2012 **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

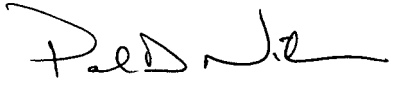
Message from the Director

The Software Engineering Institute has accomplished a great deal this year and has demonstrated how innovative, agile, and professional our men and women are. While our staff is well known for these characteristics, I still found myself impressed by the hard work and dedication shown by the SEI's men and women in 2012.

- We added more than 90 new employees this year, including a new COO, Bob Behler; a new CTO, Dr. Kevin Fall; and a new cybersecurity deputy, Ned Deets.
- We transitioned Capability Maturity Model Integration (CMMI) out of SEI into a new stand-alone organization, the CMMI Institute, owned by Carnegie Mellon.
- We supported more than 100 government and commercial organizations—and received their thanks and recognition of the value we've added to their efforts.
- We established a new SEI Innovation Center to enhance our ability to explore the emerging opportunities of software intensive systems, especially for the intelligence community.
- We've built upon our strong foundations in cybersecurity, software architecture, process improvement, and measurement and estimating, and explored new issues related to scale and computing at the edge, while providing unique technical support to our sponsors.
- On an individual level, we recognized the significant career contributions of John Foreman, who was named the sixth SEI Fellow. A member of the SEI staff for 27 years, John currently serves as associate director—military services acquisition for the SEI's Acquisition Support Program (ASP).

As we look to 2013, we see opportunity—for new research thrusts, for new collaborations with top scientists and engineers, for new contributions to our defense and federal clients, and for enhanced value to our sponsors.

Our men and women are eager to explore the frontiers of software engineering and cybersecurity—and to maintain our global reputation for quality and innovation. Thank you for an exceptional year.



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.

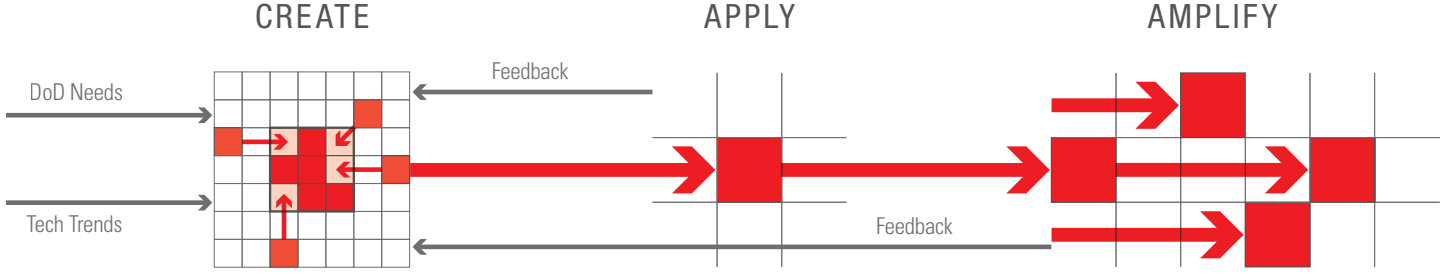
Amplify

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's staff of world-recognized leaders in software engineering works closely with defense and government organizations, industry, and academia to continually improve software-intensive systems.

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 works 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 performs research and development in the following areas:

- cybersecurity
- software architecture
- process improvement
- measurement and estimating
- unique technical support to our sponsors

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.

Growing SEI Innovation Center Explores the Art of the Possible

In its first full year of operation, the Software Engineering Institute's Innovation Center scored a number of successes—and experienced significant change. In fact, the organization just recently began operating under a new name. "We changed the name to the SEI Innovation Center late in the year," explained Matt Gaston, director of the unit. "It was necessary so that we could avoid confusion between us and other, similarly named groups."

The new name, Gaston added, also captures the essence and direction of the organization. "This is a forward-looking, proactive group," he said. "We're ready to take on almost any problem people can bring to us. It's good to have a name that reflects that."

2012 saw the SEI Innovation Center triple in size, growing from a staff of 4 early in the year to 14 by year's end—and it has need for a half-dozen more. "It's a great team," Gaston said, "with a great mix of capabilities."

What hasn't changed is the Innovation Center's charter to identify, demonstrate, extend, and apply emerging software technologies to meet critical government mission needs. "We're helping the government stay on the edge of technology," Gaston said. "We shape and leverage academic and industrial research, and promote government awareness and knowledge of emerging technologies and their applications."

The Innovation Center's capabilities cover the broad spectrum of data-intensive, scalable computing. This includes rapid prototyping, technology evaluation and demonstration, big data and analytics, autonomous systems, scalable distributed computing, applied machine learning, emerging computing architectures, information visualization, intelligence analysis, cyber operations, open innovation, and reality transfer.

During 2012, the SEI Innovation Center tackled several important projects. In one, the Innovation Center team acquired, assembled, and programmed a super computer (see related story, page 12). The team used the powerful machine to investigate heterogeneous high-performance computing (HPC) utility clouds and the software used in HPC applications. In another, the Innovation Center advanced the knowledge base in cyber intelligence by launching a project to baseline the state-of-the-practice of cyber intelligence nationally. This program, which continues into 2013, brings together the cyber intelligence knowledge and know-how of several dozen disparate entities in government, industry, and academia.

The Innovation Center's tradecraft initiative is capturing best practices and identifying key cyber intelligence gaps among its participants. Data will be used as inputs to develop and prototype tools, methods, and technologies that address critical gaps in the field.

Gaston noted the SEI Innovation Center has several interesting initiatives lined up for 2013, including a program to explore software issues in autonomous control of various vehicles and an effort to explore software producibility for future architectures. A third initiative will explore the issues around assessing open source software, taking an evidence-based approach. Overall, Gaston said, the SEI Innovation Center is moving forward in meeting its mission as an investigator and prototyper of leading-edge technologies.

"We're starting to demonstrate the art of the possible," he said, "and help others be more productive."

"We're helping the government stay on the edge of technology. We shape and leverage academic and industrial research, and promote government awareness and knowledge of emerging technologies and their applications."

—Matt Gaston

Growth in Agile Initiatives Helps DoD Apply Agility Effectively

Building on a very successful effort in 2011, the SEI's Acquisition Support Program (ASP) further expanded its investigation of agile methods for acquisition in the Department of Defense (DoD) during 2012. 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. That all adds up to an increasing demand for information about applying agile within the DoD, and for the tools, models, and processes that the SEI is producing in its multi-year agile research program.

"2012 saw us complete the preliminary version of the Agile Contingency Model," noted Mary Ann Lapham, who leads the agile effort within ASP. "The model will help the DoD determine when agile might be a good fit for specific projects, or what risks a project faces when using agile," Lapham said, noting that having that information should encourage more programs to adapt agile methods to their work.

Also completed during 2012 were a number of key technical papers and presentations. These papers represent guidebooks to program managers for assessing their organizations' readiness to implement agile methods or help program teams "translate" agile principles and terminology to traditional acquisition processes in the DoD.

By leveraging its ongoing relationships with DoD acquisition programs, the SEI is developing the resources to help the DoD make decisions about agile methods that can help it achieve its goals for speed, adaptability, and efficiency.

Meanwhile, interest in agile within the DoD acquisition community continues to grow, Lapham noted. The Agile Collaboration Group, founded by the SEI, grew rapidly in 2012, doubling in size over the course of the year. Lapham, who noted that the group includes "folks we met along our agile journey who wanted to continue to help," said members included representatives of U.S. military services, federal agencies, and contractors in the defense industry.

By leveraging its ongoing relationships with DoD acquisition programs, the SEI is developing the resources to help the DoD make decisions about agile methods that can help it achieve its goals for speed, adaptability, and efficiency.

In particular, the SEI is now capable of providing risk assessment, tailored training, and embedded advisors; can provide coaching in agile methods in the DoD environment; can assist programs in devising workable hybrid options; and can conduct program start-up workshops for programs that choose to use agile in their acquisition activity.

"Agile is not a silver bullet, but may be an answer to some of DoD's software program problems," Lapham said. "Our work has shown that agile has the potential to be a valuable option for programs that value its flexibility, speed, and delivered quality—while at the same time remaining compatible with traditional DoD acquisition practices."

"Agile is not a silver bullet, but may be an answer to some of DoD's software program problems. Our work has shown that agile has the potential to be a valuable option for programs that value its flexibility, speed, and delivered quality—while at the same time remaining compatible with traditional DoD acquisition practices."

—Mary Ann Lapham

Photo: U.S. Air Force photo/Capt. Carrie Kessler

Driving Control Standards for Unmanned Systems

More and more, traditional manned military aircraft share the skies with a new class of machines: unmanned aircraft systems (UAS)—remotely piloted aircraft, such as the Predator, Global Hawk, and Reaper along with the ground systems that control them. And other systems with varying levels of autonomy are on the way.

While these aircraft—commonly called UAVs, or unmanned aerial vehicles—have proven their value repeatedly over the past decade, the lack of a common architecture for control among the different types of these vehicles has both complicated their operation and limited their mission capabilities. Because each system is unique, ground controllers generally are able to issue commands to only one instance of one type of UAS at a time.

But now, as the use of these new vehicles increases, the SEI is helping their designers and users develop more efficient and productive ways to control them.

Charles "Bud" Hammons of the SEI's Acquisition Support Program (ASP) is leading the Institute's efforts. He's been a major participant in helping the military services and defense contractors form the Unmanned Aircraft System Control Segment Architecture Working Group (UCS WG), a new organization dedicated to establishing standards for unmanned systems.

"Systems have been built with individual, unique control systems and software up to now," Hammons said. There is limited-to-non-existent interoperability among the various UAS systems, most of which have dedicated control stations that are purpose-built and heavily depend upon human action to execute missions. "The hope is that with the UCS WG's involvement, standards can be established that allow some interoperability across ground control stations," Hammons said. The result would be cost savings when building the systems and greater efficiencies when operating them.

Hammons is also bringing the SEI's expertise to the UCS WG, which is tackling the standards issue. The success of the UCS WG depends upon harmonization with other significant standards applicable in the UAS community. The two most significant such standards are a NATO standard, STANAG 4586, and the U.S. Navy's Future Avionics Capability Environment (FACE) effort, developed under the auspices of The Open Group.

Developing the standards effort has also spurred an SEI research project for FY13, also led by Hammons, that is examining the division of labor between humans and machines in the UAS world. In the current generation of UAVs, humans are responsible for much of the work—no matter how tedious. The idea behind the research is that it may be appropriate and feasible to have the machine perform more of the labor, lightening the workload for human controllers and allowing for a more efficient use of resources.

"If a viable approach to enabling flexible division of labor between humans and automation in unmanned systems is made available to DoD, more complex operational use cases—many involving multiple platforms—will be more likely to be realized," Hammons noted. "We at the SEI are well situated to perform this research, given our existing relationships in the UAS field, which spans the DoD, Air Force, Army, and most of the stakeholders working in these initiatives."

"If a viable approach to enabling flexible division of labor between humans and automation in unmanned systems is made available to DoD, more complex operational use cases—many involving multiple platforms—will be more likely to be realized."

—Charles "Bud" Hammons

Photo: Spc. Grant Larson

SUPERCOMPUTER ADVANCES SEI INNOVATION CENTER MISSION

The SEI gained some serious computing muscle in June. That's when engineers in the SEI Innovation Center switched on its new heterogeneous high-performance computing cluster—a supercomputer.

How super is super? The new, custom-built machine harnesses two racks of equipment to provide the combined computing power of 17 machines: an Altix UV large-memory machine (which features a full terabyte of memory), eight x86 computers, three dual GP-GPU Tesla units, and four 64-core Tilera machines—all interconnected with a dual 10GB Ethernet network.

And there's room for more, noted Eric Werner of the SEI Innovation Center, which is part of the SEI's Acquisition Support Program. Werner leads the team that operates the Center's supercomputer and has begun using it for experimental work in several high-performance computing research areas.

All of that computing power is needed for the SEI Innovation Center's current focus on data intensive scalable computing (DISC), which includes image processing, graph processing, cloud computing, cloud architecture, and more, Werner said.

"This is an asset not just for the Center but for all of the SEI," Werner added, noting that other SEI programs have already expressed interest in applying the new supercomputer's capabilities to research and development programs in their areas. SEI Innovation Center team members, working with the SEI's Information Technology group, acquired the equipment and assembled the machine, incorporating expertise in supercomputers from other users and owners of similar equipment in industry. The supercomputer is located in the SEI's main Pittsburgh office near the Carnegie Mellon University campus.

FOREMAN NAMED SEI FELLOW

John Foreman was named the sixth SEI Fellow in 2012. The designation is awarded to people who have made outstanding contributions to the SEI and who continue to advise SEI leaders.

"I am very honored to be named an SEI fellow, especially considering those who came before me," Foreman said recently.

Foreman, currently the associate director–military services acquisition for the SEI's Acquisition Support Program (ASP), leads a team that provides direct acquisition and technical support to Army, Navy, and Air Force programs and organizations. He joined the SEI in 1986, and his career spans 35 years working in the complete lifecycle of software and systems as well as the development and transition of software technologies.

"Meeting the needs of military services customers—and deriving lessons learned and stimulating applicable research efforts—continues to be my focus," Foreman said.

The author of numerous technical reports, articles, and handbooks, Foreman's key publications include the *ADA Adoption Handbook* and the *Software Technology Reference Guide*.

Foreman has also stimulated development of the SEI's body of knowledge on agile methods in government acquisition, led development and execution of Process in Execution Reviews (PIERs) and Independent Technical Reviews (ITAs), oversaw evolution of the Software Acquisition Survival Skills (SASS) course, created senior leadership seminars, and directed the SEI's TIDE (Technology Insertion, Demonstration, and Evaluation) project.

Foreman has served as ASP's chief engineer for Air Force programs; directed the SEI's Dynamic Systems program; and, while "loaned" to the government, was program manager of DARPA's Software Technology for Adaptable and Reliable Systems (STARS) program.

John Foreman

Photo: NNSANews

INDEPENDENT TECHNICAL ASSESSMENTS GAUGE PROGRAM HEALTH, SPUR POSITIVE OUTCOMES

For more than a decade—since 1998—the SEI has been helping the Department of Defense (DoD) and other government agency programs assess the technical health of ongoing and completed software projects. Called independent technical assessments (ITA), these in-depth reviews typically occur during the development or acquisition of software-intensive systems and provide an objective, technical evaluation of a specific program or effort.

