Software Engineering Institute: Support of DOD Open Systems Standards

Matthew Milazzo
Thomas Merendino

October 17, 2017

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

© 2017 Carnegie Mellon University

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

DM17-0869

Carnegie Mellon University's Software Engineering Institute

Established as a DoD FFRDC at Carnegie Mellon University in 1984

Started CERT program in cybersecurity in 1988

SEI is one of two DoD FFRDC labs and the only DoD FFRDC focused on software and cybersecurity.

Over 600 Staff

Locations in Pittsburgh, Arlington, Los Angeles, Boston, San Antonio, and ***Patuxent River NAS***

Pittsburgh, PA

California, MD

Our Mission and Strategy

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

We achieve our mission through

- Research
- Collaboration
- Development and Demonstration
- Transition

SEI's Role, Capabilities, and Value Proposition

Role

- Middle position between government, DoD operational focus and R&D

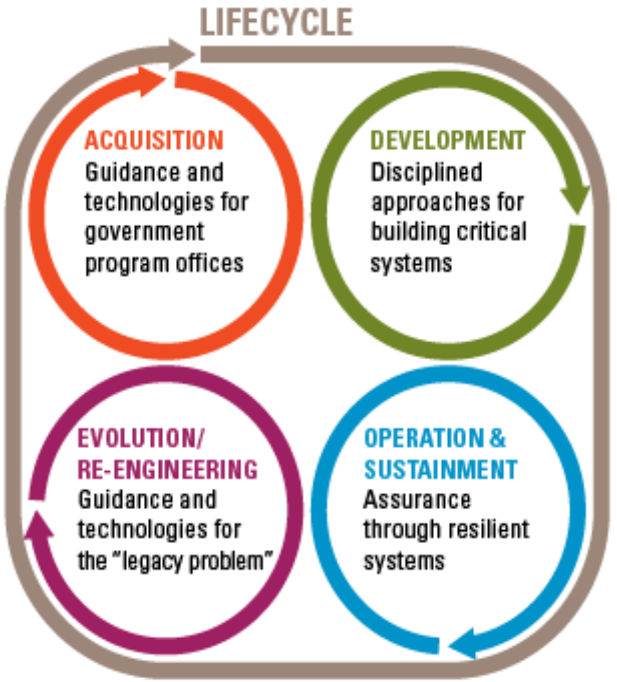
Capabilities

- Unique expertise spanning entire (software and acquisition) life cycle
- Access to data and talent including leading university R&D
- Operate along entire spectrum of fundamental research to classified

Value Proposition

- Bringing the best academic/industry/government thinking to the most challenging problems in government software and cyber domains, free of conflict of interest

Customers in DoD, Federal Agencies, IC, State Agencies, and Industry – Across Multiple Sectors



SEI Solutions Rely on Work in Our Technical Areas

Enduring

Software Engineering & Information Assurance

Enable high quality, secure software-based systems in a predictable, affordable manner

Cyber Security

Develop improved systems, repeatable practices, and capable personnel to enable cyber missions

System Verification & Validation

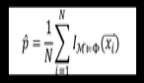
Enhance confidence in the systems engineering lifecycle with evidence-based methods and tools

Make software less costly and more resilient and mission capable by…

ruthlessly automating all aspects of design, development, integration, testing, deployment, operations, defense, and sustainment of software systems

Emerging

Data Modeling & Analytics: Develop and apply mathematically rigorous data collection, analysis, and visualization techniques

