sigma measurement strategies. Helping organizations implement AIM is one way the SEI is increasing our focus on performance results *(see page 12)*.
- The past year saw continued research by the SEI into addressing the challenges of monitoring large networks for malicious activity. The SEI's approaches rely on techniques to summarize communications between hosts on the network. Even using summary techniques, monitoring large networks operated by the U.S. government and commercial enterprises generates huge volumes of data that security analysts cannot possibly analyze unassisted. Network Situational Awareness team members in the SEI's CERT® Program have developed approaches to automate that analysis *(see page 14)*.

Through these efforts and many more—and through the dedicated work of the entire SEI team—we are well positioned for the future. We'll continue to enhance our research efforts while maintaining our excellent record of transition and acquisition support. I look forward to answering the challenges as we have done over the past quarter-century, and fully expect that the SEI will have a significant impact in 2012 and the years beyond.

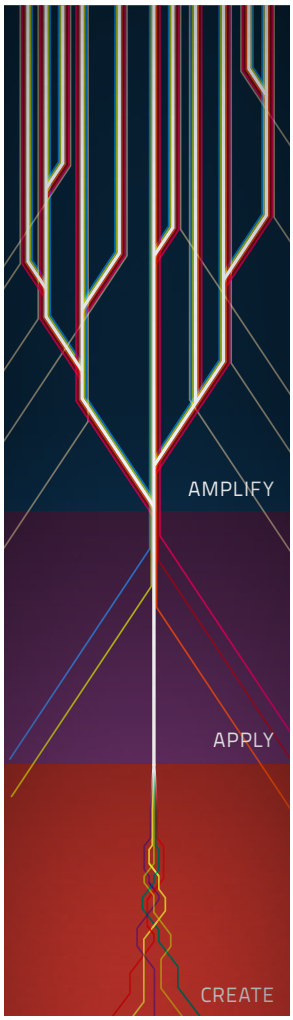
Sincerely,



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 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 community 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 community and organizations dependent on software to encourage and support the widespread adoption of new and improved technologies and solutions through

- advocacy
- books and publications
- certifications
- 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 improvements.

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

AREAS OF WORK

The SEI technical program—created and carried out by world-recognized leaders in software engineering, security, and process management—consists of four technical programs. The SEI also conducts new research into emerging topics in software and systems engineering.

Quality software that is produced on schedule and within budget is a critical component to U.S. defense systems, which is why the U.S. Department of Defense (DoD) established the SEI in 1984. Since then, the SEI has advanced software and systems engineering principles and practices, while serving as a national and international resource for the software and systems engineering communities. As an applied research and development center, the SEI brings immediate benefits to its research partners and long-term benefits to the software industry as a whole.

Operated by Carnegie Mellon University—a global research university recognized worldwide for its world-class arts and technology programs—the SEI operates at the leading edge of technical innovation. The SEI's core purpose is to help organizations improve their capabilities and to develop or acquire the right software, defect free, on time, and on budget, every time.

The SEI offers solutions to customers in the areas of

- Acquisition
- Process Management & Measurement
- Risk
- Security
- Software Development
- System Design

The SEI's technical focus areas, together with its outreach activities, are aimed at meeting the defined software engineering needs of the DoD. Within these areas of work, the SEI collaborates with defense, government, industry, and academic institutions to continuously improve software-intensive systems. The SEI's body of work in technical and management practices is focused on developing software right the first time, which results not only in higher quality, but also in predictable and improved schedule and cost.

01

OVERCOMING CHALLENGES IN THE FIELD WITH CLOUDLETS AND VIRTUAL MACHINES

A soldier on the ground learns that the enemy's position has changed. On his handheld device, he revises the diagram depicting the battlefield configuration he has just sent his commander and sends her the new image. This time, however, the message isn't getting through—an enemy attack has cut off the connection. He quickly locates another connection through a nearby Humvee and successfully sends the image.

Handheld devices offer powerful potential in the battlefield. They can aid soldiers in tasks such as speech and image recognition, natural language processing, decision making, and mission planning. This is why researchers Grace Lewis, Soumya Simanta, and Dan Plakosh, members of the SEI Research, Technology, and System Solutions (RTSS) Program, are investigating ways to best leverage the full capabilities of handhelds. The SEI team is collaborating with Mahadev Satyanarayanan, creator of the cloudlet concept and a faculty member at Carnegie Mellon University's School of Computer Science.

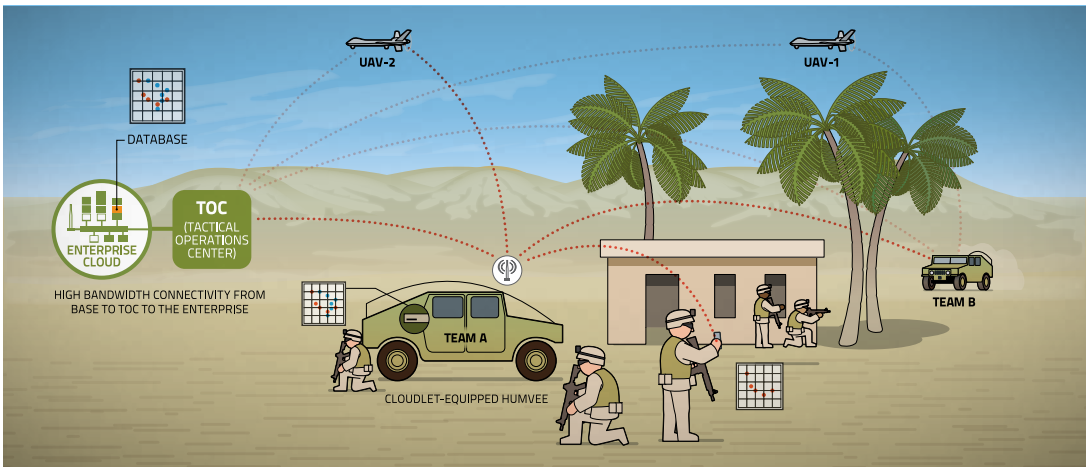
Their research addresses three main challenges. First, mobile devices offer less computational power than conventional desktops or server computers. Second, computation-intensive tasks, such as image or pattern recognition, take a heavy toll on battery power. Finally, networks have limited bandwidth and are unreliable.

"Our research explores ways to overcome these obstacles by using cloudlets, which are localized, lightweight servers running one or more virtual machines," says Lewis. When soldiers must perform tasks that consume extensive memory or processing power, they can offload them to cloudlets from their handheld mobile devices to extend processing capacity and conserve battery."

Cloudlets are located in physical proximity to the handheld devices that use them (for example, on Humvees). This reduces network latency because communication is limited to a single-hop network. Battery consumption potentially decreases through use of Wi-Fi instead of broadband wireless, which consumes more energy. From a security perspective, cloudlets can use Wi-Fi networks to take advantage of existing security policies that might prescribe, for example, certain encryption techniques or access only from specific handheld devices.

Additional advantages derive from use of virtual-machine (VM) technology. VM increases flexibility in the type and platform of applications and reduces software configuration and setup time. These properties are critical for systems used by soldiers or first responders working in dynamic and hostile environments where mission needs change rapidly and cyber resources are limited or subject to attacks. A form of VM technology called dynamic VM synthesis is particularly useful in such hostile environments. Its flexibility enables the use of opportunistically available resources, as well as rapid replacement of lost cyber resources.

Lewis summarizes her team's future direction: "This year, in the first phase, we focused on creating a cloudlet prototype. In the second phase, we'll conduct measurements to see if computations in a cloudlet provide significant reductions in device battery power. We'll also gather measurements related to bandwidth consumption to focus on optimization of cloudlet setup time. Assuming we're successful, we will use the third phase to create an experimental cloudlet cluster to explore other ways to take computation to the tactical edge."



17% COMPOUND ANNUAL GROWTH IN GOVERMENT SPENDING ON CLOUD TECHNOLOGY IS EXPECTED FROM 2009–2014. (INPUT.COM, 2009)

PHOTO COURTESY OF U.S. ARMY

GRACE LEWIS

"Assuming we're successful, we will use the third phase to create an experimental cloudlet cluster to explore other ways to take computation to the tactical edge."

— GRACE LEWIS

ROBERT FERGUSON & MIKE PHILLIPS

"We aren't just trying to sell a model or a method. We're talking about doing things in a way that has proven to work, and if you don't use the practices, you won't get the performance."

— MIKE PHILLIPS

1.7 MILLION

THE F-22'S AVIONICS SOFTWARE HAS 1.7 MILLION LINES OF CODE.

PHOTO COURTESY OF USAF

02

DRIVING PRODUCTIVITY FOR THE F-22: THE BENEFIT OF SHOULD-COST ANALYSIS

"Do more without spending more," urged Ashton Carter in a 2010 memo. Carter was then Under Secretary of Defense for Acquisition, Technology, and Logistics. His call for improved productivity advocated the use of should-cost estimates for major defense programs. Previously, program budgeting depended on estimates that forecasted what a project will cost based on past experience.

Carter called this "business-as-usual management" that essentially required programs to fully expend their budgets. Or, as the SEI's Mike Phillips said, "Once you have that estimate, well, it never seems to come in any cheaper. With the next estimate based on the one preceding it, there is never an opportunity to account for the lessons learned that help software and systems developers get better at their work."

Phillips and Robert Ferguson, both senior members of the technical staff at the SEI who work on the Software Engineering Measurement and Analysis initiative, collaborated on a should-cost analysis of the software used in the F-22 modernization program. The program, which includes upgrades to the aircraft's air-to-ground and intelligence, surveillance, and reconnaissance capabilities, was one of the first Air Force programs to use the new should-cost estimation process.

"Our estimate succeeded in finding improvements that could significantly reduce the cost of the program," said Ferguson. To calculate the should-cost estimate, the SEI used the data from the initial basis of the contractor's estimate to create a parametric estimate that closely matched the contractor's. The SEI then used the resulting model to test the sensitivity of the estimate and judge where potential savings could be found and how much could be saved. For example, team performance and estimates of quality could be compared to industry benchmarks. Contractors could then be encouraged to adopt improvements to improve development performance.

One significant source of savings came from improving quality at earlier stages of the lifecycle by adopting best practices. This reduced defects and lowered testing costs. As research has shown—including extensive data from the Team Software Process (TSP) work done at the SEI—repeated testing and defect-removal activities are very inefficient in terms of time and money. "Performance is correlated with using best practices early in the life cycle," says Phillips. "We aren't just trying to sell a model or a method. We're talking about doing things in a way that has proven to work, and if you don't use the practices, you won't get the performance."

The structure of the estimation models assumes that disciplined software development takes less effort than undisciplined development. "This is a reminder to organizations that there is value in bringing discipline to what they do. The estimation tool reflects that value. Estimators have an obligation to show managers the positive effects of high process quality and high levels of development performance. Failure to improve performance could eventually make a contractor non-competitive," Ferguson said.

Another interesting aspect of the F-22 program, according to Phillips, is the plan to focus first on software to increase capability. "People usually want to start with the hardware they want, and then develop software to support it," he said. "Now they can get a lot of capability without having to do hardware upgrades to make it work." While updated hardware is also important to the F-22, rethinking development will enable the F-22 program to get capability improvements sooner. The package of upgrades that included hardware would only have demonstrated benefit in six years; by addressing software first, the estimated time was reduced to two and a half years.

Phillips, a former Air Force test pilot, thinks this shift in thinking is an interesting change. "Think of the way banks have changed," he says. "There used to be lots of paper money going back and forth across the counter. Now the transactions are more and more electronic, and a bank is kind of like a big box with lots of ones and zeros in it. Now a supersonic jet can be thought of more and more as a bunch of ones and zeros with a plane around it."

As the role of software in Department of Defense (DoD) programs has grown, the SEI has brokered compromise between contractors and DoD programs. Both parties must work to improve processes, and they must collaborate on compromises that save time and money without sacrificing quality. Should-cost estimation for software development makes an important contribution to the ultimate goal of making everything more affordable through a collaborative approach between industry and government.

STEPHANY BELLOMO

MARY ANN LAPHAM

PHOTO COURTESY OF US ARMY
TAKEN BY SGT. MATTHEW MOELLER

"When applied properly in the right context, Agile can accelerate the delivery of high-value software capability."

— STEPHANY BELLOMO

AGILE:

An iterative and incremental (evolutionary) approach to software development. It is performed collaboratively by self-organizing teams within an effective governance framework. Our work in this area is led by Mary Ann Lapham.

03

INVESTIGATING THE VALUE OF AGILE IN ACQUISITION PROGRAMS

In 2008, then Secretary of Defense Robert Gates said, "Our conventional modernization programs seek a 99 percent solution in years. Stability and counterinsurgency missions—the wars we are in—require 75 percent solutions in months." As the challenge to provide warfighters competitive advantage has grown more acute, interest in Agile methods within the Department of Defense (DoD) acquisition community has grown.

Agile is an iterative, incremental, and collaborative approach to software development. It features a lightweight, "just-enough" governance framework and is designed to be cost effective, timely, and adaptable. These qualities appeal to the DoD, which has a need for an acquisition tempo that responds to operational tempo, a need to obtain high-quality software within a dynamic environment, and a need to focus on value.

To support the DoD's mission, the SEI's Acquisition Support Program (ASP) has been investigating Agile methods. "When applied properly in the right context, Agile can accelerate the delivery of high-value software capability," said Stephany Bellomo, chief engineer for civil and defense agencies in ASP. During the recently completed fiscal year, ASP conducted research on the successful use of Agile methods in the DoD and produced an evolutionary prototype for applying them. "Our research," noted Bellomo, "is helping us develop guidance on the use of Agile in DoD acquisitions and the Agile Contingency Model, which will help the DoD determine when Agile might be a good fit for specific DoD projects." By leveraging its ongoing relationships with DoD acquisition programs, the SEI is developing these resources to help the DoD make decisions about Agile methods that can help it achieve its goals for speed, adaptability, and efficiency.