An ITA is conducted by a team staffed with software specialists drawn from SEI programs and other experts associated with the SEI. Team members are purposely chosen for complementary backgrounds that span the subjects at issue. A typical ITA team has 5 to 10 members.

The assessments are data-driven analyses accomplished through document review and interviews with stakeholders (prime contractor, suppliers, users, and others). They are often conducted at stakeholder sites.

The final deliverable is a set of findings and recommendations that help the ITA sponsor or customer mitigate risks, leverage strengths, and produce a successful program outcome.

ITAs may be conducted when a program is experiencing problems—but often they are conducted for other reasons, such as to validate that a program is continuing to make good progress.

During 2012, the SEI performed multiple ITAs, including analyses of portions of ongoing projects for U.S. intelligence agencies, the U.S. Navy, and the U.S. Air Force. More than 100 ITAs have been performed since the late 1990s.

SEI Lends Technology and Know-How to Critical Department of Defense Cyber Exercises

In July 2012, the U.S. Cyber Command used the CERT® Exercise Network for an unprecedented joint cyber training exercise called Cyber Guard. The CERT Exercise Network provides realistic, hands-on cyber defense exercises on replicas of operational networks in actual use. The CERT Exercise Network scenarios challenge the skills of cyber warriors and provide them experience they can apply in real-world operations.

Recognizing that wide coordination is essential to defend U.S. critical infrastructures, such as utilities and finance, the command brought together hundreds of participants from the Department of Defense (DoD), National Guard, and other government agencies and academic institutions.

In a massive effort, the CERT Exercise Network development team, led by Jeff Mattson, produced a replica of the internet for the exercise in just 45 days. The network included more than 5,000 computers representing corporate enterprise, supervisory control and data acquisition (SCADA) networks, multinational companies, and universities. The CERT Exercise Network environment also included advanced user simulation and dozens of routers to model Tier 1 and 2 internet service providers. "The SEI achieved realism," Mattson said, "by including the latest malicious programs, integrating vulnerable industry control systems into a corporate network, and 'causing' a botnet attack on modeled U.S. critical infrastructure."

"A superb, world-class event," said Lt. Gen. Jon Davis, deputy commander for U.S. Cyber Command. "I saw a complete cadre of cyber warriors so energized about fighting an extremely complex, realistic cyber threat scenario."

In June 2012, the SEI also supported the International Cyber Defense Workshop (ICDW). Sponsored by the DoD's chief information officer, the ICDW takes place twice yearly. This year, for the sixth time, the SEI used the CERT Exercise Network to support the event's team-based, tactical exercises. Because cyber attacks do not respect national borders, teams from 25 nations participated, connecting to the CERT Exercise Network from around the world.

In a new twist, the exercise involved both incident response and computer forensics in realistic scenarios. The CERT Exercise Network development team modeled a multinational military network in Afghanistan. In the scenario, the network was compromised by insurgents, who infiltrated a database containing casualty and other useful information for a physical attack. Working across continents, teams of cyber defenders had to perform forensics on the database server to determine what happened and what information was compromised.

For the second challenge, the team built a workstation in the CERT Exercise Network—a captured Al Qaeda laptop with information related to a planned attack. It had a native Arabic installation of Windows and key information in English, though encrypted. Workshop teams had to determine which information was relevant and find hidden clues. They had to do nontraditional computer forensics that included intelligence analysis. Their challenge was to understand the situation on the ground and to determine when, where, and how the attack would occur. Quick turnaround was imperative. In the CERT Exercise Network, workshop teams had clickable access to forensics tools and to the scenario network and workstation. They could shoulder-surf, chat, and share information through wiki pages.

"The workshop exercise was very challenging technically," said CERT Workforce Development manager Chris May. "It required a high level of realism and broke new ground in global training—teams located on different continents all cooperating and collaborating on the same technology."


Chris May


Jeff Mattson


Lt. Gen. Jon Davis

"A superb, world-class event. I saw a complete cadre of cyber warriors so energized about fighting an extremely complex, realistic cyber threat scenario."

—Lt. Gen. Jon Davis, Deputy Commander for U.S. Cyber Command

CERT Program Expands Suite of Secure Coding Standards, Champions Adoption

Most software security vulnerabilities stem from a relatively small number of common programming errors. To reduce security vulnerabilities before software reaches the market, members of the CERT® Secure Coding Initiative have been leading the community development of secure coding standards for common programming languages, which are being adopted by major industry players.

In late 2011, industry leader Cisco Systems, Inc., adopted the CERT C Secure Coding Standard as a baseline programming standard in its product development. "An essential component of every secure software development process is a set of coding practices. Rather than formulating our own, after evaluating publicly available sets of guidelines, we decided to adopt the CERT C Secure Coding Standard," said Cisco's Martin Sebor, technical leader of the C and C++ Compiler Toolchain Team in Cisco's Network Operating System Technology Group (NOSTG).

The standard's rules and recommendations seek to eliminate insecure coding practices and undefined behaviors that can lead to exploitable vulnerabilities. By applying the CERT C Secure Coding Standard, Cisco developers can produce higher quality systems that are robust and more resistant to attack.

Having successfully coordinated the development of secure coding standards for the C, C++, and Java programming languages, which Oracle adopted in 2012, the CERT Secure Coding Team has unveiled a draft standard for Perl.

"In our analysis, we performed Perl code audits using the Source Code Analysis Lab (SCALe)," said the Secure Coding team's David Svoboda. "Many of our rules were inspired by vulnerabilities in the code we analyzed."

Additionally, the CERT Program reviewed reports from the CERT Vulnerability Notes Database to make sure the standard addressed coding errors that have resulted in past vulnerabilities in Perl programs. To augment the standard, the CERT Program invites collaboration from interested professionals in the software development and software security communities.

The CERT Secure Coding team has long contributed much-needed security enhancements to a major revision of the ISO/IEC standard for the C programming language itself. David Keaton, a member of the CERT Secure Coding team, chaired Task Group PL22.11 C of the International Committee for Information Technology Standards (INCITS). Working with SEI colleagues Svoboda and Robert C. Seacord, Keaton helped develop, refine, and introduce many of the security enhancements to ISO/IEC 9899:2011, informally referred to as C11, which was released in December 2011.

"Security features in C had been limited to the 'snprintf' function, introduced in 1999," explained Keaton. "Now, the new ISO standard includes an entire new library of secure string functions, plus an optional compilation model that makes C code more understandable by source code analyzers that perform security checks."

"This is a major accomplishment," noted Archie Andrews, technical director of CERT Secure Software and Systems. "While the SEI, as a federally funded research and development center, focuses on software engineering issues relevant to the DoD, this new standard will not only improve software developed for the DoD but all software applications written in the C programming language."

The Secure Coding Initiative's work has taken on new significance with Section 925 of the National Defense Authorization Act for Fiscal Year 2013, which requires evidence that the coding practices of government software development and maintenance organizations and contractors conform to secure coding standards approved by the Department of Defense.


David Svoboda


Robert Seacord


Archie Andrews

"An essential component of every secure software development process is a set of coding practices. Rather than formulating our own, after evaluating publicly available sets of guidelines, we decided to adopt the CERT C Secure Coding Standard."

—Martin Sebor, Technical Leader of the C and C++ Compiler Toolchain Team in Cisco's Network Operating System Technology Group

```
my $stack_from_level;
if ( $stack_from_level = RT->Config->Get('LogStackTraces') ) {
    # if option has old style '\d'(true) value
    $stack_from_level = 0 if $stack_from_level =~ /^\d+$/;
    $stack_from_level = $level_to_num{ $stack_from_level } || 0;
} else {
    $stack_from_level = 99; # don't log
}

my $simple_cb = sub {
    # if this code throw any warning we can get segfault
    no warnings;
    my %p = @_;

    # skip Log::* stack frames
    my $frame = 0;
    $frame++ while caller($frame) && caller($frame) =~ /^Log::/;
    my ($package, $filename, $line) = caller($frame);

    $p{'message'} =~ s/(?:\r*\n)+$//;
```

Building a Capability Model for Electricity Subsector Cybersecurity

As technology advances, cyber threats to the nation's electrical grid are becoming increasingly sophisticated and dynamic. In January 2012, the White House launched an initiative to enhance the security and reliability of the nation's electrical grid, led by the Department of Energy (DoE), in partnership with the Department of Homeland Security (DHS), and in collaboration with private-sector and public-sector experts.

Over just four months, members of the SEI's CERT Program worked with initiative members to produce the Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2), a self-evaluation tool that allows electric utilities and grid operators to assess their cybersecurity capabilities and prioritize their actions and investments to improve cybersecurity. The model, released by the DoE in May 2012, combines elements from existing cybersecurity efforts into a common tool that can be used consistently across the industry to understand, describe, benchmark, and share information about cybersecurity practices.

"The SEI worked in close collaboration with the DoE to lead various aspects of the ES-C2M2 development," said David White, technical manager of the Cyber Resilience Center in the CERT Program and model architect for the project. "Our team served key roles on the core model development team and provided subject matter expertise to develop the structure and content for the model and an evaluation methodology that would enable utilities to easily assess their own level of cybersecurity readiness." Members of the SEI technical staff also served on the pilot team, which facilitated self-evaluations of volunteer utilities to validate the model content and evaluation approach.

The model development team used several existing processes, models, and documents as foundational references in the creation of the ES-C2M2, including the CERT® Resilience Management Model (CERT®-RMM). The result was a scalable framework of cybersecurity capability maturity indicator levels (MILs) utilities can use to measure their cybersecurity capability performance. The model maps the MILs to cybersecurity practices, divided into 10 domains, that help utilities build their cybersecurity capabilities and improve their resilience to cyber incidents.

The ES-C2M2 suite of tools and services includes the model itself, a self-evaluation toolkit, facilitated self evaluations led on-site by ES-C2M2 team members, and benchmarking and analysis of utilities' reported data.

In a May 25 White House blog post titled "Building Cybersecurity Capability in the Electricity Sector," White House Cybersecurity Coordinator Howard A. Schmidt said, "With a waitlist of utilities eager to employ the model beyond the pilot participants, this model promises to significantly enhance our understanding of cybersecurity capabilities across the sector—a first step to understanding the cybersecurity posture of the grid. This effort will provide us with valuable insights to inform investment planning, research and development, and public-private partnership efforts."

"Our team served key roles on the core model development team and provided subject matter expertise to develop the structure and content for the model and an evaluation methodology that would enable utilities to easily assess their own level of cybersecurity readiness."

—David White

Insider Threat Team Contributes to National Insider Threat Task Force

When the U.S. government established a special task force to help the nation develop a program to deter, detect, and mitigate insider threats, it invited the CERT Program's Insider Threat team to participate, along with dozens of executive branch agencies. This National Insider Threat Task Force (NITTF) is part of a 2011 executive order calling for improvements to classified networks and responsible sharing and safeguarding of classified information.

According to Michael Theis, the CERT counterintelligence expert and member of the CERT Insider Threat team who participates on the NITTF, "Our wealth of knowledge of insider threats—including all the analysis we've done of real-world cases—made us uniquely qualified to help out."

The first step for the NITTF was to create a national policy for federal agencies. In its support of the NITTF, the CERT Program contributed to developing minimum standards for agencies to follow when running their own insider threat programs.

"Knowing what to do and how to do it are critical to the success of an insider threat program," Theis says. "And having minimum standards and effective guidance is a good way to ensure that federal agencies have that knowledge."

While working with this task force, Theis referred to substantive research the CERT Program has done on insider threats over the last 10 years. This work included analysis of more than 700 cases in the CERT insider threat database and the team's latest book: *The CERT Guide to Insider Threats*, published earlier this year. This book is a practical guide, offering specific guidance and countermeasures that staff at any organization can apply to reduce the risk of insider attack.

"Our book provides a comprehensive reference for our entire body of knowledge on insider threats," said Dawn Cappelli, one of the book's authors and a CERT Program technical manager. "We use a lot of case examples from the CERT database, and because they effectively highlight the many facets of insider threat, they prompt readers to start asking relevant questions about their own organization's exposure."

The next step for the task force will be to assess agencies against the minimum standards and then analyze new insider threats to the U.S. government along with future trends.

STUDY REVEALS INSIGHTS INTO INSIDER FRAUD FOUND IN FINANCIAL SERVICES SECTOR

The CERT Insider Threat team's latest study—analyzing 80 cases of insider fraud in financial services—revealed some interesting results: the perpetrators in more than 50 percent of the cases were managers, rather than the usual lower-level staff that has historically been responsible for committing insider fraud. The study also showed that when insiders take a "low and slow" approach—stealing smaller amounts of money or intellectual property over a long period of time—they do more damage and can elude detection for a significant period, on average longer than 2½ years.

Another surprising finding was that most of the perpetrators used the money they stole to pay for daily living expenses, rather than lead an extravagant lifestyle. While more research is needed to determine whether this approach is a growing trend, these findings provide helpful insights into the nature of insider crimes and how—with the "low and slow" approach—organizations a have a large window of opportunity to detect the fraud. To learn more, read the reports: *Insider Fraud in Financial Services* and *Insider Threat Study: Illicit Cyber Activity Involving Fraud in the U.S. Financial Services Sector.*

(Left to right) Andrew Moore, Dawn Cappelli, and Randy Trzeciak of the CERT Insider Threat team.

SEI CERTIFICATION PROGRAM EARNS ANSI ACCREDITATION

Marking a significant milestone in its effort to improve and enrich its certification programs, the Software Engineering Institute's (SEI) CERT®-Certified Computer Security Incident Handler (CSIH) certification program has earned accreditation from the American National Standards Institute (ANSI) Accreditation Program for Personnel Certification Bodies. ANSI's accreditation program is based on the American National Standard (ANS) and international standard ANSI/ISO/IEC 17024. The CERT-CSIH program is the first SEI certification to receive ANSI/ISO/IEC accreditation.

"ANSI commends the SEI for achieving accreditation and demonstrating its commitment to the continual improvement of its credentialing program," said Dr. Roy Swift, senior director of personnel credentialing accreditation programs at ANSI. "Accreditation by ANSI demonstrates compliance to a rigorous, internationally recognized accreditation process and creates a valuable market distinction for the SEI's CERT-CSIH certification."

