Software Solutions Symposium 2017

March 20–23, 2017

Struggles at the Frontiers: Persistent Pursuit of Software Assurance in the Development and Sustainment of Defense Systems

Dr. Kenneth E. Nidiffer

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

Copyright 2017 Carnegie Mellon University

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

Software Enabled Systems are Today's Strategic Resource

*Dr. Bill Scherlis**

"Software is the building material for modern society"

Manual Labor

Water

Steam

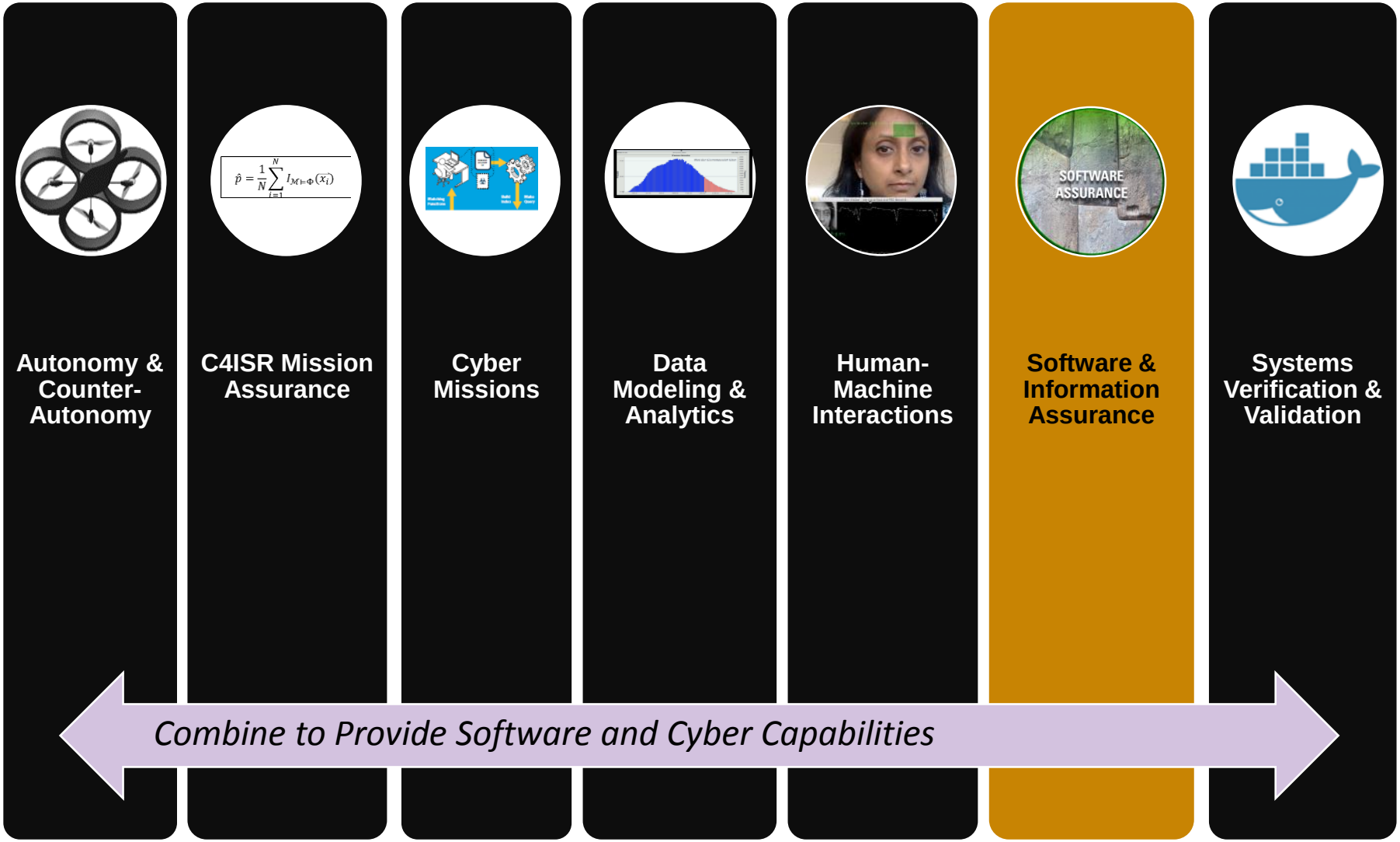
Oil

Software

Increasing globalization

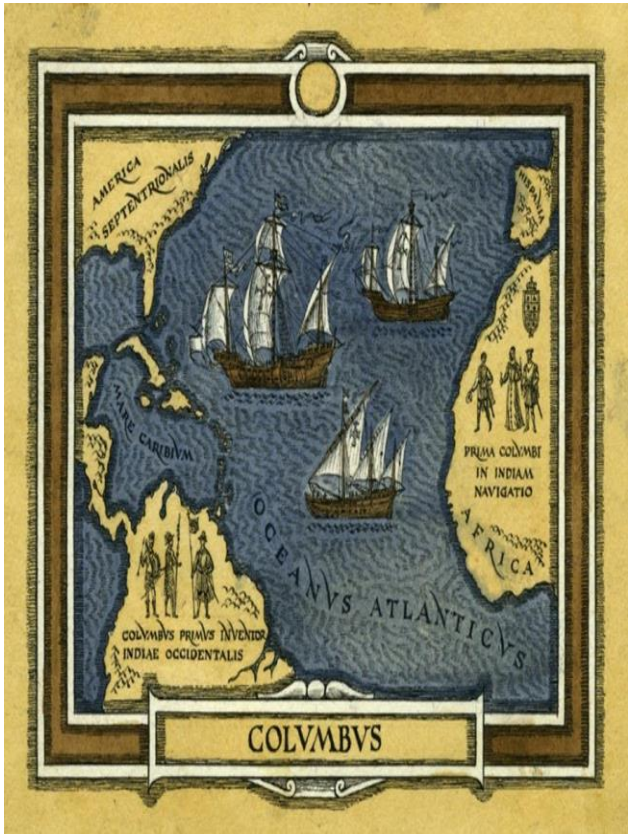
Source: SEI

SEI Works in Several Core Technical Areas



Context

- **Definition*:** The level of confidence that software functions as intended and is free of vulnerabilities, either intentionally or unintentionally designed or inserted as part of the software throughout the life cycle.
- **Perspective:** Persistent pursuit of software quality assurance is a constant struggle
- **Future:** Software enabled systems underpin the cyber environment, enabling explorations into new frontiers



