SEI 2015 Research Review

Kevin Fall, PhD

Deputy Director, Research, and CTO

kfall@cmu.edu

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

SEI and CMU

Welcome to the Software Engineering Institute

SEI is a Federally-Funded R&D Center

- Operated by Carnegie Mellon University
- Other FFRDCs: MITRE, MIT/Lincoln, LLNL, IDA, JPL

Within CMU, we resemble a “school” or “college” in the org chart

- Such as: Computer Science, Engineering, Fine Arts, Humanities/Social Science (Dietrich), Business (Tepper), Science (Mellon), Public Policy and Information Science (Heinz)
- Our ~600 employees are CMU staff members
  - Some hold additional academic titles (researcher, adjunct faculty)

R&D Work at SEI

Line funded projects (“line” and “LENS”)

- LENS = Line-funded Exploratory New Starts
- One and two year projects, with collaborators

Project work (with individual “customers”)

- PWP = Project Work Plans

As a DoD FFRDC, we are subject to ‘ceiling’ (called “STE”)

- Applies to our entire DoD-supported work

Line Funded Project Proposals

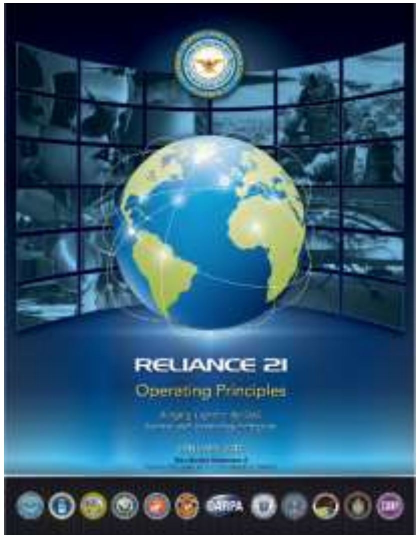
Project proposals are solicited in approximately January and April each year

- 1-2 year "Line" projects ; 1 year "LENS" projects
- Selected and approved projects start in new FY (Oct 1)

Projects for FY16 are just getting started

We collaborate with (and often fund) joint work with other parts of CMU and other research institutions

DoD Research and Engineering (R&E) Reliance 21: Operating Principles



RELIANCE 21

Operating Principles

Available at www.defenseinnovationmarketplace.mil/resources/2014-Reliance21OperatingPrinciples.pdf

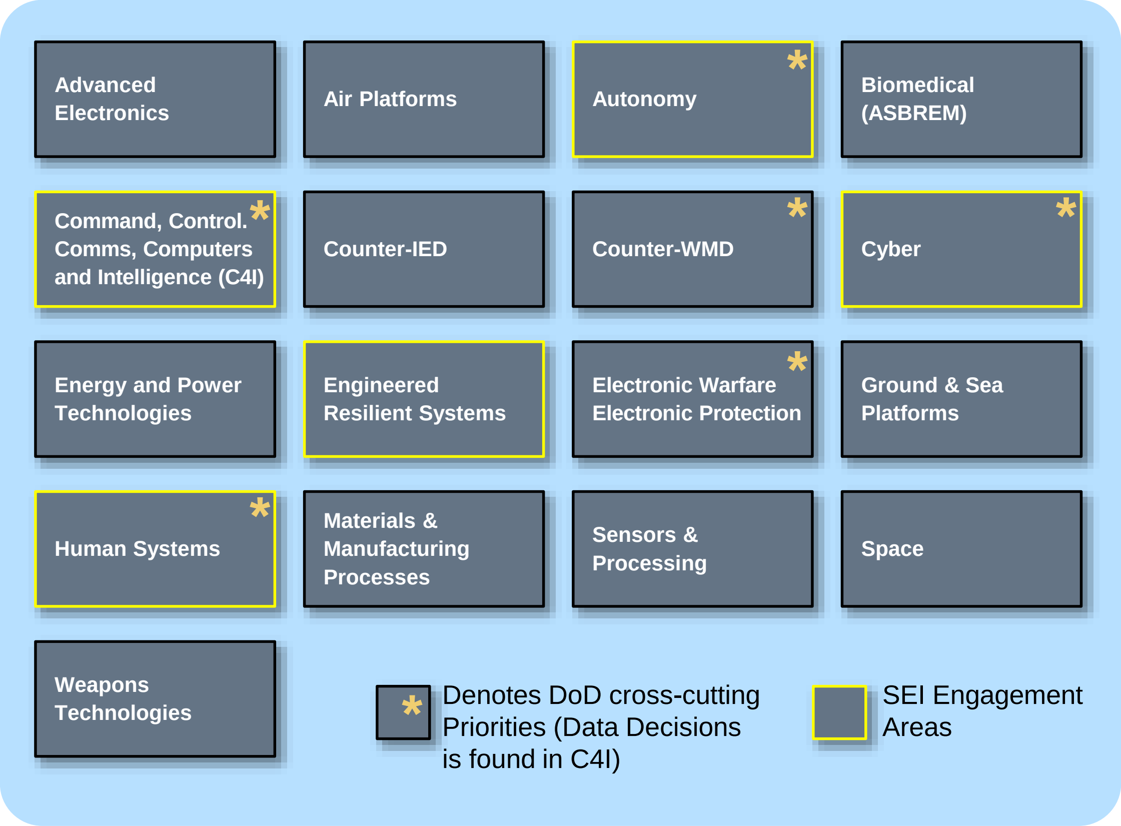
From *16th Annual Science and Engineering Technology Conference* , Al Shaffer, Principal Deputy, ASD(R&E), Mar 2015