The CERT-CSIH certification program prepares computer security incident response personnel, and other information security professionals, to participate in incident handling efforts. It also teaches them how to keep their organizations current on innovations and trends in computer security. The CERT-CSIH certification incorporates work experience, an examination, and renewal requirements.

"The SEI certification program has for years equipped computer security professionals with the skills to participate in incident handling efforts," said Jeff Welch, manager of the SEI certification program. "We are proud of our accreditation from ANSI and the additional confidence it can provide to our communities and the professionals who earn our certifications."

The SEI certification program offers certifications and authorizations in process improvement, computer security, measurement and analysis, software architecture, and service-oriented architecture. For more information about the SEI's CERT-CSIH program, visit www.sei.cmu.edu/certification/security/csih.

"The SEI certification program has for years equipped computer security professionals with the skills to participate in incident handling efforts. We are proud of our accreditation from ANSI and the additional confidence it can provide to our communities and the professionals who earn our certifications."

—Jeff Welch

MASTER OF SOFTWARE ASSURANCE CURRICULUM RECOGNIZED BY PROFESSIONAL SOCIETIES

The IEEE Computer Society (IEEE-CS) and Association for Computing Machinery (ACM) have recognized the Master of Software Assurance (MSwA) Reference Curriculum as appropriate for a master's program in software assurance. This formal recognition signifies to the educational community that the MSwA Reference Curriculum is suitable for creating graduate programs or tracks in software assurance. The IEEE-CS and ACM are community leaders in curriculum development.

CERT researchers collaborated with a team of educators from Embry-Riddle Aeronautical University, Monmouth University, and Stevens Institute of Technology to develop the MSwA curriculum. The first curriculum ever to be developed for software assurance, the MSwA curriculum identifies a core body of knowledge that educational institutions can use to develop MSwA degree programs.

In addition to the curriculum, the MSwA project team has developed

- course syllabi to support the development of a set of courses in an MSwA curriculum program
- undergraduate software assurance course outlines, a faculty resource for teaching fundamental skills to students either entering the field directly or continuing with graduate-level education
- community college course outlines for software assurance that provide students with fundamental skills for continuing with graduate-level education or provide supplementary education for students with prior undergraduate technical degrees who wish to become more specialized in software assurance

Andrew McGettrick, chair of the ACM Education Board and Council, and associate editor of the *Computer Journal*, says of these materials, "These are terrific. They are a great contribution to curricula guidance generally and I am sure will be widely welcomed. Moreover, they are particularly topical and relevant and I hope computing educators will take note."

The team is currently developing educational offerings for executives responsible for software acquisition.

Resources, including lectures and materials, to help educators get started in software assurance education are available at no cost at www.cert.org/mswa.

Meeting the Challenge of Wireless Emergency Alerts

A New Yorker passing through Kansas receives a text message on her cell phone alerting her to tornadoes closing in on the stretch of Interstate 70 down which she and her husband are driving. At the same time, other cell phone customers in the threatened area also receive the National Weather Service alert. So informed, they all can seek shelter and protect themselves. This is one of many visions for Wireless Emergency Alerts (WEA, formerly known as the Commercial Mobile Alert Service).

WEA grew out of the Warning, Alert, and Response Network (WARN) Act. It transmits three types of alerts: presidential alerts, imminent threat alerts, and America's Missing: Broadcast Emergency Response (AMBER) alerts. The system provides alerting authorities the ability to broadcast emergency alerts to customers located in the vicinity of cellular towers serving an affected area. To date, four of the largest cellular networks have agreed to participate. The system also incorporates thousands of alert originators.

Though the four large cellular networks provide WEA 90 percent geographic coverage, numerous smaller providers and thousands of alert originators still need to be integrated to maximize its reach. This is where the SEI comes in. Its role is to support the Department of Homeland Security Science and Technology Directorate by creating a strategy for integrating these alert originators into WEA.

Larry Jones, team lead for the SEI's WEA effort, noted that the SEI brings to the project its leadership in software engineering research and serves as a single source of experts from the multiple disciplines WEA development requires. "The SEI's Research, Technology, and System Solutions [RTSS] Program leads a cross-SEI team," said Jones. "That team includes experts in architecture, integration, network security, domain knowledge and project management."

To be effective, the strategy must provide paths of integration into the systems for the thousands of alert originators. These include all state, county, and city governments, as well as local districts for fire protection, transit, and public utility services. Complicating matters, the overall effort involves aspects of international cooperation.

The challenges are many:

- Alert originators use many different types of software.
- The documentation available for the existing systems varies widely.
- The security of systems varies.
- The originators' readiness to integrate with WEA varies.

What's more, Jones observed that the alert originators' current use of the required protocol varies. "WEA will use the Common Alerting Protocol (CAP)," said Jones. "CAP has a 90-character limit, which originators feel limits their ability to describe a situation to users. So, WEA will have varying needs to be supplemented by other existing emergency alert systems, such as TV, radio, and social media."

Jones added that a one-size-fits-all strategy definitely will not work. "Alert originators work in vastly different contexts and necessarily have vastly different origination systems," said Jones. "For example, San Diego County is the size of Connecticut. Residents speak English, Spanish, Tagalog, Vietnamese, and many other languages. Its territory includes coastline, mountains, and desert, which are prone to different types of emergencies, from tsunami to landslides to wildfires." Consequently, said Jones, "the alert system that San Diego uses will differ from that used by, say, a county in Montana with a population of less than 5,000."

The overall WEA effort is extensive and involves several other organizations working on other aspects of the project. Collaborators on WEA include the Applied Physics Laboratory at Johns Hopkins University and the RAND Corporation.

Larry Jones

WEA provides alerting authorities the ability to broadcast emergency alerts to customers located in the vicinity of cellular towers serving an affected area. To date, four of the largest cellular networks have agreed to participate. WEA also incorporates thousands of alert originators that still need to be integrated to maximize its reach. This is where the SEI comes in. Its role is to create the integration strategy.

SEI-CMU Collaboration Seeks Increased Situational Awareness for Warfighters at the Tactical Edge

At the Department of Defense (DoD), interest has grown in outfitting warfighters with handheld computing devices to support their missions in tactical and hostile environments. However, current mobile systems either provide too much information, or the data is fragmented across multiple systems. SEI researchers Soumya Simanta and Gene Cahill are working with Brad Myers and his student, Kerry Chang, at the Carnegie Mellon University (CMU) Human Computer Interaction Institute to address these problems.

Simanta explains that "data in tactical environments resides in silos and cannot be shared and tailored easily." Cahill adds, "There are many data sources and no way to integrate them quickly because software development takes place far from the tactical environment." In the time it takes a request from the field to go up the chain of command to development and certification, the original need will have gone unmet while new needs will have emerged.

With current smartphone software, users can personalize the device's appearance, but they cannot add new capabilities easily, such as creating their own filters. And vast amounts of data make customized filters important. An Army National Guard captain, discussing current challenges, concluded that "we end up with too little information because we have too much information."

SEI researchers want to give warfighters more control over accessing the right information at the right time. To address this need, Simanta, Cahill, and their colleagues are developing the Edge Mission-Oriented Tactical App Generator, or eMONTAGE, a Java-based application that operates on an Android smartphone platform. The initial focus of eMONTAGE was to enable soldiers to create a form-based app for rapid data entry directly on the phone without writing code. The current focus is to reduce data volume and to increase data relevancy. eMONTAGE enables warfighters to create context-specific filters, mash data from multiple sources, and view the results on a unified display, all without writing code. Cahill analogizes that "adding a new feature at runtime is like the difference between cooking yourself and choosing something from a menu." This capability will enable warfighters to make the best use of the data available to them.

In August 2012, Simanta and Cahill participated in activities at the U.S. Special Operations Command/Naval Postgraduate School Tactical Network Testbed at Camp Roberts, California. Both soldiers and civilians provided positive feedback. They also offered additional ideas for other environments in which eMONTAGE could be used, especially for first responders.

Simanta emphasizes that eMONTAGE "can mash geospatial data" from historical, real-time, DoD, and publically available data sources. For example, Simanta and Cahill integrated weather alerts from the National Weather Service (NWS) into the app. They used NWS event logs to extract geo-located alerts generated by the Integrated Public Warnings and Alert System and display them on a map. This demonstrated how eMONTAGE can turn raw data into useful information for smartphone users in crisis situations.

In future work, Simanta and Cahill intend to improve the app's performance and security by adding a caching mechanism, additional data sources, and standard security mechanisms. They also plan to transition this technology to collaborators in the DoD and government.

SEI researchers want to give warfighters more control over accessing the right information at the right time. To meet this challenge, the SEI's Soumya Simanta, Gene Cahill, and their colleagues are developing the Edge Mission-Oriented Tactical App Generator, or eMONTAGE, a Java-based application that operates on an Android smartphone platform.

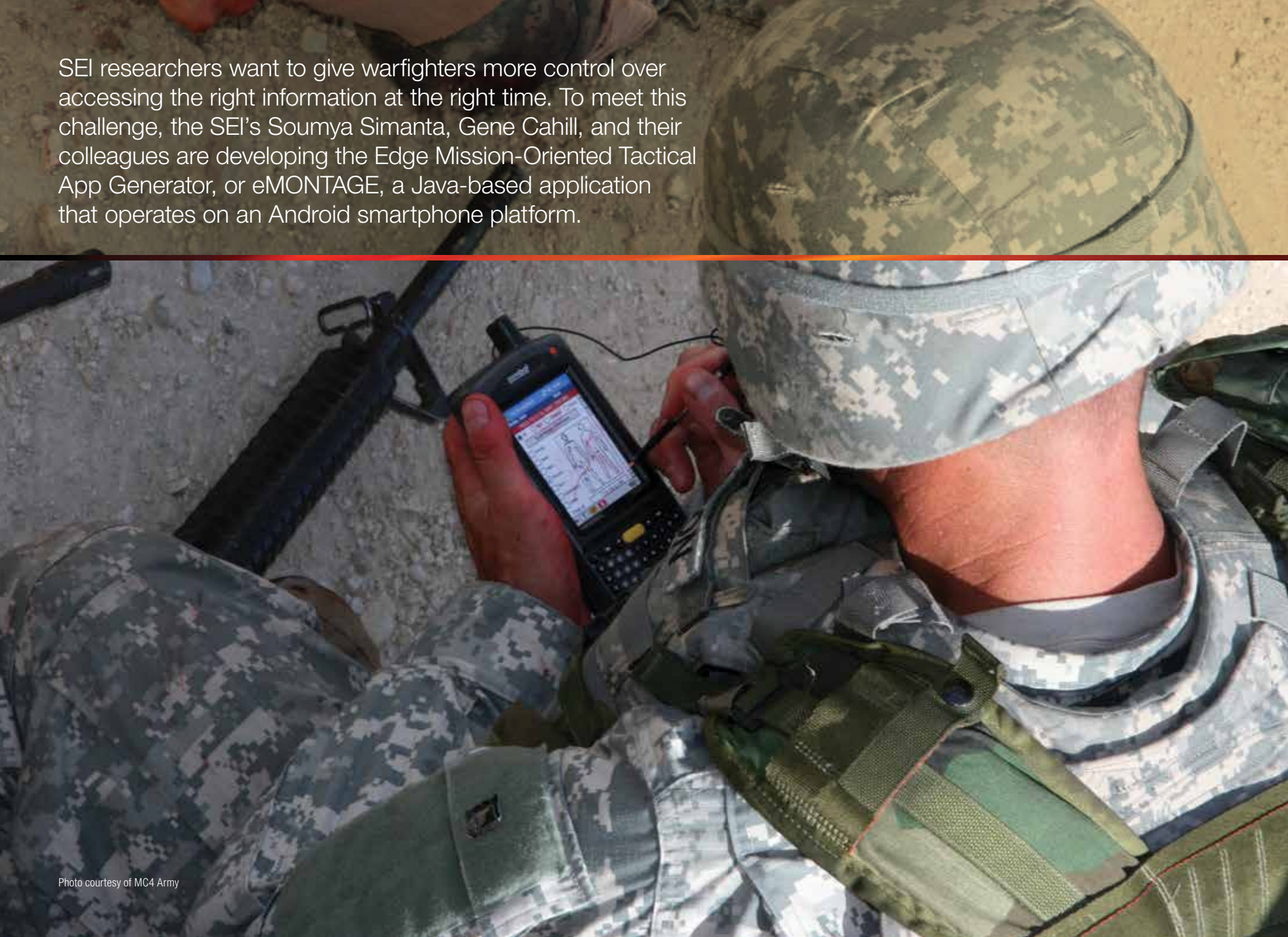


Photo courtesy of MC4 Army

SEI Helps Shape Research Agenda on Managing Technical Debt

Twenty years after noted software engineer Ward Cunningham first articulated the concept of technical debt, the problem remains a concern in the field of software engineering. Today's larger, more complex, and more interdependent systems only exacerbate the consequences of technical debt and demand more urgent efforts to address it. Experts at the SEI have been on the case, helping to drive research on managing technical debt in large-scale systems. In June, in conjunction with the International Conference on Software Engineering (ICSE), the SEI conducted its third International Workshop on Managing Technical Debt. In addition, the SEI's Robert Nord and Ipek Ozkaya, and their colleague, Philippe Kruchten from the University of British Columbia, collaborated to coedit a special issue of *IEEE Software* devoted to the topic.

Technical debt refers to the degraded quality and required rework resulting from short-term decisions made to expedite software development and delivery. Decisions that defer work in areas such as modifiability, portability, and documentation represent a kind of "loan" that allows developers to deliver on time. However, once the developers incur this debt, they become subject to "interest" charges in the form of higher long-term rework costs as time passes, customer requirements evolve, and intervening versions, perhaps carrying their own technical debt, are released. These costs may ultimately exceed the value of the original loan.

"We're researching an architecture-focused measurement framework for managing technical debt," said Robert Nord, senior member of the technical staff at the SEI. "Our work is informed by real-world examples we've gathered from the Technical Debt Workshops." The Workshop on Managing Technical Debt took place June 4, 2012. "The purpose of this third workshop," said Nord, "was to discuss managing technical debt as a part of the research agenda for the software engineering field. In particular, we focused on industry challenges for the research community in eliciting and visualizing causes of debt and creating payback strategies."