Source: SEI

*Source: DoDI 5200.44 Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN), and 2013 NDAA S933

Software Assurance is a Constant Purpose, and Software-Enabled Systems are Moving Targets

- Constant purpose
  - Software assurance provides the required level of confidence that software functions as intended (and no more) and is free of vulnerabilities, either intentionally or unintentionally designed or inserted in software, throughout the lifecycle*
- Moving target
  - The changing and expanding role that software plays in cyberspace means that the development of software-enabled systems must continue to evolve while we pursue software quality

*Source: DoDI 5200.44 Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN), and 2013 NDAA S933

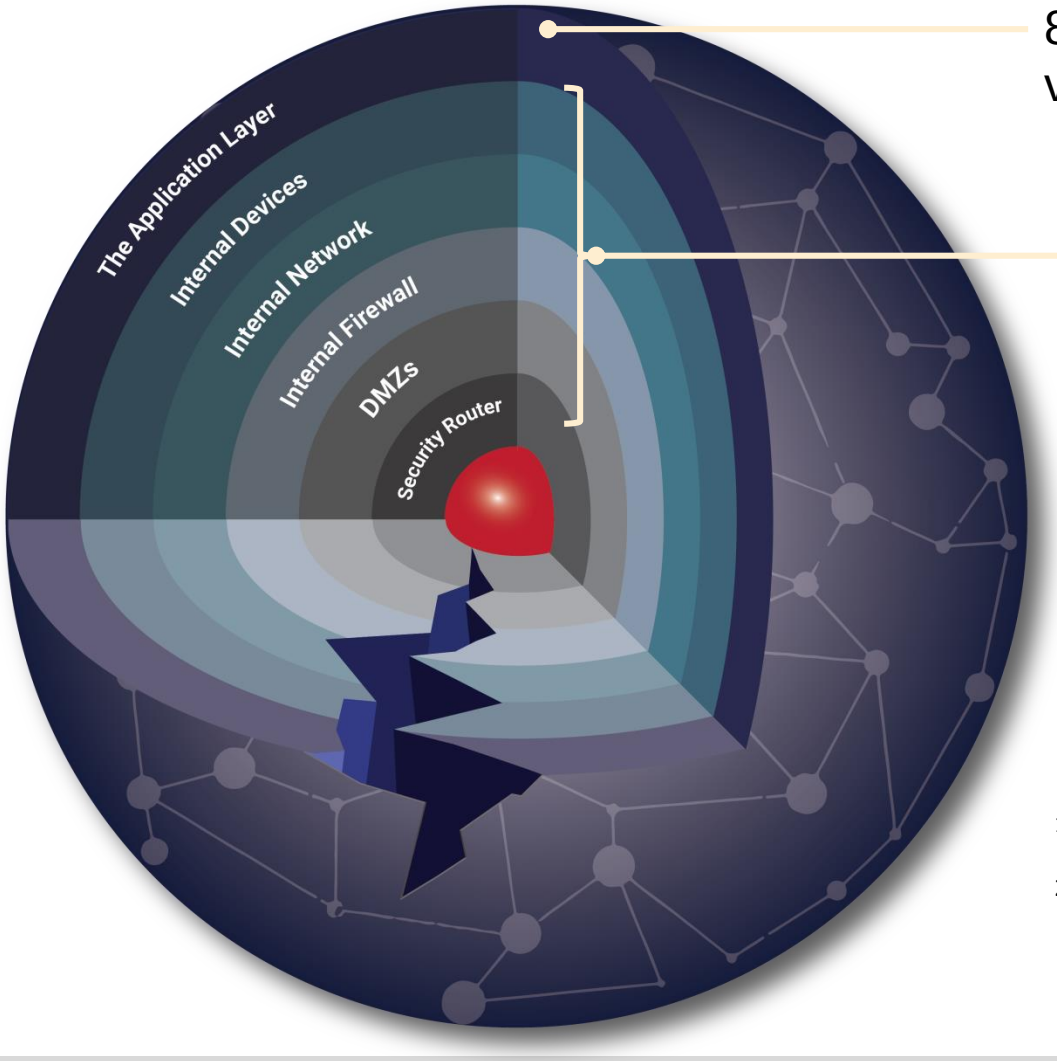
Software Assurance Struggles at the Frontiers

1. Increasing complexity of software assurance
2. Satisfying unique operational mission and business needs
3. Solving the SDLC* software tool chasm
4. Addressing limited spectrum availability
5. Handling the expanding code base
6. Understanding attack patterns, vulnerabilities, and weaknesses
7. Increasing vulnerabilities
8. Designing-in software quality over the lifecycle
9. Reducing technical debt
10. Working in the infancy of software engineering discipline

* SDLC: System Development Life Cycle

Increasing Complexity of Software Assurance

First Line of Defense in Software Assurance is the Application (Software) Layer



84% of breaches exploit vulnerabilities in the Application[1]

Yet, funding for IT defense vs. software assurance is 23-to-1[2]

1. Clark, Tim, *Most cyber Attacks Occur from this Common Vulnerability,* Forbes. 03-10-2015
2. Feiman, Joseph, *Maverick Research: Stop Protecting Your Apps; It's Time for Apps to Protect Themselves,* Gartner. 09-25-2014. G00269825

SEI Technical Themes

SEI Technologies Address DoD Software Assurance Challenges

In the broad sense as defined by the DoD challenges and underscored by the SEI Technical Insight.