PHOTO COURTESY OF US ARMY
TAKEN BY MASS COMMUNICATION SPECIALIST 2ND CLASS SANDRA M. PALUMBO

PHOTO BY FLAVIO ENSIKI

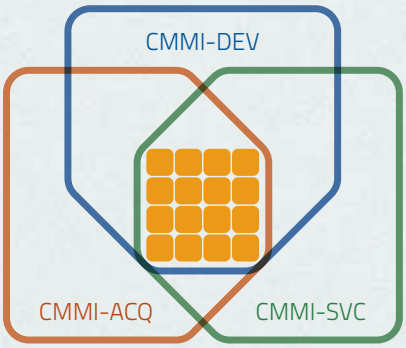
04

CECOM SOFTWARE ENGINEERING CENTER AMONG FIRST TO ADOPT THREE-MODEL CMMI APPROACH

The U.S. Army Communications-Electronics Command (CECOM) Software Engineering Center (SEC) this year became one of the first organizations to adopt a process improvement strategy that employs all three CMMI models: CMMI for Acquisition, CMMI for Development, and CMMI for Services. The SEC's mission is "to provide life-cycle software solutions and services that enable warfighting superiority and information dominance across the enterprise."

"The SEC recognized that the work it performs extends beyond the focus of a single model for process improvement," said Alex Stall, senior member of the technical staff at the SEI. "Building on the success of an SEC-wide Maturity Level 2 SCAMPI using CMMI for Development, it has identified areas in which it makes sense to use all three models to support process improvement across the organization." Stall's colleague Rusty Young, also a senior member of the technical staff, added that initial efforts have focused on identifying areas in which each model can be used exclusively to help the SEC meet process improvement and maturity-level objectives.

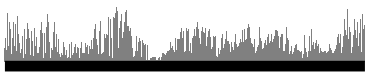
"SEC is a large, diverse organization that provides life-cycle software engineering capabilities that span the various phases of the Defense Acquisition Management Framework," said Vickie Papia, chief, Strategic Transformation Division. "After achieving a CMMI-DEV Maturity Level 2 rating in 2010, we expanded our improvement initiative and created a model approach using the CMMI for ACQ/DEV/SVC to address the diversity of work within the SEC. We are implementing best practices of the models to improve our acquisition, development, and services processes across the SEC to gain process efficiencies while keeping a focus on customer needs, and to deliver timely, quality products and services to the soldier in the field."



THE CMMI MODEL FRAMEWORK:
There are three CMMI models: CMMI for Acquisition (ACQ), CMMI for Services (SVC), and CMMI for Development (DEV). The new CMMI V1.3 allows blending process areas from multiple models supporting continuous improvement and for more rapid achievement of business results.

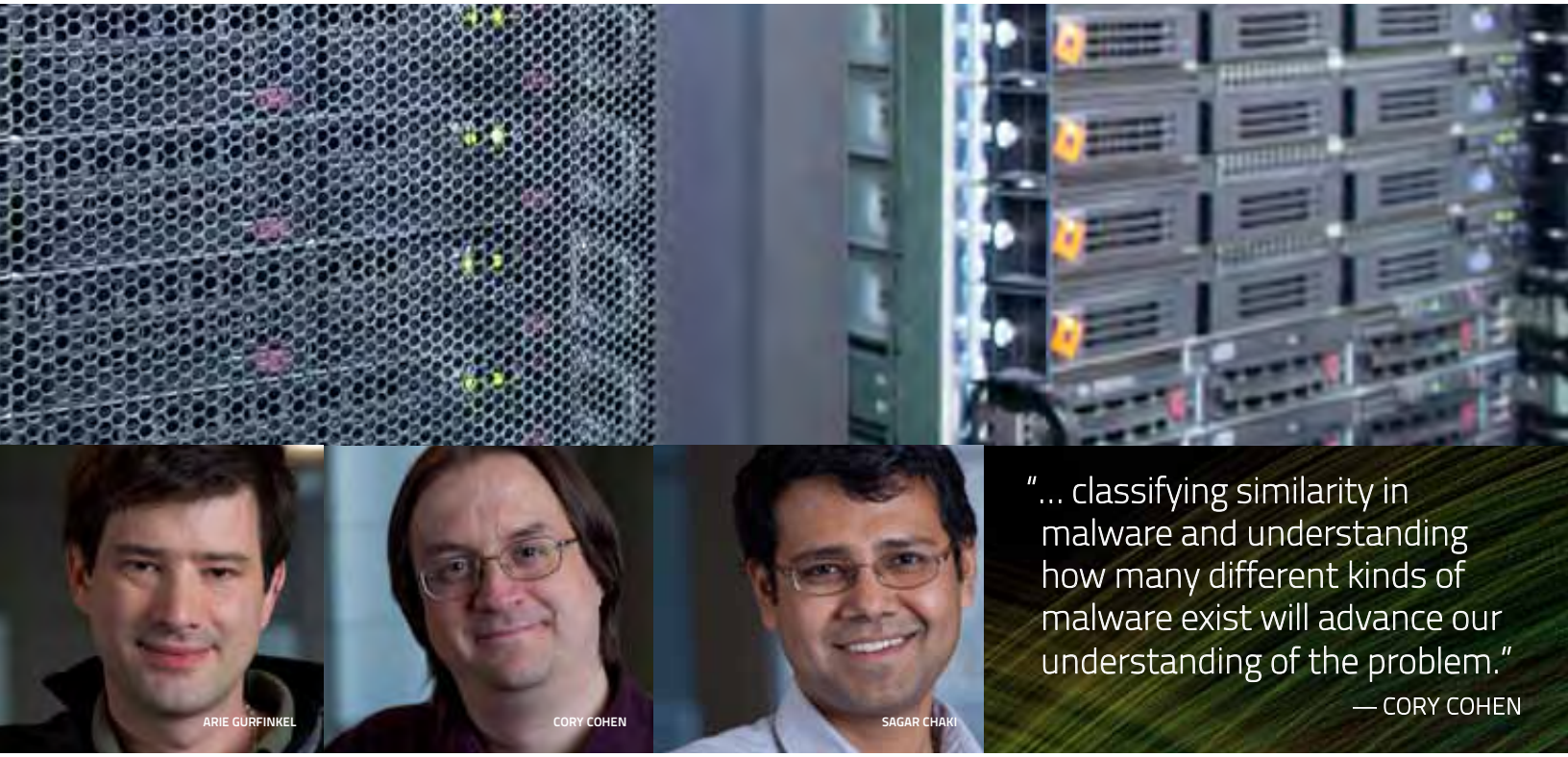
05 USING MACHINE LEARNING TO DETECT MALWARE

Malware, or malicious software, aims to disrupt operation, gather private information, and gain unauthorized access to system resources. SEI researcher Arie Gurfinkel noted that malware "spans the merely annoying to the financially dangerous to issues of national security." Government and industry are increasingly concerned with malware, but much debate exists about the scope of the problem. Cory Cohen, a malware analyst with CERT, explained that experts' counts range from 300,000 malware encounters per week to much higher numbers. Cohen's SEI colleague Sagar Chaki pointed out, "The measurement problem is also a research problem."



+17 MILLION

THERE ARE MORE THAN 17 MILLION ARTIFACTS IN THE CERT MALWARE CATALOG.



ARIE GURFINKEL

CORY COHEN

SAGAR CHAKI

"... classifying similarity in malware and understanding how many different kinds of malware exist will advance our understanding of the problem."
— CORY COHEN

By a simple count, malware numbers are very high. But evidence indicates that most malware can be sorted into families of common origin. A few dozen families may account for the majority of detected malware instances. Chaki, who leads an SEI research effort to study malware detection, said that his team's approach involved "getting a handle on the sheer number of malware encounters by finding similarities among them."

"We have no ground truth in the malware domain," added Cohen, so "classifying similarity in malware and understanding how many different kinds of malware exist will advance our understanding of the problem."

Chaki, Cohen, and Gurfinkel are investigating executable software binaries that often take the form of malware. The variety and number of malware encounters make it difficult to construct a solution with a finite set of functions and mathematical operations. The team thought machine learning could provide a more effective solution. In machine learning, software can be "trained" on a set of known positive and negative examples.

The SEI team developed a method using a form of machine learning called classification, which detects provenance similarities in binaries. These similarities indicate that the binaries were compiled from similar source code and with similar compilers. Using sample binaries to create a training set, the team trained a classifier and then used it to predict the similarity of other binaries. Using machine learning, the team seeks to overcome the weaknesses of current labor-intensive manual techniques and of automated techniques that produce high false-positive or false-negative rates.

So far, the team has sampled open-source software because the field lacks information about malware source codes and compilers. But the team thinks a classifier that detects provenance similarity in open-source functions will also work with malware functions because variations between codes and compilers are largely independent of the software itself. While identifying similarities between binary functions remains a challenge, the team presented its preliminary results in a well-received paper at the 2011 Knowledge, Discovery, and Data Mining Conference in San Diego, California.

Eyeing future work, Gurfinkel explains there is still a scalability problem to solve: "The task needs to move from 'given one thing, is another thing similar or not?' to 'given one thing, find all things similar to it.'" Further research will explore other ways of detecting similarities between functions.

06

ACCELERATED IMPROVEMENT METHOD (AIM) AT WORK IN THE AUTOMOTIVE INDUSTRY: THE SEI AND URBAN SCIENCE

Gene Miluk, a senior member of the technical staff at the SEI, has been working with the consulting and software solutions firm Urban Science to help it enhance its process improvement capability. Miluk has extensive experience working with client organizations undertaking software process improvement, acquisition improvement, and technology transition. "Urban Science is working to develop a whole new generation of web-based tools to support its analytics technology," said Miluk. "This is a perfect example of a company searching for a better process technology and doing the necessary work to implement it. Their staff was great to work with, and they are now teaching their own people."

Urban Science, headquartered in Detroit, is a global company of automotive retail performance experts that provides advanced consulting and software solutions to help its clients increase market share and improve profitability. It has clients in more than 60 countries. The company uses scientific analysis and process-optimizing software to help automotive manufacturers better evaluate, structure, and manage their dealer networks and marketing programs. This year, with Miluk's help, Urban Science adopted the Accelerated Improvement Method (AIM), a process improvement methodology developed at the SEI.

Process improvement is nothing new to Urban Science. For their new software development project, CIO Greg Davidson wanted a fast, effective approach. The company looked to AIM to provide a more structured approach to software development that would complement other methods used by Urban Science, such as Scrum. Using disciplined AIM processes starting with the Team Software Process (TSP), the company set goals to deliver high-quality software on time and within budget. In 2011, the company piloted AIM with positive results, and is now introducing it across the organization, with Kevin Davies, global director of technology, managing the implementation. "This initiative is not only improving how our IT organization functions, but will create greater transparency into IT for the whole company and provide a structured framework where all parties involved know what their responsibilities are and what they can expect," said Davies.

Helping organizations implement AIM is one way the SEI promotes adoption of CMMI to achieve process performance results. AIM speeds CMMI adoption through a tailored version of TSP and Six Sigma measurement strategies. The AIM approach first focuses on appropriate training and gaining buy-in with senior management. It then works through the chain of command to middle- and first-line management, and finally to the developers who staff self-directed teams on initial AIM pilot projects.

When the AIM project pilots are complete, the focus moves to the organizational level through the use of TSP+ (a tailored form of TSP that incorporates elements from CMMI). TSP+ extends to the process group, which is responsible for CMMI implementation. AIM is then implemented project by project, instantiating the CMMI practices that apply to development projects.

Kathy Krauskopf, quality assurance manager for Urban Science, said, "Based on my experience in the past with CMMI (CMM at the time), I believed AIM would deliver process improvement benefits faster than the traditional IDEAL model. And this is what is happening." Krauskopf noted that Urban Science has trained 30 developers in TSP fundamentals along with 24 leaders and team members, and has 3 pilots underway using TSP. With the help of an on-staff coach and a coach/TSP instructor, Urban Science now has three teams using TSP.

"Our experience with the SEI has been very positive," said Krauskopf. "The SEI has done everything it can to make sure this is a success for us."

30%|80%

AIM HAS BEEN FOUND TO TYPICALLY ACHIEVE 30% PRODUCTIVITY GAINS WHILE REDUCING DELIVERED DEFECT RATES BY 80% NOMINALLY WITHIN 18 MONTHS FOR SMALL-TO-MEDIUM SIZED ORGANIZATIONS. (IMPLEMENTATION GUIDANCE FOR THE ACCELERATED IMPROVEMENT METHOD (AIM), SEI, DECEMBER 2010)

"Urban Science is working to develop a whole new generation of web-based tools to support its analytics technology," said Miluk. "This is a perfect example of a company searching for a better process technology and doing the necessary work to implement it."

— GENE MILUK

GENE MILUK

PHOTO COURTESY OF EXPERTINFANTRY.COM
TAKEN BY SGT LARRY AARON, 55TH SIGNAL CO. COMBAT CAMERA

Well-defined, defensible network perimeters are being challenged by cloud computing, insider threats, and the prevalence of socially engineered application-level attacks over network-based attacks.

07

MEETING THE CHALLENGE OF LARGE NETWORK MONITORING

The past year saw continued research by the SEI into addressing the challenges of monitoring large networks for malicious activity. The SEI's approaches rely on techniques to summarize communications between hosts on the network. Even using summary techniques, monitoring large networks operated by the U.S. government and commercial enterprises generates huge volumes of data that security analysts cannot possibly analyze without assistance.

Network Situational Awareness (NetSA) team members in the SEI's CERT® Program have developed approaches to automate that analysis. Both the U.S. Department of Homeland Security (DHS) and the Department of Defense (DoD) have applied these approaches to help security analysts monitor for unauthorized access of U.S. government networks and systems. In 2011, NetSA researchers developed new analytics, trained government personnel on their use, and delivered other resources to support Einstein, a capability used by the United States Computer Emergency Readiness Team (US-CERT), and Centaur, a capability used at the U.S. Cyber Command, the Defense Information Systems Agency (DISA), and the military services to defend DoD networks.

Aside from sheer volume, there are other challenges. For instance, organizations have traditionally monitored traffic at the perimeter of their networks. But well-defined, defensible network perimeters are being challenged by cloud computing, insider threats, and the prevalence of socially engineered application-level attacks over network-based attacks. Organizations are beginning to invest in and rely more on sensing outside of traditional network perimeters.