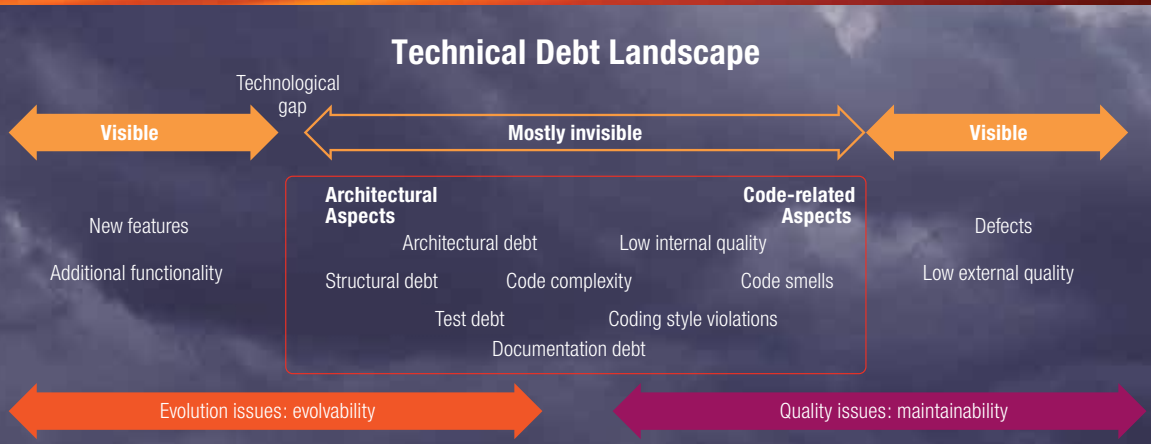
The SEI's early efforts in this area aimed to provide software engineers visibility into technical debt from strategic and architectural perspectives. "This work produced a release planning framework," said Ipek Ozkaya, a senior member of the technical staff working on technical debt management. "The release planning framework clarifies how to integrate architectural concerns with agile project management methods, such as Scrum. It also helps users relate requirements with architectural decisions. Understanding these dependencies helps software developers make informed decisions about architectural technical debt."

One major theme of the SEI's research on technical debt is identifying metrics that can be extracted from the code and module structures of software systems and using them to provide insights into architectural dependencies that impact system-wide architectural rework. By doing so, Nord, Ozkaya, and their colleagues hope to enhance software development efficiency and quality.

Ipek Ozkaya and Robert Nord

"We're researching an architecture-focused measurement framework for managing technical debt. Our work is informed by real-world examples we've gathered from the Technical Debt Workshops."

—Robert Nord



AQOS HELPS APPLICATIONS USING WIRELESS NETWORKS ADAPT IN CRITICAL FIELD MISSIONS

This past year saw continued work in the field of adaptive quality of service (AQoS), a solution that has captured the attention of the Navy Research Lab and the Army Research Lab. With ad hoc wireless networks, which are often quickly assembled in the field to support decision makers in crisis scenarios, failure is not a viable option. A delay or loss due to overwhelming bandwidth demand could contribute to mission failure.

The SEI's work in AQoS aids commanders' decision-making by enabling applications that use wireless networks to automatically, continuously, and effectively adapt to available resources when those resources are outstripped by demand. AQoS enables applications, such as messaging-, voice-, and video-based applications, to react to the network's available bandwidth capacity by reducing the load while continuing to serve mission requirements. The AQoS approach provides adaptation mechanisms that allow application performance to degrade gracefully and recover in a way that maximizes mission value.

A number of SEI researchers collaborated in 2012 to develop an algorithm, the Distributed QoS Resource Allocation Model (D-Q-RAM), to enable applications to adapt in a distributed, near-optimal manner without the need to know, estimate, or predict available network resources at any moment in time. Future work includes examining issues related to scale and determining if the algorithms maintain optimality.

The team conducts quarterly experiments at the United States Special Operations Command (USSOCOM)-Naval Post Graduate Field Experimentation Cooperative at Camp Roberts, California. These efforts serve to further their research and integrate the work with others through scenario-based exercises.

Photo: MC4 Army

RESEARCH SEEKS HARMONY BETWEEN ACQUISITION STRATEGY AND SOFTWARE ARCHITECTURE

Increasingly, major defense acquisition programs rely on software to provide substantial portions of system performance—yet software is often a minor consideration when program decisions are made. "Business and mission goals end up out of alignment with software architecture," explained Lisa Brownsword of the SEI's Acquisition Support Program. "This degrades the product, adds cost, and increases schedule risk."

Brownsword leads an SEI team exploring ways to help organizations "harmonize their acquisition strategy with their software architecture," she said.

"Complex acquisition programs have diverse sets of stakeholders whose goals and priorities may be misaligned," she said. "Operational users, combatant commanders, funding authorities, and acquisition team members often think they have the same priorities, but actually vary widely in terms of the goals and features they consider most important."

By examining the relationships among four elements (business and mission goals, acquisition strategy, quality attributes, and software and system architectures), Brownsword's team pinpoints patterns of alignment or misalignment—anti-patterns—that tend to keep the software architecture and acquisition strategy in harmony or to pull them apart.

Identifying anti-patterns, Brownsword said, is just the start of addressing the problems of misalignment. "Characterizing the general shape of an acquisition model that would avoid or minimize these anti-patterns is a next step toward developing a way to help programs avoid these anti-patterns," she said.

By identifying and deconflicting mission and business goals, acquisition strategy and software architecture will fall into closer alignment—and, in turn, result in more effective and efficient software-reliant systems.

"It's interesting work, and the potential payoff is significant," Brownsword noted. "Better management visibility and control of critical business and mission tradeoffs—program offices explicitly aligning strategy and architecture—means acquisitions are more likely to produce effective software-reliant systems."

"Better management visibility and control of critical business and mission tradeoffs—program offices explicitly aligning strategy and architecture—means acquisitions are more likely to produce effective software-reliant systems."

—Lisa Brownsword

"This architecture is scalable at a hardware and software level, and is rapidly configurable to accommodate a variety of missions."

—Mike Bandor

MODULAR OPEN SYSTEMS APPROACH TO SOFTWARE ARCHITECTURE SPEEDS SATELLITES INTO SPACE

Hundreds of satellites circle the earth every day—almost all of them are unique machines that took months or years to plan, develop, and build. But does it have to be that way? Is it possible to reduce the time to launch a new satellite to a few weeks or even days?

For the first time in the space age, the answer to that question is yes. And the SEI is helping the Department of Defense's (DoD) Operationally Responsive Space (ORS) Office make it happen.

"The SEI has worked with ORS nearly since its inception in 2007," noted the SEI's Mike Bandor. Bandor, part of the SEI's Acquisition Support Program, leads the Institute's involvement with ORS.

In 2012, the SEI helped ORS develop the first-ever modular, open systems approach (MOSA) architecture in space. "This architecture is scalable at a hardware and software level, and is rapidly configurable to accommodate a variety of missions," Bandor explained. With the MOSA architecture, every satellite need not be a "one off"—a unique, complex, single instance of a space vehicle. Indeed, one goal for ORS and MOSA is to be able to assemble and launch a satellite mission in a week's time from existing components. Another goal is to design and build new satellites for new missions in a year or less. The use of MOSA enables those types of timelines.

The SEI, Bandor said, has been working closely with the ORS Office and the prime contractors in the areas of flight software architecture, software development and maintenance strategies, information assurance, and the development of the Space Plug-and-Play Architecture (SPA) standards.

Three SEI Projects Support Data-Driven Decision Making in Software Engineering

The SEI's drive toward an empirically grounded, data-driven approach to software engineering begins with one thing: data. Data is the key element underpinning every research effort, and successful analysis turns data into insights that can influence decision making and improve performance. Three efforts are underway to create accessible, unique data resources for use by the SEI, the Department of Defense (DoD), and the larger research community.

One project aims to improve the quality and usability of the data reported to the DoD by contractors on the Software Resources Data Report (SRDR). "These reports contain a lot of unique, valuable information about large-scale development," said Dave Zubrow, chief scientist for the Software Engineering Process Management Program, "but its use has been limited by the way it's been structured and stored." Collaborating with the Air Force Cost Analysis Agency, the SEI has begun an effort to transform the information into a repository containing clean, query-able data with supporting information.

A second effort involves the creation of a repository for the data reported from teams using the Team Software Process (TSP). The data span over a decade and come from hundreds of projects. "Rarely is such detailed data collected from software development projects. While big data is a popular topic, detailed data with this level of granularity is sometimes even more important in understanding what happened in software projects and predicting future performance," said Zubrow.

A third project involves accessing data to gain insight into projects using agile methods. For this project, the SEI is collaborating with Rally Software, a company specializing in agile application lifecycle management. "We're working with Rally because agile is a widely-used method and we have a common interest in understanding what agile practices are being used, how effective they are, and the performance of projects using agile," said Zubrow. Improved access to, and analysis of, data enables empirically grounded insights that can be used to evaluate performance and establish benchmarks and heuristics.

"While big data is a popular topic, detailed data with this level of granularity is sometimes even more important in understanding what happened in software projects and predicting future performance"

— David Zubrow

Building Safety-Critical Systems

In safety-critical systems, a software error can mean serious injury or loss of life. As a result, organizations that develop critical software must comply with a growing number of government standards and regulations. A narrow focus on compliance, however, can lead to missed opportunities, according to Jim Over, manager of the SEI's Team Software Process (TSP) initiative. "While meeting these standards is a requirement, the problem is that an organization can develop a culture focused on compliance instead of measured performance and continuous improvement," said Over.

Beckman Coulter, a company that manufactures and markets biomedical testing instrument systems, tests, and supplies, began introducing TSP in 2009 as part of their effort toward what Rick Marshall describes as a push for "differentiated quality" in the marketplace. Marshall, Director of Software Engineering for Clinical Information Systems at Beckman Coulter, said, "We have successful processes in place that are compliant and yield predictable quality, but we are developing even more complex and interoperable systems requiring a higher level of certainty around quality. Our old processes just weren't scalable to the systems we wanted to build in the future."

TSP has now been deployed at seven locations in India, the United States, and Germany, with more sites planned. In three years, they have achieved 90 percent adoption across Beckman Coulter Diagnostics. According to Scott Van Eps, Staff Software Development Engineer, TSP integrated well with FDA regulations and other standards while also providing a common language among multiple groups. Projects are typically cross-site, and TSP helps everyone use the same methods for planning, scheduling, and tracking work, even if they are countries apart.

The primary benefit of using TSP, however, is the ability to measure and manage quality throughout the development process. "Quality cannot be tested in," said Over. "Trying to manage quality without numbers is just talk. What differentiates the TSP is the data-driven team quality management practices that have improved pretest yields to 99 percent or better." High maintenance costs after a release and limited visibility into what those costs would be were factors that contributed to Beckman Coulter's decision to adopt TSP. "We don't want to spend time after a release correcting newfound defects and re-issuing maintenance releases," said Marshall. "We're reaping the benefits now on some of our recent releases developed using TSP." Beckman Coulter TSP projects have demonstrated from 5 to 20 times fewer defects after release.

While Beckman Coulter's use of TSP was planned for new development, they decided to try something new in 2010: applying TSP late in the development stage to a project already in system test. A hardware and software system was being developed for hematology, and they needed to reduce defects and develop a predictable schedule for release. Working with the SEI, they identified areas of TSP that could be readily applied at this stage in the project with minimal impact to the current schedule. They developed "just in time" training to introduce TSP principles as they were needed. This effort yielded good results for the new system: 3.4 percent schedule predictability, 10 times improvements in system reliability, and satisfied customers noting no major issues after release.

These practices and results are not unique to Beckman Coulter. They apply broadly and should be of particular importance to any government or industry software-reliant system with safety-critical requirements.

"What differentiates the TSP is the data-driven team-quality management practices that have improved pre-test yields to 99 percent or better."

—James Over

Toward Guaranteed Software Quality

The average schedule overrun for an information technology project is 27 percent, while about one in six projects racks up a cost overrun of 200 percent and a schedule overrun of almost 70 percent. Extra time and money don't necessarily buy quality. Software bugs are so prevalent that they cost the United States an estimated $59.5 billion a year.

The most shocking thing about these numbers is that many people are no longer shocked to hear them. Perhaps that's why David Ratnaraj, Program Manager at Advanced Information Services, Inc. (AIS), garnered a lot of attention at a recent SEI software symposium when he presented the results of a project to modernize a computer system for a large federal government organization. The project was done on a firm, fixed-price contract (which is a contract where the buyer pays only the negotiated amount, regardless of the contractor's real cost). It was delivered four weeks ahead of schedule, met all federal security mandates, and had a defect rate of only 0.097 defects per thousand lines of code in production, meaning it was essentially defect free. This extremely low defect rate enables AIS to offer a lifetime warranty on software defects, which is almost unheard of in the industry.

Most of the questions from the audience were, predictably, related to how those results were achieved. "These are problems that the software engineering community has been trying to address since the idea of a 'software crisis' emerged in 1968," said Girish Seshagiri, Founder of AIS. When Seshagiri founded AIS in 1986, he realized the first step in fixing cost, schedule, and quality problems in his own organization was to fully understand the process he was using to develop software. To that end, AIS began implementing the Capability Maturity Model (CMM) in 1992 and has now been appraised at Capability Maturity Model Integration (CMMI) level 5. "We saw a significant decrease in schedule variation as we implemented CMM, and another large drop when we started using TSP about four years later," said Seshagiri. "We believe sincerely that level 5 is not the end, it's the beginning," he said. "Reaching level 5 means we understand our variation, a fundamental element in predicting performance, and implementing TSP gives us the consistent results we need. Now we can predict quality: we know what the defects are going to be, and where. Having detailed data is what allows us to know if we'll be able to execute a firm, fixed-price contract economically."

Seshagiri recently took his message about quality and predictability before the Senate Armed Services Committee, where he spoke about the importance of putting quality first. "In all other engineering and manufacturing activities, it is a given that having low defects reduces cost, increases market share, and improves satisfaction. Only in software production are people still asking if quality costs more," he said. Clouding the issue is the fact that the costs of acceptance testing and fixing defects found in production are not charged to development, and the person who injected the defect is not usually the person who pays to fix it. Seshagiri speculates that once the total costs of poor quality are considered, greater emphasis will placed on ensuring developers make software right in the first place and stand behind their products.

Quality

"Reaching level 5 means we understand our variation, a fundamental element in predicting performance, and implementing TSP gives us the consistent results we need. Now we can predict quality: we know what the defects are going to be, and where. Having detailed data is what allows us to know if we'll be able to execute a firm, fixed-price contract economically."