Focus Areas:

- the behavior as built: architecture evaluation, code analysis, security patterns, etc.
- the behavior during evolution: system monitoring and self-adaptation, etc.
- the affordability: cost estimation, sustainment work, etc.
- the quality: defect modeling, architectural fault modeling, requirements engineering, etc.
- the mission success: acquisition support, acquisition dynamics, acquisition and architecture alignment, etc.

Satisfying Unique Operational Mission and Business Needs

Practical Answers for a Complicated World – Intelligent Integrated Solutions

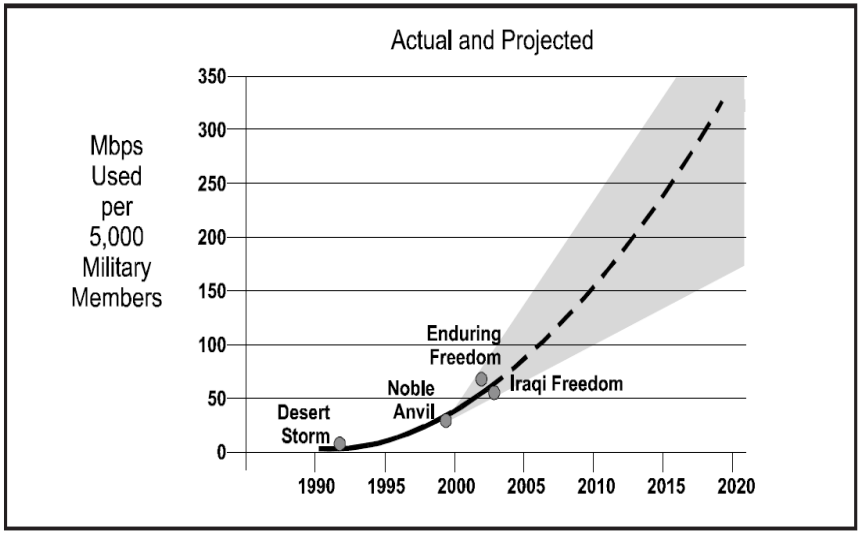
Source: SEI

Addressing Limited Spectrum Availability

Spectrum-based Technologies - Key to DoD Mission and Commercial Business Needs