08

CERT APPLIES SECURE CODING EXPERTISE TO NEW JAVA STANDARD

Members of the Secure Coding Initiative, part of the SEI's CERT® Program, work with software developers and software development organizations to eliminate vulnerabilities resulting from coding errors before the software is deployed. In September 2011, Addison-Wesley Professional published *The CERT® Oracle® Secure Coding Standard for Java* by Fred Long, Dhruv Mohindra, and CERT researchers Robert C. Seacord, Dean F. Sutherland, and David Svoboda.

The standard developed out of a collaboration between the Secure Coding Team and Oracle's Java platform developers. The Secure Coding Team also elicited feedback from the programming and software security community on proposed rules and recommended practices. The result is the first authoritative compilation of code-level requirements for secure Java systems.

"Conformance to these coding standards will allow developers to produce code that is free from those coding errors known to result in exploitable vulnerabilities," said Seacord, the CERT team lead for secure coding. "We want to establish a set of rules that allow programmers to produce secure software and systems." Seacord also noted that the secure coding standards establish a set of requirements for code security against which software can be evaluated.

Secure Coding Standard for Java joins the CERT Program's coding standard for the C programming language as well as the C++ standard, which is in development.

09

CERT ENHANCES THE USABILITY OF THE SMART GRID MATURITY MODEL WITH VERSION 1.2

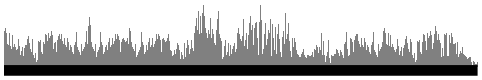
Utility companies worldwide are using digital smart grid technology to modernize the aging analog power grid. Nearly 120 utilities have charted their smart grid strategies by using the Smart Grid Maturity Model (SGMM).

The SGMM is a management tool developed by utilities, stewarded by the SEI as part of its Smart Grid Initiative, and supported by the U.S. Department of Energy and many other stakeholders. Utilities use the SGMM suite of products to plan their smart grid implementation, prioritize their options, and measure their progress.

In September 2011, the SEI released Version 1.2 of the SGMM suite. Version 1.2 clarifies utility characteristics and explanations so that utility companies can more easily identify which areas of the model apply to them. The revised assessment survey allows participating utilities to better assess their smart grid progress against other utilities. Navigation workshops, in which SEI-Certified SGMM Navigators work directly with utilities, now provide improved guidance. Navigator training has also been made more efficient and effective, and licensing to deliver the Navigation Process has been opened to all qualified applicants.

10 BUILDING PUBLIC-PRIVATE PARTNERSHIPS IN CRITICAL INFRASTRUCTURE

More than 80 percent of the nation's critical infrastructures are owned by private commercial organizations. The complexity and interconnectedness of networks and information technology that underpin these critical infrastructures make them hard to protect, and make it hard to measure their resilience. Cyber attacks on these networks and systems could adversely affect the national economy or government services, or could otherwise put the security of the United States at risk.



+80% OF THE NATION'S CRITICAL INFRASTRUCTURES ARE OWNED BY COMMERCIAL ORGANIZATIONS.

Critical infrastructures are "those physical and cyber-based systems essential to the minimum operations of the economy and government. They include, but are not limited to, telecommunications, energy, banking and finance, transportation, water systems, and emergency services, both governmental and private."

— FROM PRESIDENTIAL DECISION DIRECTIVE 63

Partnership between the government and infrastructure owners and operators is an important factor in our national cyber security. Partnerships facilitate fast and effective communication about threats, vulnerabilities, and incidents. If needed, the government can assist in the response to cyber security incidents. This helps industry mitigate threats and protect its business. Partnerships also enable the government to understand changing information technology and industry's security challenges.

The SEI participates in many initiatives that contribute to building public-private partnerships. For example, the Department of Defense (DoD) has an initiative to work more closely with the defense industrial base (DIB); that is, defense contractors, which often have sensitive but unclassified information on their enterprise networks. The goal of this initiative is to help them improve their ability to protect this information and respond to threats to its exposure. Information exchange enables both the DoD and its contractors to work more effectively and to act quickly if a security issue arises. The SEI is helping to establish a collaborative capability for government and industry partners to share information and for the industry partners to share information among themselves. The identity of industry partners is protected when they communicate with each other, promoting an anonymous, free flow of information even among competitors.

The SEI plays a similar role in a Department of Homeland Security (DHS) initiative to exchange information with critical infrastructure providers with the goal of enabling these providers to better secure the networks that the infrastructure relies on. Especially challenging is the need to determine how to help industry identify, respond to, and prevent attacks that commercial solutions do not yet detect and mitigate.

Another example of a public-private partnership is in the Cyber Resilience Review (CRR), which the DHS offers to critical infrastructure owners and operators. The approach was designed by the SEI, which helps with implementing the reviews. Based on the CERT Resilience Management Model, the CRR helps give a clear picture of an infrastructure's security and resilience, along with improvement recommendations. More than a hundred CRRs have been conducted in sectors such as finance and energy. The ultimate goal of the public-private partnership is to help protect critical, privately owned national and economic assets.

11

PUTTING THE CERT RESILIENCE MANAGEMENT MODEL INTO PRACTICE

CERT® Resilience Management Model (CERT-RMM) users have many resources for putting the model into practice: CERT-RMM Compass diagnostics, capability appraisals, users group workshops, and guidance on measuring progress. The CERT-RMM is the foundation for improving an organization's ability to provide essential services in the presence of operational stress or disruption. In 2011, the CERT-RMM team built on its research to develop and launch the following products.

CERT-RMM Compass helps an organization quickly evaluate its resilience practices. This lightweight, questionnaire-based diagnostic is available for piloting and has been piloted in several organizations.

The *CERT-RMM Capability Appraisal* rigorously examines an organization's implementation of resilience processes defined in the CERT-RMM. The SEI provides training, apprenticeships, and certification for lead appraisers. In 2011, 12 candidates started their apprenticeships, preparing to qualify as the first set of lead appraisers outside the SEI.

The *CERT-RMM Users Group Workshop Series* gives participants hands-on experience with applying the CERT-RMM. They prepare for each of four, two-day workshops with activities such as defining an improvement objective, using CERT-RMM Compass, preparing a presentation for management buy-in, and drafting an action plan. At each workshop, they report on their progress and get feedback from workshop leaders and other participants. Because the workshop enables participants to solve a problem in their own organization, the changes they implement become institutionalized—part of the way they do business. And the improvements in organizational practice resulting from the workshops pave the road for future improvements.

"CERT-RMM and the CERT-RMM Users Group guide me into assuring that my team is doing the right things in the right manner," said Gregory Crabb, inspector in charge of Revenue, Product and Global Security, U.S. Postal Inspection Service. "Managing a security and resilience program can be challenging; participating in the Users Group gives me peace of mind that I am investing my limited resources in the most effective manner based on strong measurement and financial analysis."

Echoing Crabb's experience, Lockheed Martin's Lynn Penn noted, "The CERT-RMM class provided Lockheed Martin participants with a solid framework for measuring organizational and operational resilience, but the RMM Users Group gave us a greater appreciation of the issues surrounding resilience." Penn is director of strategic process engineering for Lockheed Martin. "The diversity of perspectives from industry, finance, government, and education helped to associate actual problems with model constructs," she added. "Hearing about the real-world issues that other organizations had, and how they conquered or planned to conquer them, helped us to be better able to support our own operational teams and to establish a strategy for our organization."

The CERT-RMM team also continued to pursue its research in the area of measurement, which is essential for all resilience-improvement efforts. Measures can indicate whether an organization is implementing the improved process and whether it makes a difference. To help CERT-RMM users select and apply resilience measures, the SEI is developing an initial set of resources, which currently include an approach, templates, and guidance that allows users to define measures tailored to their organizations' needs.

"The CERT-RMM class provided Lockheed Martin participants with a solid framework for measuring organizational and operational resilience."

— LYNN PENN, DIRECTOR OF STRATEGIC PROCESS ENGINEERING FOR LOCKHEED MARTIN

26 PROCESS AREAS ARE MEASURED IN THE CERT RESILIENCE MANAGEMENT MODEL.

8–10

THE DOD HAS A PROJECTED 8 TO 10 YEARS TO ADAPT ITS SYSTEMS TO MULTICORE PROCESSORS.

PHOTO COURTESY OF MEDICAL COMMUNICATIONS FOR COMBAT CASUALTY CARE (MC4 ARMY)

DIONISIO DE NIZ

BJÖRN ANDERSSON

"Our protocol is the first one that allows multicore software to switch modes while meeting all timing requirements."

— BJÖRN ANDERSSON

12

SEI ATTACKS MULTICORE CHALLENGES TO MISSION-CRITICAL DOD SYSTEMS

Advances in processor technology have shifted from faster processors to those that execute more instructions in parallel. These processors, called multicores, present challenges to software developers. Because multiple cores share memory, executing a function in one core can interfere with executing a function in another core. Stakeholders in the Department of Defense (DoD) and in industry fear multicore failure in systems such as aircraft and missiles, where lives are at stake.

Dionisio de Niz leads an SEI research effort to improve multicore processors. He explains that "for two cores performing two functions, execution times increase up to three times." Arie Gurfinkel, a teammate of de Niz, adds that "the consequences of defects in mission-critical systems could be deadly, and the right answer delivered too late would become the wrong answer." But the DoD will have to use multicores within 8 to 10 years, stressed team member Sagar Chaki, "because their ability to acquire single-core processors from chip manufacturers will run out."

Multicore processors do provide benefits. For instance, with multicores, developers can make advantageous tradeoffs regarding size, weight, and power. "Unmanned aerial vehicles (UAVs) are getting smaller and more agile," said de Niz, so they require more capabilities in fewer processors. Research, Technology, and System Solutions (RTSS) Program Director Linda Northrop noted that "multicore is the hardware of today, and it will be important for the DoD to exploit this technology."

The team is investigating several challenges of multicore programming. It's working on a technique using harmonic periods, which split task execution across two cores (migrating the task from one core to another) to prevent idle time in cores that cannot run a whole task. This maximizes the workload under strict deadlines and guarantees the same percentage of available processor capacity as in a single core.

SEI researcher Björn Andersson and collaborators from the Polytechnic Institute of Porto worked on software timing requirements. They developed a mode-change protocol for multicores with several operational modes, such as aircraft taxi, takeoff, flight, and landing modes. Andersson explained, "Our protocol is the first one that allows multicore software to switch modes while meeting all timing requirements. This lets software designers add or remove software functions while ensuring safety."

The multicore team is also working on power optimization. "UAVs, robots, and smartphones run on batteries, and warfighters can perform longer missions if batteries last longer," said team member Gabriel Moreno. Moreno and de Niz developed a new frequency-scaling algorithm that avoids processor partitions, so it can assign different speeds to individual cores. The method provides better power efficiency than was possible before.

Chaki and Gurfinkel worked on migrating real-time, embedded systems from single-core to multicore platforms. They want to apply regression verification to help enable this migration. Regression verification determines the behavioral equivalence of two related programs so that the computation effort of verification is proportional to the amount of difference between the programs rather than to their size.

Addressing the challenges of multicore programming is crucial to the DoD and industry, and the team's work will help migration from single to multiple cores occur more safely and efficiently.


KURT WALLNAU

"XSEDE gives us the opportunity to advance SEI research by understanding how these large, amorphous, distributed organizations work."

— KURT WALLNAU

13

SEI TEAM JOINS NATIONAL SCIENCE FOUNDATION EFFORT ON EXTREME SCIENCE

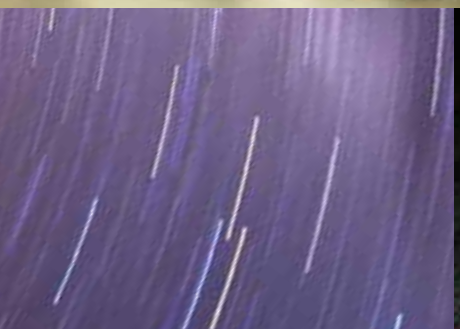
In March 2011, the National Science Foundation (NSF) selected 17 organizations, including Carnegie Mellon University (CMU), to partner on the Extreme Science and Engineering Discovery Environment (XSEDE) project. XSEDE is a five-year, $121-million effort aiming to create "the most advanced, powerful, and robust collection of integrated digital resources and services in the world." XSEDE will build on the TeraGrid supercomputing network and provide researchers open access to state-of-the-art computational tools and digital resources. CMU's team includes the Pittsburgh Supercomputing Center (PSC) and the SEI.

"On one level, we face a familiar challenge in introducing changes in engineering culture and practice: The computational science community supported by NSF, and by XSEDE, has deep and varied technical expertise but lacks a sustainable sense of common engineering practice," said Kurt Wallnau, senior member of the technical staff in the Research, Technology, and System Solutions (RTSS) Program at the SEI. "On another level, we face new challenges that stem from the need to think about computational science less as an amorphous community and more as a socio-technical ecosystem with institutional structures, niches, interests, and incentives. Thinking and working at ecosystem scale forces us to think about engineering in new and unfamiliar ways, but it also offers new opportunities to improve the scale, effectiveness, and adoption of software engineering practices."

Wallnau noted that the SEI is playing a lead role in software development and integration on the project. It also holds leadership positions in the project's systems engineering group, and it is contributing to the development of software architecture for XSEDE. "We're working to fit all these things together," said Wallnau.

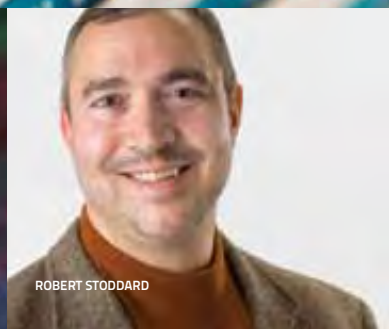
The SEI XSEDE team also includes the following members of the technical staff: Felix Bachmann, Michael Gagliardi, Altaf Hossain, Scott Hissam, Mike Konrad, and Suzanne Miller. Joseph Batman and Paul Clements, both former members of the SEI staff, also contributed to this effort. The team sees great opportunity in this work. As Wallnau observed, "XSEDE gives us the opportunity to advance SEI research by understanding how these large, amorphous, distributed organizations work."

