Struggles at the Frontiers of Quality Measurement: Special Focus on Achieving System and Software Assurance for Software-Reliant Systems

Dr. Kenneth E. Nidiffer

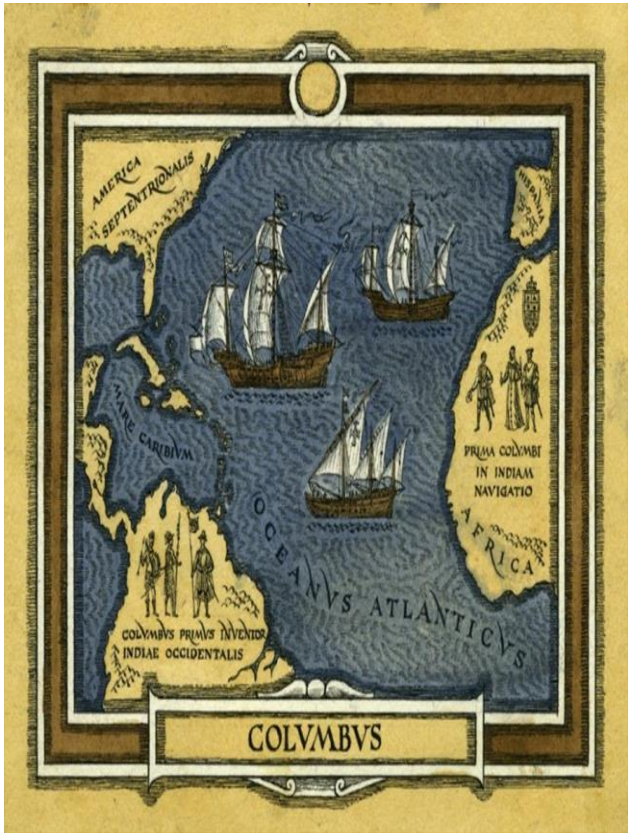
Seventeenth Practical Software and Systems Measurement Users' Group Workshop
Measurement: A Foundation for Affordable Solutions

Lockheed Martin Global Vision Center
Crystal City, Arlington, VA

22–26 February 2016
Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

Content: Frontiers of Quality Measurement

- Context: Measurement of software quality is a continuous purpose, and software is a moving target
- Perspectives: Struggles in the persistent pursuit of software quality assurance measurement
- Future: Closing the gaps in effective software quality assurance measurement to meet the needs of society



Source: SEI

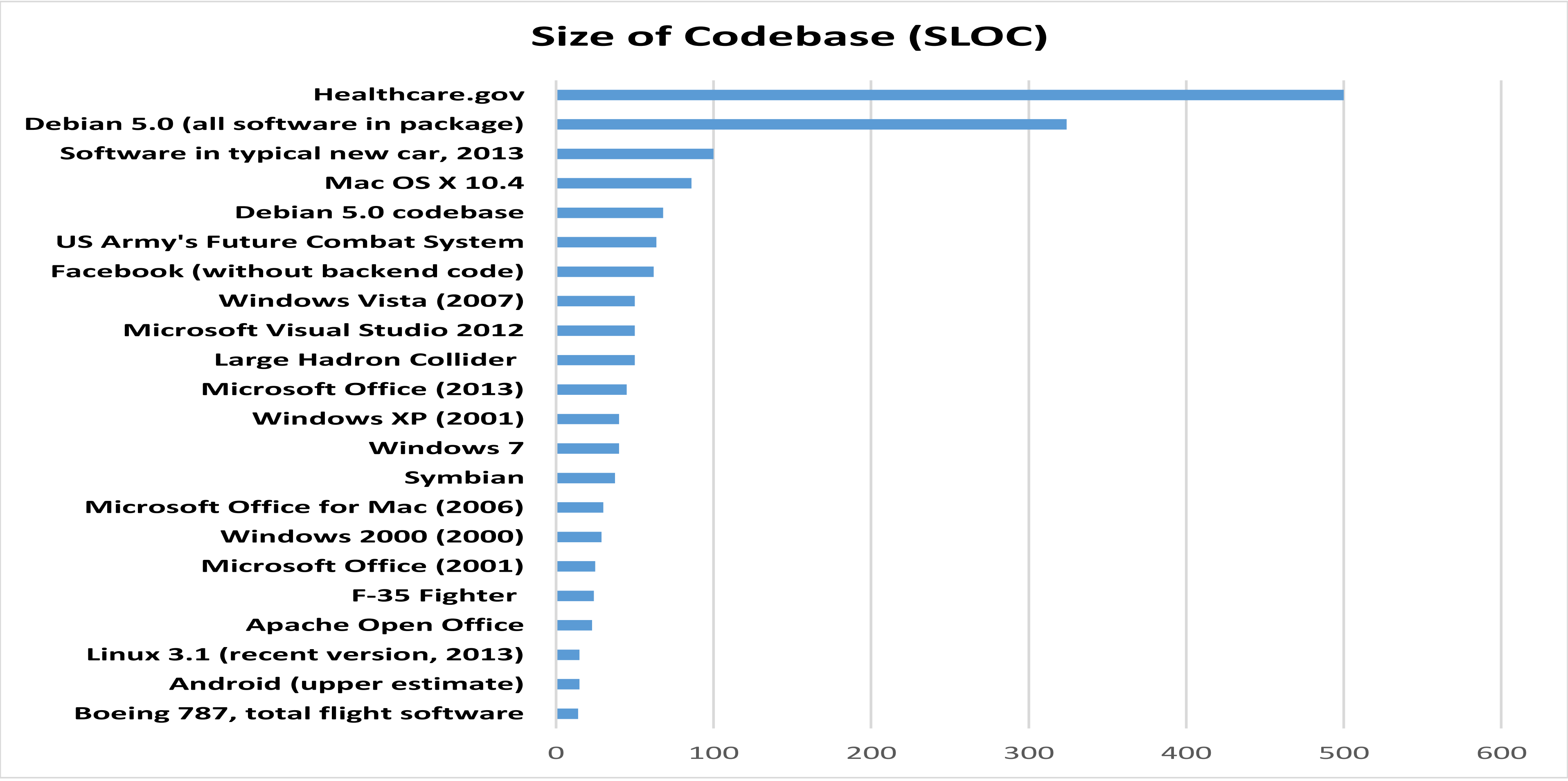
Context: Measurement of Software Quality Assurance Is a Continuous Objective, and Software Is a Moving Target

Context: Software Quality Is a Continuous Objective, and Software Is a Moving Target

- Continuous Objective
  - Information need for software assurance measurement: To provide the level of confidence that software functions as intended (and no more) and is free of vulnerabilities, either intentionally or unintentionally designed or inserted as part of the software throughout the lifecycle.*
- Moving target
  - The changing and expanding roll that software plays in cyberspace means software engineering must continue to evolve in the ongoing pursuit of software quality.

*** NDAA 2013 Section 933**

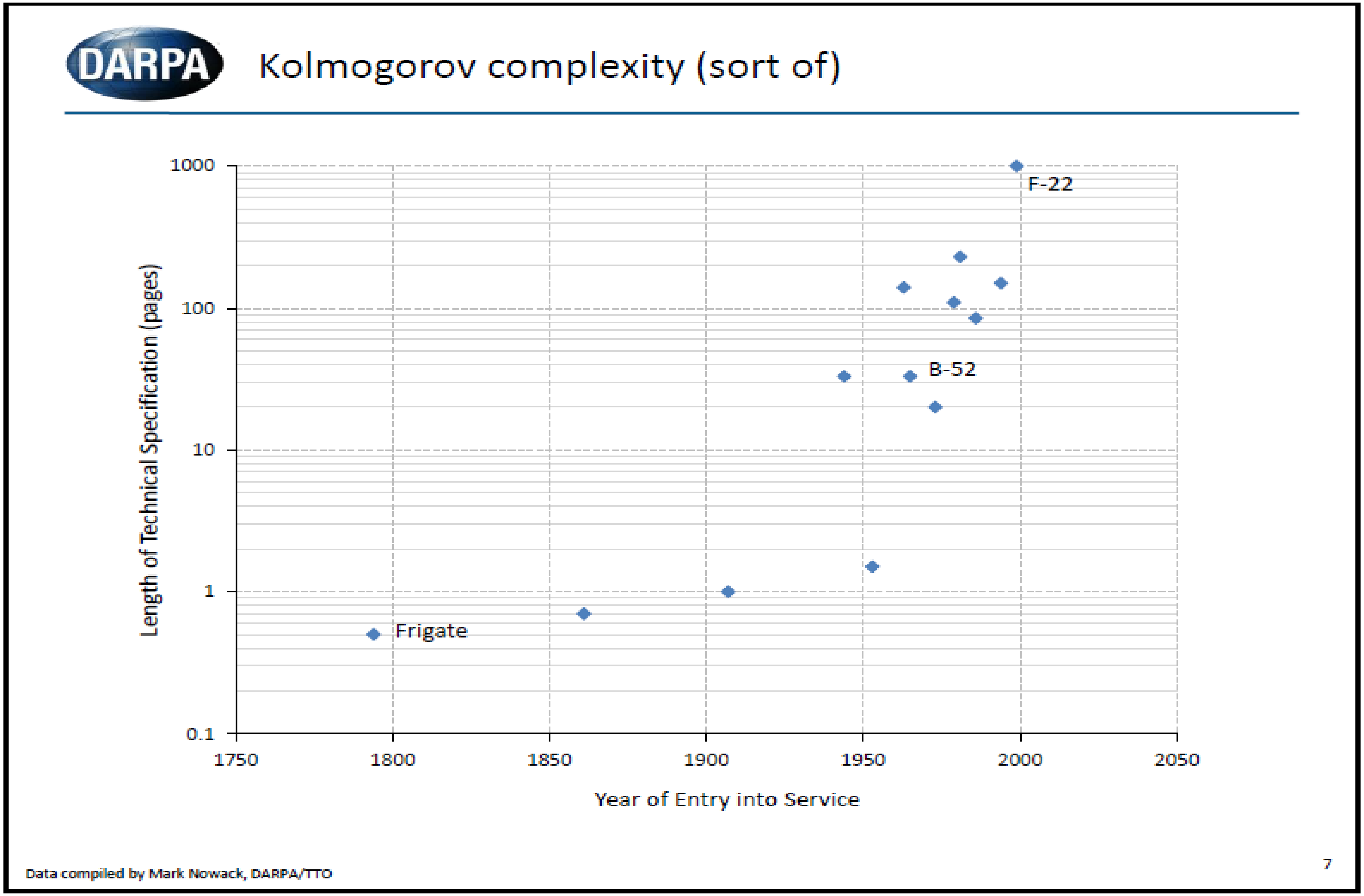
Context: Software Is a Moving Target: Expanding Codebase