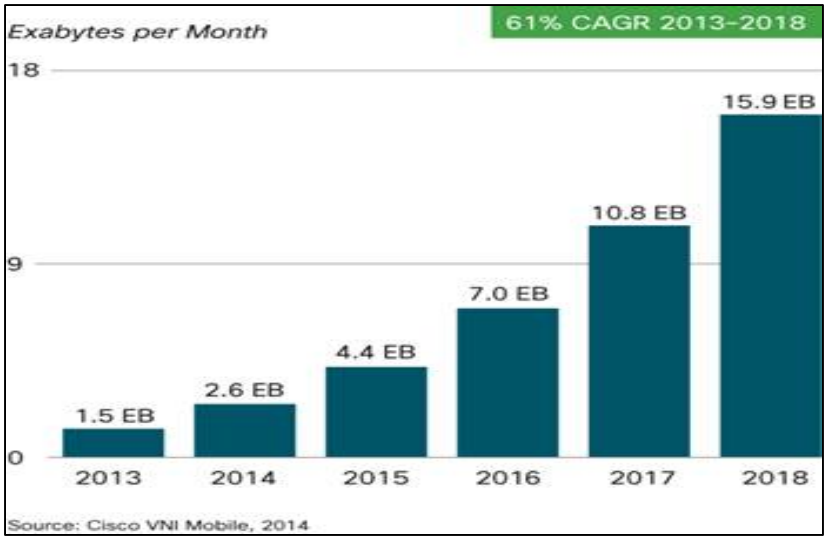
DoD Mission

- Increasing spectrum needs



Commercial Business

- Increasing spectrum needs



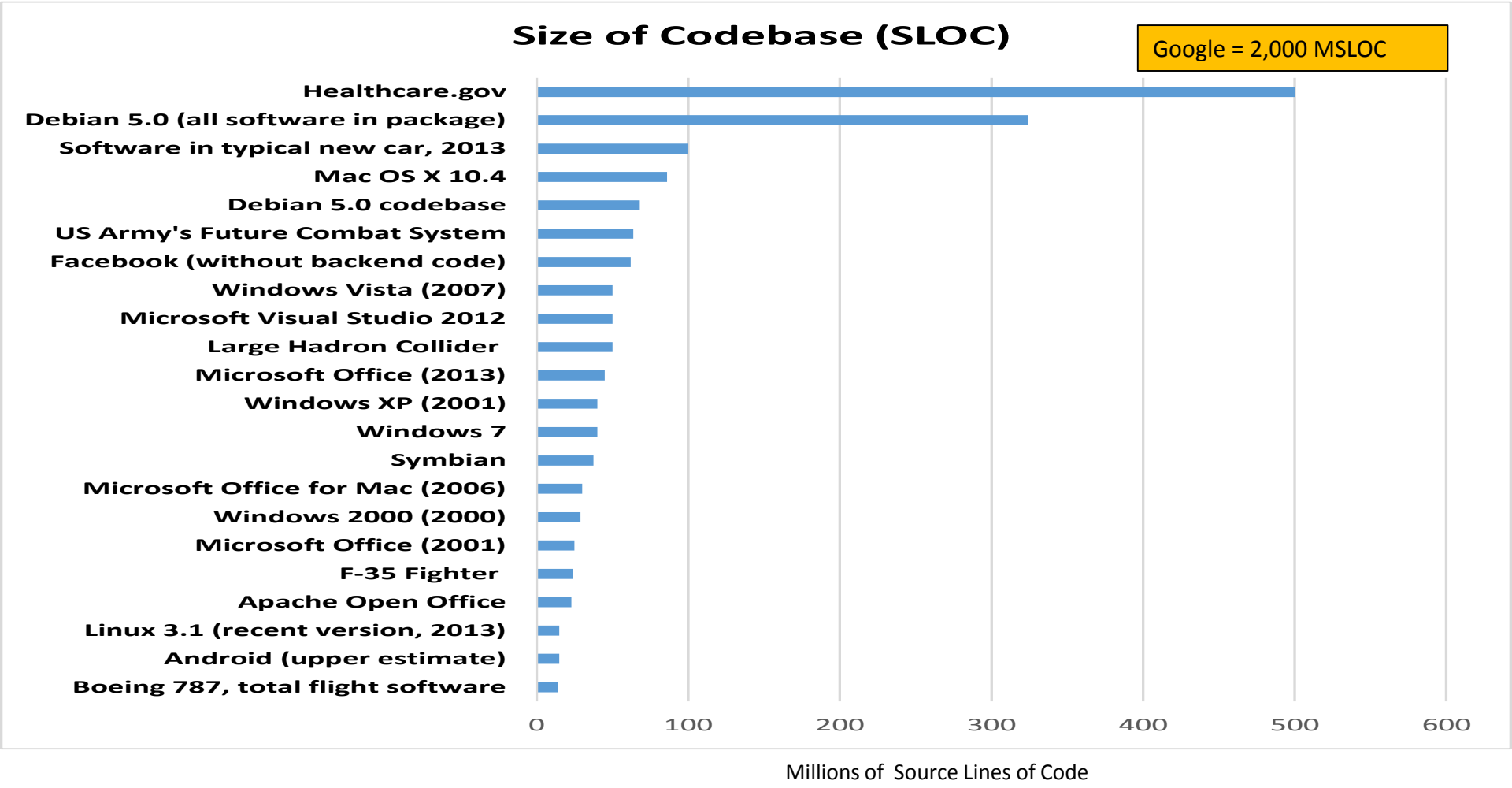
Exploding requirements for information and mobility!

CAGR = compound annual growth rate

Source: Kenneth R. Turner, Dep. Director, Spectrum Policy and International Engagements, DoD Chief Information Officer

Handling the Expanding Code Base

Software Is Dramatically Expanding with Limited Natural Governance



Source: David McCandless, Information is Beautiful, 21 September 2016 web retrieval

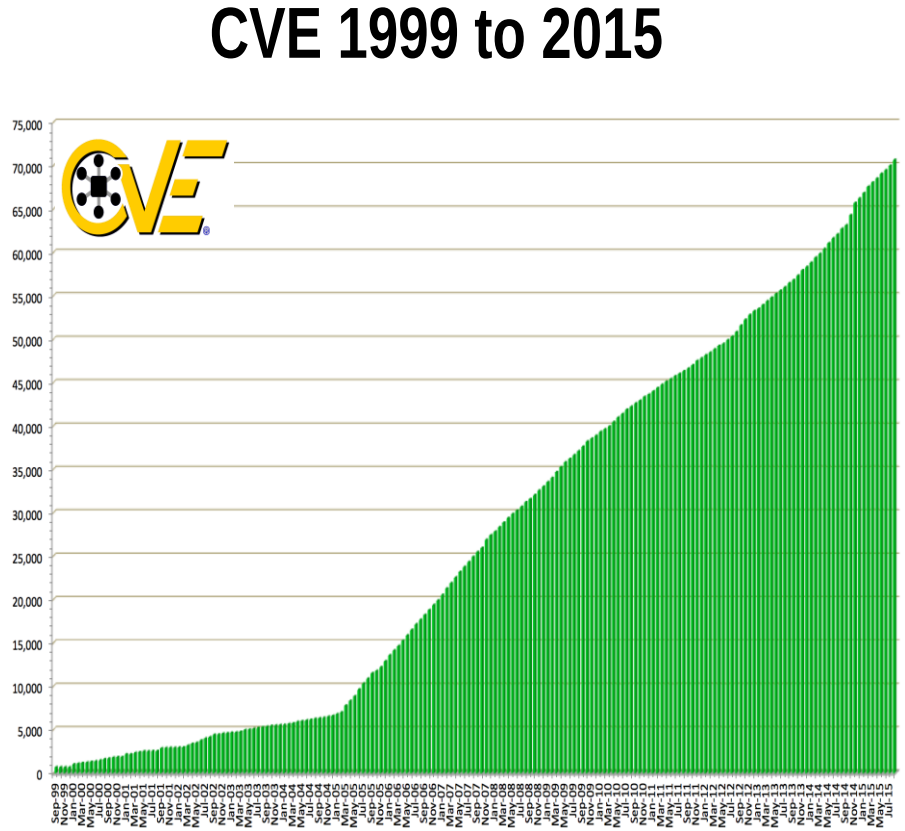
Understanding Attack Patterns, Vulnerabilities, and Weaknesses