PHOTO COURTESY OF US ARMY AFRICA



"We're tapping into other methods, such as scenario planning, to address the unique needs of early life-cycle cost estimation."

— ROBERT STODDARD



ROBERT STODDARD

14

SEI RESEARCH GROUP SEEKS MORE ACCURATE COST ESTIMATION

The difficulty of accurately estimating development costs for new Department of Defense (DoD) systems has been well documented, and cost overruns in new systems development are well known. This difficulty is compounded by the fact that estimates are now prepared much earlier in the acquisition lifecycle, well before there is concrete technical information available on the program to be developed. To address the challenge of accurate cost estimation, the Cost Estimation Research Group in the SEI's Software Engineering Process Management Program developed a new approach, Quantifying Uncertainty in Early Lifecycle Cost Estimation (QUELCE).

QUELCE elicits information about program change-driver uncertainties common to program execution in a DoD major defense acquisition program lifecycle. It synthesizes analytical techniques such as scenario planning, Bayesian Belief Network (BBN) modeling, and Monte Carlo simulation into an estimation method that quantifies uncertainties, allows subjective inputs, visually depicts influential relationships among program change drivers and outputs, and assists with the explicit description and documentation underlying an estimate. "The innovation in this SEI solution rests with the desire to think out of the box from traditional parametric cost estimation," said Robert Stoddard of the SEI's Cost Estimation Research Group. "We're tapping into other methods, such as scenario planning, to address the unique needs of early life-cycle cost estimation."

The Cost Estimation Research Group detailed its work in the SEI technical report *Quantifying Uncertainty in Early Lifecycle Cost Estimation (QUELCE)*. In addition to Stoddard, the group includes Robert Ferguson, Dennis Goldenson, James McCurley, and David Zubrow, all senior members of the SEI technical staff. The group looks forward to pilot applications of QUELCE by cost estimators in DoD environments.

40% RISE IN COST OVERRUNS ON DOD SYSTEMS PROJECTS, ACCORDING TO A RECENT GAO REPORT

MARK KASUNIC

"Our goal is to improve this process by introducing effective and automated scanning, and by preventing bad data from entering the system in the first place."

— MARK KASUNIC

$600 BILLION

ACCORDING TO A 2009 GARTNER REPORT, THE ANNUAL COST OF POOR DATA TO U.S. INDUSTRY HAS BEEN ESTIMATED AT $600 BILLION.

PHOTO BY FLAVIO ENSIKI

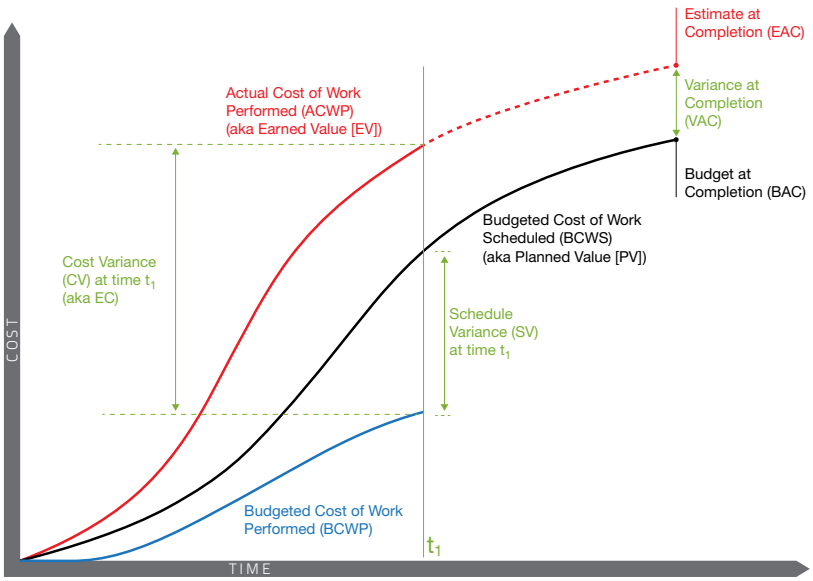
15

SEI EXPLORES METHODS TO IMPROVE DATA QUALITY THROUGH ANOMALY DETECTION AND NET SAVINGS FOR GOVERNMENT AND INDUSTRY

Successful organizations understand the importance of measuring and analyzing data. They rely on data about their products, processes, and projects to make decisions and develop plans. But ensuring information quality is a big challenge for most organizations. In fact, they may not even be aware of just how good—or bad—their data are. And poor data quality leads to poor decisions.

Poor data quality is a pervasive problem in both industry and government. According to a 2009 Gartner report, the average organization loses $8.2 million annually because of poor data quality. The annual cost of poor data to U.S. industry has been estimated at $600 billion.

Government and industry both want to know: "How can we improve, evaluate, and standardize the quality of data we use?" To begin tackling this problem, SEI researchers collaborated with the Office of the Under Secretary of Defense (OSD) for Acquisition, Technology, and Logistics (AT&L), Acquisition Visibility (AV). The researchers, headed up by Mark Kasunic of the SEI's Measurement and Analysis Team, set out to evaluate statistical methods for improving on existing, manual methods of anomaly detection. To do so, the team leveraged actual data in the Earned Value Management (EVM) Central Repository (CR). The EVM Central Repository supports the centralized reporting, collection, and distribution for key acquisition EVM data, such as Contract Performance Reports (CPRs), Contract Funds Status Report (CFSR), Integrated Master Schedule (IMS) for ACAT 1C & 1D (MDAP), and ACAT 1A (MAIS) programs.



Key Concepts of Earned Value Management

The SEI team profiled and analyzed many months of EVM project data. It focused on identifying data anomalies involving cost estimates and performance values that seemed unusual when compared to the time-series values comprising the remainder of the data series. These unusual data values are considered outliers and tagged as anomalies. By creating graphic profiles of the data, the team uncovered anomalies that could be clearly observed as spikes or drops. The data-visualization methods appeared to be much more efficient and effective at identifying bad data than current methods.

"Once we discovered this, we consulted with our collaborator on our findings," said Kasunic. "The findings were passed to a group of analysts to confirm whether the anomalies were of the type that the analysts would have flagged for further investigation." Kasunic noted that that the government does not have the staff to systematically evaluate large volumes of data; a systematic and automated way to screen data and discover data anomalies would lead to significant improvement, saving many analyst staff hours.

Checking the quality and accuracy of data is part of a process developed at the SEI called the Measurement and Analysis Infrastructure Diagnostic (MAID). MAID, which looks at the entire data life-cycle to ensure high quality, is a set of organized criteria that helps organizations discover the strengths and weaknesses of their information-measurement systems.

"Government analysts responsible for this do a tremendous job," said Kasunic. "Our goal is to improve this process by introducing effective and automated scanning, and by preventing bad data from entering the system in the first place. The statistical methods we've applied have the potential to help them discover anomalies in the EVM system more quickly and with fewer resources. We hope this will ensure that information reported to Congress is highly accurate."

16

NORTHROP NAMED SEI FELLOW

In 2011, Linda Northrop became an SEI fellow, a designation awarded to people who have made an outstanding commitment to the SEI and who continue to advise SEI leaders on key issues. Northrop, director of the Research, Technology, and System Solutions Program, is the fifth SEI fellow.

Northrop is the first woman to be named an SEI fellow and the first female program director at the SEI. "I have never been just the manager but have always been involved in research and technical work," said Northrop. She originated the *Framework for Software Product Line Practice,* led a study of ultra-large-scale systems, and coauthored books on both topics.

Northrop's leadership catalyzed widespread adoption of software product lines and software architecture. She believes that her work is "not so much about marketing products but about making a difference." She founded the Software Product Lines Conference; forged the merger with its European counterpart, the Program Family Engineering Workshop; and initiated the SEI Architecture Technology User Network (SATURN) Conference.

Northrop has 35 years of experience in software engineering, more than 50 publications, and almost 300 presentations. Her honors include the New York State Chancellor's Award for Excellence in Teaching, Carnegie Science Award of Excellence for Information Technology, and Association of Computing Machinery Distinguished Service Award. But for Northrop, the measure of her impact so far is leadership. "I loved being an educator," she said, and she sees a similarity in her current role, in which, as program director, "I lead people to go further than I could go on my own."

"I lead people to go further than I could go on my own."

— LINDA NORTHROP

5 AS OF FISCAL YEAR 2011, THE SEI HAS NAMED JUST FIVE FELLOWS.

17

MATT GASTON REFLECTS ON SEI INNOVATION CENTER ACCOMPLISHMENTS FOR 2011

In 2010, the SEI and Carnegie Mellon University (CMU) had the idea to create an innovation center, and in 2011, under sponsorship, developed a concept of operations (CONOPS) for a national innovation center. Today, SEI Innovation Center Director Matt Gaston says the center is tackling two challenges for the U.S. intelligence community and expects to expand.

Q WHAT IS THE VISION FOR THE SEI INNOVATION CENTER?

A As part of a federally funded research and development center run by a university, we are working to become a mechanism that helps the government assess and leverage leading-edge technologies from the computing and information sciences for mission-critical cyber and intelligence needs. The world outside of government is innovating information technologies very rapidly. The government needs to keep pace. So, we are helping the government connect with innovative technologies and apply them to its work.

The Center can do this in two key ways: by providing a view into research to identify solutions and make them relevant and, on the mission side, by working with customers on their greatest mission challenges. To borrow a phrase from Randy Bryant (dean of Carnegie Mellon's School of Computer Science): Our technical focus area is data-intensive scalable computing. We work on the question "How do we bring innovation to bear on real government challenges?"

Q WHAT HAS HAPPENED SINCE YOU FINALIZED THE CONOPS FOR THE SEI INNOVATION CENTER?

A In our inaugural year, we've secured two major sponsors and two major projects. In the first project, we are supporting the efforts of our sponsor to move to the cloud. In particular, we're helping with various aspects of heterogeneous high-performance computing (HPC) utility clouds. That sponsor has given us funding to purchase an instance of their infrastructure, which we will stand up at the SEI for research and development use. Our research will focus on using HPC utility clouds to dynamically provision mission applications that require a great deal of computing power and resources onto a common infrastructure.

Our second sponsor funded an unclassified cyber-intelligence pilot aimed at increasing awareness of network activity, and cyber threat activity, in the private sector. We are taking information from commercial and open-source providers and fusing it into a more complete picture of current activity. We're then providing a reporting stream back to the private sector. This establishes an intelligence testbed for technologies and techniques used for processing, analyzing, and reporting on a lot of information.

One of the assumptions going into all of our work was that the SEI Innovation Center would focus on building prototype technology capability; in other words, on building software, not thinking about software or processes or engineering, but actually doing software.

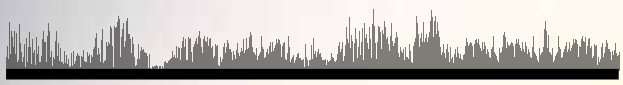
Q DO YOU CONNECT WITH OTHER PARTS OF THE SEI AND CAMPUS?

A Collaboration is very much a part of the SEI Innovation Center's approach. Though we are in the formative stages, we are managing our growth and establishing collaborative ties with all the SEI technical programs, and we are actively looking for projects on which we can work together. We are also looking at appropriate mechanisms to collaborate closely with the CMU campus. While we refine these mechanisms, we're building relationships with the School of Computer Science and the Carnegie Institute of Technology.

"We've gotten feedback from people saying that this kind of hands-on, experiential learning 'will be incredibly helpful to DoD program offices.'"

— BILL NOVAK

BILL NOVAK



90% THE "90 PERCENT SYNDROME" OFTEN EMERGES IN THE LATE STAGES OF DEVELOPMENT WHEN PROGRESS ON THE EFFORT SEEMS TO STALL AT APPROXIMATELY 90% DONE, AND THEN INCHES SLOWLY FORWARD TO EVENTUAL COMPLETION.

PHOTO COURTESY OF US MARINE CORPS (USMC)
TAKEN BY CPL BRYSON K. JONES

18

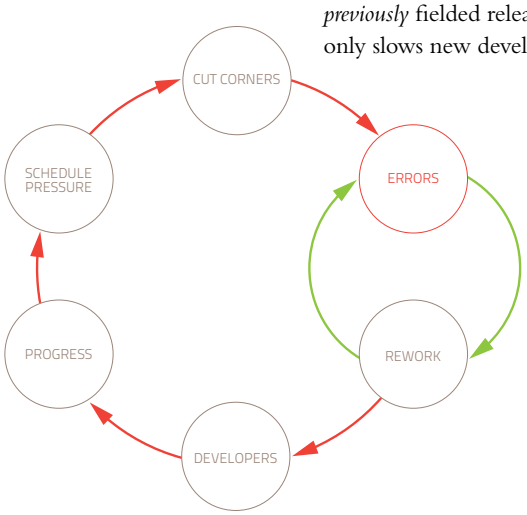
ACQUISITION MODEL TO HELP PROGRAM OFFICES AVOID COMMON PITFALLS

An acquisition project starts with the best intentions: to field a high-quality system that provides new or improved capabilities to the warfighter. Unfortunately, somewhere between the prototype and deployment of the finished system, the effort goes awry, and the system, as initially envisioned, takes much longer than expected, or may never come to fruition.

The problem is common enough that SEI researchers aggregated work on five independent technology assessments (ITAs) from 2006–2009 to develop a model of this acquisition scenario, which they titled "The Evolution of a Science Project." The scenario goes like this: A project begins with an informal team of operational people building a small, throwaway, proof-of-concept prototype to solicit funding. A successful initial deployment of the prototype builds demand for more capabilities and broader deployment. The project builds on top of the initial prototype to save time, but then starts to find increasing architectural, robustness, performance, usability, and documentation issues. As developers spend more time supporting field users, development progress slows. A lack of either project management experience or a formal organization also creates problems as developers try to scale the effort up into a formal program, resulting in a difficult transition as warfighters wait years for a production-quality system.