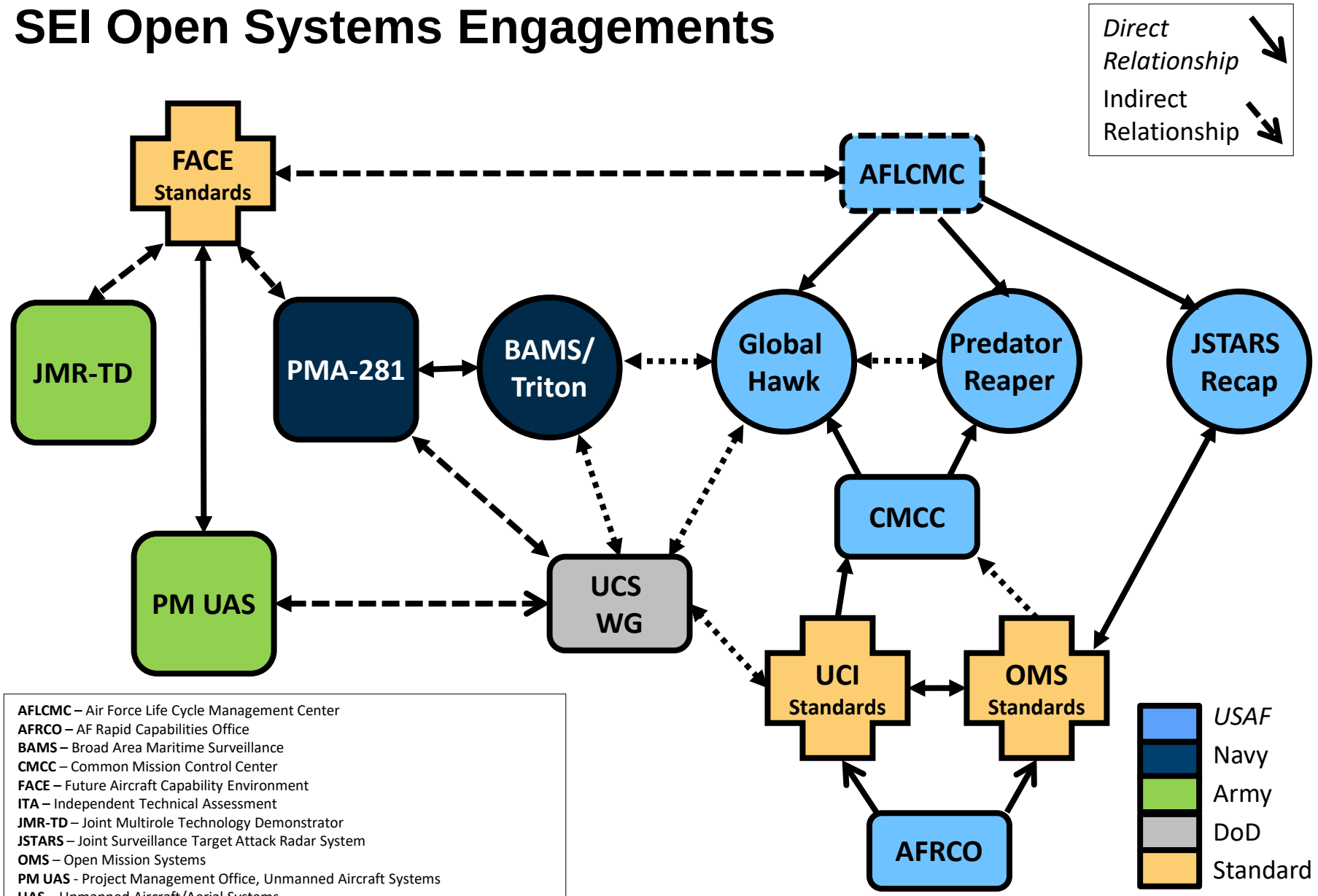


C4ISR Mission Assurance: Enable timely decisions that account for risk metrics personnel

Autonomy & Counter-Autonomy: Develop evidence that indicates the trustworthiness, dependencies, & vulnerabilities of autonomous systems

Human-Machine Interactions: Invent, assess, improve comprehensible, safe, and trustworthy technologies for humans to use and team with machines