—Girish Seshagiri, Founder, Advanced Information Services, Inc.

Costs
Delays
Errors

Research Forum Examines Agile in Complex, Large-Scale Environments

In the field of software process improvement, the Capability Maturity Model Integration (CMMI) is a dominant force. For the past two decades, the SEI and its partners have built on the CMMI's foundation, laid by Watts Humphrey and other software process pioneers, refining the method and expanding its scope. But new process methods have emerged in commercial software development organizations, especially agile methods.

As part of its commitment to advance new research on software process improvement, the SEI hosted the Agile Research Forum in August 2012. The forum brought together researchers and practitioners from many countries to discuss how agile approaches can overcome the challenges of complexity, exacting regulations, and schedule pressures in large-scale development projects.

Featured speakers at the forum included Mary Ann Lapham, Ipek Ozkaya, James Over, Douglas Schmidt, Anita Carleton, and Teri Takai. Carleton, director of the SEI's Software Engineering Process Management Program, organized the event.

Lapham, senior researcher with the SEI Acquisition Support Program, examined "Agile Methods: Tools, Techniques, and Practices for the DoD Community," describing research on how to help the Department of Defense (DoD) overcome technical and cultural resistance to agile methods. Ozkaya, senior researcher in the SEI Research, Technology, and System Solutions Program, presented "Strategic Management of Architectural Technical Debt," highlighting how to spot the sources of technical debt in a project, track it, and use it to advantage.

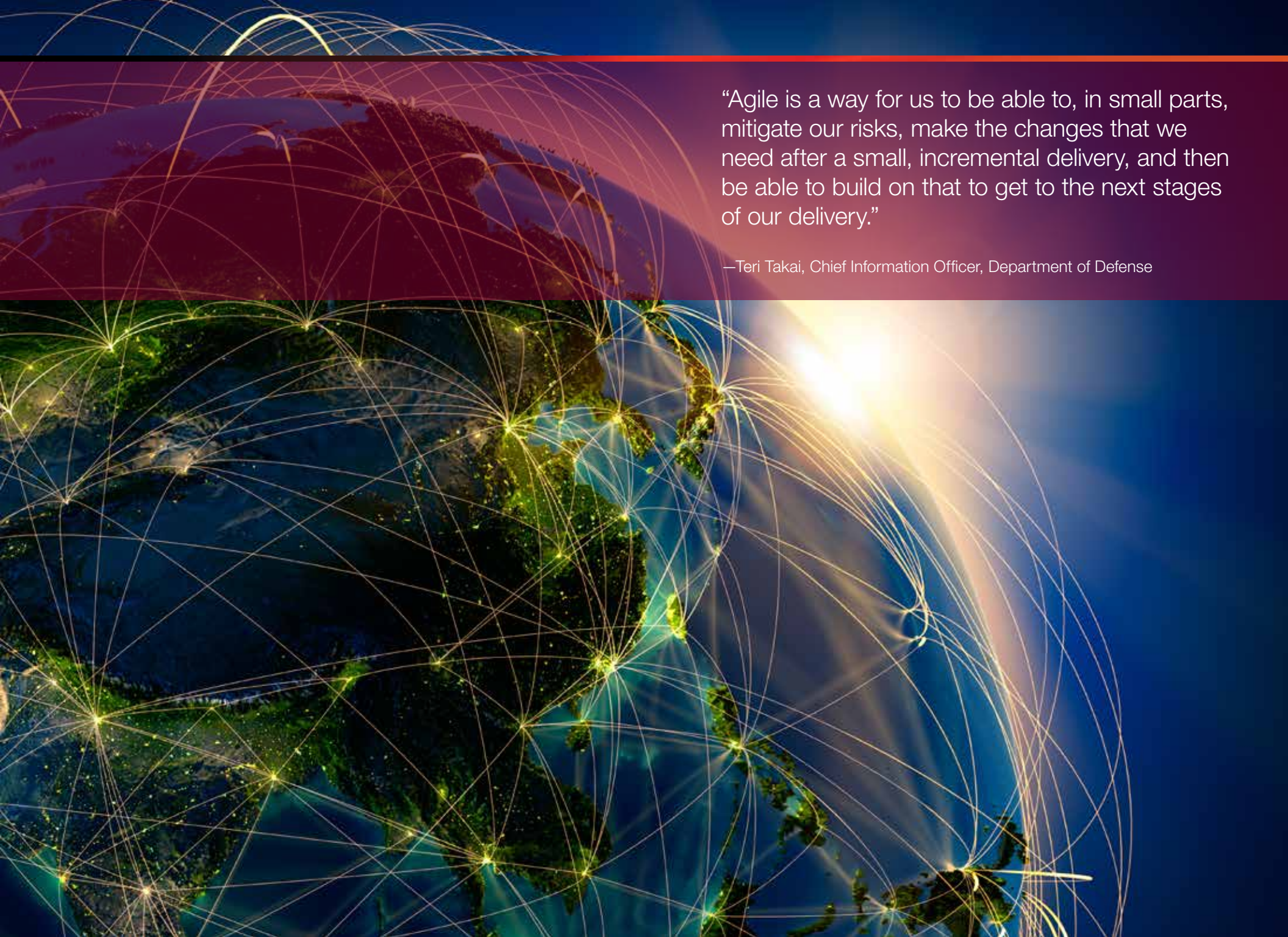
James Over, manager of the Team Software Process (TSP) Initiative in the SEI Software Engineering Process Management Program, presented "Agility and Discipline," sharing insights from research and experience in balancing agility and discipline.

Schmidt, SEI visiting scientist and associate chair of the Department of Electrical Engineering and Computer Science at Vanderbilt University, discussed "The Importance of Applying Agile Technologies to Key DoD Software Initiatives," exploring what's at stake for large-scale development organizations considering or adopting agile technologies. Schmidt, former chief technology officer for the SEI, discussed how agile methods can encourage more effective collaboration among users, developers, testers, and certifiers of common operating platform environments (COPEs) to help the DoD build integrated, interoperable, and affordable software-reliant systems more successfully.

"Much research remains to be done to optimize the ways in which software engineers apply agile methods to develop software-reliant systems in both government and industry," said Carleton. Agile methods promise to simplify software development and acquisition, which is key to reducing costs. Experts agree these methods have much to offer. For instance, in her remarks at the forum, Teri Takai, Chief Information Officer of the DoD, said, "Agile is a way for us to be able to, in small parts, mitigate our risks, make the changes that we need after a small, incremental delivery, and then be able to build on that to get to the next stages of our delivery."

Other forum presenters focused on how to resolve conflicts between traditional acquisition and agile development approaches, how to use technical debt to advantage, and how to infuse agile methods with discipline, without overloading it.

One of the key messages emerging from the forum was that, while agility in business, management, and technical dimensions is essential, it's not the only solution to the complex set of problems facing software development organizations. Additional research and engineering investment will continue to be needed to devise appropriate methods, tools, and techniques that will enable agility at scale. To help meet these objectives, the SEI is committed to sponsoring future research in agile and other process improvement methods relevant to commercial and government software organizations.



"Agile is a way for us to be able to, in small parts, mitigate our risks, make the changes that we need after a small, incremental delivery, and then be able to build on that to get to the next stages of our delivery."

—Teri Takai, Chief Information Officer, Department of Defense

ACCENTURE CITES BENEFIT OF LONG RELATIONSHIP WITH SEI IN CONGRESSIONAL TESTIMONY

The SEI and Accenture, an important SEI partner, have enjoyed a working relationship for 10 years. Accenture, a global management consulting and technology services company, employs more than 250,000 and serves clients in more than 120 countries. Accenture collaborates with its clients to help them become high-performance businesses and government organizations. And it is a long-time user of the SEI's process improvement methods.

The SEI's relationship with Accenture was highlighted in congressional testimony on August 1, 2012, by William D. Green, executive chairman of the board at Accenture and a member of the Committee on Research Universities, Board on Higher Education and Workforce Policy and Global Affairs, at the National Research Council of the National Academies. Green cited Accenture's work with the SEI as an example of a productive relationship between research universities and the private sector. Testifying before the U.S. House Subcommittee on Research and Science Education, part of the Committee on Science, Space, and Technology, Green emphasized how these collaborations between business and research universities are fueling American innovation and the creation of jobs.

"Developed by SEI, the Capability Maturity Model Integration for Development, CMMI-DEV, in particular, is one of the most used quality models in the world and is the de facto standard for software development improvement," Green testified. "Accenture was one of SEI's earliest business partners and began implementing its models with clients in the mid-1990s. Today, our partnership with SEI continues. A number of Accenture employees are certified [CMMI] appraisers and instructors, our business teams provide some client consulting related to implementation of SEI products, and we have also used the standards and models created by SEI for our own corporate benefit. Accenture is one of the largest users of the standards in the world, and we currently apply them to our largest delivery centers."

William D. Green, Executive Chairman of the Board of Accenture

Photograph courtesy of the Committee on Science, Space and Technology, United States House of Representatives.

CMMI SERVICES TO BE PROVIDED THROUGH NEW CMMI INSTITUTE

In 2012, Carnegie Mellon University formed a new institute to provide services related to the Capability Maturity Model Integration (CMMI). The new organization, the CMMI Institute, now manages all CMMI training, certification, licensing, and appraisal services as well as future model development that were previously managed by the Software Engineering Institute (SEI). The SEPG Conference Series, People Capability Maturity Model (PCMM), and the Data Management Maturity (DMM) Model are also moving to the CMMI Institute.

"Formation of a new organization to manage CMMI services allows for greater commercial amplification of the CMMI product suite," said Kirk Botula, CEO of the CMMI Institute. "We look forward to working with our network of partners to promote worldwide adoption and use of the models as a way to improve software development, acquisition, and service processes in government and industry."

The CMMI suite of products was developed at the SEI in conjunction with government and industry groups. The suite includes CMMI for Development (CMMI-DEV), CMMI for Acquisition (CMMI-ACQ), CMMI for Services (CMMI-SVC), and People CMM. The Data Management Maturity Model, developed in conjunction with the Enterprise Data Management Council and other partners, is based on CMMI.

"As a federally funded research and development center, the SEI was pleased to develop and steward the progress of the CMMI models," said Paul Nielsen, director and CEO of the SEI. "As with many research programs, though, we are even more pleased when something moves out of the research institute and into widespread adoption in practice."

The SEI will continue its broad-based research and development of software engineering and cybersecurity technologies and methods. The SEI continues to offer training for the Team Software Process, software architecture, software product lines, measurement and analysis, acquisition practices, cybersecurity, and CERT-RMM.

For more information, see the CMMI Institute website at **www.cmmiinstitute.com**.

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

The PDC 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 delivery channels, and by encouraging and recognizing individual accomplishments in various disciplines through professional certificate programs.

For more information about SEI training, visit www.sei.cmu.edu/training.

For more information about the SEI professional certificate requirements, visit www.sei.cmu.edu/training/certificates/.

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 Architecture Tradeoff Analysis Method, CERT Information Security, CERT Resilience Management Model, Service-Oriented Architecture, Smart Grid, Software Architecture, Software Engineering Measurement and Analysis, and Team Software Process.

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

In fiscal year 2012, the SEI Partner Network consisted of 448 Partner organizations.

In 2012, the functions of the SEI Partner Network moved to Clearmodel and the CMMI Institute, which are part of Carnegie Innovations, a technology commercialization enterprise and 100-percent-controlled subsidiary of Carnegie Mellon University. Please visit http://partners.clearmodel.com for current information about the Partner Network.

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 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 cosponsored in 2012 are

- FloCon 2012
- SATURN 2012
- SEPG North America 2012
- SEPG Europe 2012
- TSP Symposium 2012

For more information about SEI conferences and events, visit www.sei.cmu.edu/events.

SEI Certification Program
The SEI Certification Program grants professional certifications to individuals who have the skills, abilities, and knowledge needed for various disciplines. SEI certifications are based on SEI research and published bodies of knowledge, and are assessed using industry-leading methods.

The SEI now has certification programs in, Architecture Tradeoff and Analysis Method, Information and Network Security, Resilience Management, Smart Grid Management, Software Architecture, Software Engineering Measurement and Analysis, Team Software Process, and Personal Software Process.

In 2012, certain administrative support functions for SEI Certifications moved to Clearmodel, Inc., but the SEI continues to evaluate and approve certification applications and grant certification credentials.

For more information, visit www.sei.cmu.edu/certification.

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.

From left to right:
Kevin Fall Deputy Director, Research, Chief Technology Officer
Paul D. Nielsen Director and Chief Executive Officer
Robert Behler Deputy Director and Chief Operating Officer

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

Matt Gaston
Director, SEI Innovation Center

Peter Menniti
Director, Financial and Business Services

Linda Northrop
Director, Research, Technology, and System Solutions

Richard Pethia
Director, Networked Systems Survivability

David Thompson
Director, Information Technology and Security

Mary Catherine Ward
Acting Director, Acquisition Support Program

Articles

Albarghouthi, A.; Gurfinkel, A. & Chechik, M. "From Under-Approximations to Over-Approximations and Back." *Proceedings of 18th International Conference on Tools and Algorithms for the Construction and Analysis of Systems (TACAS'2012)* (April 2012).

Albarghouthi, A.; Li, Y.; Gurfinkel, A. & Chechik, M. "UFO: A Framework for Abstraction- and Interpolation-Based Software Verification." *Proceedings of the 24th International Conference on Computer Aided Verification (CAV 2012)* (July 2012).

Allen, Julia. "Measures for Managing Operational Resilience." *EDPACS: The EDP Audit, Control, and Security Newsletter* (December 2011).

Andersson, Bjorn; Chaki, Sagar; de Niz, Dionisio; Dougherty, Brian; Kegley, Russell & White, Jules. "Non-Preemptive Scheduling with History-Dependent Execution Time." *Proceedings of the 24th Euromicro Conference on Real-Time Systems (ECRTS)* (July 2012).

Bass, Len & Nord, Robert L. "Understanding the Context of Architecture Evaluation Methods." *Proceedings of the Joint 10th Working IEEE/IFIP Conference on Software Architecture (WICSA) and the 6th European Conference on Software Architecture (ECSA)* (August 2012).

Chaki, Sagar; Gurfinkel, Arie & Strichman, Ofer. "Regression Verification for Multi-Threaded Programs." *Proceedings of the 13th International Conference on Verification, Model Checking, and Abstract Interpretation* (January 2012).