Bill Novak, senior member of the SEI technical staff with the Acquisition Support Program, noted that there are at least two dynamics at work behind the scenes in this scenario. "First, the project is often initiated by operational users who may lack software acquisition expertise," Novak said. "They focus primarily on quick deployment and operational support, which can result in informal requirements, poor design and code quality, and inadequate documentation."

The second dynamic is called "firefighting." "People who are slated to do new development of the *next* release must be diverted to fix problems in *previously* fielded releases," said Novak. "This not only slows new development, but the lack of developers can inject additional problems in the next release that will require even more people to fix."



"Firefighting" to fix defects slows development, increases schedule pressure, undermines quality, and inserts even more defects.

Andy Moore, from the Enterprise Threat and Vulnerability Management team in the CERT Program, described a couple of preliminary findings from the modeling effort. "The accumulation of undiscovered rework from development of the science project prototype moves the development efforts past a tipping point of escalating repair work during the follow-on development." The tipping point was found to contribute to the "90 Percent Syndrome" experienced in many software development efforts, causing the program to shift from completing normally, to having defects accumulate as rapidly as they can be corrected. Moore commented that "this syndrome occurs during the later stages of development when progress drastically slows down as a much bigger percentage of the effort is devoted to repair work rather than development."

Some of the key factors behind reaching the tipping point include

- excessive pressure being applied to the developers
- an emphasis on meeting schedule, rather than on quality
- the timing of the transition from prototype to production development (an earlier transition has fewer undiscovered defects in it)

"These are preliminary findings, as we will be performing additional model validation in the coming year," Novak pointed out, while observing that, "the model's qualitative behavior is similar to what we observe in actual programs."

The SEI's work to date on the project will be captured in an upcoming technical report: *The Evolution of a Science Project: System Dynamics Modeling of a Recurring Software-Reliant Acquisition Behavior.* The team also plans to create an interactive classroom game based on the model to teach better decision making for the defense acquisition workforce that can help lead to better program outcomes. "We've gotten feedback from people saying that this kind of hands-on, experiential learning 'will be incredibly helpful to DoD program offices,'" said Novak.

19

CERT EXERCISE NETWORK (XNET) INSTRUMENTAL IN SUCCESSFUL TEST OF CYBER ATTACK READINESS

In May 2010, leaders of the U.S. Cyber Command had a problem: Where could they find a range to run cyber defense exercises involving a complex scenario, dozens of simulated but realistic networks, and participants scattered across the Department of Defense (DoD)? And could that range be ready in record time? They found their solution at the SEI, which developed the CERT Exercise Network (XNET)—a next-generation cybersecurity training and simulation platform for realistic, scalable, scenario-driven cybersecurity exercises.

XNET provided the range, the instrumentation, and the thousands of virtual computers needed for Cyber Command's week-long exercise called Cyber Flag 12-1. The exercise involved more than 300 participants from across the DoD who worked together to detect and respond to real-world cyber threats on a virtualized network topology like their own.

Jeff Mattson, who managed the SEI's XNET development team, described the challenge of running useful exercises: "You want to be able to train as you fight. You can't play war games on your production network without risking potential damage. XNET provided a large, complex, highly instrumented network that allowed Cyber Command to run realistic cyber threat, defense, and response operations."

In addition to high fidelity, XNET offers a highly extensible and dynamic environment that allows organizations to start, stop, and reset the network resources on the fly. "You can easily manipulate the XNET environment," said Chris May, technical manager for the CERT Program's Cyber Workforce Development Team. "Unlike more monolithic ranges, we could dynamically change the environment based on the conditions in the scenario."

The Cyber Flag exercise used a variety of scenarios based on likely adversary actions in real-world events. Participants were split into two teams to practice offensive and defensive tactics. Opposing forces tried to infiltrate Cyber Command's virtual network using malware and other forms of network intrusion.

Air Force Lt. Col. William Hutchison, who led the Cyber Flag exercise, saw value in the results: "Exercises like Cyber Flag are important because they provide an assessment and a validation of how well U.S. Cyber Command can perform its real-world mission to operate and defend the DoD networks across the full range of cyber operations."

Mattson's team worked in record time. It had the Cyber Flag range environment up and running in only 6 months—much faster than the 18 months typically required for planning and development. Hutchison described the team's work this way: "Only a select few in the community believed the XNET team could accomplish what they did in the needed, high-risk timeframe. We put our faith in May, his team, and the XNET product, and they exceeded our expectations."

Because the Cyber Flag exercise was such a success, U.S. Cyber Command plans to run one every year, and May has a new goal for XNET. "Next year, we want to raise the level of fidelity even further—enabling commanders to validate the mission-readiness of units or teams that have to support real-world operations. They want to use XNET to train and verify that they can accomplish the DoD's cyber mission under any conditions. XNET can help them do just that."

300 DURING CYBER FLAG 12-1, MORE THAN 300 PARTICIPANTS FROM ACROSS THE DOD COLLABORATED OVER THE XNET PLATFORM ON CYBER DEFENSE EXERCISES.

PHOTO COURTESY OF USAF
TAKEN BY TECH. SGT. CECILIO M. RICARDO JR.

"Exercises like Cyber Flag are important because they provide an assessment and a validation of how well U.S. Cyber Command can perform its real-world mission to operate and defend the DoD networks across the full range of cyber operations."

— AIR FORCE LT. COL. WILLIAM HUTCHISON

SEI PROFESSIONAL DEVELOPMENT CENTER

The SEI Professional Development Center incorporates education, training, and credentials, all of which enable individuals to benefit from SEI research in multiple disciplines.

The center provides continuing education for engineering and software professionals in government, industry, and academia.

THE SEI ADDRESSES PROFESSIONAL DEVELOPMENT NEEDS BY

- designing and developing training that is accessible and effective with classroom, blended, and distance learning
- encouraging and recognizing individual accomplishments in various disciplines through certificate programs
- enhancing individual career opportunities through SEI Certification

FOR MORE INFORMATION ABOUT SEI TRAINING, VISIT
www.sei.cmu.edu/training

FOR MORE INFORMATION ABOUT SEI CERTIFICATION, VISIT
www.sei.cmu.edu/certification

SEI CONFERENCES & EVENTS

As part of its strategy to apply the latest research, the SEI offers conferences, workshops, and user-group meetings. These events represent technical work and research performed by the SEI and its collaborators in the areas of process improvement, software architecture and product lines, security, acquisition, and interoperability. Individuals from around the world attend SEI conferences and events to

- connect with industry leaders
- share best practices
- network with peers
- find potential solutions
- gather the latest research and trends in software and systems engineering

SOME OF THE EVENTS THAT THE SEI SPONSORED AND CO-SPONSORED IN 2011 ARE

- CMMI Workshop 2011
- FloCon 2011
- SATURN 2011
- SEPG North America 2011
- SEPG Europe 2011
- SEPG Latin America 2011
- TSP Symposium 2011

FOR MORE INFORMATION ABOUT SEI CONFERENCES AND EVENTS, VISIT
www.sei.cmu.edu/events

SEI PARTNER NETWORK

The SEI Partner Network is an elite group of SEI-trained organizations on the leading edge of software engineering processes and technologies. SEI Partners are licensed to deliver SEI services in the following areas:

- Architecture Tradeoff Analysis Method
- CERT Information Security
- CMMI and SCAMPI Appraisals
- People Capability Maturity Model
- Service-Oriented Architecture
- Smart Grid
- Software Architecture
- Software Engineering Measurement and Analysis
- Team Software Process

By delivering services worldwide, SEI Partners provide a critical distribution channel for accomplishing the SEI mission.

In fiscal year 2011, the SEI Partner Network consisted of 448 Partner organizations.

FOR MORE INFORMATION ABOUT THE SEI PARTNER NETWORK, VISIT **www.sei.cmu.edu/partners**

SEI AFFILIATE PROGRAM

Through the SEI Affiliate Program, sponsoring organizations contribute technical staff members to the SEI's ongoing effort to define superior software and systems engineering best practices. Affiliates lend their technical knowledge and experience to SEI teams investigating specific technology domains.

Affiliates are immersed in the inquiry and exploration of new tools and methods that promise to increase productivity, make schedules predictable, reduce defects, and decrease costs.

FOR MORE INFORMATION ABOUT THE SEI AFFILIATE PROGRAM, VISIT **www.sei.cmu.edu/careers/affiliates**

SEI 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.

ALAN J. MCLAUGHLIN

Chair, Board of Visitors
Consultant; Former Assistant Director, MIT Lincoln Laboratory

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

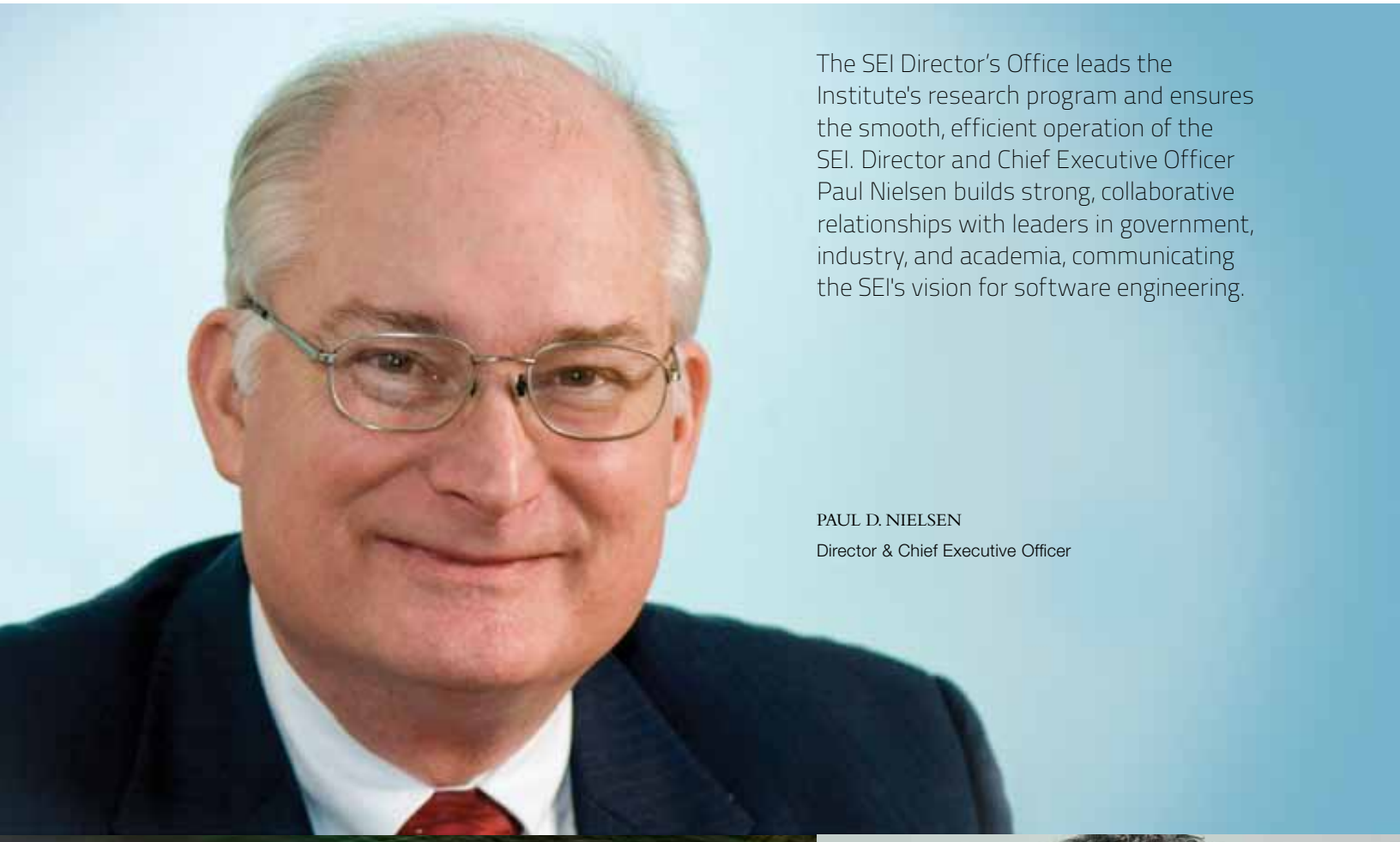
TOM LOVE

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

DONALD STITZENBERG

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

SEI DIRECTOR'S OFFICE



The SEI Director's Office leads the Institute's research program and ensures the smooth, efficient operation of the SEI. Director and Chief Executive Officer Paul Nielsen builds strong, collaborative relationships with leaders in government, industry, and academia, communicating the SEI's vision for software engineering.

PAUL D. NIELSEN
Director & Chief Executive Officer

PETER MENNITI
Acting Chief Operating Officer
Director, Financial and Business Services

SEI MANAGEMENT

The SEI Management Team comprises the directors of the research programs, technology transition, and business and technology functions of the SEI.

JOHN BRAMER

Director, Program Development and Transition

ANITA CARLETON

Director, Software Engineering Process Management

LINDA NORTHROP

Director, Research, Technology, and System Solutions

RICHARD PETHIA

Director, Networked Systems Survivability

TERRY ROBERTS

Executive Director, Acquisition Support Program/Interagency and Cyber

DAVID THOMPSON

Director, Information Technology and Security

KEY PUBLICATIONS

ARTICLES

Blanchette, Stephen & Bergey, John. "The Chief Software Architect in U.S. Army Acquisition." *CrossTalk, The Journal of Defense Software Engineering 23*, 6 (November 2011): 18-23.

Bletsas, K. & Andersson, B. "Preemption-Light Multiprocessor Scheduling of Sporadic Tasks with High Utilization Bound." *Real-Time Systems 47*, 4 (July 2011): 319-355.

Chaki, Sagar & Gurfinkel, Arie. "Automated Assume-Guarantee Reasoning for Omega-Regular Systems and Specifications." *Innovations in Systems and Software Engineering (ISSE) 7,* 2 (June 2011): 131-139.

Lewis, Grace; Morris, Ed.; Simanta, Soumya & Smith, Dennis. "Service-Orientation and Systems of Systems." *IEEE Software* (January/February 2011).