SEI Open Systems Engagements



AFLCMC – Air Force Life Cycle Management Center
AFRCO – AF Rapid Capabilities Office
BAMS – Broad Area Maritime Surveillance
CMCC – Common Mission Control Center
FACE – Future Aircraft Capability Environment
ITA – Independent Technical Assessment
JMR-TD – Joint Multirole Technology Demonstrator
JSTARS – Joint Surveillance Target Attack Radar System
OMS – Open Mission Systems
PM UAS - Project Management Office, Unmanned Aircraft Systems
UAS – Unmanned Aircraft/Aerial Systems
UCS WG – UAS Control Segment Working Group

AF Guidance for Open Systems Development

SEI facilitated elicitation of list of scenario descriptions from AF leadership meant to articulate and assess the benefits that the Air Force Enterprise would derive from programs adopting open systems:

- Successful standards adoption (e.g. UAI)
- Unsuccessful standards adoption (e.g. ADA)
- Other scenarios including:
  - Airworthiness
  - Nuclear Certification
  - Positive Cyber Resilience
  - Platform-Agnostic Capabilities
  - Restrictive and Expansive IA

Tutorials on Open Systems Architecture

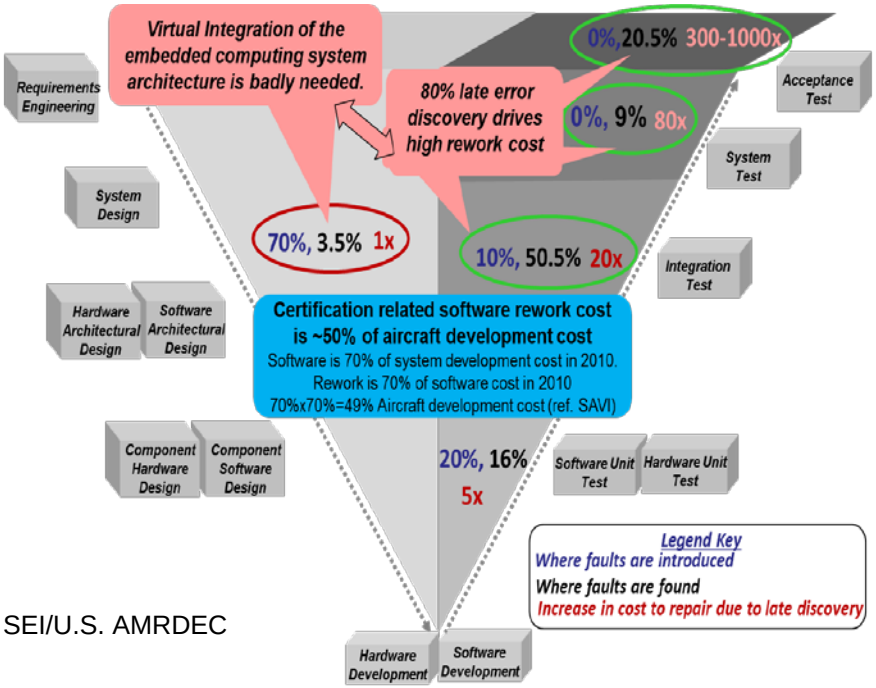
SEI develops and provides DOD and Government customers custom instructional tutorials - e.g. “Introduction to Open Systems” developed under USAF tasking that introduces concepts for open systems and architectures with a focus on software.

- Used to issue additional guidance, describes benefits and challenges of adopting open architectures and standards
- Highlights technical and acquisition challenges

SEI Research w/Open Systems Focus

ACVIP (Architecture Centric Virtual Integration Process)

- Research at Redstone Arsenal/Huntsville focuses on reducing cost of integration.
- Element of model-based engineering.
- Bringing FACE and AADL as components in the virtual integration process



SEI/U.S. AMRDEC

SW Product Line – previous SEI research now in practice

- SWpL shown to enable common core software assets to be deployed in multiple heterogeneous environments – build on hardware product line practices…Back to the Future.

LOCAL CONTACT INFORMATION

Annie Drazba

Email: drazba@sei.cmu.edu

Telephone: +1 240-237-8032

U.S. Mail

Software Engineering Institute
23076 Three Notch Road
Suite 201
California, MD 20619

Website

www.sei.cmu.edu/contact.cfm