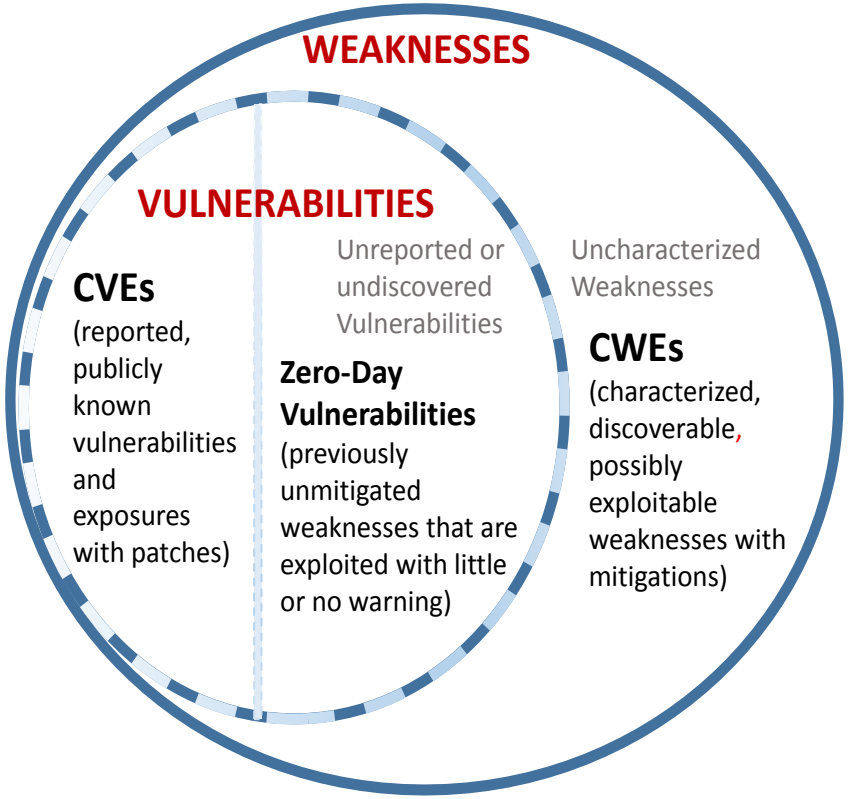
Source: Bob Martin, MITRE

- **"Actions"** include architecture choices; design choices; added security functions, activities, and processes; physical decomposition choices; static and dynamic code assessments; design reviews; dynamic testing; and pen testing.
- Vulnerability is the intersection of three elements: a system susceptibility or flaw, attacker access to the flaw, and attacker capability to exploit the flaw.

Increasing Vulnerabilities

Reported Common Vulnerabilities and Exposures (CVE)