Operational Framework of the DoD S&T Joint Planning and Coordination process (updated January 2014)

- Executes the DoD R&E Strategies
  - Portfolio Management Infrastructure to enable:
  - Information sharing
  - Alignment of effort against capability gaps
  - Coordination of priorities and investments
  - Exploit synergies and develop new opportunities
  - Support for scientists and engineers across the DoD R&E Enterprise
- Communities of Interest (COI)
  - 17 cross-domain technical areas, each with their own Steering Group Lead and multiple technical ‘challenge areas’ or sub groups, staffed with Subject Matter Experts (SMEs)
  - Specific cross-cutting technology areas where there is substantial investment across multiple Components

Reliance 21: Communities of Interest (CoIs)

Mission: Leverage **global commercial** and **non-commercial research and development (R&D)** to ensure superior and affordable development in areas critical to defense, including but not limited to:



Advanced Electronics	Air Platforms	Autonomy *	Biomedical (ASBREM)
Command, Control. Comms, Computers and Intelligence (C4I) *	Counter-IED	Counter-WMD *	Cyber *
Energy and Power Technologies	Engineered Resilient Systems	Electronic Warfare Electronic Protection *	Ground & Sea Platforms
Human Systems *	Materials & Manufacturing Processes	Sensors & Processing	Space
Weapons Technologies			

* Denotes DoD cross-cutting Priorities (Data Decisions is found in C4I)

□ SEI Engagement Areas

- 17 **cross-domain** technical areas, each with their own Steering Group Lead and multiple technical ‘challenge areas’ or sub groups, staffed with Subject Matter Experts (SMEs) **Each with an international focus**
- Specific cross-cutting technology areas where there is substantial investment **across multiple Components**

What You Will Hear

The 2015 Research Review covers the line-funded work from FY15 (our FY starts Oct 1) and area introductions, three keynote talks, and two talks from CMU’s Cylab

Technical details can be shared if:

- It is covered by a ‘Fundamental Research’ exclusion
- Contains no sensitive information (PII, etc)
- They are already available in public

For some projects, additional detail may be possible to discuss elsewhere.

Topics for the Research Review

Acquisition and Management

Assured Design

C4I

Human Factors

Cylab Presentations – Usable Security/Privacy, Facial Recognition

Verification and Validation

Cybersecurity

Motivation: Software and Complexity

Composing [simple] software components leads to complexity

- that is difficult to reason about and secure
- especially when networked together across organizations

At least 75% of organizations rely on open-source software

- and it is not immune from seemingly simple problems
- (e.g., Heartbleed, Shellshock, etc)

Neither is non-open/proprietary embedded system software

- (e.g., Toyota, Boeing 787 shutdown)

IoT will likely increases the challenges

- different expertise, use cases, security needs, privacy issues

How to achieve (software) *capabilities with confidence*?