Millions of Source Lines of Code

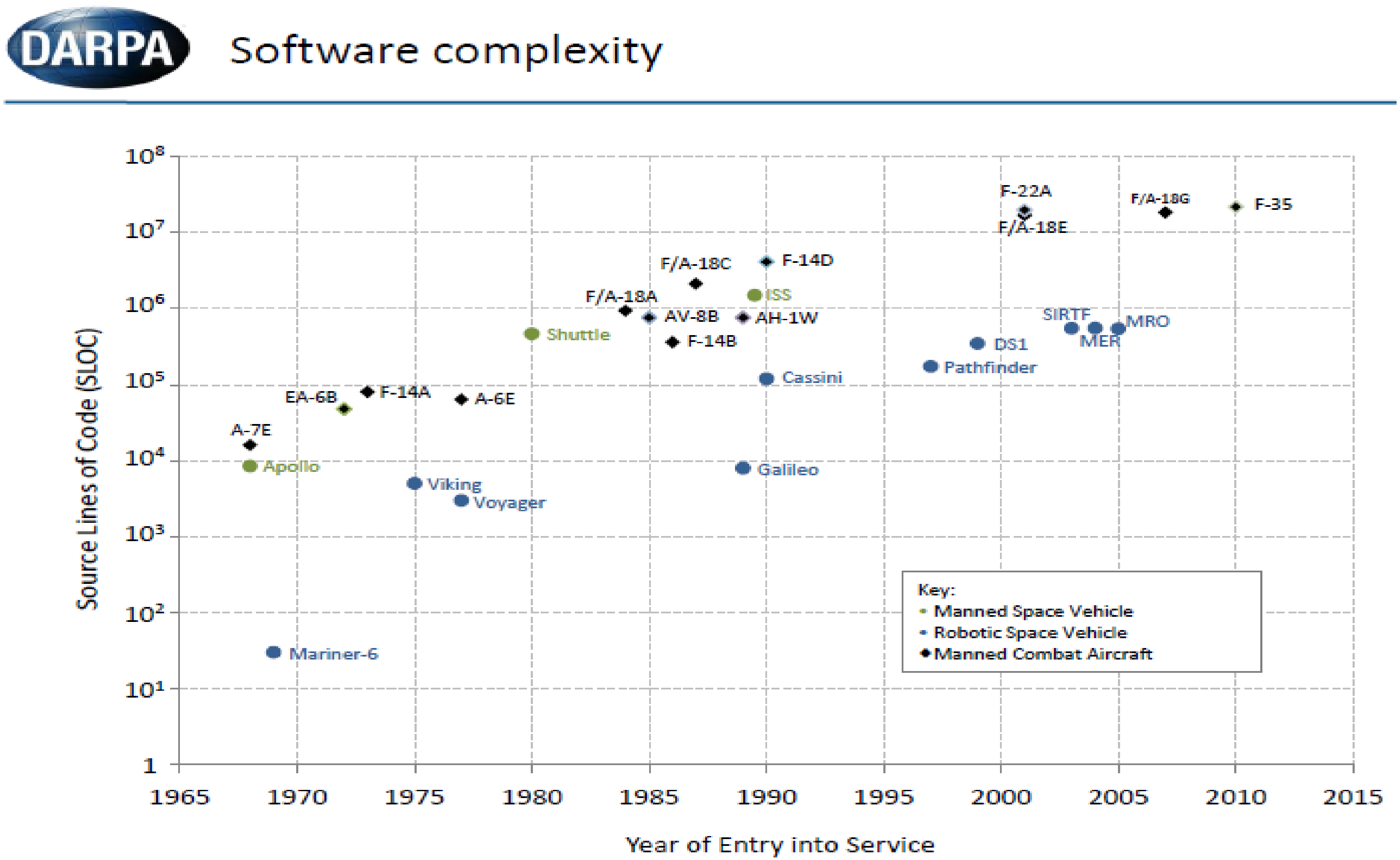
Source: David McCandless – Software is Beautiful, 12 August 2015, Web Retrieval

Context: Software Is a Moving Target:
Pages of Technical Specifications



DARPA = *Defense Advanced Research Projects Agency*

Context: Software Is a Moving Target:
Software Complexity – Source Lines of Code



Dvorak, D. ed, NASA Study on Flight Software Complexity, Jet Propulsion Laboratory, California Institute of Technology, 5 March2009
Borden, D., Software Acquisition Process Improvement, NAVAIR, undated
Agle, D.C., Where Hunters Growl, Air & Space magazine, March 2011

A Quick Look at Applying Better Buying Power Principles (BBP) for Programmatic Systemic Problems

Data should drive policy. Outside my door, a sign is posted that reads, "In God We Trust; All Others Must Bring Data." The quotation is attributed to W. Edwards Deming, the American management genius who built Japan's manufacturing industry after World War II. The three annual reports on *The Performance of the Defense Acquisition System* that we have published are based on this premise.

It is difficult to manage something you cannot measure. Despite the noise in the data, it is possible to pull out the correlations that matter most and to discover those that have no discernible impact. As we have progressed through the various editions of BBP guided by the results of this analysis, we have adjusted policy, such as preferred contract type and incentive structure.

—Frank Kendall, Under Secretary of Defense for Acquisition, Technology, and Logistics, Defense AT&L, Jan-Feb 2016

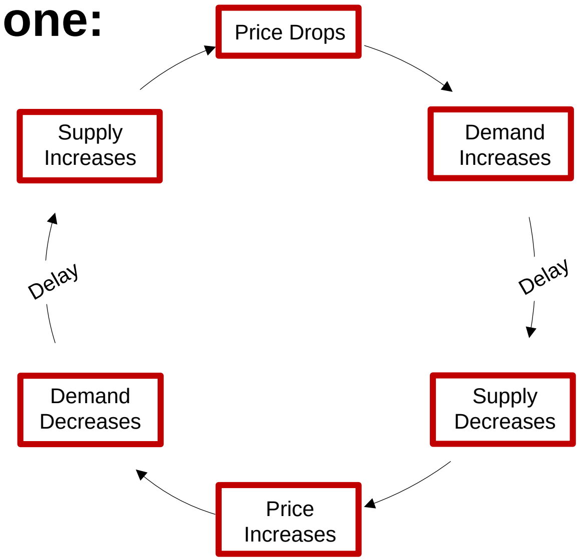
Can System Processes Trap Us into Behaviors? Example: Archetype

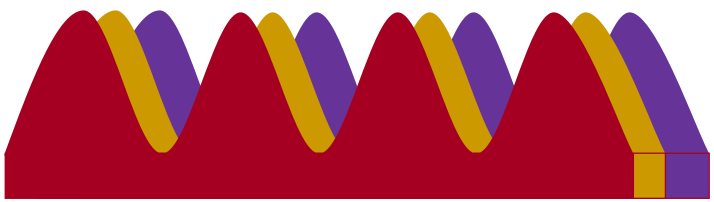
Inside a complex, dynamic system, people's actions can be at the mercy of that system's dynamics. Such patterns occur in real estate cycles:

As price drops…

→ demand increases	(*get a good deal*)
→ …and after a delay…	(*takes time to buy*)
→ supply decreases	(*not many houses left*)
→ price increases	(*supply and demand*)
→ demand decreases	(*too expensive now)*
→ …and after a delay…	(*more people must sell*)
→ supply increases	(*plenty of houses*)
→ and price drops	(*supply and demand*)

Since this is a *loop*, let's draw it as one:

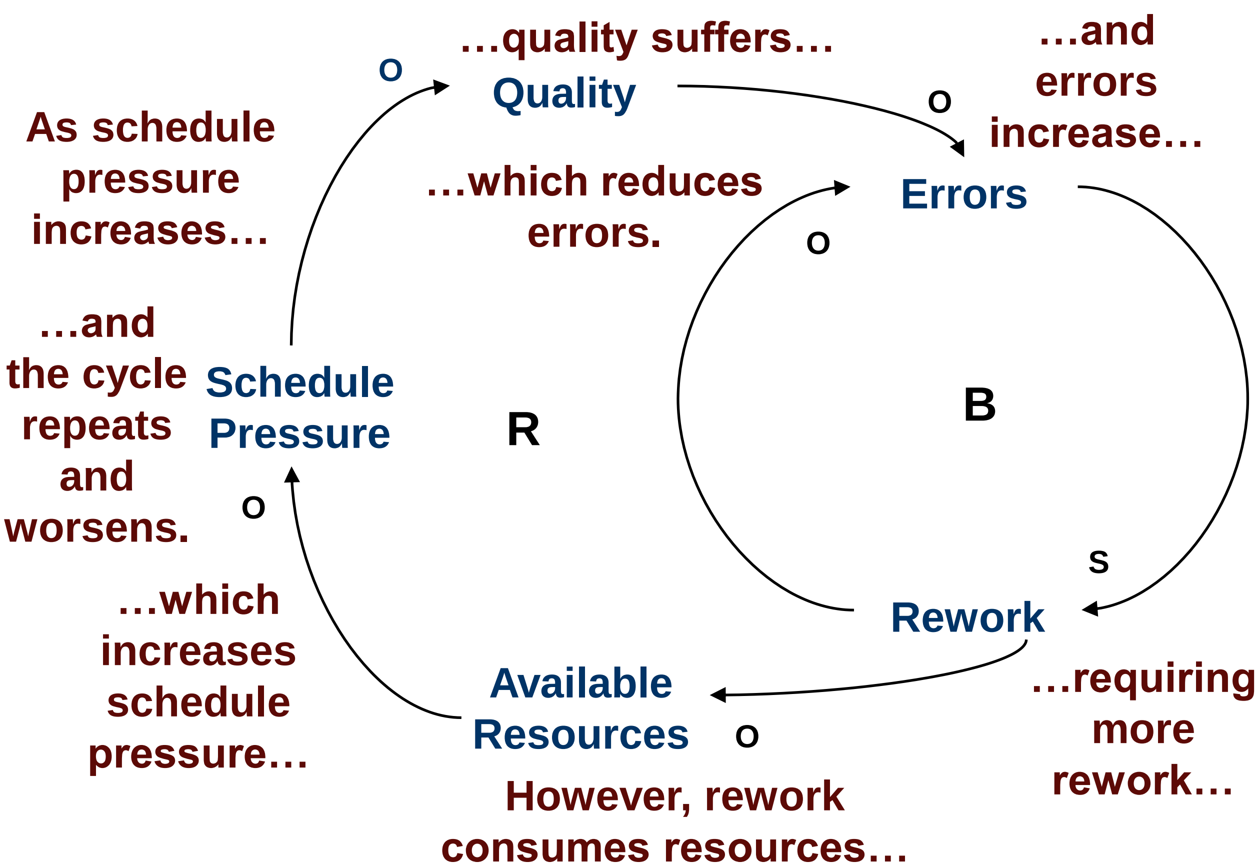




Source: SEI

Acquisition Archetypes

“Happy-Path Testing” Process (i.e., Sacrificing Quality)



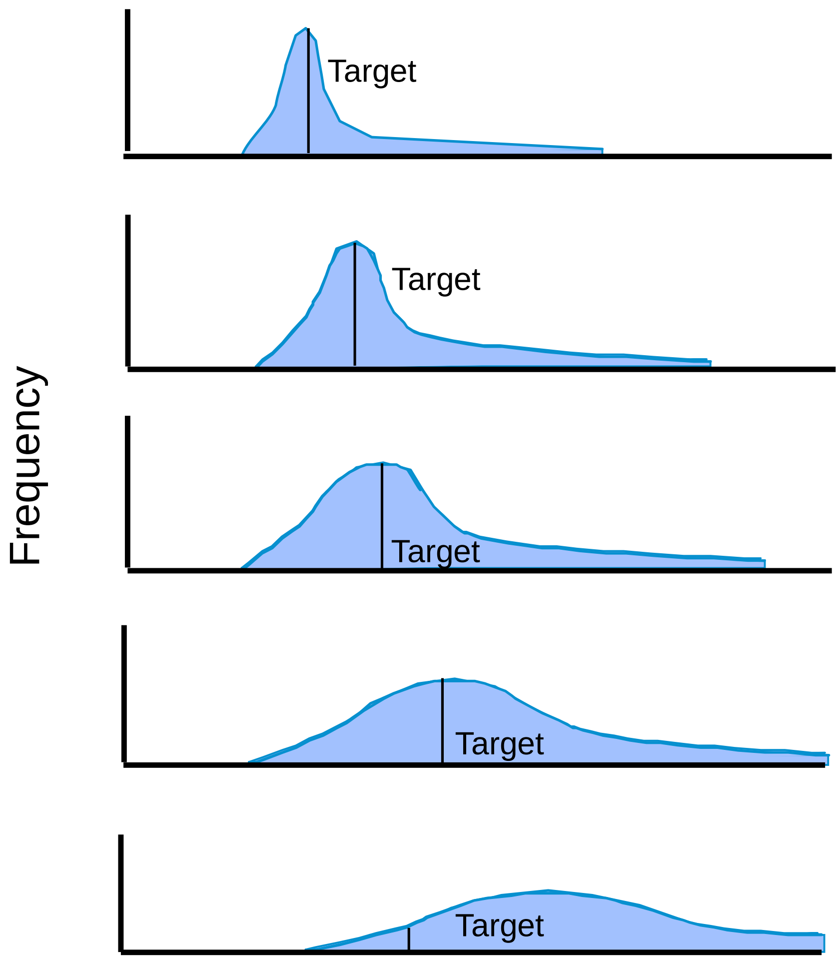
As schedule pressure increases, processes are shortcut, quality suffers, and errors increase—requiring more rework. However, rework consumes resources, which increases schedule pressure, and the cycle repeats and worsens.