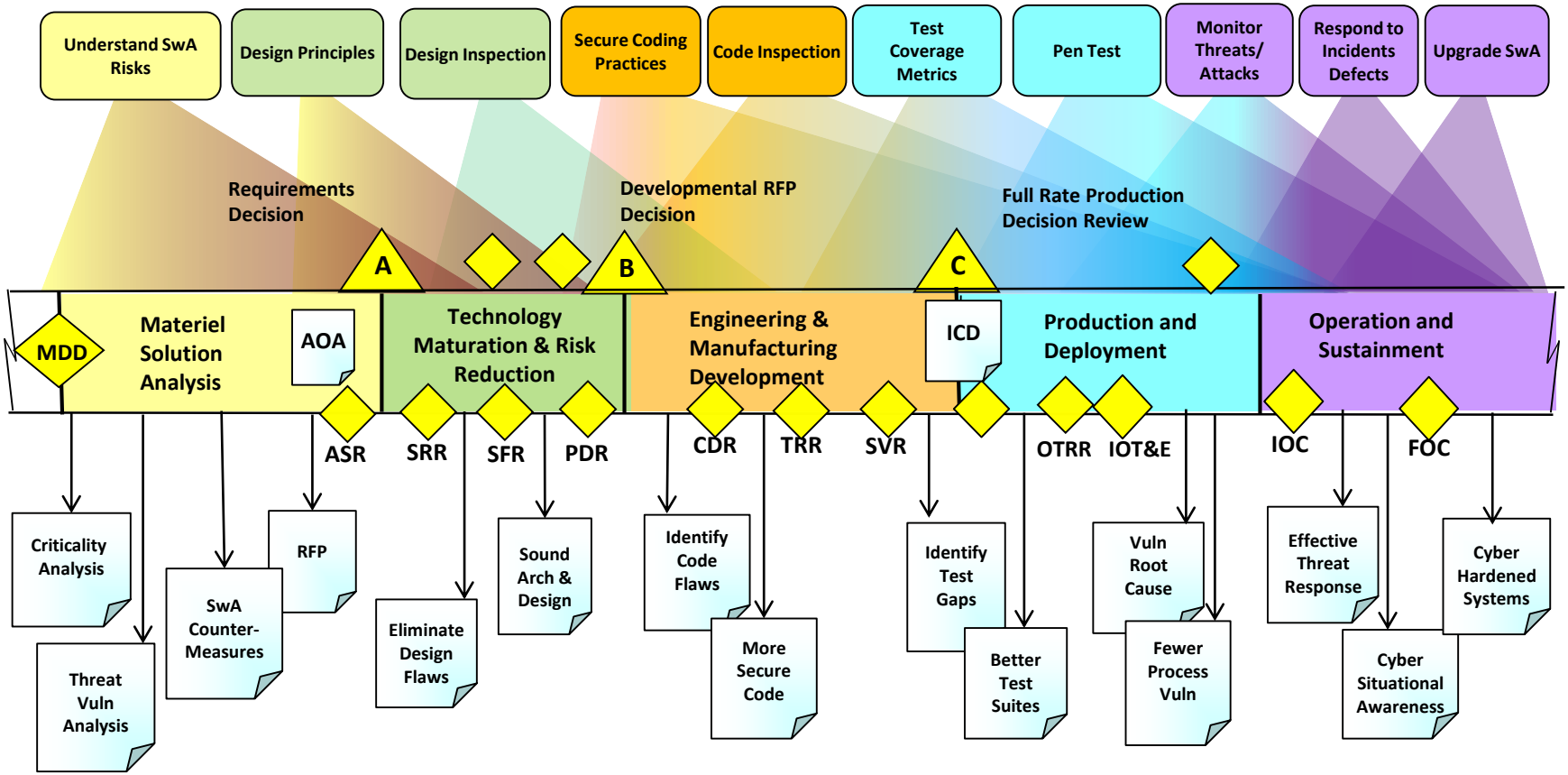




Source: Dr. Robert A. Martin, MITRE Corporation, August 2015

Designing-in System Acquisition Quality Over the Lifecycle

Continuous Engineering Over The Life Cycle



Software assurance must be baked-in throughout entire system lifecycle

Source: OSD/DASD/SE

Distribution Statement A – Approved for public release. Distribution is unlimited.

SEI Supporting JFAC* Pilot Program

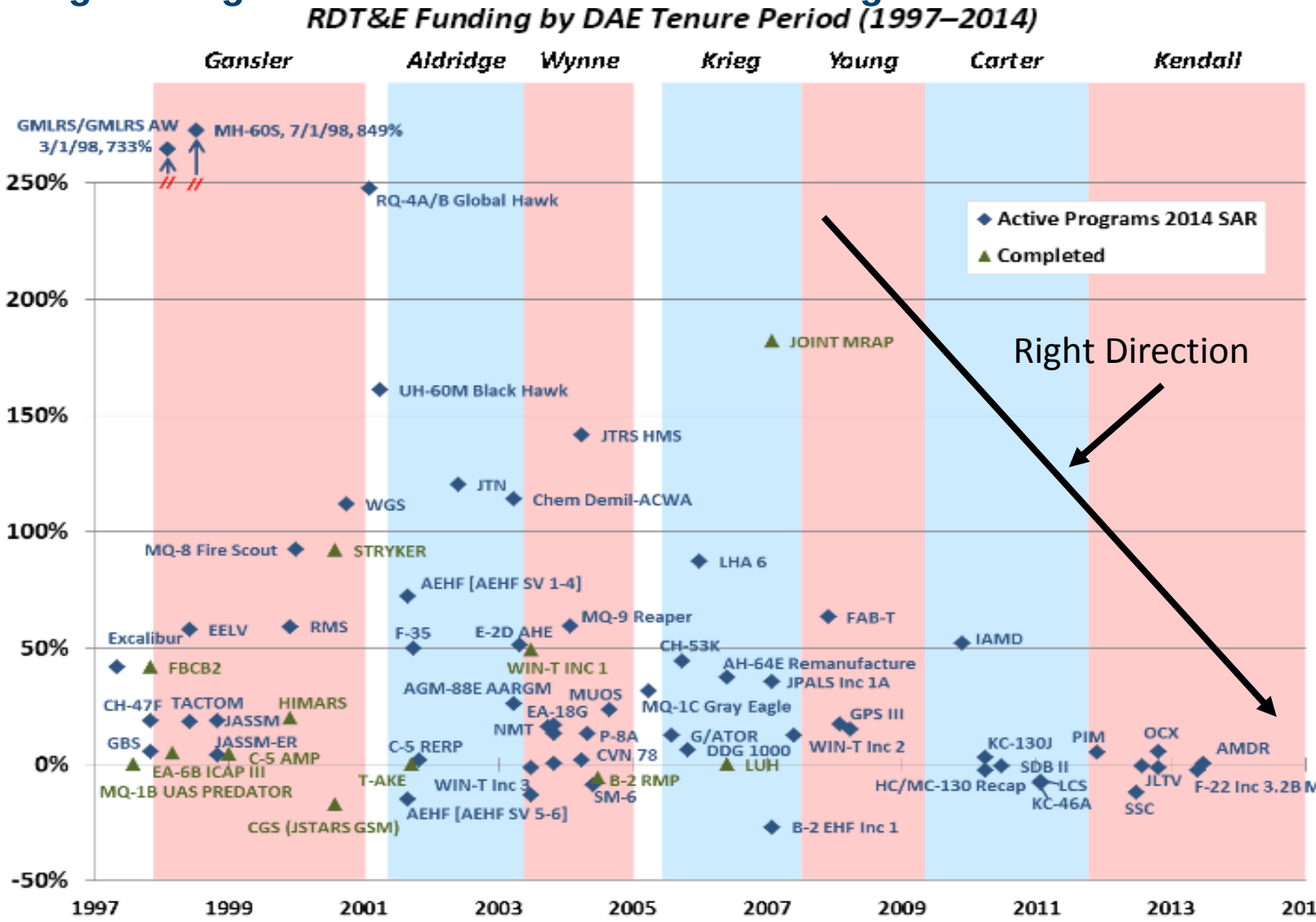
Focused on Solving the SDLC Software Assurance Tool Chasm

- The JFAC is a federation of DoD organizations that have a shared interest in promoting software and hardware assurance in defense acquisition programs, systems, and supporting activities.
- SEI provides experience SEI technical staff to support the dynamic and evolving needs of the JFAC, such as the SDLC software assurance tool chasm