Lewis, Grace; Morris, Edwin; Simanta, Soumya & Smith, Dennis. "Service Orientation and Systems of Systems." *IEEE Software 1*, 28 (2011): 58-63.

Moore, Andrew P.; Cappelli, Dawn M.; Caron, Thomas C.; Shaw, Eric; Spooner, Derrick & Trzeciak, Randall F. "A Preliminary Model of Insider Theft of Intellectual Property." *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA) and SEI 2*, 1 (March 2011): 28-49.

Moore, Andrew. "A Preliminary Model of Insider Theft of Intellectual Property." *Journal of Wireless Mobile Networks, Ubiquitous Computing and Dependable Applications.* (March 2011): 28-49.

Moore, Andrew; Cummings, Adam & Spooner, Derrick. "Modeling and Analysis of Insider Fraud." *2010 CERT Annual Research Report*. September 2011.

BOOKS & BOOK CHAPTERS

Allen, Julia H.; Caralli, Richard A. & White, David, W.; *CERT Resilience Management Model (RMM): A Maturity Model for Managing Operational Resilience*. Addison-Wesley Professional, 2010 (ISBN: 9780321712431).

Avgeriou, Paris; Grundy, John; Hall, Jon, G.; Lago, Patricia & Mistrik, Ivan., eds. "Business Goals and Architecture." *Relating Software Requirements and Architectures.* Springer, 2011.

Caralli, Richard A.; Allen, Julia H. & White, David W. *CERT Resilience Management Model (RMM): A Maturity Model for Managing Operational Resilience.* Addison-Wesley Professional, 2011 (ISBN: 978-0321712431).

Chrissis, Mary Beth; Konrad, Michael D. & Shrum, Sandra. *CMMI for Development: Guidelines for Process Integration and Product Improvement, Third Edition*. Addison-Wesley Professional, 2011 (ISBN: 0-321-71150-5).

Forrester, Eileen C.; Buteau, Brandon, L. & Shrum, Sandra. *CMMI for Services: Guidelines for Superior Service, Second Edition*. Addison-Wesley Professional, 2011 (ISBN: 0-321-71152-1).

Gallagher, Brian P.; Phillips, Mike; Richter, Karen & Shrum, Sandra. *CMMI for Acquisition: Guidelines for Improving the Acquisition of Products and Services, Second Edition*. Addison-Wesley Professional, 2011 (ISBN: 0-321-71151-3).

Humphrey, Wattas & Over, James W. *Leadership, Teamwork, and Trust: Building a Competitive Software Capability.* Addison-Wesley Professional, 2010 (ISBN: 0-321-62450-5).

Long, Fred; Mohindra, Dhruv; Seacord, Robert C.; Sutherland, Dean F. & Svoboda, David. *The CERT Oracle Secure Coding Standard for Java.* Addison-Wesley Professional, 2011 (ISBN: 978-0-321-80395-5).

Tilley, Scott & Parveen, Tauhida. *Software Testing in the Cloud: Migration & Execution*. Springer, 2011.

KEYNOTES

Bass, Len. "Map-Reduce," Architecting Cloud Applications Workshop, held in conjunction with WICSA 2011, (June 2011)

Carleton, Anita. "Do Your Users Care if You Use Agile?" Lean Software & Systems Conference (May 2011)

Nielsen, Paul D. Lean Software & Systems Conference (May 2011)

Over, James. "Failure Is Not an Option," TSP Symposium (September 2011) and SEPG Europe 2011 (June 2011)

Place, Pat. "SOA and the Cloud: SEI Perspective," SOA, Cloud Computing, and Virtualization (May 2011)

Smith, Dennis. "The Impact of Emerging Software Paradigms on Software Quality and User Expectations," Profes Conference 2011 (June 2011)

PODCASTS & WEBINARS

Bachmann, Felix; McHale, Jim & Nord, Robert. "Architecture+TSP = High Quality+Fast," (April 2011) www.sei.cmu.edu/library/abstracts/webinars/Architecture-plus-TSP-equals-High-Quality-plus-Fast.cfm

Baker, Michele & Blash, Deen. "SEPG North America 2011 Volunteer Webinar," March 2011. www.sei.cmu.edu/library/abstracts/webinars/SEPGNA11volunteerwebinar.cfm

Blash, Deen; Buttles-Valdez, Palma; McGraw, Shane. "Improving Customer Satisfaction: A People CMM Perspective," October 2010. www.sei.cmu.edu/library/abstracts/webinars/Improving-Customer-Satisfaction-A-People-CMM-Perspective.cfm

Buttles-Valdez, Palma & Weymss, Gian. "What's Happening at SEPG North America 2011: A Portland Preview," January 2011. www.sei.cmu.edu/library/abstracts/webinars/SEPG-North-America-2011-A-Portland-Preview.cfm

Caralli, Rich & White, David. "How Resilient Is My Organization?" December 2010. www.cert.org/podcast/show/20101209caralli.html

Chick, Timothy. "Making Agile Work for You," July 2011. www.sei.cmu.edu/library/abstracts/webinars/Making-Agile-Work-for-You.cfm

CMMI Product Team. "Ask the CMMI Experts," August 2011. www.sei.cmu.edu/library/abstracts/webinars/Ask-the-CMMI-Experts.cfm

Forrester, Eileen. "Are You Ready for the Release? What You Need to Know About CMMI V1.3," November 2010. www.sei.cmu.edu/library/abstracts/webinars/Are-You-Ready-for-the-Release-What-You-Need-to-Know-About-CMMI-V13.cfm

Gennari, Jeff & Allen, Julia. "Building a Malware Analysis Capability," July 2011. www.cert.org/podcast/mp3/2/20110712gennari-full.mp3

Hanley, Michael & Allen, Julia. "Indicators and Controls for Mitigating Insider Threat," January 2011. www.cert.org/podcast/show/20110125hanley.html

Jones, Lawrence & Konrad, Michael. "Capability Maturity Model Integration V1.3 and Architecture-Centric Engineering," January 2011. www.sei.cmu.edu/library/abstracts/webinars/Capability-Maturity-Model-Integration-and-Architecture-Centric-Engineering.cfm

Lambo, Brett & Butkovic, Matt. "Conducting Cyber Exercises at the National Level," February 2011. www.cert.org/podcast/show/20110222lambo.html

Lewis, Grace. "Emerging Technologies for Software-Reliant Systems," March 2011. www.sei.cmu.edu/library/abstracts/webinars/Emerging-Technologies-for-Software-Reliant-Systems.cfm

Lewis, Grace. "Service Oriented Architecture: A Quality Attribute Perspective," June 2011. www.sei.cmu.edu/library/abstracts/webinars/Service-Oriented-Architecture-A-Quality-Attribute-Perspective.cfm

Mead, Nancy; Hilburn, Thomas & Linger, Richard. "Software Assurance: A Master's Level Curriculum," October 2010. www.cert.org/podcast/show/20101026mead.html

Merrell, Sam; Haller, John, & Huff, Philip. "Public-Private Partnerships: Essential for National Cyber Security," November 2010. www.cert.org/podcast/show/20101130merrell.html

Miller, Phillip. "Panel Discussion of the Master of Science in Information Technology-Software Engineering Management," November 2010. www.sei.cmu.edu/library/abstracts/webinars/Panel-Discussion-of-the-Master-of-Science-in-Information-Technology-Software-Engineering-Management.cfm

Nicoll, Alex & Allen, Julia. "Why Organizations Need a Secure Domain Name System," September 2011. www.cert.org/podcast/mp3/2/20110906nicoll-full.mp3

Ross, Ron, Cebula, Jim & Allen, Julia. "Integrated, Enterprise-Wide Risk Management: NIST 800-39 and CERT-R," March 2011. www.cert.org/podcast/show/20110329ross.html

Spring, Jonathan & Allen, Julia. "Controls for Monitoring the Security of Cloud Services," August 2011. www.cert.org/podcast/mp3/2/20110802spring-full.mp3

Trzeciak, Randall F. "Securing Information in the Health-Care Industry: Network Security, Incident Management, and Insider Threat," October 2010. www.sei.cmu.edu/library/abstracts/webinars/Securing-Information-in-the-HealthCare-Industry-Network-Security-Incident-Management-and-Insider-Threat.cfm

Weinstock, Charles B. "Assurance Cases for Medical Devices," May 2011. www.sei.cmu.edu/library/abstracts/webinars/Assurance-Cases-for-Medical-Devices.cfm

White, David & Allen, Julia. "Using the Smart Grid Maturity Model (SGMM)," May 2011. www.cert.org/podcast/mp3/2/20110505white-full.mp3

White, David. "Empower Your Smart Grid Transformation," March 2011. www.sei.cmu.edu/library/abstracts/webinars/Empower-Your-Smart-Grid-Transformation.cfm

Willett, Alan "Preview of SEPG Europe 2011: Global Excellence in Software and Security," May 2011. www.sei.cmu.edu/library/abstracts/webinars/Preview-of-SEPG-Europe-2011.cfm

Zimmermann, Olaf. "Architectural Knowledge Management: Decision Guidance in Service-Oriented Architecture Design," February 2011. www.sei.cmu.edu/library/abstracts/webinars/Architectural-Knowledge-Management-Decision-Guidance-in-Service-Oriented-Architecture-Design.cfm

WORKSHOPS & TUTORIALS

Abrahão, Silvia; Nolan, Andy; Clements, Paul & McGregor, John D. "First International Workshop on Quantitative Methods in Software Product Line Engineering (QMSPLE)." Munich, Germany (August 2011).

Brown, Nanette & Nord, Robert. "Strategic Management of Technical Debt." Working IEEE/IFIP Conference on Software Architecture (WICSA) 2011, Boulder, CO (June 2011).

Burton, Daniel & Nichols, William. "Exploring TSP: An Introduction." TSP Symposium 2011, Atlanta, GA (September 2011).

Buttles-Valdez, P. J. "A Holistic Approach to Software Assurance." Department of Homeland Security's 15th Semi-Annual Software Assurance (SwA) Forum, Arlington, VA (September 2011).

Brown, Nanette; Krutchen, Phillippe; Nord, Rod & Ozkaya, Ipek. "Strategic Management of Technical Debt." Seventh SEI Software Architecture Technology User Network (SATURN) 2011, Burlingame, CA (May 2011).

Cappelli, Dawn & King, Chris. "Insider Threat Workshop." Dulles, VA (November 2010).

Cappelli, Dawn & Montelibano, Joji. "Insider Threat Workshop." Arlington, VA (May 2011).

Chastek, Gary & McGregor, John D. "Production Planning in a Software Product Line Organization." 15th International Software Product Line Conference (SPLC 2011), Munich, Germany (August 2011).

Chick, Tim. "Making Agile Work for You." GA and AL Spin Tour (April 2011).

Forrester, Eileen. "CMMI for Services: Agile Strategy." StepTalks 2011, Lisbon, Portugal (April 2011).

Goldenson, Dennis & McCurley, James. "Performance Effects of Measurement and Analysis: Project, Product, and High Maturity." 10th Annual CMMI Technology Conference and User Group, Denver, CO (November 2010).

Hayes, Will & Stall, Alexander. "Sampling in SCAMPI V1.3." SEPG North America 2011, Portland, OR (March 2011).

Jones, Lawrence & Konrad, Michael. "CMMI V1.3 and Architecture." SEPG North America 2011, Portland, OR (March 2011).

Jones, Larry & Konrad, Mike. "Capability Maturity Model Integration (CMMI) V1.3 and Architecture-Centric Engineering." SEPG Europe Conference, Dublin, Ireland (June 2011).

KEY PUBLICATIONS

Klein, John. "Requirements-Driven Architecture." Seventh SEI Software Architecture Technology User Network (SATURN) 2011, Burlingame CA (May 2011).

Kruchten, Phillippe; Nord, Robert & Ozkaya, Ipek. "Second International Workshop on Managing Technical Debt (MTD 2011)," International Conference on Software Engineering (ICSE) 2011, Honolulu HI (May 2011).

Lewis, Grace. "MESOCA 2011 Workshop." 2011 IEEE International Workshop on Maintenance and Evolution of Service-Oriented and Cloud-Based Systems." Williamsburg, VA (September 2011).

Masters, Steve. "Using Organizational Business Objectives to Guide a Process Improvement Program." SEPG North America 2011, Portland, OR (March 2011).

McGregor, John D. & Muthig, Dirk. "Management and Operation of a Software Product Line." 15th International Software Product Line Conference (SPLC 2011), Munich, Germany (August 2011).

McHale, James. "The TSP Cost Model: Plan for Success, Plan for Quality." Measurement and Analysis Workshop, High Maturity Workshop, Vienna, VA (2011).

Miluk, Gene. "Changing Behavior: The Key to Adoption of Complex Process Technology." SEPG North America 2011, Portland, OR (March 2011).

Miller, Suzanne. "Leading by Example: Applying CMMI for Services to Your Engineering Process Group." SEPG North America 2011 Portland, OR (March 2011).

Mondragon, Oscar & Willett, Alan. "Applying TSP for Services: Seven Key Lessons Learned." TSP Symposium 2011, Atlanta, GA (September 2011).

Moore, Andy & Hanley, Mike. "Insider Threat Workshop." Arlington, VA, September 2011.

Nichols, William. "A Cost Model and Tool to Support Quality Economic Trade-off Decisions." ICSSP 2011, Prague, Czech Republic (May 2011).

Over, James. "Software Quality Management Throughout the Software Lifecycle." QWEST Conference, Boston, MA, (April 2011).

Trzeciak, Randy & Cummings, Adam. "Insider Threat Workshop." Arlington, VA, March 2011 and July 2011.

Trzeciak, Randy & Shaw, Eric. "Insider Threat Tutorial." New York, NY, April 2011 and June 2011.

Trzeciak, Randy. "Insider Threat Tutorial." Federal Reserve Bank, October 6, 2010.

Trzeciak, Randall; Forrester, Eileen; Moss, Michele; & Croll, Paul. "What the Good Guys and Bad Guys Have Taught Us about our OSP in a Cyber Environment." SEPG North America 2011, Portland, OR (March 2011).

Vallespir, Diego & Nichols, William. "A PSP Analysis of Defects Injected During Detailed Design." TSP Symposium 2011, Atlanta, GA (September 2011).