Source: SEI

Source: SEI based on the “Fixes that Fail” systems archetype

Part of the Solution: Benefits in Terms of Predictability (Accuracy, Variance, Efficiency)

Predicted Performance



Process Characteristics

Focus is on continuous quantitative improvement

Process is measured and controlled

Process is characterized for the organization and is proactive

Process is characterized for projects and is often reactive

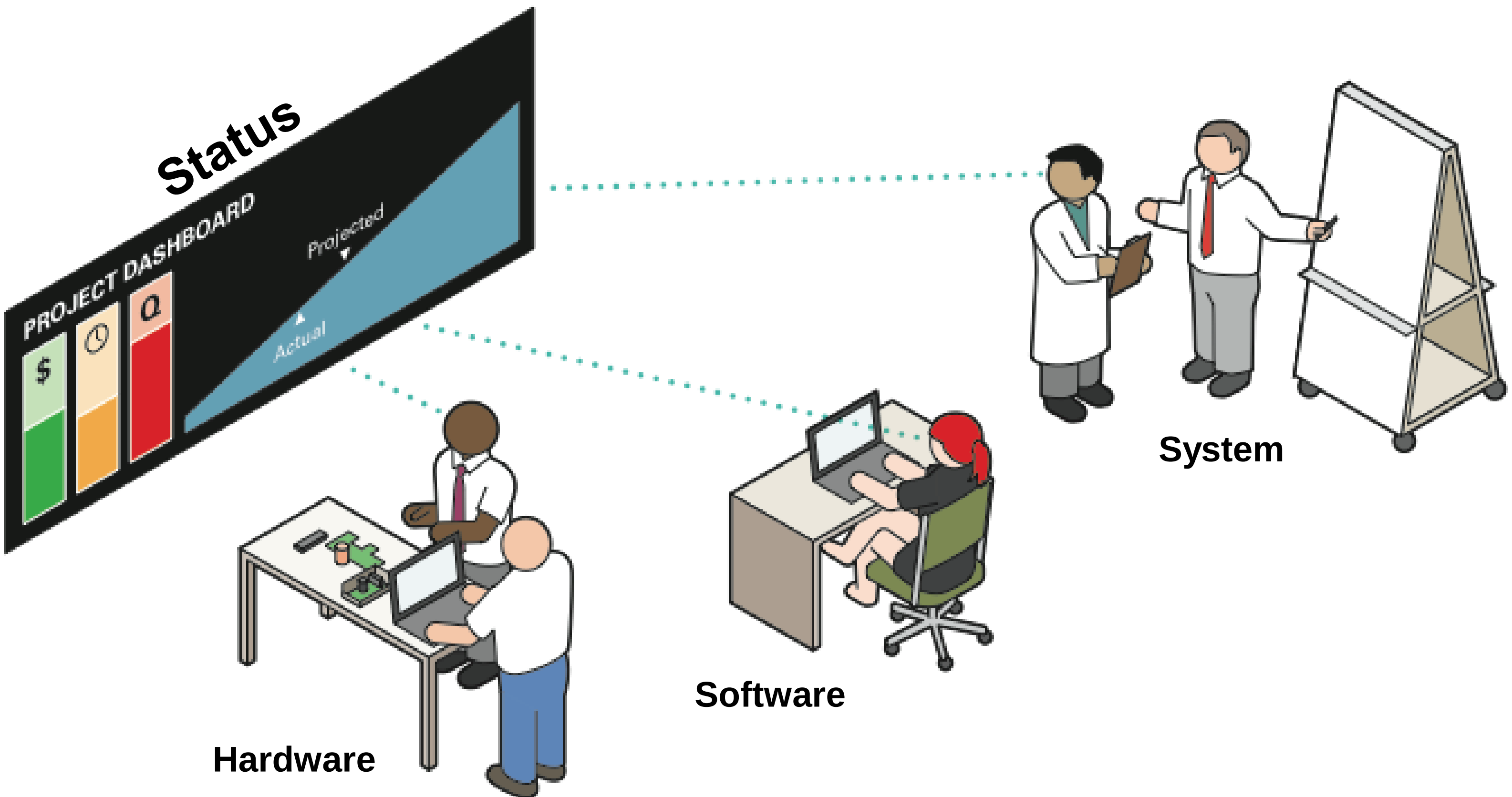
Process is unpredictable, poorly controlled, and reactive

Source: SEI

Example: Part of Solution: Measurement and Analysis (MA)

A Support Process Area at Maturity Level 2

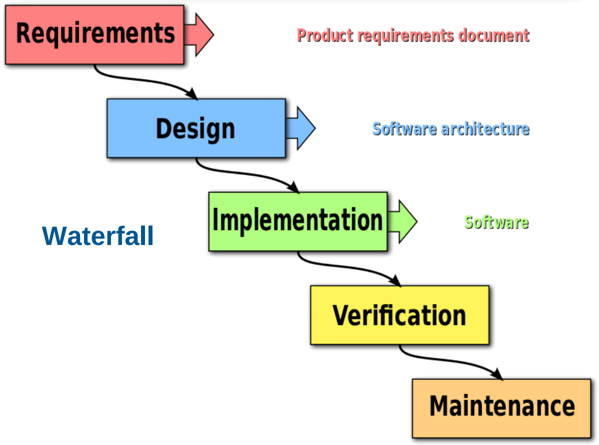
Purpose: Develop and sustain a measurement capability used to support management information needs.



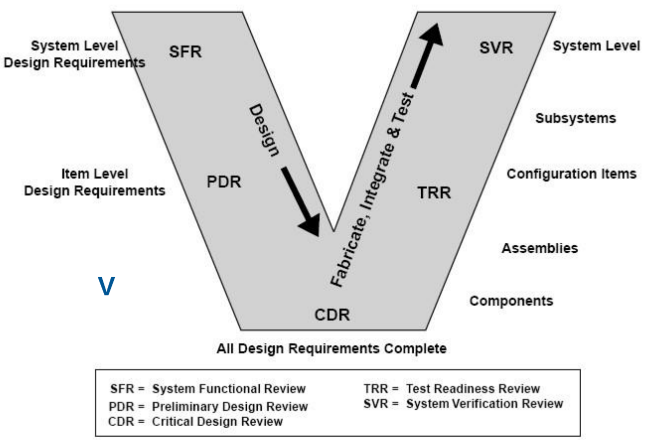
Part of Solution: Increasing Use of Innovative Processes, Methods, and Tools

Predictive Models

Waterfall

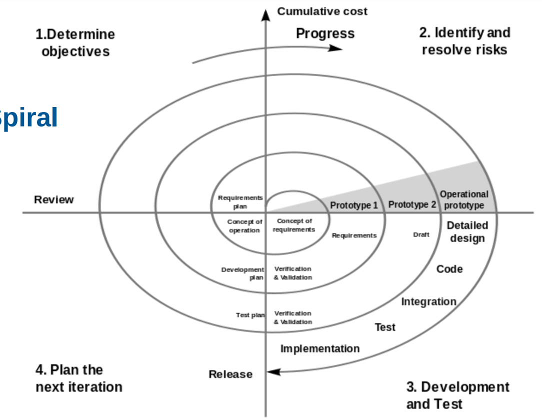


V

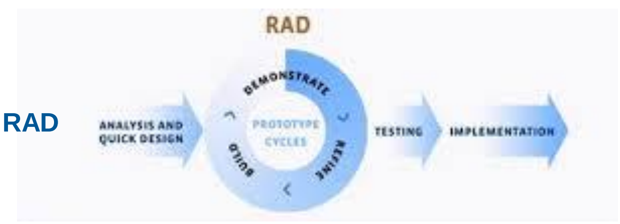


Iterative Models

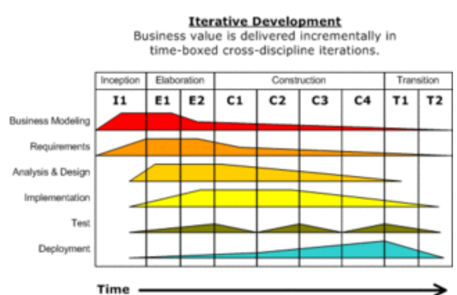
Spiral



RAD

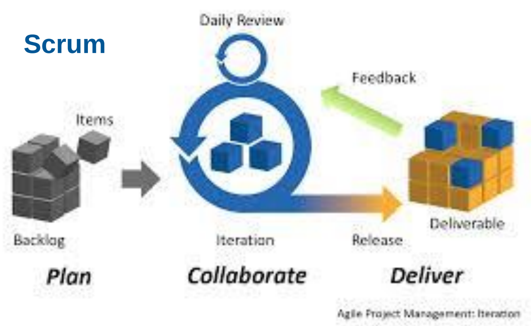


RUP



Adaptive Models

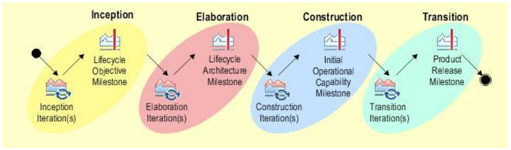
Scrum



XP

OpenUP

Source: Noblis

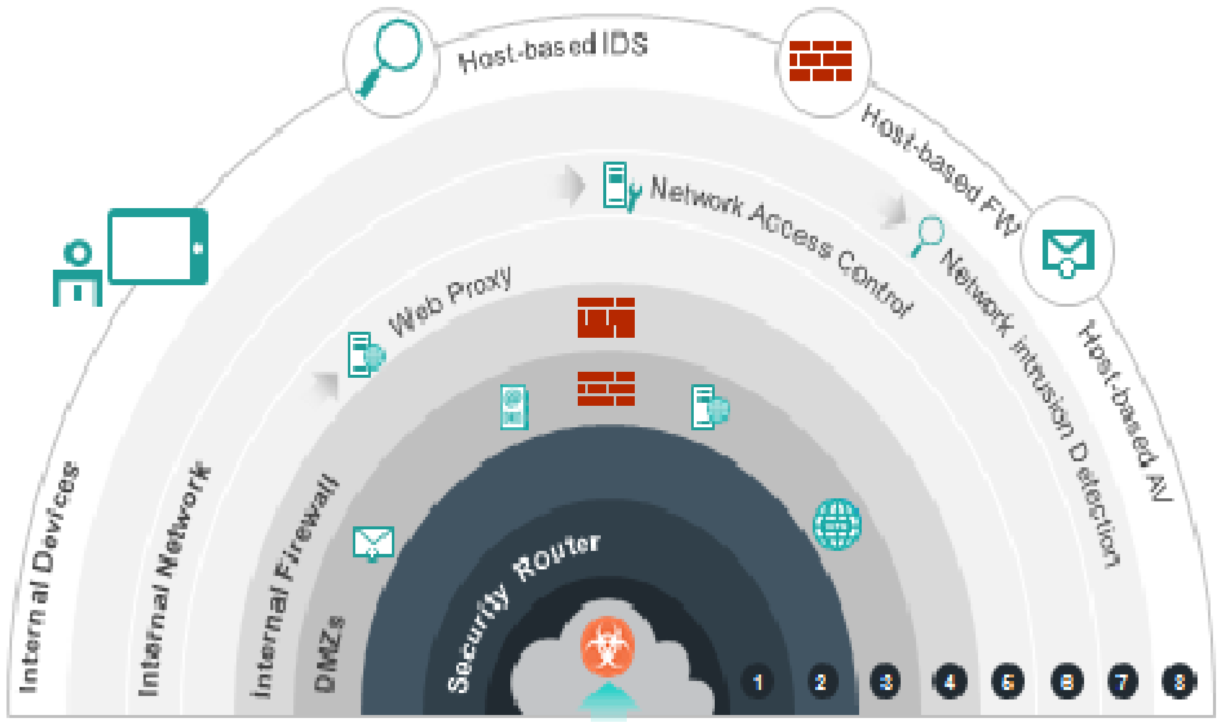


Thinking Outside the Box on Potential Software Assurance Measurement Opportunities