*JFAC: D0D Joint Federated Assurance Center

Reducing Technical Debt

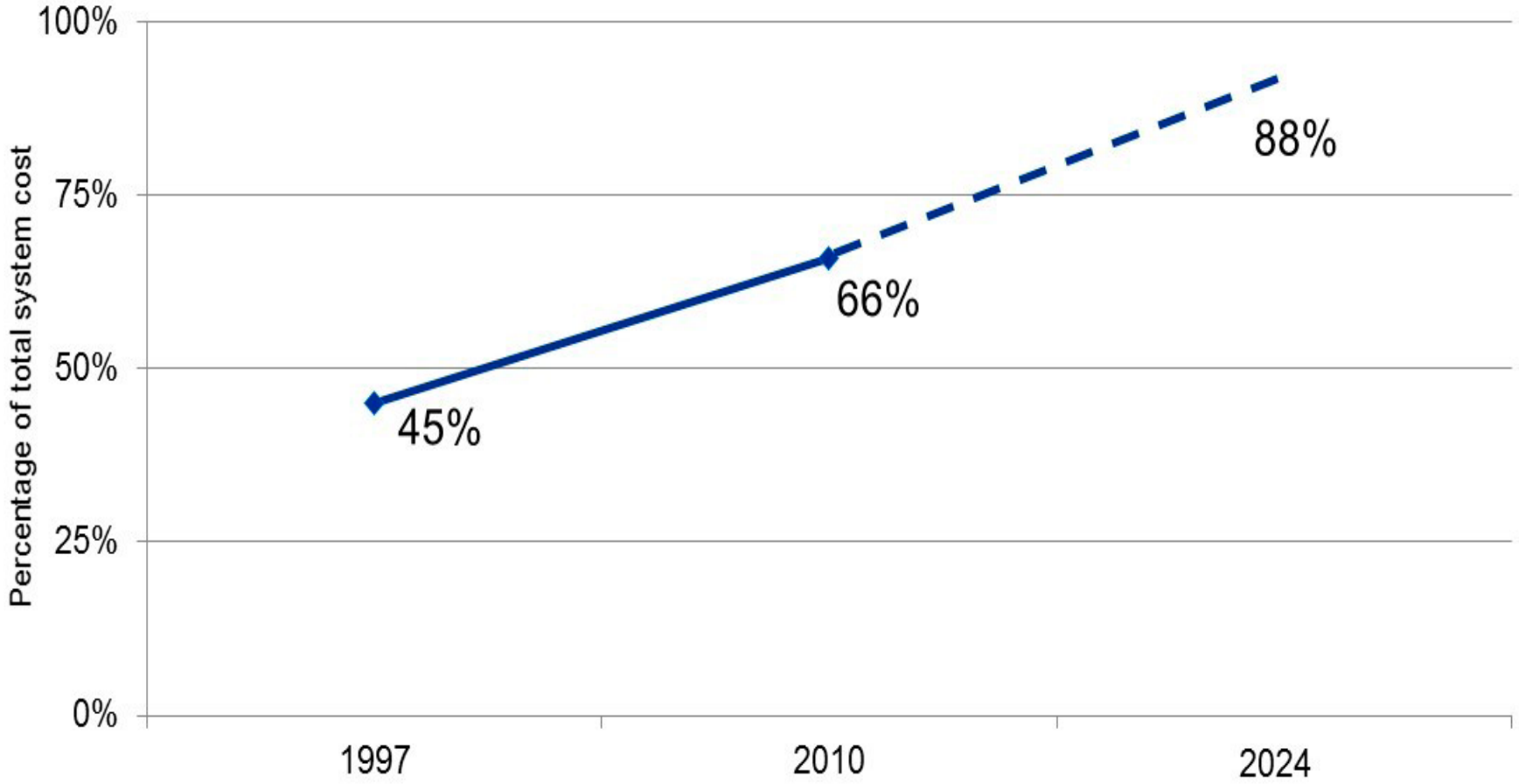
Engineering Assurance into the Fabric of Programs



Source: PERFORMANCE OF THE DEFENSE ACQUISITION SYSTEM 2015 ANNUAL REPORT Sept 16, 2015

Reducing Technical Debt

Aircraft Software Development and Rework Cost



Reference: U.S. Air Force Scientific Advisory Board. Sustaining Air Force Aging Aircraft into the 21st Century (SAB-TR-11-01). U.S. Air Force, 2011.

Working in the Infancy of the Software Engineering Discipline

Integrate Software and Systems Engineering with a Focus on Cyber

	Physical Science	Bioscience	Computer/Software/Cyber Science
Origins/History	Begun in antiquity	Begun in antiquity	Mid-20th century
Enduring Laws	Laws are foundational to furthering exploration in the science	Laws are foundational to furthering exploration in the science	Only mathematical laws have proven foundational to computation
Framework of Scientific Study	Four main areas: astronomy, physics, chemistry, and earth sciences	Science of dealing with health maintenance and disease prevention and treatment	• Several areas of study: computer science, software/systems engineering, IT, HCI, social dynamics, AI • All nodes are attached to and rely on a netted system
R&D and Launch Cycle	10–20 years	10–20 years	Significantly compressed; solution time to market must happen very quickly