Claycomb, W.R. "Insider Threats to Cloud Computing: Directions for New Research Challenges," *Proceedings of IEEE COMPSAC 2012* (July 2012).

Cowley, Jennifer & Radford-Davenport, Julie. "Qualitative Differences Between a Focus Group and Online Forum Hosting a Usability Design Review: A Case Study." *Proceedings of the 53rd Annual Human Factors and Ergonomics Society Annual Meeting* (September 2011).

de Niz, Dionisio; Wrage, Lutz; Storer, Nathaniel; Rowe, Anthony & Rajkumar, Ragunathan. "Utility-Based Resource Overbooking For Cyber-Physical Systems." *Proceedings of the ACM/IEEE Third International Conference on Cyber-Physical Systems* (April 2012).

Ferguson, Robert; Goldenson, Dennis; McCurley, James; Stoddard, Robert & Zubrow, David. "An Innovative Approach to Quantifying Uncertainty in Early Lifecycle Cost Estimation." *DACS Journal of Software Technology* (February 2012).

Franklin, Jason; Chaki, Sagar; Datta, Anupam; Mccune, Jonathan & Vasudevan, Amit. "Parametric Verification of Address Space Separation." *Proceedings of the First Conference on Principles of Security and Trust (POST'12), part of ETAPS 2012* (April 2012).

Goldenson, Dennis. "Using Predictive Modeling in Software Development: Results from the Field," (December 2011). blog.sei.cmu.edu/post.cfm/using-predictive-modeling-in-software-development-results-from-the-field

Gurfinkel, Arie. "WHALE: An Interpolation-Based Algorithm for Inter-Procedural Verification." *Proceedings of the 13th International Conference on Verification, Model Checking, and Abstract Interpretation (VMCAI)* (January 2012).

Gurfinkel, Arie; Chechik, Marsha & Albarghouthi, Aws. "Craig Interpretation." *Proceedings of the 19th International Static Analysis Symposium (SAS 2012)* (September 2012).

Hanley, Michael; Moore, Andrew & Mundie, David. "A Pattern for Increased Monitoring of Departing Insiders." *Proceedings of the 2012 Conference on Pattern Languages of Programs* (October 2011).

Hansen, J.; Hissam, S.; Plakosh, D. & Wrage, L. "Adaptive Quality of Service in Mobile Ad Hoc Wireless Networks." *Proceedings of the 2012 IEEE Wireless Communications and Networking Conference (WCNC 2012)* (April 2012).

Highfill, Darren; Bass, Len; Ivers, James; Lipson, Howard; Allgood, Glenn; Kuruganti, Teja & Nutaro, Jim. "The Witch Doctor vs. the Engineer—Why Believe Either One?" *Proceedings of the SCADA Security Scientific Symposium* (January 2012).

Mead, Nancy. "Need Software Engineers to Develop Secure Software? Put it in Your Job Descriptions!" *Cutter IT Journal* (November 2011).

Mead, Nancy; Allen, Julia & Hawthorne, Beth. "Transitioning from Software to Software Assurance" *IEEE Computer, Build Your Career: Hot Sectors* (April 2012).

Mead, Nancy & Hilburn, Tom. "The Growing Demand for Software Assurance." *IEEE Build Your Career.*

Moore, Andrew & Mundie, David. "A Pattern for Trust Trap Mitigation." *Proceedings of the 2012 Conference on Pattern Languages of Programs* (October 2011).

Moreno, Gabriel & de Niz, Dionisio. "An Optimal Real-Time Voltage and Frequency Scaling for Uniform Multiprocessors." *The Proceedings of the IEEE International Conference on Embedded and Real-Time Computing Systems and Applications (RTCSA 2012)* (August 2012).

Nichols, William. "Plan for Success, Model the Cost of Quality," *Software Quality Professional*, *14*, 2 (March 2012).

Nord, Robert L.; Ozkaya, Ipek; Kruchten, Philippe & Gonzalez, Marco. "In Search of a Metric for Managing Architectural Technical Debt." *Proceedings of the Joint 10th Working IEEE/IFIP Conference on Software Architecture (WICSA) & 6th European Conference on Software Architecture (ECSA)* (August 2012).

Nord, Robert L.; Ozkaya, Ipek & Sangwan, Raghvinder S. "Making Architecture Visible to Improve Flow Management in Lean Software Development." *IEEE Software Special Issue on Lean Software Development* (September/October 2012).

Zubrow, Dave. "High Maturity Software Engineering Measurement and Analysis," (February 2012). blog.sei.cmu.edu/post.cfm/high-maturity-software-engineering-measurement-and-analysis

Books & Book Chapters

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

Cappelli, Dawn M.; Moore, Andrew P. & Trzeciak, Randall F. *The CERT Guide to Insider Threats: How to Prevent, Detect, and Respond to Information Technology Crimes (Theft, Sabotage, Fraud)*. Addison-Wesley Professional, 2012 (ISBN-10: 0321812573).

Fieler, Peter F. & Gluch, David P. *Model-Based Engineering with AADL: An Introduction to the SAE Architecture Analysis & Design Language*. Addison-Wesley Professional, 2012 (ISBN-10: 0-321-88894-4).

Stoddard, Bob. "FMECA Applied to Software Development." *Design for Reliability*. Edited by Dev G. Raheja & Louis J. Gullo, Wiley, 2012 (ISBN: 978-1-1183-1003-8).

Keynotes

Blanchette, Stephen Jr. "Perspectives on Service-Oriented Architectures," NATO Consultation, Command and Control Agency (NC3A) Service Oriented Architecture Technology Watch Day (February 2012).

Cappelli, Dawn. "Adapting to Changing Risk Environments— How Resilient is My Organization?" *Australian Defense Magazine* Cyber Security Summit (May 2102).

Carleton, Anita. "The Future: How Good Are We at Predicting It?" 2012 SEPG Europe 2012 (June 2012).

Carleton, Anita & Jordan, Angel. "30 Years of Process Improvement and Counting: A Retrospective of What's New," SEPG Europe 2012 (June 2012).

Claycomb, William. "An Overview of the Insider Threat Center at CERT," International Carnahan Conference on Security Technology (October 2011).

Claycomb, William. "Risk Mitigation Strategies: Lessons Learned from Actual Insider Attacks," CollaborateCom (October 2011).

Ferguson, Robert & Stoddard, Robert. "Quantifying Uncertainty in Early Lifecycle Cost Estimates (QUELCE) Estimation Method," SEPG North America (March 2012).

Lewis, Grace. "Cloud Computing: Implications for Software Architecture, Software Process and Latin America," SEPG Latin America (November 2011).

Montelibano, Joji. "Insider Threat Mitigation Strategies," Cyber Ark (October 2011).

Moore, Andrew. "What You Need to Know About Insider Theft of Intellectual Property (IP)," Lockheed Information Assurance Conference (June 2012).

Northrop, Linda. "The Impact of Scale: Ultra-Large-Scale Systems Six Years After the Study," St. Andrews 2012 Workshop on LSCITS/ULSS (September 14, 2012).

Northrop, Linda. "The Impact of Scale," Open System Software (OSS) Conference (October 2011).

Ruefle, Robin. "CSIRT Development: Past, Present, and Future," Latin American and Caribbean TLD Association First Brazilian CSIRT Forum (March 2012).

Seacord, Robert. "The Source Code Analysis Laboratory (SCALe)," Blackberry Security Summit (June 2012).

Zubrow, David. "Engineering for Success, the Future is Now," Improving Systems and Software Engineering Conference (ISSEC 2012) (August 2012).

Zubrow, David. "Meeting Future Market Demands: Process Improvement Today and Tomorrow," SEPG Asia-Pacific 2012 (September 2012).

Podcasts & Webinars

Allen, Julia; Butkovic, Matthew & Lafky, Deborah. "Considering Security and Privacy in the Move to Electronic Health Records," (December 2011). www.cert.org/podcast/show/20111220lafky.html

Allen, Julia & Crabb, Greg. "US Postal Inspection Service Use of CERT-RMM," (August 2012). www.cert.org/podcast/show/20120821crabb.html

Allen, Julia & Curtis, Pamela. "Measuring Operational Resilience," (October 2011). www.cert.org/podcast/show/20111004allen.html

Allen, Julia & Allen, Dennis. "How to Become a Cyber Warrior," (July 2012). www.cert.org/podcast/show/20120131allen2.html

Allen, Julia & Young, Lisa. "Insights from the First CERT Resilience Management Model Users Group," (July 2012). www.cert.org/podcast/show/20120717young.html

Bachman, Felix. "Architecting Software the SEI Way—Architecture Evaluation: A Tool for Designing Systems That Meet Users' Needs," (April 2012). www.sei.cmu.edu/library/abstracts/webinars/Architecture-Evaluation-A-Tool-for-Designing-Systems-That-Meet-Users-Needs.cfm

Cappelli, Dawn & Trzeciak, Randy. "Insider Threat: Three Faces of Risk," (September 2012). www.bankinfosecurity.com/webinars/insider-threat-3-faces-risk-w-296

Chick, Timothy A. & Miluk, Gene. "Getting the Performance You Need from Processes That Work: The CMMI Accelerated Improvement Method," (March 2012). www.sei.cmu.edu/library/abstracts/webinars/Getting-the-performance-you-need-from-processes-that-work-The-CMMI-Accelerated-Improvement-Method.cfm

Klein, John. "Architecting Software the SEI Way—Analyzing and Evaluating Enterprise Architectures," (April 2012). www.sei.cmu.edu/library/abstracts/webinars/Analyzing-and-Evaluating-Enterprise-Architectures.cfm

Konrad, Mike. "Using the CMMI to Improve Your Software Development Capability," (January 2011). cmmiinstitute.com/resource/capability-maturity-model-integration-cmmi-v1-3-and-architecture-centric-engineering-webinar/

Lapham, Mary Ann. "SEI Agile Research Forum: Agile Methods: Agile Methods—Tools, Techniques, and Practices for the DoD Community," (August 2012). www.sei.cmu.edu/library/abstracts/webinars/Tools-Techniques-and-Practices-for-the-DoD-Community.cfm

McCurley, James & Stoddard, Robert. "QUELCE: Quantifying Uncertainty in Early Lifecycle Cost Estimation," (November 2012). www.sei.cmu.edu/podcasts/index.cfm?getRecord=BD60D188-AC6E-714B-10F420705985285B&wtPodcast=QuantifyingUncertaintyinEarlyLifecycleCostEstimation

McHale, J.D. "A Brief Survey of the Team Software Process," (January 2012). www.sei.cmu.edu/library/abstracts/webinars/A-Brief-Survey-of-the-Team-Software-Process.cfm

Montelibano, Joji; Ross, Ron & Allen, Julia. "NIST Catalog of Security and Privacy Controls, Including Insider Threat," (April 2012). www.cert.org/podcast/show/20120424ross.html

Over, James. "Agility and Discipline," (April 2012). www.sei.cmu.edu/library/abstracts/webinars/Agility-and-Discipline.cfm

Ozkaya, Ipek. "SEI Agile Research Forum: Strategic Management of Architectural Technical Debt," (August 2012). www.sei.cmu.edu/library/abstracts/webinars/Strategic-Management-of-Architectural-Technical-Debt.cfm

Schmidt, Douglas. "SEI Agile Research Forum: The Importance of Applying Agile Technologies to Key DoD Software Initiatives," (August 2012). www.sei.cmu.edu/library/abstracts/webinars/The-Importance-of-Applying-Agile-Technologies-to-Key-DoD-Software-Initiatives.cfm

Stoddard, Robert & McCurley, James. "Quantifying Uncertainty in Early Lifecycle Cost Estimation," (November 2012). www.sei.cmu.edu/podcasts/index.cfm?getRecord=BD60D188-AC6E-714B-10F420705985285B&wtPodcast=QuantifyingUncertaintyinEarlyLifecycleCostEstimation

White, David. "The California Energy Commission and SGMM: Partners for a Future Vision of Smart Grid," (March 2012). www.sei.cmu.edu/library/abstracts/webinars/The-California-Energy-Commission-and-SGMM.cfm

Wojcik, Rob. "Architecting Software the SEI Way—Software Architecture Fundamentals: Technical, Business, and Social Influences," (April 2012). www.sei.cmu.edu/library/abstracts/webinars/Software-Architecture-Fundamentals-Technical-Business-and-Social-Influences-2.cfm

Zubrow, David. "The Importance of Data Quality," (October 2012). www.sei.cmu.edu/podcasts/index.cfm?getRecord=2D20D3AC-9E21-AC54-D796FCD84E67A288&wtPodcast=TheImportanceofDataQuality

Workshops and Tutorials

Cappelli, Dawn & King, Chris. "Insider Threat Workshop." Adelaide, Australia (May 2012).

Cappelli, Dawn; Claycomb, William & Moore, Andrew. "Insider Threat Challenge Problem Workshop." Arlington, VA (February 2012).

Cappelli, Dawn; Claycomb, William; Moore, Andrew & Trzeciak, Randy. "Insider Threat: Cyber and Behavioral Aspects Symposium." Pittsburgh, PA (June 2012).

Carleton, Anita. "Software Engineering Process Management (SEPM) Update." Minneapolis, MN (October 2011).

Chick, Timothy and Miluk, Gene. "*Navigating your Quality Journey: How to Engineer Exceptional Quality Software."* Pittsburgh, PA (September 2012).

Claycomb, William. "Insider Threats to Cloud Computing: Directions for New Research Challenges." Izmir, Turkey (July 2012).

Ellison, Robert. "Supply Chain Risk Management." Federal Virtual Training Environment (September 2012).

Ferguson, Robert. Presentation the Practical Systems and Software Measurement User Group Conference (July 2012).

Ferguson, Robert & Stoddard, Robert. "Quantifying Uncertainty in Early Lifecycle Cost Estimates (QUELCE) Estimation Method." Albuquerque, NM (March 2012).

Glover, Margaret Tanner; Zubrow, Dave; and O'Toole, Patrick. "Meet the International Improvement League: Fighting for Good Processes Everywhere." Albuquerque, NM (March 2012).

Jones, Larry & Konrad, Mike. "Architecture: Why your CMMI V1.3 implementation is incomplete without it! " Denver, CO (November 2011).

Keaton, David. "Secure Coding." Linthicum, MD (April 2012).