Four Examples

Thinking Outside the Box is Important

Today's View of Security



84% of breaches exploit vulnerabilities in the application layer

Yet the ratio of spending between perimeter security and application security is **23-to-1**

- Gartner Maverick Research: Stop Protecting Your Apps; It's Time for Apps to Protect Themselves (2014)

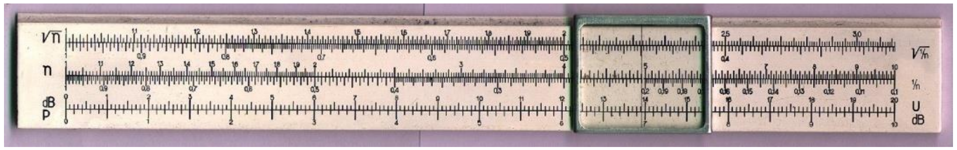
Hewlett Packard Enterprise

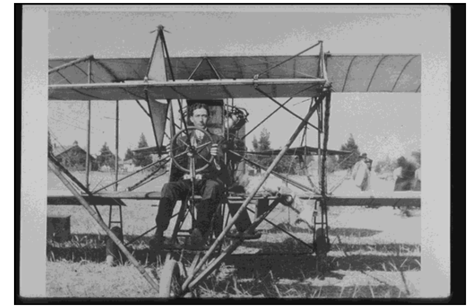
Example 1

A Quick Look at System Sustainment and Opportunities for Software Assurance Measurement

Context: Software Is a Moving Target:
Aircraft Growth of Software Over Time

In The Beginning





1960s

1970s

1980s

1990s

2000+

F-4A
1,000 LOC

F-15A
50,000 LOC

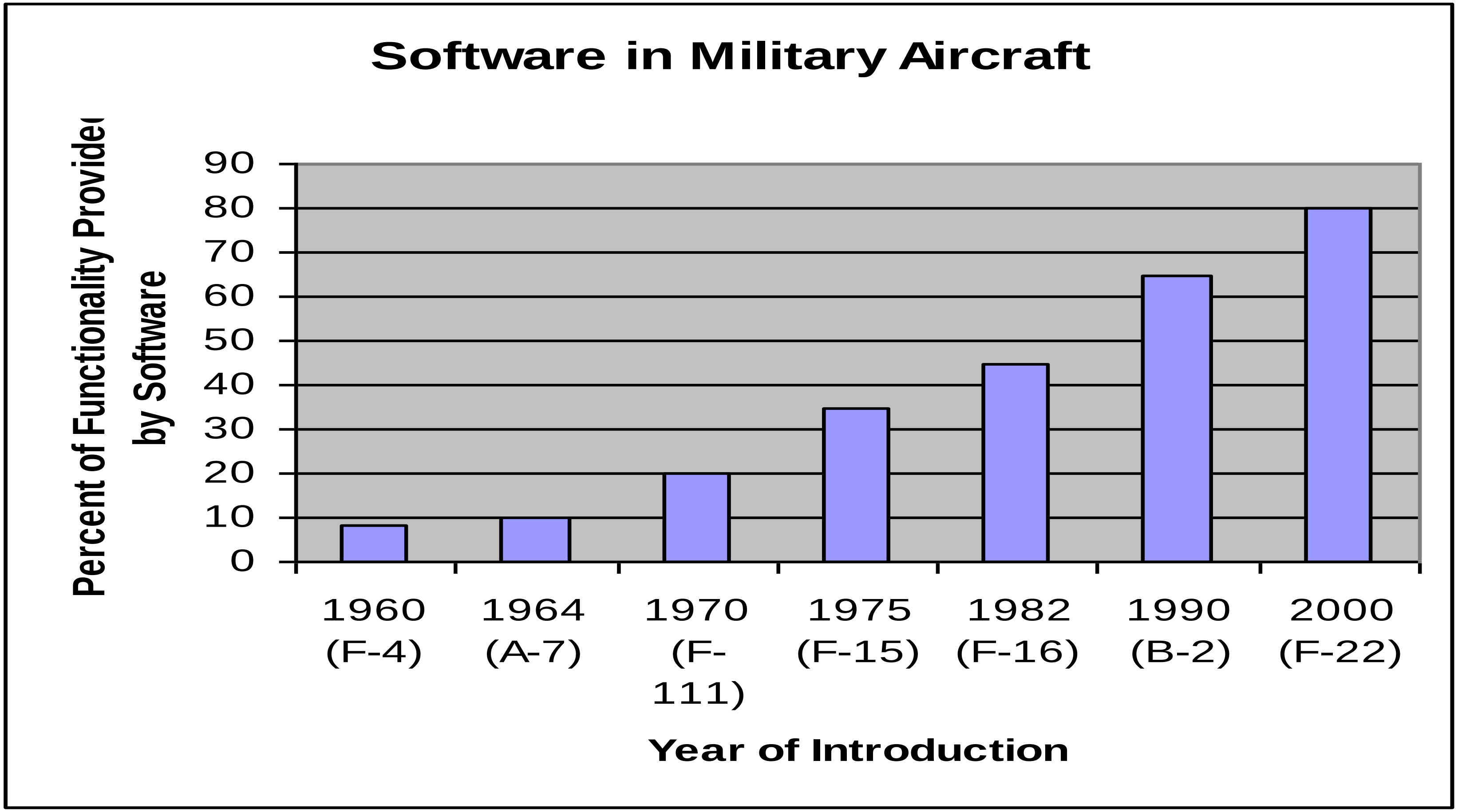
F-16C
300K LOC

F-22
1.7M LOC

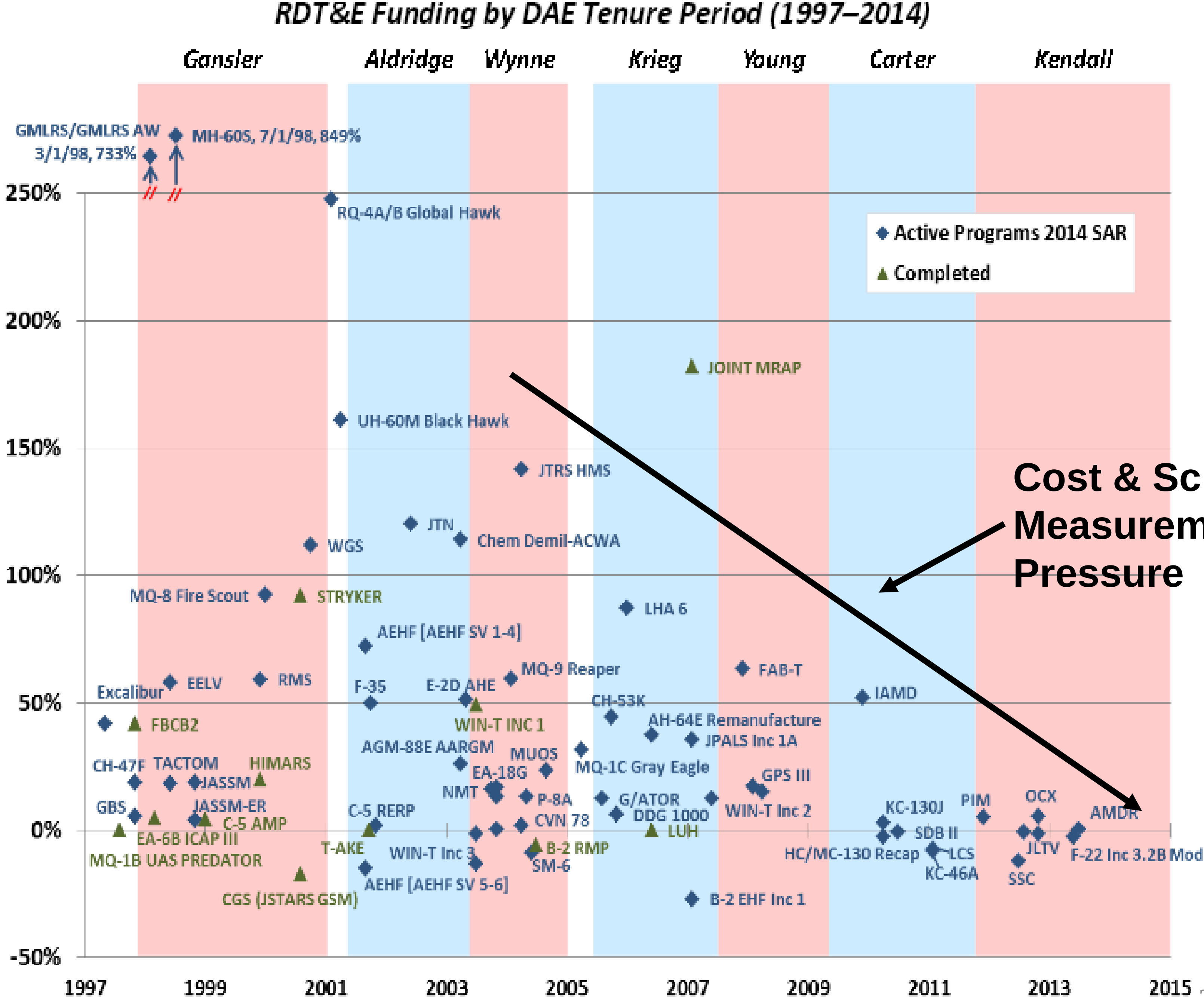
F-35
>6M LOC

Permission provided for use by author by Lockheed Martin Corporation

Context: Software Is a Moving Target:
Percent of Functionality Provided by Software