HCI: human–computer interaction; AI: artificial intelligence

Source: SEI

Software Assurance Struggles at the Frontiers

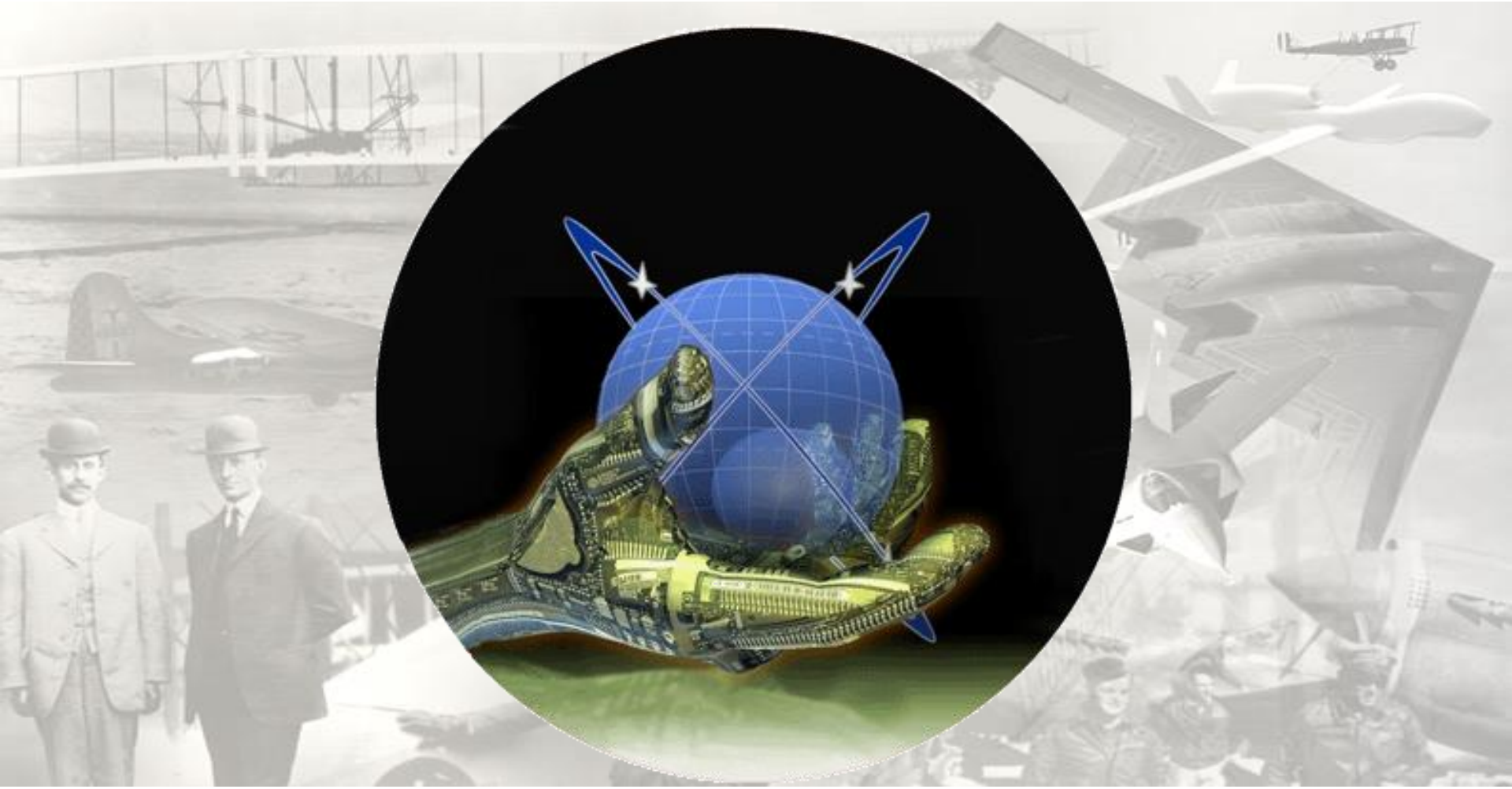
1. Increasing Complexity of Software Assurance
2. Satisfying unique operational mission and business needs
3. Solving the SDLC Software Tool Chasm
4. Addressing limited spectrum availability
5. Handling the expanding code base
6. Understanding attack patterns, vulnerabilities, and weaknesses
7. Increasing vulnerabilities
8. Designing-in software quality over the lifecycle
9. Reducing Technical Debt
10. Working in the infancy of software engineering discipline

SEI Technologies Address DoD Software Assurance Challenges

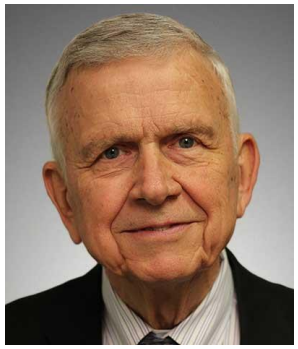
Today's Presentations of SEI's Contributions

- Software Vulnerabilities Track
  - Relationship Between Design Flaws and Software Vulnerabilities
  - Predicting Software Bug Closure Rates and Reliability Growth with Weibull Modeling
  - Using Malware Analysis to Identify Overlooked Security Requirements
- Modernization and Sustainment Track
  - Case Study - Successful Government Roadmap Modernization Project
  - Panel - Software Sustainment: Continuous Engineering to Deliver Warfighter Capability
  - Methodology for the Cost Benefit Analysis of a Large Scale Multi-phasic Software Enterprise Migration

Questions?



Contact Information



Dr. Kenneth E. Nidiffer, Director of Strategic Plans for Government Programs

Software Engineering Institute, Carnegie Mellon University

Office: + 1 703-247-1387

Fax: + 1 703-908-9235

Email: nidiffer@sei.cmu.edu

References

Gallagher, B.; Nidiffer, K. & Saga, R. The Ordered Process for Improving Agile Engineering Outcomes, CrossTalk, Nov/Dec 2016

JFAC Collaboration Portal https://intelshare.intelink.gov/sites/jfac/

SEI Training: Manage Cybersecurity Risk Across the Lifecycle - The CERT Software Assurance Framework (SAF) Assessment

SEI Training: Architecture Tradeoff Analysis Method (ATAM)

SEI Training: Security Requirements Engineering Using the SQUARE Method

SEI Training: Team Software Process (TSP)

Source Code Analysis Laboratory (SCALe), SEI Technical Note, CMU/SEI-2012-TN-013, 2013

Quantifying Uncertainty in Early Lifecycle Cost Estimation (QUELCE), Technical Report, CMU/SEI-2011-TR-026, 2011

Alberts, C.; Woody, C.; & Dorofee, A. *Evaluating Security Risks using Mission Threads*(CMU/SEI-2014-TN-025), 2014.