Kruchten, Philippe; Nord, Robert L. & Ozkaya, Ipek. "Strategic Management of Technical Debt." Zurich, Switzerland (June 2012).

Martin, Dave & Miluk, Gene. "CMMI Workshop." Minneapolis, MN (October 2011).

McCurley, James & Ferguson, Robert. "An Approach to Quantifying Uncertainty in Early Lifecycle Cost Estimation." Portsmouth, VA (August 2012).

McHale, James & Kasunic, Mark. "Exploring TSP: An Introduction." Pittsburgh, PA (September 2012).

Miluk, Gene & McHale, James. "Introduction to the Accelerated Improvement Method (AIM)." Albuquerque, NM (March 2012).

Montgomery, Austin & White, David. "SGMM Stakeholder Panel." Washington, DC (October 2011).

Ruefle, Robin. "Evaluating CSIRTs." Sao Paulo, Brazil (March 2012).

Ruefle, Robin & Mundie, David. "Advanced Incident Handling." Panama City, Panama (April 2012).

Seacord, Robert. "Challenge Problem Technical Workshop on Secure Coding for SCADA Devices." Richland, WA (May 2012).

Seacord, Robert. "Integral Security." Pittsburgh, PA (November 2011).

Seacord, Robert. "Secure Coding." Sofia, Bulgaria (August 2012).

Seacord, Robert. "TEAM/SOAR-Lite Software Assurance (SwA) Workshop." Alexandria, VA (July 2012).

Seacord, Robert & Sutherland, Dean. "Don't be Pwned: A Very Short Course on Secure Programming in Java." San Francisco, CA (October 2011).

Stoddard, Robert W. "An Overview of the SEI QUELCE Cost Estimation Method." Salt Lake City, UT (April 2012).

Svoboda, David. "Secure Coding." Helsinki, Finland (April 2012).

Svoboda, David. "Secure Coding." Krakow, Poland (April 2012).

Trzeciak, Randy & Zajicek, Mark. "Insider Threat Workshop." Columbia, SC (April 2012).

Trzeciak, Randy & Griffin, Russ. "Insider Threat Workshop." Army War College, Carlisle, PA (June 2012).

White, David & Mullaney, Julia. "Smart Grid Maturity Model Leadership Workshop." Pittsburgh, PA (January 2012).

Woody, Carol & Mead, Nancy. "Software Assurance Methods in Support of Cyber Security." McLean, VA (December 2011).

Young, Lisa. "CERT-RMM Tutorial." Albuquerque, NM (March 2012).

Zajicek, Mark & Mundie, David. "Fundamentals of Incident Handling." Pittsburgh, PA (February 2012).

Zajicek, Mark. "Fundamentals of Incident Handling—Train the Trainer." Pittsburgh, PA (April 2012).

Zajicek, Mark. "Creating and Managing CSIRTs—Train the Trainer." Pittsburgh, PA (June 2012)

Zubrow, David & Ferguson, Robert. "QUELCE: Quantifying Uncertainty in Early Lifecycle Cost Estimation." Los Angeles, CA (November 2011).

SEI Reports (Unlimited Distribution) Published October 1, 2011–September 30, 2012

Alberts, Christopher J. & Dorofee, Audrey J. *Mission Risk Diagnostic (MRD) Method Description.* www.sei.cmu.edu/library/abstracts/reports/12tn005.cfm

Alberts, Christopher J.; Allen, Julia H. & Stoddard, Robert W. *Risk-Based Measurement and Analysis: Application to Software Security.* www.sei.cmu.edu/library/abstracts/reports/12tn004.cfm

Allen, Julia H. & Young, Lisa R. *Report from the First CERT-RMM Users Group Workshop Series.* www.sei.cmu.edu/library/abstracts/reports/12tn008.cfm

Allen, Julia H.; Curtis, Pamela D. & Parker Gates, Linda. *Using Defined Processes as a Context for Resilience Measures.* www.sei.cmu.edu/library/abstracts/reports/11tn029.cfm

Bellomo, Stephany. *A Closer Look at 804: A Summary of Considerations for DoD Program Managers.* www.sei.cmu.edu/library/abstracts/reports/11sr015.cfm

Campbell, Grady; Levinson, Harry & Librizzi, Richard. *An Acquisition Perspective on Product Evaluation.* www.sei.cmu.edu/library/abstracts/reports/11tn007.cfm

Chaki, Sagar; Creel, Rita C.; Davenport, Jeff; Kinney, Mike; McCormick, Benjamin & Popeck, Mary. *Standards-Based Automated Remediation: A Remediation Manager Reference.* www.sei.cmu.edu/library/abstracts/reports/11sr016.cfm

Cummings, Adam; Lewellen, Todd; McIntire, David; Moore, Andrew P. & Trzeciak, Randall F. *Insider Threat Study: Illicit Cyber Activity Involving Fraud in the U.S. Financial Services Sector.* www.sei.cmu.edu/library/abstracts/reports/12sr004.cfm

de Niz, Dionisio; Feiler, Peter H.; Gluch, David P & Wrage, Lutz. *A Virtual Upgrade Validation Method for Software-Reliant Systems.* www.sei.cmu.edu/library/abstracts/reports/12tr005.cfm

Elm, Joseph & Goldenson, Dennis. *The Business Case for Systems Engineering Study: Results of the Systems Engineering Effectiveness Survey.* www.sei.cmu.edu/library/abstracts/reports/12sr009.cfm

Feiler, Peter H.; Seibel, Joe & Wrage, Lutz. *What's New in V2 of the Architecture Analysis & Design Language Standard?* www.sei.cmu.edu/library/abstracts/reports/11sr011.cfm

Ferguson, Robert; Goldenson, Dennis; McCurley, James; Stoddard, Robert W.; Zubrow, David & Anderson, Debra. *Quantifying Uncertainty in Early Lifecycle Cost Estimation (QUELCE).* www.sei.cmu.edu/library/abstracts/reports/11tr026.cfm

Fisher, David. *Principles of Trust for Embedded Systems.* www.sei.cmu.edu/library/abstracts/reports/12tn007.cfm

Hanley, Michael & Montelibano, Joji. *Insider Threat Control: Using Centralized Logging to Detect Data Exfiltration Near Insider Termination.* www.sei.cmu.edu/library/abstracts/reports/11tn024.cfm

Householder, Allen D. & Foote, Jonathan M. *Probability-Based Parameter Selection for Black-Box Fuzz Testing.* www.sei.cmu.edu/library/abstracts/reports/12tn019.cfm

Kasunic, Mark; McCurley, James; Goldenson, Dennis & Zubrow, David. *An Investigation of Techniques for Detecting Data Anomalies in Earned Value Management Data.* www.sei.cmu.edu/library/abstracts/reports/11tr027.cfm

King, Christopher. *Spotlight On: Malicious Insiders and Organized Crime Activity.* www.sei.cmu.edu/library/abstracts/reports/12tn001.cfm

Lapham, Mary Ann; Miller, Suzanne; Adams, Lorraine; Brown, Nanette; Hackemack, Bart; Hammons, Charles (Bud); Levine, Linda & Schenker, Alfred. *Agile Methods: Selected DoD Management and Acquisition Concerns.* www.sei.cmu.edu/library/abstracts/reports/11tn002.cfm

Moore, Andrew P.; Hanley, Michael & Mundie, Dave. *A Pattern for Increased Monitoring for Intellectual Property Theft by Departing Insiders.* www.sei.cmu.edu/library/abstracts/reports/12tr008.cfm

Montelibano, Joji & Moore, Andrew P. *Insider Threat Security Reference Architecture.* www.sei.cmu.edu/library/abstracts/reports/12tr007.cfm

Morrow, Tim; Seacord, Robert; Bergey, John & Miller, Philip. *Supporting the Use of CERT Secure Coding Standards in DoD Acquisitions.* www.sei.cmu.edu/library/abstracts/reports/12tn016.cfm

Nichols, William R. *Results of SEI Line-Funded Exploratory New Starts Projects.* www.sei.cmu.edu/library/abstracts/reports/12tr004.cfm

Novak, William E; Moore, Andrew P. & Alberts, Christopher J. *The Evolution of a Science Project: A Preliminary System Dynamics Model of a Recurring Software-Reliant Acquisition Behavior.* www.sei.cmu.edu/library/abstracts/reports/12tr001.cfm

Novakouski, Marc; Lewis, Grace; Anderson, William & Davenport, Jeff. *Best Practices for Artifact Versioning in Service-Oriented Systems.* www.sei.cmu.edu/library/abstracts/reports/11tn009.cfm

Novakouski, Marc & Lewis, Grace. *Interoperability in the e-Government Context.* www.sei.cmu.edu/library/abstracts/reports/11tn014.cfm

Partridge, Kevin G. & Young, Lisa R. *CERT® Resilience Management Model (CERT®-RMM) V1.1: NIST Special Publication Crosswalk Version 1.* www.sei.cmu.edu/library/abstracts/reports/11tn028.cfm

Partridge, Kevin G. & Young, Lisa R. *CERT® Resilience Management Model (RMM) v1.1: Code of Practice Crosswalk Commercial Version 1.1.* www.sei.cmu.edu/library/abstracts/reports/11tn012.cfm

Resilient Enterprise Management Team. *CERT® Resilience Management Model Capability Appraisal Method (CAM) Version 1.1.* www.sei.cmu.edu/library/abstracts/reports/11tr020.cfm

Seacord, Robert C.; Dormann, Will; McCurley, James; Miller, Philip; Stoddard, Robert W.; Svoboda, David & Welch, Jefferson. *Source Code Analysis Laboratory (SCALe).* www.sei.cmu.edu/library/abstracts/reports/12tn013.cfm

Stoddard, Robert, et al. *Results of SEI Line-Funded Exploratory New Starts Projects.* www.sei.cmu.edu/library/abstracts/reports/12tr004.cfm

Whisnant, Austin & Faber, Sid. *Network Profiling Using Flow.* www.sei.cmu.edu/library/abstracts/reports/12tr006.cfm