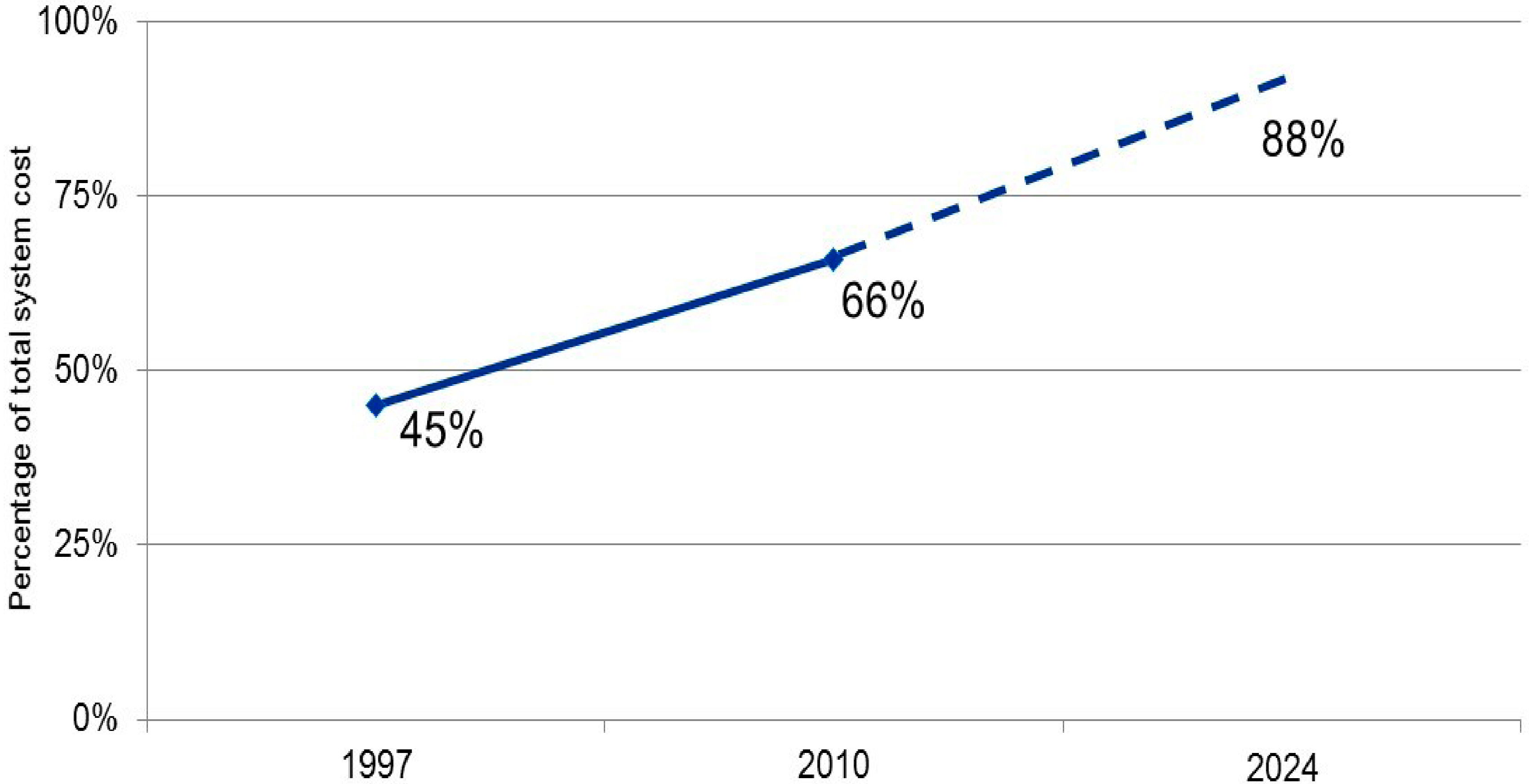


Source: NASA Planetary Spacecraft Fault Management Workshop, April 14-16, 2008, New Orleans



PERFORMANCE OF THE DEFENSE ACQUISITION SYSTEM 2015 ANNUAL REPORT Sep. 16, 2015

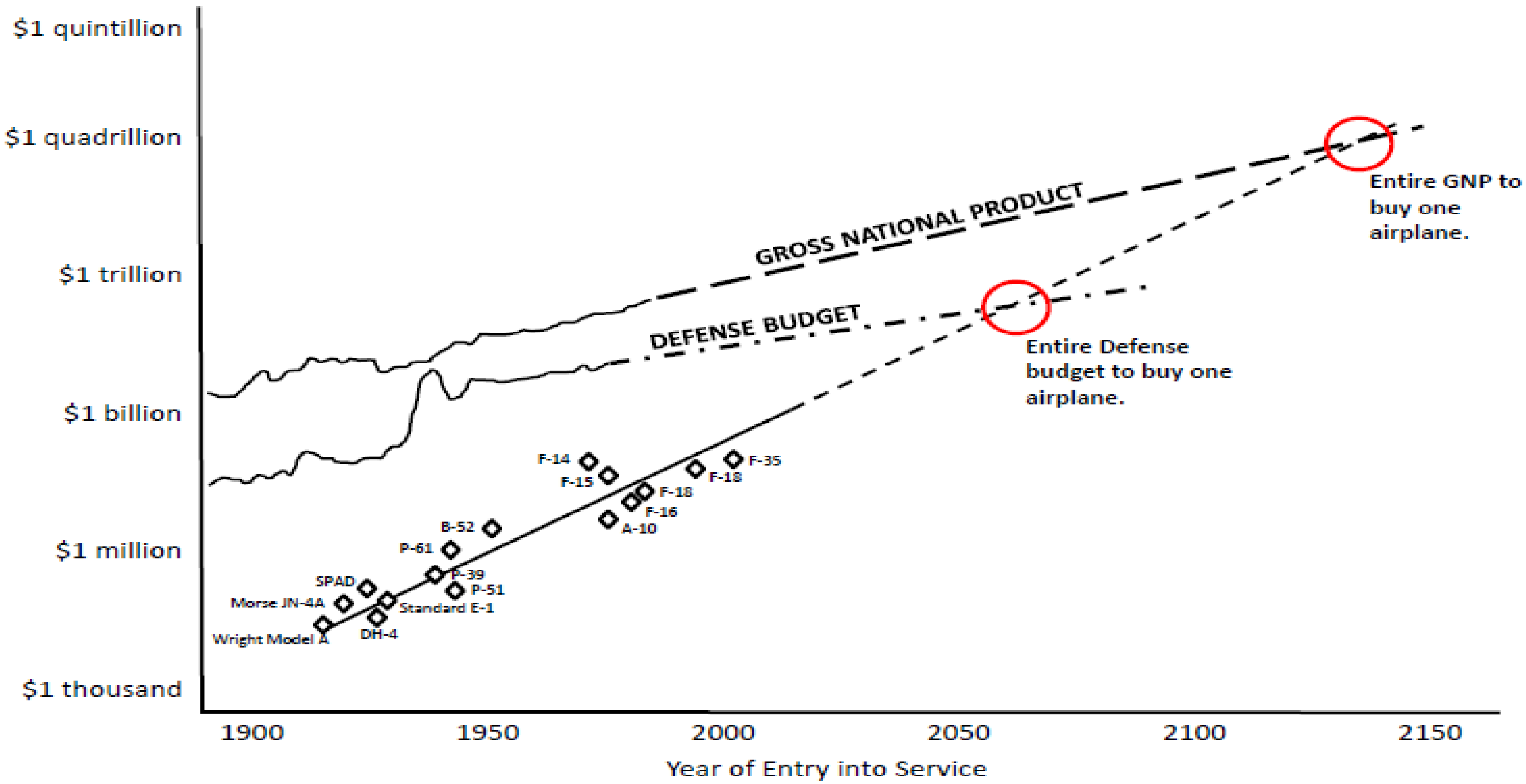
Context: Software Is a Moving Target: Aircraft Software Development and Rework Cost



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.

Context: Software Is a Moving Target:
Cost Growth of Aircraft

DARPA Cost growth



Example 2

A Quick Look at Emerging Technologies and Opportunities for Software Assurance Measurement

Context: Software Is a Moving Target: Importance of Software and System Engineering Measurement

1: Foundations for SwA

- Software Composability
- "Science of Security"
- Modeling, Simulation, Testing, & Certification
- Tailored Trustworthy Spaces
- Scaling of Assurance Techniques
- Digital Curation and Forensics

2: Processes, Methods, Measurement of Secure Systems Engineering Development

- Vulnerability Prevention and Detection Tools & Techniques (CWE, CAPEC)
- Architecture for Built-In Secure Systems
- SwA for Agile Software Methodologies
- Operational Resilience (RMM)
- Maturity Cultivatio SwA (JFAC)
- Model-Based Engineering and Auto-code Generation Tools

3: SwA Management & Operation

- SwA Workforce Development
- SwA Core Competencies, Education, & Training
- Metrics
- Using Big Data Analysis to Advance Software Assurance Techniques
- SwA Economic Incentives
- Real-Time Modification of Systems
- Effective Acquisition Policy & Guidance

4: Emerging & Disruptive Technology

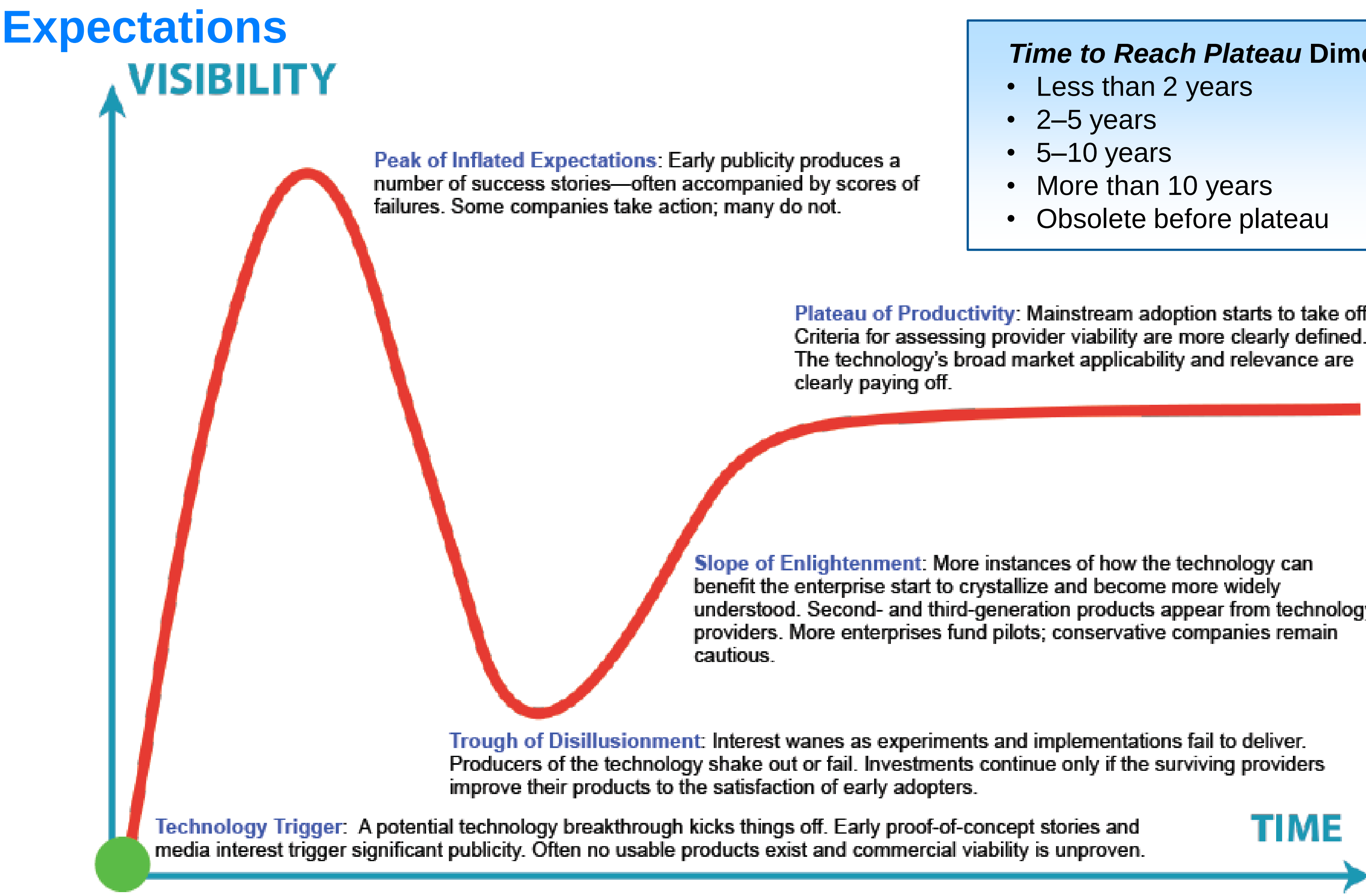
- SwA in Highly Parallel, High-Performance Computing Environments
- Security of Mobile Applications & Platforms
- Security in Sociotechnical Computing