Willet, Alan. "Team Software Process: High Performance Individuals—High Performance Teams." StepTalks 2011, Lisbon, Portugal (April 2011).

Young, Rawdon; Penn, Mary Lynn & Hayes, Will. "CMMI Version 1.3 High Maturity—We Thought but Now We Know." SEPG North America 2011, Portland, OR (March 2011).

Zubrow, David. "Avoiding Measures Without Meaning." CIISA conference, Guadalajara, Jalisco, Mexico, (May 2011).

SEI REPORTS (UNLIMITED DISTRIBUTION) PUBLISHED 01 OCT 2010 - 30 SEP 2011

Albert, Cecilia & Rosemergy, Steve. *A Framework for Evaluating Common Operating Environments: Piloting, Lessons Learned, and Opportunities.* www.sei.cmu.edu/library/abstracts/reports/10sr025.cfm

Allen, Julia H. & Curtis, Pamela D. *Measures for Managing Operational Resilience.* www.sei.cmu.edu/library/abstracts/reports/11tr019.cfm

Anderson, William; Andrews, Archie D.; Brown, Nanette; Cohen, Cory; Craig, Christopher; Daly, Tim; de Niz, Dionisio; Diaz-Pace, Andres; Feiler, Peter H.; Fisher, David; Gluch, David P.; Hansen, Jeffrey; Hansson, Jörgen; Hudak, John J.; Lakshmanan, Karthik; Linger, Richard C.; Lipson, Howard F.; Moreno, Gabriel; Morris, Edwin J.; Mutlu, Onur; Nord, Robert; Ozkaya, Ipek; Plakosh, Daniel; Pleszkoch, Mark; Rajkumar, Ragunathan; Seibel, Joe; Simanta, Soumya; Weinstock, Charles B. & Wrage, Lutz. *Results of SEI Independent Research and Development* Projects. www.sei.cmu.edu/library/abstracts/reports/11tr002.cfm

Andrews, Archie D. & McCune, Jonathan M. *Trusted Computing in Embedded Systems Workshop.* www.sei.cmu.edu/library/abstracts/reports/11sr002.cfm

Bianco, Philip; Lewis, Grace; Merson, Paulo & Simanta, Soumya. *Architecting Service-Oriented Systems.* www.sei.cmu.edu/library/abstracts/reports/11tn008.cfm

Blanchette, Stephen; Albert, Cecilia & Garcia-Miller, Suzanne. *Beyond Technology Readiness Levels for Software: U.S. Army Workshop Report*. www.sei.cmu.edu/library/abstracts/reports/10tr044.cfm

Cebula, James J. & Young, Lisa R. *A Taxonomy of Operational Cyber Security Risks.* www.sei.cmu.edu/library/abstracts/reports/10tn028.cfm

Chaki, Sagar; Creel, Rita C.; Davenport, Jeff; Kinney, Mike; McCormick, Benjamin & Popeck, Mary. *Standards-Based Automated Remediation: A Remediation Manager Reference Implementation*. www.sei.cmu.edu/library/abstracts/reports/11sr007.cfm

CMMI Product Team. *CMMI for Acquisition, Version 1.3*. www.sei.cmu.edu/library/abstracts/reports/10tr032.cfm

CMMI Product Team. *CMMI for Services, Version 1.3*. www.sei.cmu.edu/library/abstracts/reports/10tr034.cfm

CMMI Product Team. CMMI® for Development, Version 1.3 CMMI-DEV, V1.3. www.sei.cmu.edu/library/abstracts/reports/10tr033.cfm

Ellison, Robert J.; Alberts, Christopher J.; Creel, Rita C.; Dorofee, Audrey J. & Woody, Carol. *Software Supply Chain Risk Management: From Products to Systems of Systems.* www.sei.cmu.edu/library/abstracts/reports/10tn026.cfm

Fisher, David; McCune, Jonathan M. & Andrews, Archie D. *Trust and Trusted Computing Platforms.* www.sei.cmu.edu/library/abstracts/reports/11tn005.cfm

Gross, Charlene. *A Decision Framework for Selecting Licensing Rights for Noncommercial Computer Software in the DoD Environment*. www.sei.cmu.edu/library/abstracts/reports/11tr014.cfm

Haller, John; Merrell, Samuel A.; Butkovic, Matthew J. & Willke, Bradford J. *Best Practices for National Cyber Security: Building a National Computer Security Incident Management Capability, Version 2.0*. www.sei.cmu.edu/library/abstracts/reports/11tr015.cfm

Hammerstein, Josh & May, Christopher. *The CERT Approach to Cybersecurity Workforce Development*. www.sei.cmu.edu/library/abstracts/reports/10tr045.cfm

Hanley, Michael. *Deriving Candidate Technical Controls and Indicators of Insider Attack from Socio-Technical Models and Data*. www.sei.cmu.edu/library/abstracts/reports/11tn003.cfm

Hanley, Michael; Dean, Tyler; Schroeder, Will; Houy, Matt; Trzeciak, Randall F. & Montelibano, Joji. An Analysis of Technical Observations in Insider Theft of Intellectual Property Cases. www.sei.cmu.edu/library/abstracts/reports/11tn006.cfm

Hansen, Jeffrey; Hissam, Scott; Meyers, Craig; Morris, Edwin J.; Daniel Plakosh, Soumya Simanta, Lutz Wrage. *Adaptive Flow Control for Enabling Quality of Service in Tactical Ad Hoc Wireless Networks.* www.sei.cmu.edu/library/abstracts/reports/10tr030.cfm

Heckathorn, Matthew. *Network Monitoring for Web-Based Threats.* www.sei.cmu.edu/library/abstracts/reports/11tr005.cfm

Kasunic, Mark; Zubrow, David & Harper, Erin. *Issues and Opportunities for Improving the Quality and Use of Data in the Department of Defense.* www.sei.cmu.edu/library/abstracts/reports/11sr004.cfm

Klein, John & Gagliardi, Michael J. *A Workshop on Analysis and Evaluation of Enterprise Architectures.* www.sei.cmu.edu/library/abstracts/reports/10tn023.cfm

Kumar, Satyendra & Ramakrishnan, M. IEEE *Computer Society/Software Engineering Institute Software Process Achievement (SPA) Award 2009*. www.sei.cmu.edu/library/abstracts/reports/11tr008.cfm

Lewis, Grace; Smith, Dennis B. & Kontogiannis, Kostas. *Proceedings of the Fourth International Workshop on a Research Agenda for Maintenance and Evolution of Service-Oriented Systems (MESOA 2010)*. www.sei.cmu.edu/library/abstracts/reports/11sr008.cfm

Linger, Richard C. Daly, Tim; Pleszkoch, Mark. *Function Extraction (FX) Research for Computation of Software Behavior: 2010 Development and Application of Semantic Reduction Theorems for Behavior Analysis.* www.sei.cmu.edu/library/abstracts/reports/11tr009.cfm

McHale, Jim; Chick, Timothy A. & Miluk, Gene. *Implementation Guidance for the Accelerated Improvement Method (AIM)*. www.sei.cmu.edu/library/abstracts/reports/10sr032.cfm

Mead, Nancy R.; Allen, Julia H., Ardis, Mark A.; Hilburn, Thomas B.; Kornecki, Andrew J. & Linger, Richard C. *Software Assurance Curriculum Project Volume III: Master of Software Assurance Course Syllabi*. www.sei.cmu.edu/library/abstracts/reports/11tr013.cfm

Mead, Nancy R.; Hawthorne, Elizabeth K. & Ardis, Mark A. *Software Assurance Curriculum Project Volume IV: Community College Education*. www.sei.cmu.edu/library/abstracts/reports/11tr017.cfm

Miluk, Gene; McHale, Jim & Chick, Timothy A. *Guide for SCAMPI Appraisals: Accelerated Improvement Method (AIM)*. www.sei.cmu.edu/library/abstracts/reports/10sr021.cfm

Moore, Andrew P.; Capelli, Dawn; Caron, Thomas C.; Shaw, Eric D.; Spooner, Derrick & Trzeciak, Randall F. *A Preliminary Model of Insider Theft of Intellectual Property.* www.sei.cmu.edu/library/abstracts/reports/11tn013.cfm

Nord, Robert; McHale, Jim & Bachmann, Felix. *Combining Architecture-Centric Engineering with the Team Software Process.* www.sei.cmu.edu/library/abstracts/reports/10tr031.cfm

Novakouski, Marc; Simanta, Soumya; Peterson, Gunnar; Morris, Edwin J. & Lewis, Grace. *Performance Analysis of WS-Security Mechanisms in SOAP-Based Web Services.* www.sei.cmu.edu/library/abstracts/reports/10tr023.cfm

Osiecki, Lawrence T.; Phillips, Mike & Scibilia, John. *Understanding and Leveraging a Supplier's CMMI Efforts: A Guidebook for Acquirers (Revised for V1.3)*. www.sei.cmu.edu/library/abstracts/reports/11tr023.cfm

Parker Gates, Linda. *Strategic Planning with Critical Success Factors and Future Scenarios: An Integrated Strategic Planning Framework*. www.sei.cmu.edu/library/abstracts/reports/10tr037.cfm

Phillips, Mike. *CMMI for Acquisition (CMMI-ACQ) Primer, Version 1.3*. www.sei.cmu.edu/library/abstracts/reports/11tr010.cfm

SCAMPI Upgrade Team. *Appraisal Requirements for CMMI Version 1.3 (ARC, V1.3)*. www.sei.cmu.edu/library/abstracts/reports/11tr006.cfm

SCAMPI Upgrade Team. *Standard CMMI Appraisal Method for Process Improvement (SCAMPI) A, Version 1.3: Method Definition Document*. www.sei.cmu.edu/library/abstracts/reports/11hb001.cfm

Seacord, Robert C., Dormann, Will; McCurley, James; Miller, Philip; Stoddard, Robert W.; Svoboda, David & Welch, Jefferson. *Source Code Analysis Laboratory (SCALe) for Energy Delivery Systems.* www.sei.cmu.edu/library/abstracts/reports/10tr021.cfm

SGMM Team. *Smart Grid Maturity Model SGMM Model Definition*. www.sei.cmu.edu/library/abstracts/reports/11tr025.cfm

Shoemaker, Dan; Mead, Nancy R. & Ingalsbe, Jeff. *Integrating the Master of Software Assurance Reference Curriculum into the Model Curriculum and Guidelines for Graduate Degree Programs in Information Systems*. www.sei.cmu.edu/library/abstracts/reports/11tn004.cfm