SEI STAFF AND OTHER CONTRIBUTORS

AS OF SEPTEMBER 30, 2012

Full-Time & Part-Time Staff

Lisa Abel
John James Ackley
Lorraine J. Adams
Steve Ader
Laura Aguera
Cecilia Albert
Christopher J. Alberts
Michael J. Albrethsen
Jared C. Allar
Dennis M. Allen
Julia H. Allen
Noelle K. Allon
Amanda Alvarez
Rogelio G. Alvillar
Kathryn M. Ambrose-Sereno
Kelly R. Anderson
Laura Anderson
Richard C. Anderson
William B. Anderson
Bjorn Andersson
Archie D. Andrews
John F. Antonucci
Jeffrey Jules Apolis
Leena Arora
Christopher A. Atwood
Felix Herbert Bachmann
Marie A. Baker
Karen A. Balistreri
Vincent F. Balistreri
Jeffrey Balmert
Ronald M. Bandes
Michael Bandor
Richard E. Barbour
Michelle Barker
Hollen L. Barmer
Jeffrey J. Basista
Roger A. Beard
Dwight S. Beaver
Stephen R. Beck
Robert F. Behler
Habiba Belguedj
Stephany Bellomo
Klaus Bellon
Jonathan F. Bender
Brian D. Benestelli
Kathleen E. Bennett
John K. Bergey
Anna M. Berta
James Besterci
Robert Beveridge
Philip Bianco
Stephanie L. Bianco
David Biber
Daniel R. Bidwa
Darlene R. Bigos
Adrienne N. Bishop
Bethany M. Blackhurst
Stacie A. Blakley
Stephen Blanchette
Deen Blash
Jeffrey L. Boleng
Elaine Bolster
Elizabeth W. Borza
Joshua J. Bowen
Randall R. Bowser
Andrew D. Boyd
Diane I. Bradley
John R. Bramer
Kara Branby
Pamela A. Brandon
Heidi A. Brayer
Rex E. Brinker
Rita M. Briston
Rhonda M. Brown
Lisa L. Brownsword
C D. Burton
Matthew J. Butkovic
Tamara L. Butler
Palma Buttles-Valdez
Nickolas S. Byers
Gene M. Cahill
Anthony F. Calabrese
Rachel L. Callison
Kimberley S. Campbell
Linda M. Campbell
Linda L. Canon
Peter S. Capell
Dawn M. Cappelli
Richard A. Caralli
Anita D. Carleton
Cassandra L. Carricato
Ryan M. Casey
William Casey
Angela L. Castellano
Yolanda Castellano
James J. Cebula
Anthony M. Cebzanov
Sagar J. Chaki
Gary J. Chastek
Mary Jo Chelosky
Timothy A. Chick
Leslie R. Chovan
Mary Beth Chrissis
Natalie Chronister
Matthew T. Churilla
Jason W. Clark
Kathleen Clarke
William R. Claycomb
Matthew F. Coates
Cory F. Cohen
Julie B. Cohen
Sanford (Sholom) G. Cohen
Constantine A. Cois
Mary Lou Cole
James J. Conley
Anne M. Connell
Carol L. Connelly
John R. Connelly
James P. Conrad
Robert D. Conway
Christine M. Cooney
Stephen P. Cooney
Rebecca Cooper
Russell A. Cooper
Patricia A. Copelin
Daniel L. Costa
Randy Crawford
Rita C. Creel
Lucy M. Crocker
Larry J. Crowe
Stephanie D. Crowe
Michael E. Crowley
Natalie A. Cruz
Adam B. Cummings
Sally Cunningham
Pamela Curtis
Steven R. Custer
Tenai J. Cutting
Jerome Czerwinski
Rebecca A. D'acunto
Roman Danyliw
Amanda Darcy
Rosemary J. Darr
Jeffrey H. Davenport
John Dayton
Dionisio De Niz Villasenor
Gina C. Decola
Edward H. Deets
Grant W. Deffenbaugh
Nathan L. Dell
Kareem Demian
Matthew J. Desantis
Edward Desautels
Aaron M. Detwiler
Jill Diorio
John V. Diricco
Robert M. Ditmore
Mary C. Dixon
Linda Dolphin
Carol A. Dominick
George D. Doney
Patrick J. Donohoe
William A. Dormann
Audrey J. Dorofee
James C. Douglass
Joan Preston Downing
Margie Ann Drazba
Michael W. Duggan
Catherine A. Duncan
Evelyn Duncan
Madelaine Dusseau
Ladonna R. Dutton
John Dwyer
Karin Chen Dwyer
James R. Edmondson
Danielle L. Edwards
Eileen A. Eicheldinger
Robin N. Eisenhart
Robert Ellison
Joseph P. Elm
Linda M. Elmer
Harold Ennulat
Lover E. Epps
Alan T. Evans
Felicia Evans
Sidney L. Faber
Michele E. Falce
Robert Fantazier
Kimberly Farrah
Matthew A. Fazekas
Maureen E. Fechik
Jeffrey Federoff
Peter H. Feiler
Robert W. Ferguson
Aimee Filippi
Amy Finkbeiner
Francis E. Finley
Donald G. Firesmith
Kodiak Firesmith
William L. Fithen
Robert W. Floodeen
Lori Flynn
Jonathan M. Foote
Justin W. Forbes
John T. Foreman
Eileen C. Forrester
Kunta Fossett
Summer Fowler
Tracey E. Fox
Jonathan J. Frederick
David C. French
Michelle C. Fried
Richard I. Friedberg
Jennifer R. Fritsch
Brent R. Frye
Michael J. Gagliardi
Brian W. Gardiner
Matthew Gaston
Linda Parker Gates
Jeffrey Gennari
Robert George
Joseph A. Giampapa
Ryan M. Gindhart
Dennis R. Goldenson
Carla A. Grandillo-Spotts
Michael D. Greenwood
David E. Gregg
Lora K. Gress
Russell W. Griffin
Phillip A. Groce
Charlene C. Gross
Jon L. Gross
Jacqueline Grubbs
Rajasekhar Gudapati
Arie Gurfinkel
Rotem Guttman
David A. Guzik
Shannon R. Haas
Barton L. Hackemack
Nancy L. Hags
John T. Haller
William R. Halpin
Jeffrey Hamed
Joshua A. Hammerstein
Charles B. Hammons
Michael Hanley
Jeffery Hansen
Stephen D. Hardesty
Erin Harper
Gibbie Lu Hart
Jeffrey S. Havrilla
John J. Hawrylak
Eric J. Hayes
William S. Hayes
Matthew Heckathorn
Jacquelyn J. Henderson
Sharon Henley
Christopher Herr
Donald K. Hess
Charles K. Hines
Scott A. Hissam
Barbara J. Hoerr
Bryon J. Holdt
Lorraine M. Hollabaugh
Charles Holland
Andrew Hoover
Daniel P. Horvath
Allen Householder
John W. Huber
John J. Hudak
Clifford C. Huff
Lyndsi Hughes
Alexa Huth
Carly L. Huth
Jennifer L. Hykes
Christopher Inacio
Terry Ireland
James Ivers
Vanessa B. Jackson
Carol A. Jarosz
Michael Jehn
Zachary R. Jensen
George M. Jones
Lawrence G. Jones
Jacob M. Joseph
Patricia Junker
Matthew H. Kaar
Stephen Kalinowski
Derrick H. Karimi
Rachel A. Kartch
Mark D. Kasunic
Harry P. Kaye
David Keaton
Kristi L. Keeler
Tracey A. Kelly
Robert C. Kemerer
Brent Kennedy
Jennifer Kent
Carolyn M. Kernan
Suellen M. Kiger
Christopher King
Kimberly D. King-Cortazzo
John R. Klein
Mark H. Klein
Stacy L. Klein
Mark Klepach
Dan J. Klinedinst
Georgeann L. Knorr
Andrew J. Kompanek
Michael D. Konrad
Keith Korzec
John J. Kostuch
Paul Krystosek
Robert E. Kubiak
Amy L. Kunkle
David S. Kyle
Michael L. Lambert
Robert J. Lang
Debra J. Lange
Mary Ann Lapham
Frank Latino
Alyssa Le Sage
Bernadette Ledwich
Harry L. Levinson
Todd B. Lewellen
Darrell C. Lewis
Grace A. Lewis
Michele G. Ley
Alena M. Leybovich
Amy J. Leyland
Joshua B. Lindauer
Martin M. Lindner
Howard F. Lipson
Murray R. Little
Baozhu H. Liu
Joanne F. Lohuis
Gregory Longo
Melissa Ludwick
Richard W. Lynch
Marlene T. Macdonald
Rudolph T. Maceyko
Brian A. Mack
Lisa M. Makowski
Constantine J. Mamakos
Yitzhak H. Mandelbaum
Arthur A. Manion
Jay Marchetti
Attilio A. Marini
Gail Markis
Tamara L. Marshall-Keim
Theodore F. Marz
Lisa A. Masciantonio
Laura L. Mashione
Stephen M. Masters
Kelly B. Matrazzo
Troy P. Mattern
Joseph P. Matthews
Roxanne Matthews
Barbara A. Mattis
Jeffrey A. Mattson
Christopher J. May
Joseph Mayes
John J. Mcallister
Jason D. Mccormick
James Mccurley
Kathleen M. McDonald
Patricia McDonald
Shane P. McGraw
James D. McHale
David McIntire
Bernadette McLaughlin
Michael McLendon
Joseph A. McLeod

Jason R. Mcnatt
Deborah S. McPherson
William K. McSteen
Nancy R. Mead
Andrew O. Mellinger
Peter J. Menniti
Thomas J. Merendino
Samuel A. Merrell
Jennifer C. Mersich
Leigh B. Metcalf
Bryce L. Meyer
Toby J. Meyer
Bertram C. Meyers
Amy Miller
Gerald Miller
Suzanne M. Miller
Eugene E. Miluk
Marion V. Moeser
Soumyo Moitra
Elizabeth A. Monaco
Juan M. Montelibano
Austin P. Montgomery
Andrew P. Moore
Darlene V. Moore
Jose Morales
Damon Morda
Gabriel A. Moreno
John F. Morley
Edwin J. Morris
Timothy B. Morrow
Anna Mosesso
David A. Mundie
Robert S. Murawski
David Murphy
Michael P. Murray
Paul J. Murray
Mark Musolino
Lynne Naelitz
Melissa S. Neely
Cynthia L. Nesta
Gail L. Newton
John O. Nicholas
William R Nichols
Alex Nicoll
Kenneth Nidiffer
Paul D. Nielsen
Crisanne C. Nolan
Richard A. Nolan
Robert Nord
Mika North
Linda M. Northrop
William E. Novak
Marc R. Novakouski
Kevin Nowicki
Ray Y. Obenza
Patricia A. Oberndorf
Matthew O'Hanlon
Sharon R. Oliver
Michael F. Orlando
Brittney Osikowicz
Kristofer M. Ostergard
James W. Over
Ipek Ozkaya
Mariann Palestra
Timothy Palko
Kathryn C. Palmquist
M. Steven Palmquist
Amanda Parente
Allison M. Parshall
Kevin G. Partridge
Nicole M. Pavetti
Carmal Payne
David J. Pekular
Kelwyn O. Pender
Brenda A. Penderville
Samuel Perl
Sharon K. Perry
Richard D. Pethia
David M. Phillips
Dewanne M. Phillips
Janet R. Philpot
Daniel Pipitone
Patrick Place
Daniel Plakosh
Alicia N. Poling
William Pollak
Marsha M. Pomeroy-Huff
Mary E. Popeck
Douglass E. Post
Jerome J. Pottmeyer
John M. Prevost
Sean P. Provident
Kara M. Quinto
Traci M. Radzyniak
Angela Raible
James C. Ralston
Eric L. Rankin
Donald M. Ranta
Adam W. Rathbun
Adam Rauf
Frank J. Redner
Aaron K. Reffett
Colleen A. Regan
David Reinoehl
Janet Rex
Clifford E. Rhoades
Mary Ellen Rich
Nathaniel J. Richmond
John E. Robert
Terry W. Roberts
Stacy L. Rodgers
Lawrence R. Rogers
James D. Root
Steven W. Rosemergy
Robert Rosenstein
Sheila L. Rosenthal
Dominic A. Ross
Christian Roylo
Bradley P. Rubbo
Daniel J. Ruef
Robin M. Ruefle
Paul Ruggiero
Kristopher Rush
Mary Lou Russo
Mary Lynn Russo
Charles J. Ryan
Venkatavijaya
Samanthapudi
Thomas M. Sammons
Charmaine C. Sample
Geoffrey T. Sanders
Concetta R. Sapienza
Emily E. Sarneso
Vijay S. Sarvepalli
Jeffrey A. Savinda
Thomas P. Scanlon
Alfred R. Schenker
David A. Scherb
Robert B. Schiela
Andrew L. Schlackman
Steven Scholnick
Patricia L. Schreiber
James N. Schubert
Kenneth Schultz
Giuseppe Sciulli
Tina Sciullo-Schade
Philip A. Scolieri
David Scott
Shirley Scott
William S. Scully
Robert C. Seacord
Joseph Seibel
James S. Semler
Gregory E. Shannon
Ryan S. Shaw
Sharon L. Shaw
Aaron R. Shelmire
David J. Shepard
Nataliya Shevchenko
Timothy J. Shimeall
Rita M. Shoemaker
Linda E. Shooer
William P. Shore
Sandra L. Shrum
George J. Silowash
Soumya Simanta
Matthew P. Sisk
Lisa D. Sittler
Carol A. Sledge
Michelle A. Slusser
James Smith
Kenneth L. Smith
Lenny D. Smith
Timur D. Snoke
Tara R. Sparacino
Debra A. Spear
James Spencer
Derrick Spooner
Jonathan M. Spring
Bryan J. Springer
Alexander Stall
Stephen B. Stancliff
Lauren M. Stanko
Jonathan D. Steele
Katie J. Steiner
Lizann Stelmach
Julie D. Stephenson
James F. Stevens
Robert Stoddard
Michael Stone
Edward R. Stoner
Elizabeth M. Straitiff
Jeremy R. Strozer
Gregory A. Such
Siobhan P. Sullivan
Dean F. Sutherland
David Svoboda
Lucille R. Tambellini
Joseph A. Tammariello
Christopher Taschner
Brady Tello
Geoffrey P. Terrell
Michael Theis
Marcia J. Theoret
Jeffrey Thieret
Kimberly E. Thiers
Alisa M. Thomas
Mark Thomas
William R. Thomas
David K. Thompson
Michele A. Tomasic
Barbara J. Tomchik
Carolyn Tomko
Brian M. Torbich
Troy Townsend
Susan J. Trankocy
Helen L. Trautman
Donovan Truitt
Randall F. Trzeciak
Barbara Tyson
David E. Ulicne
Jeanette Urbanek
Vijay Sai Vadlamudi
Michelle A. Valdez
Christine Van Tol
Mary Van Tyne
Kevin Vargo
Kay L. Vinay
Alexander Volynkin
Cal F. Waits
Todd O. Waits
Dawann J. Wallace
Kurt C. Wallnau
Cynthia E. Walpole
Pennie B. Walters
Mary C. Ward
George W. Warnagiris
David A. Warren
Andrea L. Wasick
Rhiannon L. Weaver
Charles B. Weinstock
Jefferson P. Welch
Rosslyn G. Wemyss
Eric B. Werner
James T. Wessel
Austin Whisnant
Barbara-Jane White
David W. White
Joseph E. Wickless
Amanda Wiehagen
Emerson R. Wiley
Pamela J. Williams
William R. Wilson
Craig J. Wink
Brian D. Wisniewski
Robert M. Wojcik
William G. Wood
Carol S. Woody
Kathryn Palermo Worthy
Lutz Wrage
Evan C. Wright
Michael A. Wright
Joseph Yankel
Hasan Yasar
Jamie L. Yoder
Lisa R. Young
Rawdon R. Young
Cat B. Zaccardi
Mark T. Zajicek
Marianne Zebrowski
John Zekany
Xiaobo Zhou
Aaron J. Zitkovich
David Zubrow
Michael J. Zuccher

Other Contributors

Drew Allison
Chigani Amine
Joseph Batman
John Benito
Jorge Boria
Pablo Breuer
Michael Bridges
Nanette Brown
Yuanfang Cai
Robert Cannon
James Carlini
David Carney
Jeffrey Carpenter
Sandra Cepeda
Peter Chen
Brad Clark
Samuel Clements
Hunter Dailey
Noopur Davis
Charles DiFatta
Catherine Dodge
Brian Dougherty
Kieran Doyle
Larry Druffel
Matthew Falzon
Jack Ferguson
Richard Forno
Derek Gabbard
Hillel Glazer
David Gluch
Jeffrey Hansen
Ray Jones
Roderick Jones
Frederick Kazman
Ronald Kohl
Brian Larson
Derek Lee
Mary Lynn
Robert McFeeley
John McGregor
Nader Mehravari
Paulo Merson
Sally Miller
Thomas Miller
Judah Mogilensky
Kevin Moore
James Nash
So Norimatsu
Said Nurhan
Chris O'Brien
Heather Oppenheimer
Patrick O'Toole
Manuel Pais
Malcolm Patrick
Theresa Payton
Neil Peterson
Donn Philpot
Jeffrey Pinkckard
Adam Porter
Greg Porter
Terry Rout
Daniel Roy
Raghvinder Sangwan
Kevin Schaaff
Douglas C. Schmidt
Barry Schrimsher
Lee Scott
Lui Sha
Eric Shaw
Donald Sheehan
Larry Silverman
Judith Stafford
Kevin Sullivan
Peter Sullivan
Agapi Svolou
Scott Tilley
Brett Tjaden
Angela Tuffley
Ricardo Valerdi
Giuseppe Valetto
Kenneth VanWyk
Daniel Wall
Charles Wallen
Christopher White
Allen Willett

Affiliates

Yoshiro Akiyama
Johnny Dale Childs
Michael Clement
Chris Geary
Bonnie Hammer
Paul Kimmerly
Lisa Ming
Jose Arturo Mora-Soto
Richard Murphy
Jose Ortiz
MaryLynn Penn
Pascal Rabbath
William Schambura
Martin Sebor
Noriaki Suzuki
Amit Trivedi
Diego Vallespir

The *SEI Year in Review* is produced by SEI Corporate Communications

Manager, Corporate Communications
Janet Rex

Manager, Public Relations
Richard Lynch

Manager, Technical Communications
William Thomas

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

Design
Klaus Bellon

Illustration
Kurt Hess
Todd Loizes

Digital Production
Melissa Neely

Photography
Tim Kaulen, Photography and Graphic Services, Mellon Institute

Production
Joshua Bowen
David Gregg

Web Design
Maureen Fechik
Jeffrey Federoff

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.

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**

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.

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