5: Critical Infrastructure

- Designing Secure Cyber-Physical Systems
- Electronic Effects in SwA
- Global Supply-Chain Security
- Critical Infrastructure Resiliency & Catastrophic Recovery
- Intrinsic Internet Infrastructure Security

Source: SEI

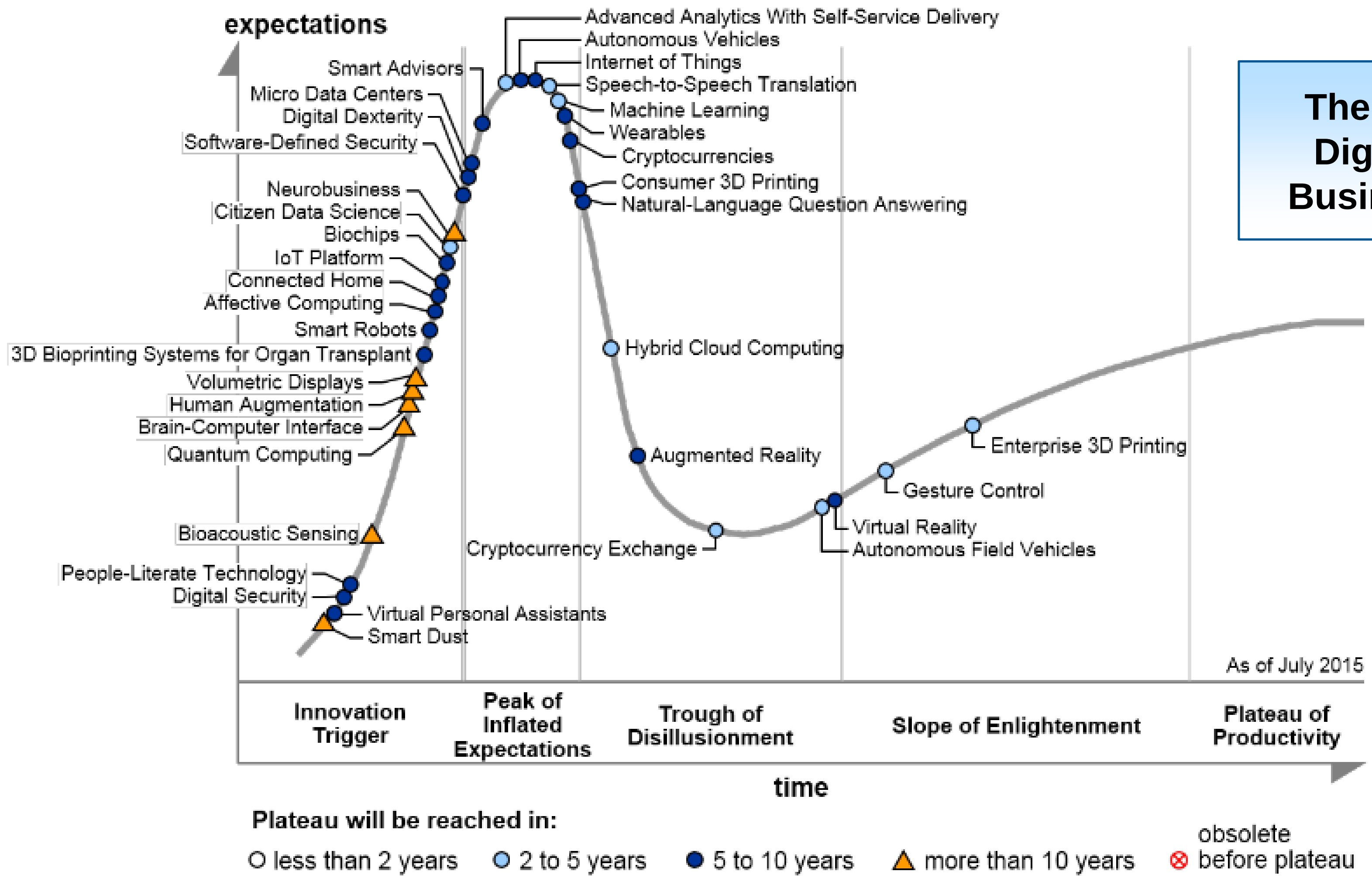
Gartner's Five-Stage Technology Life Cycle



***Time to Reach Plateau* Dimension**
- Less than 2 years
- 2–5 years
- 5–10 years
- More than 10 years
- Obsolete before plateau

Source: Gartner Hype Cycle for Emerging Technologies. Credit: © 2015 Gartner, Inc., and/or its Affiliates. All Rights Reserved.

Gartner's 2015 Hype Cycle for Emerging Technologies



Theme: Digital Business

Source: Gartner Hype Cycle for Emerging Technologies. Credit: © 2015 Gartner, Inc., and/or its Affiliates. All Rights Reserved.

Selected Emerging Technologies

Technologies that we are already working with

- Machine learning

Near-Term Technologies (Now – 2 Years)

- Hybrid cloud computing
- Internet of Things (IoT)
- Software crowdsourcing

Mid-Term Technologies (2–5 Years)

- Citizen data science
- Digital security
- HCI++
- Software-defined anything/everything
- Software-defined security

Long-Term Technologies (5+ Years)

- Artificial intelligence for user-centric systems

Source: SEI

Machine Learning

Technologies that we are already working with

Discipline that provides computers with the ability to learn from data without being explicitly programmed.

- **Supervised learning** aims at learning classifications or estimations
- **Unsupervised learning** aims to extract anomalies, patterns, and relationships from data via methods such as clustering, dimensionality reduction, and density estimation

Main challenges

- Adequacy of data sets
- Algorithm design
- System performance
- Resource utilization
- Behavior verification

Source: SEI

Tag Cloud for Machine-Learning Research @ CMU (http://ml.cmu.edu/research/)

Internet of Things (IoT)

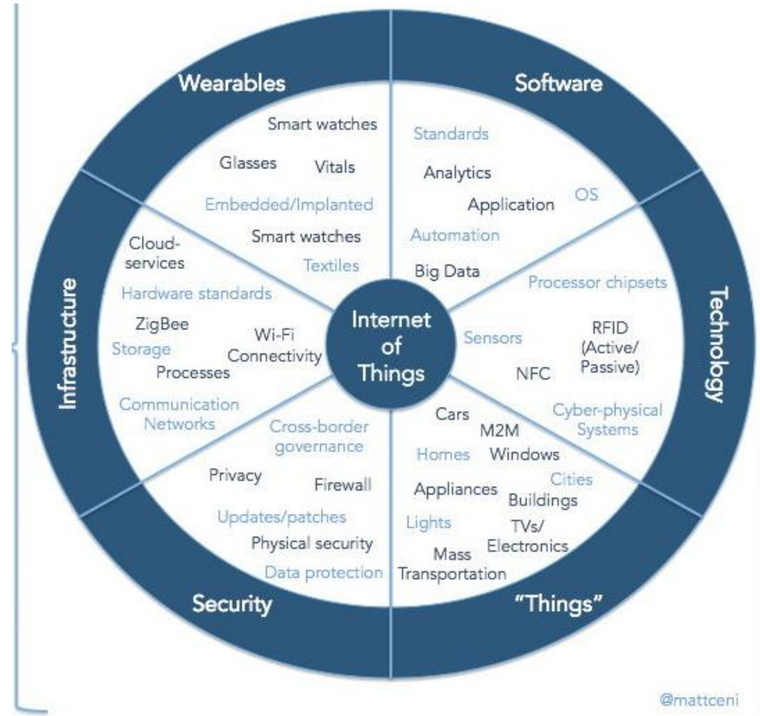
Near-Term Technologies

(Now – 2 Years)

Network of dedicated physical objects that contain embedded technology to communicate and sense or interact with their internal states or the external environment — includes things, communication, applications, and data analysis

Main challenges

- Privacy and security
- Lack of standards
  - Protocols and data integration
- The three Vs of data: volume, velocity, variety
  - New Vs: veracity, validity, volatility, visualization, vulnerability, and value



Source: SEI

Permission for diagram use by Carnegie Mellon University consistent with its status as a non-profit University for any purpose the institution sees fit by Matt Ceniceros, @mattceni, mattceni.com

Interesting Fact: Top Jobs in the Next 7 Years According to Gartner: Jobs Are Data and Measurement Intensive

Integration Specialists

Digital Business Architects

Regulatory Analysts

Risk Professionals

Source: Businesscloudnews.com

Source: linkedin.com

Source harringtonstarr.com

Source: risenetworks.org

Example 3

A Quick Look at Potential Cybersecurity and Opportunities for Software Assurance Measurement

Context: Software Is a Moving Target: Importance of Software and System Engineering Measurement

1: Foundations for SwA

- Software Composability
- "Science of Security"
- Modeling, Simulation, Testing, & Certification
- Scaling of Assurance Techniques
- Tailored Trustworthy Spaces
- Digital Curation and Forensics

2: Processes, Methods, Measurement of Secure Systems Engineering Development

- Vulnerability Prevention and Detection Tools & Techniques (CWE, CAPEC)
- Architecture for Built-In Secure Systems
- SwA for Agile Software Methodologies
- Operational Resilience (RMM)
- Maturity Cultivation SwA (JFAC)
- Model-Based Engineering and Auto-code Generation Tools

3: SwA Management & Operation

- SwA Workforce Development
- Metrics
- SwA Core Competencies, Education, & Training
- Using Big Data Analysis to Advance Software Assurance Techniques
- SwA Economic Incentives
- Effective Acquisition Policy & Guidance
- Real-Time Modification of Systems

4: Emerging & Disruptive Technology

- SwA in Highly Parallel, High-Performance Computing Environments
- Security in Sociotechnical Computing
- Security of Mobile Applications & Platforms

5: Critical Infrastructure

- Designing Secure Cyber-Physical Systems
- Electronic Effects in SwA
- Global Supply-Chain Security
- Critical Infrastructure Resiliency & Catastrophic Recovery
- Intrinsic Internet Infrastructure Security

Source: SEI

Context: Software Is a Moving Target: Importance of Software Engineering Measurement