SEI STAFF AND OTHER CONTRIBUTORS

As of September 30, 2011

FULL-TIME & PART-TIME STAFF

Lisa M. Abel
John James Ackley
Lorraine J. Adams
Steve Ader
Laura Aguera
Cecilia Albert
Christopher J. Alberts
Jared C. Allar
Dennis Allen
Julia H. Allen
Noelle Allon
Kathryn Mary Ambrose
Kelly Anderson
William B. Anderson
Bjorn A. Andersson
Archie Andrews
John F. Antonucci
Jeffrey J. Apolis
Leena Arora
Felix Bachmann
Marie A. Baker
Sriram Balasubramaniam
Karen Ann Balistreri
Vincent F. Balistreri
Jeffrey Balmert
Ronald Bandes
Michael Bandor
Richard E. Barbour
Hollen L. Barmer
Jeffrey J. Basista
Leonard J. Bass
Dwight S. Beaver
Stephany Bellomo
Klaus Bellon
Jonathan Bender
Kate Bennett
John K. Bergey
Anna Maria Berta
James Edward Besterci
Donald R. Beynon
Philip Bianco
David Biber
Daniel R. Bidwa
Darlene R. Bigos
Adrienne Nicole Bishop
Bethany M. Blackhurst
Stacie A. Blakley
Stephen Blanchette
Deen S. Blash
Elaine W. Bolster
Elizabeth Borza
Randall R. Bowser
Andrew D. Boyd
Diane I. Bradley
John Bramer
Kara Branby
Pamela Brandon
Heidi Brayer
Rex E. Brinker
Rita M. Briston
Rhonda M. Brown
Lisa L.Brownsword
Philip Burdette
Joshua W. Burns
C Daniel Burton
Matthew Butkovic
Palma Jeanne Buttles-Valdez
Nickolas S. Byers
Rachel Callison
Grady H. Campbell
Kimberley S. Campbell
Linda M. Campbell
Linda Canon
Peter S. Capell
Dawn M. Cappelli
Richard A. Caralli
Anita D. Carleton
Ryan M. Casey
William Casey
Yolanda Castellano
James Cebula
Anthony M. Cebzanov
Sagar J. Chaki
Gary J. Chastek
Mary Jo Chelosky
Timothy A. Chick
Valerie Chilson
Clyde G. Chittister
Leslie R. Chovan
Mary Beth C. Chrissis
Matthew Thomas Churilla
Mia Teresa Ciorra
Kathleen Clarke
William R. Claycomb
Matthew F. Coates
Cory F. Cohen
Julie B. Cohen
Sanford (Sholom) G. Cohen
Constantine Aaron Cois
Mary Lou Cole
James Conley
Anne Marie Connell
Carol L. Connelly
John R. Connelly
James Paul Conrad
Robert Conway
Christine Cooney
Stephen Patrick Cooney
Rebecca Lynn Cooper
Patricia A. Copelin
Rita C. Creel
Lucy M. Crocker
Larry J. Crowe
Stephanie Dawn Crowe
Michael E. Crowley
Natalie Cruz
Adam B. Cummings
Sally A. Cunningham
Pamela D. Curtis
Kathleen A. Cywinski
Jerome Czerwinski
Rebecca A. D'Acunto
Eugene Terrence Dailey
Roman Danyliw
Rosemary J. Darr
Jeff Davenport
Dionisio De Niz Villasenor
Gina Christine Decola
Grant Deffenbaugh
Nathan Dell
Kareem Demian
Patrick Dempsey
Matthew J. Desantis
Edward Desautels
Aaron M. Detwiler
Jill Diorio
John V. Diricco
Mary Claire Dixon
Linda Dolphin
Carol A. Dominick
Patrick J. Donohoe
William A. Dormann
Audrey J. Dorofee
Chad R. Dougherty
James C. Douglass
Joan P. Downing
Margie Ann Drazba
Michael Welsh Duggan
Catherine A. Duncan
Evelyn Duncan
Madelaine G. Dusseau
John Dwyer
Karin Dwyer
Amber Lee Edwards
Danielle L. Edwards
Eileen A. Eicheldinger
Robin N. Eisenhart
Robert J. Ellison
Joseph P. Elm
Linda M. Elmer
Tamara L. English
Harold Ennulat
Lover Epps
Alan Evans
Felicia L. Evans
Sidney Faber
Michele Elaine Falce
Robert Joseph Fantazier
Kimberly J. Farrah
Maureen Fechik
Jeffrey B. Federoff
Peter H. Feiler
Robert W. Ferguson
Aimee F. Filippi
Amy Finkbeiner
Donald G. Firesmith
Kodiak Firesmith
William L. Fithen
Robert W. Floodeen
Jonathan M. Foote
Justin Forbes
John T. Foreman
Eileen C. Forrester
Kunta Fossett
Summer Craze Fowler
Tracey E. Fox
Jonathan Frederick
David French
Michelle Fried
Richard Friedberg
Jennifer R. Fritsch
Brent R. Frye
Michael J. Gagliardi
Matthew E. Gaston
Linda Parker Gates
Matthew Geiger
Jeffrey S. Gennari
Robert George
Joseph Giampapa
Adam John Giran
John B. Goodenough
Walter J. Goss
Carla Anne Grandillo-Spotts
Michael D. Greenwood
David E. Gregg
Ruth Gregg
Lora Gress
Russell Griffin
Phillip A. Groce
Charlene C. Gross
Jon L. Gross
Rajasekhar Gudapati
Arie Gurfinkel
David A. Guzik
Shannon Rose Haas
Bart L. Hackemack
Nancy L. Hags
John Haller
William Halpin
Josh Hammerstein
Charles B. Hammons
Michael Hanley
Dana Hanzlik
Stephen Dennis Hardesty
Erin Harper
Gibbie Lu Hart
Jeffrey S. Havrilla
John Hawrylak
Eric J. Hayes
William S. Hayes
Amanda Hays
Matthew A. Heckathorn
Jackie Henderson
Sharon Henley
Christopher Herr
Donald Kurt Hess
Charles Hines
Scott A. Hissam
Barbara J. Hoerr
Lorraine Marie Hollabaugh
Dan P. Horvath
Mohammed A. Hossain
Allen D. Householder
John W. Huber
Clifford C. Huff
Lyndsi A. Hughes
Alexa Huth
Jennifer Hykes
Chris Inacio
Terry A. Ireland
James Ivers
Nancy Janda
Carol A. Jarosz
Cherie Lanae Jeffries-Dorsey
Michael Jehn
Zachary Jensen
George M. Jones
Lawrence G. Jones
Patricia Junker
Matthew Kaar
Stephen Kalinowski
Rachel A. Kartch
Mark D. Kasunic
David Kaufman
Harry P. Kaye
David Keaton
Kristi L. Keeler
Tracey A. Kelly
Robert Kemerer
Brent Kennedy
Jennifer Ann Kent
Carolyn M. Kernan
Suellen Kiger
Una Kilberg
Peter J. Kim
Christopher King
Kimberly D. King-Cortazzo
John R. Klein
Mark H. Klein
Stacy Lynette Klein
Mark Klepach
Georgeann L. Knorr
Andrew J. Kompanek
Michael D. Konrad
Keith A. Korzec
John J. Kostuch
Paul N. Krystosek
Robert E. Kubiak
Amy Kunkle
Michael L. Lambert
Robert J. Lang
Debra J. Lange
Mary Ann Lapham
Frank Latino
Alyssa M. Le Sage
Bernadette Ledwich
Linda Levine
Harry L. Levinson
Darrell Craig Lewis
Grace A. Lewis
Alena Leybovich
Amy J. Leyland
Joshua B. Lindauer
Martin M. Lindner
Howard F. Lipson
Reed Little
Baozhu Helen Liu
Angela M. Llamas-Butler
Joanne F. Lohuis
Gregory Gerald Longo
Melissa Ludwick
Richard W. Lynch
Marlene T. Macdonald
Rudolph T. Maceyko
Brian A. Mack
Donna E. Mahoney
Lisa M. Makowski
Constantine Mamakos
Arthur A. Manion
Attilio A. Marini
Lisa Marino
Gail Markis
Tamara Lea Marshall-Keim
Theodore F. Marz
Lisa A. Masciantonio
Laura L. Mashione
Stephen M. Masters
Joseph P. Matthews
Roxanne Matthews
Barbara A. Mattis
Jeffrey Mattson
Christopher J. May
Joseph M. Mayes
Jason David McCormick
James McCurley
Kathleen McDonald
Patricia McDonald
Shane P. McGraw
James D. McHale
Bernadette McLaughlin
Michael McLendon
Joseph A. McLeod
Joseph E McManus
Jason McNatt
Deborah McPherson
William K. McSteen
Nancy R. Mead
Peter J. Menniti
Thomas J. Merendino
Samuel Merrell
Leigh B. Metcalf
Bryce Meyer

Toby Meyer
Bertram C. Meyers
Amy Miller
Gerald Miller
Suzanne M. Miller
Eugene E. Miluk
Soumyo Moitra
Elizabeth Ann Monaco
Juan Montelibano
Austin Montgomery
Andrew P. Moore
Darlene V. Moore
Kevin Moore
Jose A. Morales
Damon Morda
Gabriel A. Moreno
John Frederick Morley
Edwin J. Morris
Debra T. Morrison
Timothy B. Morrow
Anna Mosesso
David A. Mundie
Robert Murawski
David J. Murphy
Michael P. Murray
Paul Jay Murray
Lynne Marie Naelitz
Melissa Neely
Cynthia L. Nesta
Gail L. Newton
John O. Nicholas
William Nichols
Alex Nicoll
Kenneth Nidiffer
Paul D. Nielsen
Crisanne Nolan
Richard A. Nolan
Robert Nord
Mika North
Linda M. Northrop
William E. Novak
Marc R. Novakouski
Ray Y. Obenza
Patricia A. Oberndorf
Matthew O'Hanlon
Michael F. Orlando
Brittney Osikowicz
James W. Over
Ipek Ozkaya
Kathryn Rose Palermo
Mari Ann Palestra
K. Claire Palmquist
M. Steven Palmquist
Amanda Parente
Allison Parshall
Kevin G. Partridge
Nicole Pavetti
Carmal Payne
David J. Pekular
Kelwyn O. Pender
Brenda Ann Penderville
Samuel J. Perl
Sharon Kathleen Perry
Linda Hutz Pesante
Richard D. Pethia
David Michael Phillips
Dewanne M. Phillips
Janet S. Philpot
Daniel Pipitone
Patrick Place
Daniel Plakosh
William Pollak
Marsha M. Pomeroy-Huff
Mary E. Popeck
Douglass Post
Jerome J. Pottmeyer III
John M. Prevost
Traci M. Radzyniak
Angela Raible
James C. Ralston
Donald M. Ranta
Michael Rattigan
Adam J. Rauf
Frank J. Redner
Aaron Kyle Reffett
Colleen Regan
David Reinoehl
Janet Rex
Clifford Rhoades
Mary Ellen Rich
Nathaniel Richmond
John E. Robert
Terry Roberts
Stacy Rodgers
Lawrence R. Rogers
Steve W. Rosemergy
Robert Rosenstein
Dominic A. Ross
Christian Roylo
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
Concetta R. Sapienza
Emily Elizabeth Sarneso
Vijay S. Sarvepalli
Jeff Savinda
Thomas Scanlon
Alfred R. Schenker
David A. Scherb
Robert B. Schiela
Andrew Schlackman
Doug Schmidt
Steve Scholnick
Patricia Schreiber
James Schubert
Kenneth Schultz
Giuseppe Sciulli
Tina Sciullo-Schade
Philip A. Scolieri
Shirley Scott
William S. Scully
Robert C. Seacord
Joseph Robert Seibel
Gregory E. Shannon
Ryan Shaw
Sharon L. Shaw
Aaron Rhys Shelmire
David J. Shepard
Nataliya Shevchenko
Timothy J. Shimeall
Rita Shoemaker
Linda E. Shooer
William Shore
Sandra L. Shrum
George J. Silowash
Soumya Simanta
Matthew Perry Sisk
Lisa D. Sittler
Carol A. Sledge
Michelle A. Slusser
James Smith II
Kenneth L. Smith
Lenny D. Smith
Timur D. Snoke
Tara Sparacino
Debra A. Spear
James L. Spencer
Derrick Spooner
Jonathan Spring
Bryan Springer
Alex Paul Stall
Jonathan Steele
Kate Steiner
Lizann Stelmach
Julie Stephenson
James F. Stevens
Robert Stoddard
Michael Patrias Stone
Edward R. Stoner
Elizabeth M. Straitiff
Kenneth M. Stupak
Gregory Such
Siobhan Sullivan
Dean Sutherland
David M. Svoboda
Lucille Tambellini
Joe Tammariello
Christopher Taschner
Geoffrey P. Terrell
Marcia J. Theoret
Jeffrey E. Thieret
Kimberly E. Thiers
Alisa Thomas
Mark E. Thomas
William R. Thomas
David K. Thompson
Michele A. Tomasic
Barbara J. Tomchik
Carolyn Tomko
Susan J. Trankocy
Helen Trautman
Donovan Truitt
Randall F. Trzeciak
Barbara A. Tyson
David Ulicne
Jeanette Urbanek
Vijay Sai Vadlamudi
Michelle A. Valdez
Christine M. Van Tol
Mary Van Tyne
Kevin Vargo
Kay L. Vinay
Cal F. Waits
Todd Waits
Kurt C. Wallnau
Cynthia E. Walpole
Pennie B. Walters
Mary Catherine Ward
George W. Warnagiris
David Warren
Trina Washington
George M. Weaver
Rhiannon Weaver
Charles B. Weinstock
Jefferson P. Welch
Rosslyn G. Wemyss
James T. Wessel
Barbara-Jane White
David W. White
Joseph E. Wickless
Emerson R. Wiley
Pamela Jayne Williams
William R. Wilson
Brian D. Wisniewski
Robert M. Wojcik
William G. Wood
Carol S. Woody
Lutz Wrage
Evan Wright
Michael Alan Wright
Charles G. Yarbrough
Hasan Yasar
Lisa Renee Young
Rawdon Young
Cat B. Zaccardi
Mark T. Zajicek
Marianne C. Zebrowski
John J. Zekany
Xiaobo Zhou
David Zubrow

AFFILIATES

Yoshihiro Akiyama
Ye Peter Chen
Johnny Dale Childs
Michael Rodger Clement
Tom Dover
Daniel S. Foster
Chris Geary
Bonnie S. Hammer
Paul Kimmerly
Bruce Lewis
Nader Mehravari
Lisa Ming
Ryan Moore
Jose Arturo Mora-Soto
Jose Ortiz
Mary Lynn Penn
Jay Pickerill
Pascal Rabbath
William Aschambura
Martin Sebor
Brett Tjaden
Amit Trivedi
Diego Vallespir
James Wilson

OTHER CONTRIBUTORS

Drew Allison
Joseph J. Batman
Pablo Breuer
Michael Bridges
Sandra L. Cepeda
Peter P. Chen
Hunter Lucas Daley
Noopur Davis
Larry Druffel
Derek M. Gabbard
Hillel Glazer
David P. Gluch
Jeffrey Hansen
Ray Jones
Frederick Kazman
Ronald Kohl
Derek S. Lee
Anupama Manne
Robert S. Mcfeeley
Paulo F. Merson
Thomas R. Miller
James Nash
Said Nurhan
Patrick J. O'Toole
Malcom A. Patrick
Gunnar Peterson
Jeffrey Pinckard
Adam A. Porter
Gregory Porter
Raghvinder Sangwan
Kevin Peter Schaaff
Barry Glen Schrimsher
Lui Sha
Eric D. Shaw
Donald Sheehan
Judith A. Stafford
Kevin Sullivan
Peter J. Sullivan
Scott R. Tilley
Giuseppe Valetto
Kenneth Van Wyk
Daniel S. Wall

To determine how to put the SEI to work for your organization, contact SEI Customer Relations at 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 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. The SEI also supports a select group called SEI Partners, which are organizations and individuals trained and licensed by the SEI to deliver SEI products and services.

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**

COPYRIGHTS

The SEI Year in Review is produced by SEI Corporate Communications

Manager, Corporate Communications
Janet Rex

Manager, Public Relations
Richard Lynch

Editorial
Hollen Barmer
Heidi Brayer
Ed Desautels
Claire Dixon
Dana Hanzlik
Erin Harper
Eric Hayes
Jennifer Kent
Tamara L. Marshall-Keim
Bill McSteen
Brittney Osikowicz
Linda Pesante
Paul Ruggiero
William Thomas
Pennie Walters
Barbara White

Design
Daniel Pipitone

Illustration
Kurt Hess
Todd Loizes

Digital Production
Melissa Neely

Photography
Tim Kaulen, Photography and Graphic Services, Mellon Institute

Production
David Gregg

Web Design
Maureen Fechik

Cover Image
Data visualization by Chris Harrison, Human-Computer Interaction Institute at Carnegie Mellon University

SOFTWARE ENGINEERING INSTITUTE
CARNEGIE MELLON UNIVERSITY

4500 Fifth Avenue
Pittsburgh, PA 15213-2612
Phone: 412-268-5800
Toll free: 1-888-201-4479
Fax: 412-268-5758
www.sei.cmu.edu
info@sei.cmu.edu

SEI WASHINGTON, DC

NRECA Building
Suite 200
4301 Wilson Boulevard
Arlington,VA 22203

SEI LOS ANGELES, CA

2401 East El Segundo Boulevard
El Segundo, CA 90245

SEI EUROPE

An der Welle 4
60 322 Frankfurt
Germany

Software Engineering Institute
Carnegie Mellon