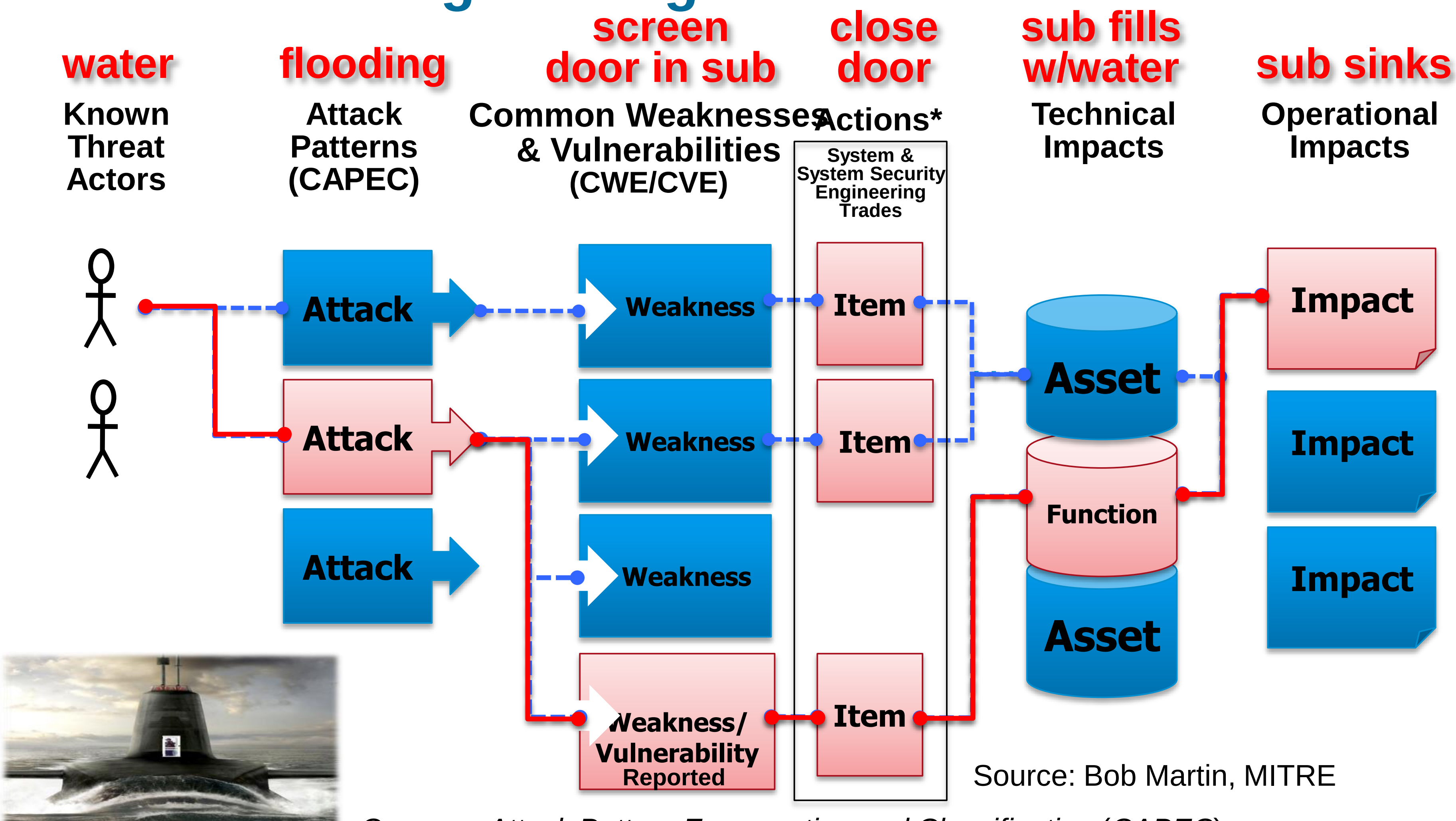
Argument: Need to advance the state of the practice of **software engineering** to improve the **quality** of systems that depend on software

- **Quality is a property/attribute of a system – must be designed in!**

Software engineering requires analysis and synthesis

- **Analysis: decompose a large problem into smaller, understandable pieces**
  - **Abstraction is the key**
- **Synthesis: build (compose) a software from smaller building blocks**
  - **Composition is challenging**

Context: Software Is a Moving Target: Importance of Software Engineering Measurement



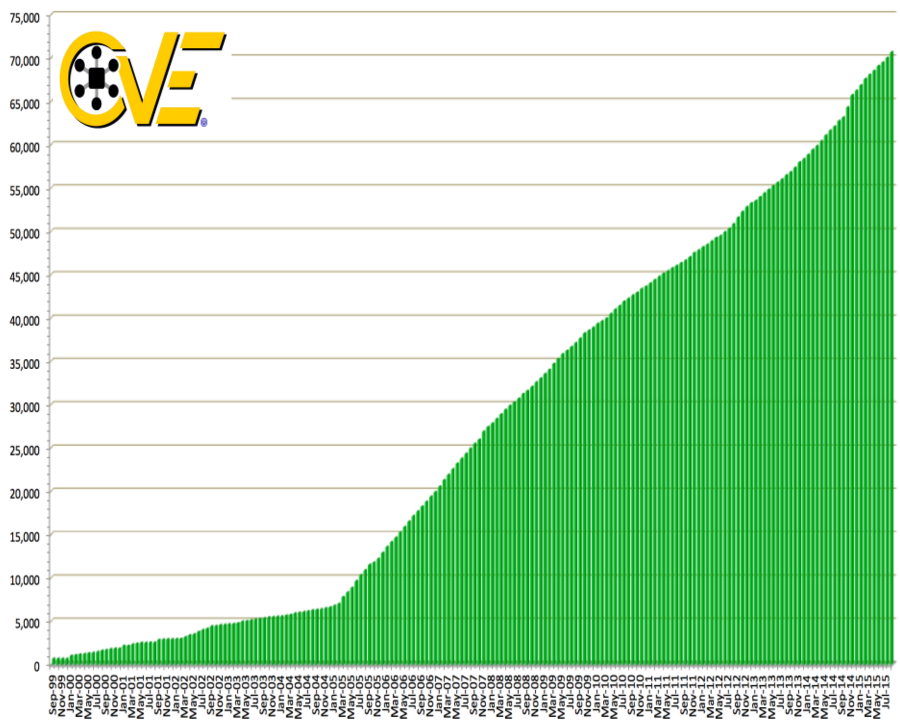
Source: Bob Martin, MITRE

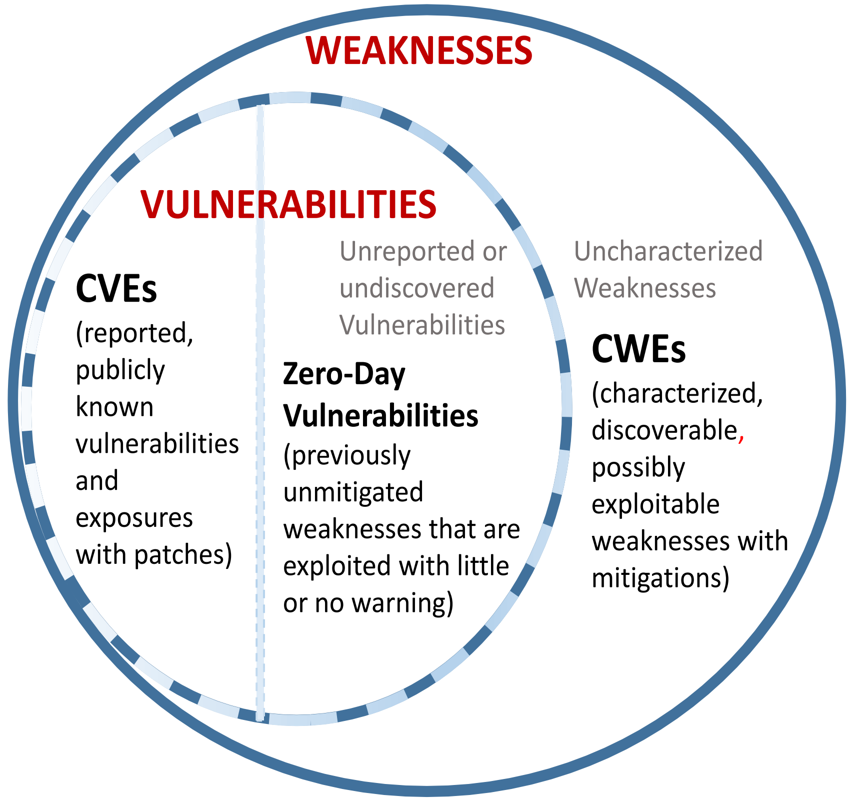
Common Attack Pattern Enumeration and Classification (CAPEC)

* ***Actions*** **include architecture choices; design choices; added security functions, activities, & processes; physical decomposition choices; static & dynamic code assessments; design reviews; dynamic testing; and pen testing.**

Context: Software Is a Moving Target: Reported Common Vulnerabilities and Exposures (CVE)

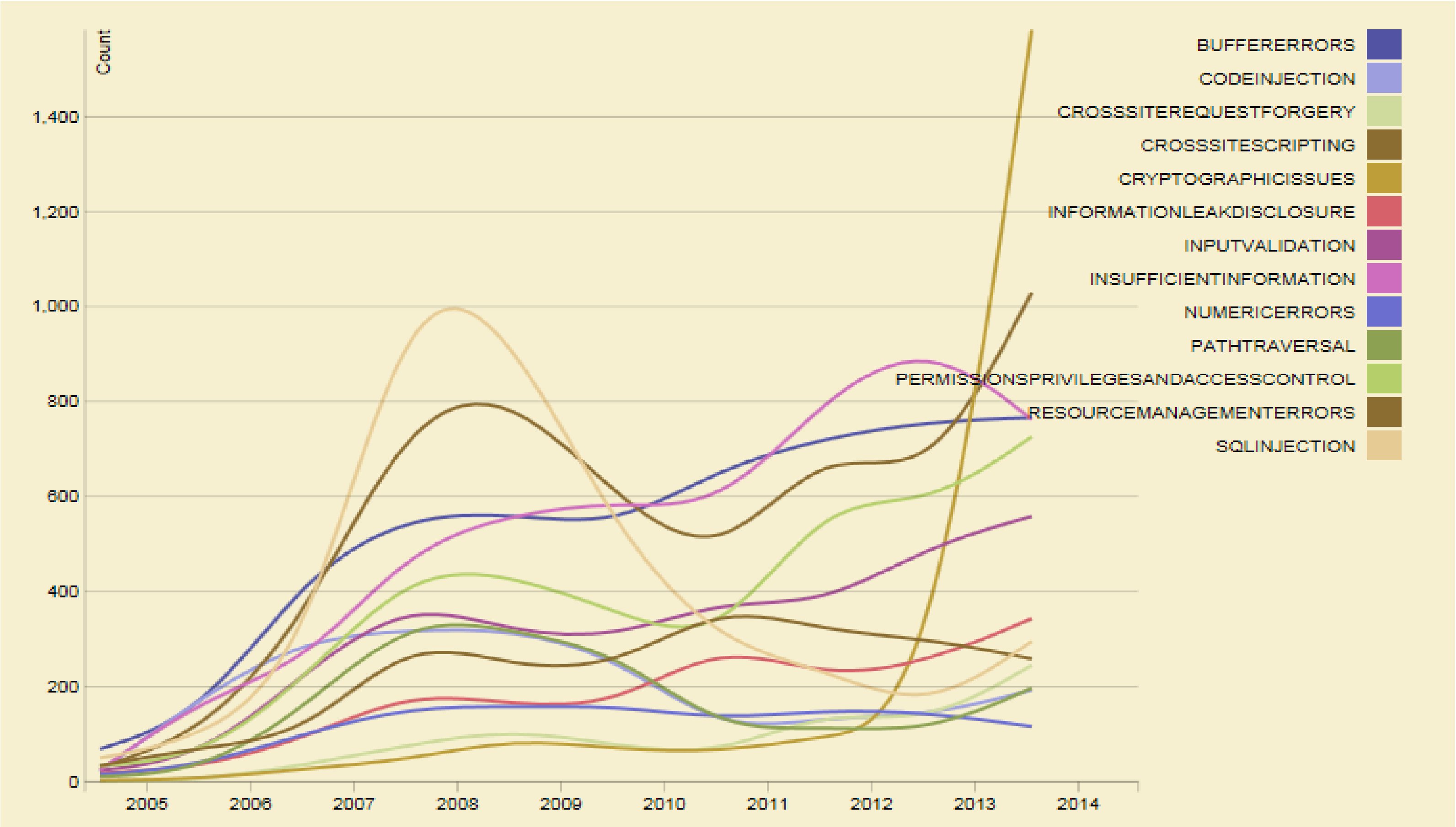
CVE 1999 to 2015





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

Context: Software Is a Moving Target: Common Weakness Enumeration (CWE*)



Source: NIST, National Vulnerability Database, 12 August 2015, web retrieval.

* CWE provides a unified, measurable set of software weaknesses.

Measurement Data

Los Angeles Times | Visual Brow

Anthem hack exposes data on 80 million; experts warn of identity theft

cnet | Search CNET | Reviews | News | Video

Cost of Anthem's data breach likely to exceed $100 million

Context: Software Is a Moving Target: Importance of Software Engineering Measurement

1: Foundations for SwA

- Software Composability
- "Science of Security"
- Modeling, Simulation, Testing, & Certification
- Tailored Trustworthy Spaces
- Scaling of Assurance Techniques
- Digital Curation and Forensics

2: Processes, Methods of Secure Systems Engineering Development

- Vulnerability Prevention and Detection Tools & Techniques (CWE, CAPEC)
- Architecture for Built-In Secure Systems
- SwA for Agile Software Methodologies
- Operational Resilience (RMM)
- Maturity Cultivation SwA (JFAC)
- Model-Based Engineering and Auto-code Generation Tools

3: SwA Management & Operation

- SwA Workforce Development
- Metrics
- SwA Core Competencies, Education, & Training
- Using Big Data Analysis to Advance Software Assurance Techniques
- SwA Economic Incentives
- Effective Acquisition Policy & Guidance
- Real-Time Modification of Systems

4: Emerging & Disruptive Technology

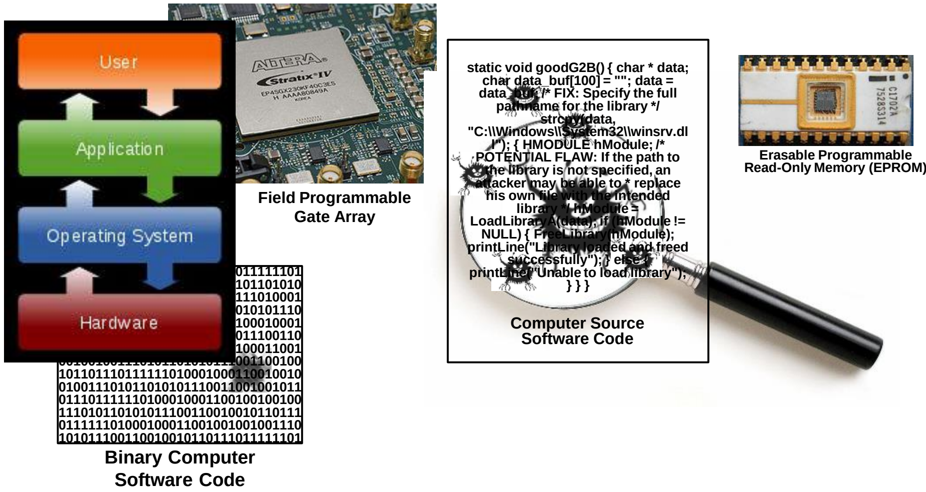
- SwA in Highly Parallel, High-Performance Computing Environments
- Security in Sociotechnical Computing
- Security of Mobile Applications & Platforms

5: Critical Infrastructure

- Designing Secure Cyber-Physical Systems
- Electronic Effects in SwA
- Global Supply-Chain Security
- Critical Infrastructure Resiliency & Catastrophic Recovery
- Intrinsic Internet Infrastructure Security

Source: SEI

Joint Federated Assurance Center (JFAC)



Assure Mission SW and HW Security Across the entire lifecycle

Mandate:

- **Congress directed DoD to "provide for the establishment of a joint federation of capabilities to support the trusted defense system needs…to ensure security in the software and hardware developed, acquired, maintained, and used by the Department" (FY14 NDAA, Sect. 937).**

Expected Outcomes/Deliverables:

- **Federated cross-DoD awareness and coordination of software and hardware assurance (SwA/HwA) capabilities and expertise**
- **Development and sharing of SwA/HwA vulnerability assessment best practices, tested tools, and proven processes**
- **Identification of R&D needs to advance SwA/HwA capabilities for programs in acquisition, operational systems, and legacy systems and infrastructure**

Key Participants:

- **Sponsor(s): ASD(R&E)/DASD(SE)**
- **Contributors: CIO, AF, Army, Navy, USMC, NSA, NRO, MDA, DISA, DMEA**

Approach:

- **Establish Federation of SwA and HwA capabilities to support programs in DoD acquisition planning and execution**
- **Support program offices across lifecycle by identifying and facilitating access to DoD SwA and HwA expertise and capabilities, including policies, guidance, requirements, best practices, contracting language, training, and testing support**
- **Identify and address SwA and HwA capability gaps across the DoD**
- **Coordinate with DoD R&D for SwA and HwA**
- **Procure, manage, and distribute enterprise licenses for SW and HW assurance tools**
- **Reach out to other govt departments and agencies, industry, academia**

Milestones:

Formed Steering Committee and Working Groups	07-2014
Initiated first series of technical tasks	09-2014
Charter signed by Deputy Secretary of Defense	02-2015
Congressional Report on funding, organization, management, and operations of JFAC signed & submitted	03-2015
CONOPS signed by stakeholders of Federation	10-2015
Joint Federated Assurance Center (JFAC) IOC	03-2016
Capability Assessment, Gap Analysis, Strategic Plan	09-2016

Example 4

A Quick Look at Potential Business Resilience and Opportunities for Software Assurance Measurement

Disruptive Events…

Natural or Manmade Accidental or Intentional Small or Large Information Technology or Not	• Fire • Flooding • IT failures • Earthquakes • Cyber attacks • Severe weather • Network failures • Technology failures • Organizational changes • Loss of service provider • Strikes or other labor actions • Loss of customer or trading partner • Chemical, biological, nuclear hazards • Unavailability of workforce • Failed internal processes • Supply-chain disruption • Employee kidnappings • Workplace violence • Data corruption • Product failure • Power outages • Civil unrest • Terrorism • Fraud • Etc.

Result in

Interruption of Business Processes

Source: SEI

…through which risks are realized

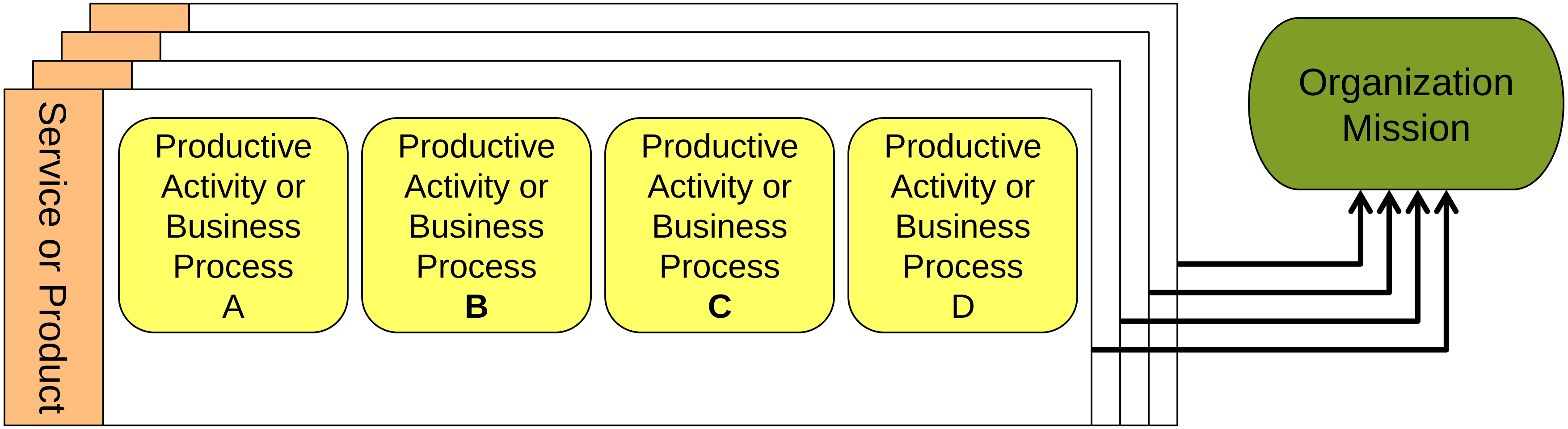
Expansion of Risk Environment

- Globalization
- Operational complexity
- Pervasive use of technology
- Intertwining of cyber and physical domains
- Increased role of cybersecurity in securing physical assets
- Movement toward intangible assets
- Global economic pressures
- Regulatory and legal boundaries
- Geopolitical pressures

Source: SEI

Successful management of operational risk may require a (significant) shift in thinking and approach.

Productive Activities and Business Processes



Activities that the organization (and/or its suppliers) perform to ensure that services and products are generated

A service or product is made up of one or more productive activities

Mission of productive activities is to enable service/product mission

Source: SEI

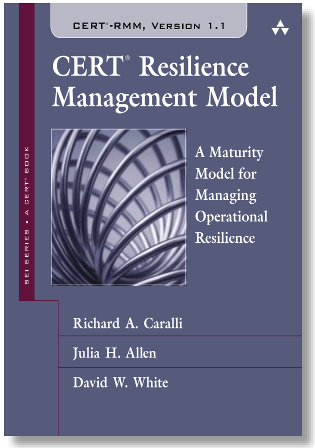
CERT® Resilience Management Model

Engineering	(Module 5)
ADM	Asset Definition and Management
CTRL	Controls Management
RRD	Resilience Requirements Development
RRM	Resilience Requirements Management
RTSE	Resilient Technical Solution Engineering
SC	Service Continuity

Enterprise Management	(Module 6)
COMM	Communications
COMP	Compliance
EF	Enterprise Focus
FRM	Financial Resource Management
HRM	Human Resource Management
OTA	Organizational Training and Awareness
RISK	Risk Management

Operations	(Module 7)
AM	Access Management
EC	Environmental Control
EXD	External Dependencies Management
ID	Identity Management
IMC	Incident Management and Control
KIM	Knowledge and Information Management
PM	People Management
TM	Technology Management
VAR	Vulnerability Analysis and Resolution

Process Management	(Module 9)
MA	Measurement and Analysis
MON	Monitoring
OPD	Organizational Process Definition
OPF	Organizational Process Focus



Source: SEI

Perspectives:

Struggles in Software Engineering and the Persistent Pursuit of Software Quality Assurance Measurement

Struggles in Software Engineering and the Persistent Pursuit of Software Quality Assurance Measurement:

Some Things We Know About Software

- Ubiquitous
- Codebase is increasing
- Vulnerabilities (defects, flaws) are increasing
- Represents increasingly more system functionality and cost
- Research needed to address significant challenges
- Software-reliant systems are becoming more complex and intertwined
- Nationally and globally important
- Need to manage software systems better
- Software quality must be engineered/designed in

Pursuit of software quality measurement is increasingly more important!

Infancy of Software Engineering Assurance Measurement

Source: SEI

Infancy of Software Engineering

	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/ treatment	• Several areas of study: computer science, software/systems engineering, IT, HCI, social dynamics, AI • All nodes attached to/rely on netted system
R&D and Launch Cycle	10–20 years	10–20 years	Significantly **compressed**; solution time to market needs to happen very quickly

Source: SEI

HCI: Human Computer Interaction; AI: Artificial intelligence

Software Provides Great Capabilities to Bifurcated Communities: Benefits Measured Differently

SAMSUNG

Google

Source: SEI

Software Is Today's Strategic Resource as Measured by Increased Globalization

Increasing Globalization

Source: SEI

Software is the foundation of the cyber environment, enabling explorations into new frontiers – its profound effect is yet to be effectively measured

[Tianhe-2 Supercomputer]

Summary

- Assured software represents the building blocks for the modern society
- The software assurance measurement community has made a good start, but more work is needed
- It must close the gaps in the development of effective software and system measurement capabilities

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