- **… Can we just ‘build it better’?**

Software Engineering and Cybersecurity

Software Engineering includes studies of

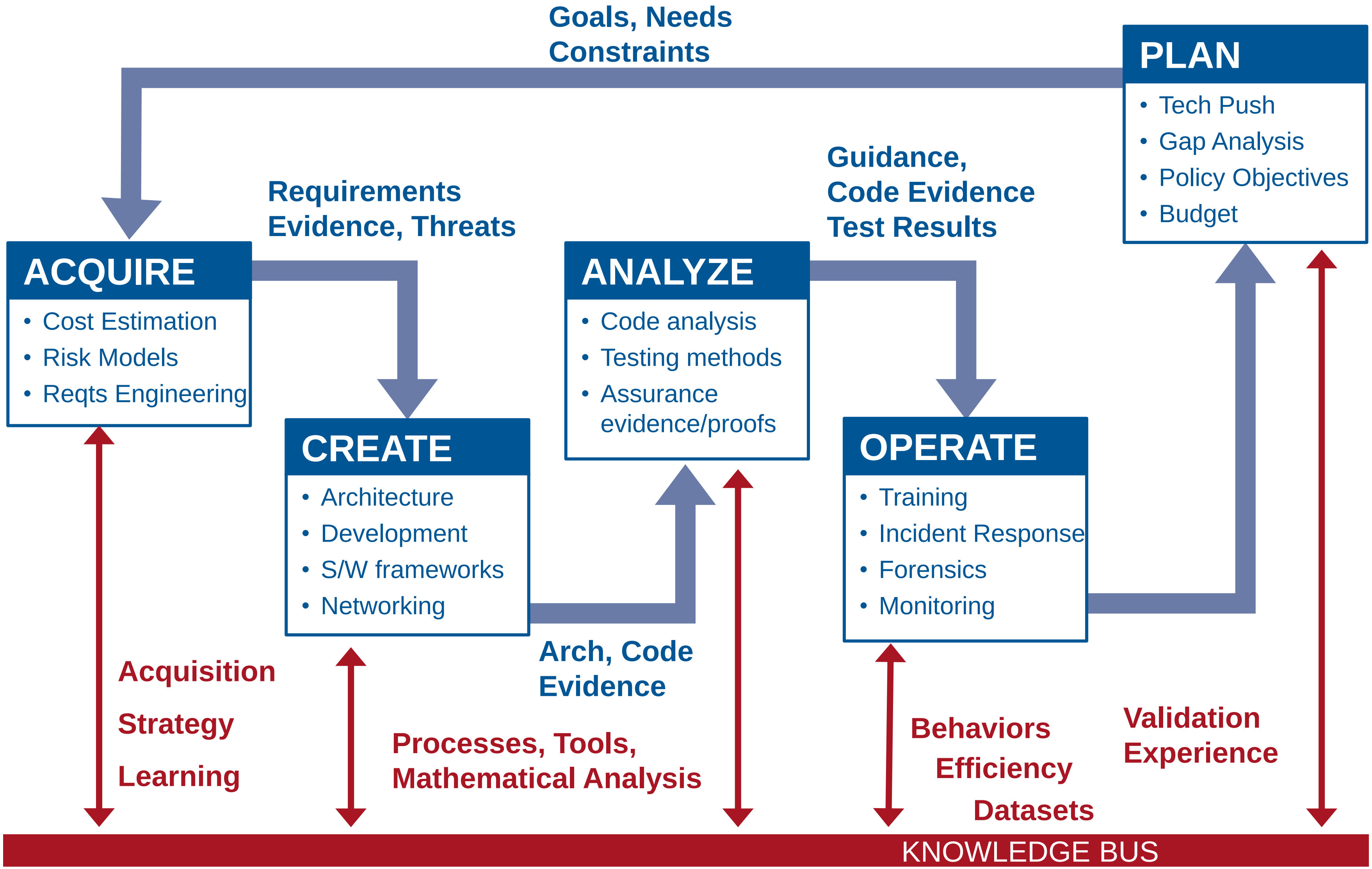
- Software development efficiency and metrics (faults, function points)
- Requirements and validation, verification and formal methods
- Scale, operational performance, configuration management
- Software development techniques and languages
- Logic / model theory and related mathematics

Cybersecurity includes studies of

- Malware analysis and countermeasures
- Forensics
- Incident response, remediations, and threat intelligence
- Software development techniques
- Cryptography and related mathematics

Well, there's *some* overlap

Technical Strategic Framework



Goals, Needs
Constraints

PLAN

- Tech Push
- Gap Analysis
- Policy Objectives
- Budget

Requirements
Evidence, Threats

Guidance,
Code Evidence
Test Results

ACQUIRE

- Cost Estimation
- Risk Models
- Reqts Engineering

ANALYZE

- Code analysis
- Testing methods
- Assurance evidence/proofs

CREATE

- Architecture
- Development
- S/W frameworks
- Networking

OPERATE

- Training
- Incident Response
- Forensics
- Monitoring

Arch, Code
Evidence

Acquisition

Strategy

Learning

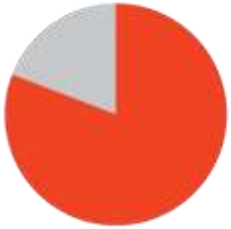
Processes, Tools,
Mathematical Analysis

Behaviors
Efficiency
Datasets

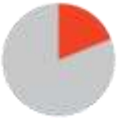
Validation
Experience

KNOWLEDGE BUS

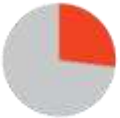
Lifecycle View



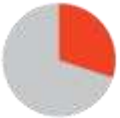
More than 81% do not coordinate their security practices in various stages of the development life cycle.□



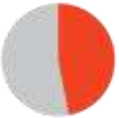
19% fail to carry out security requirement definition.



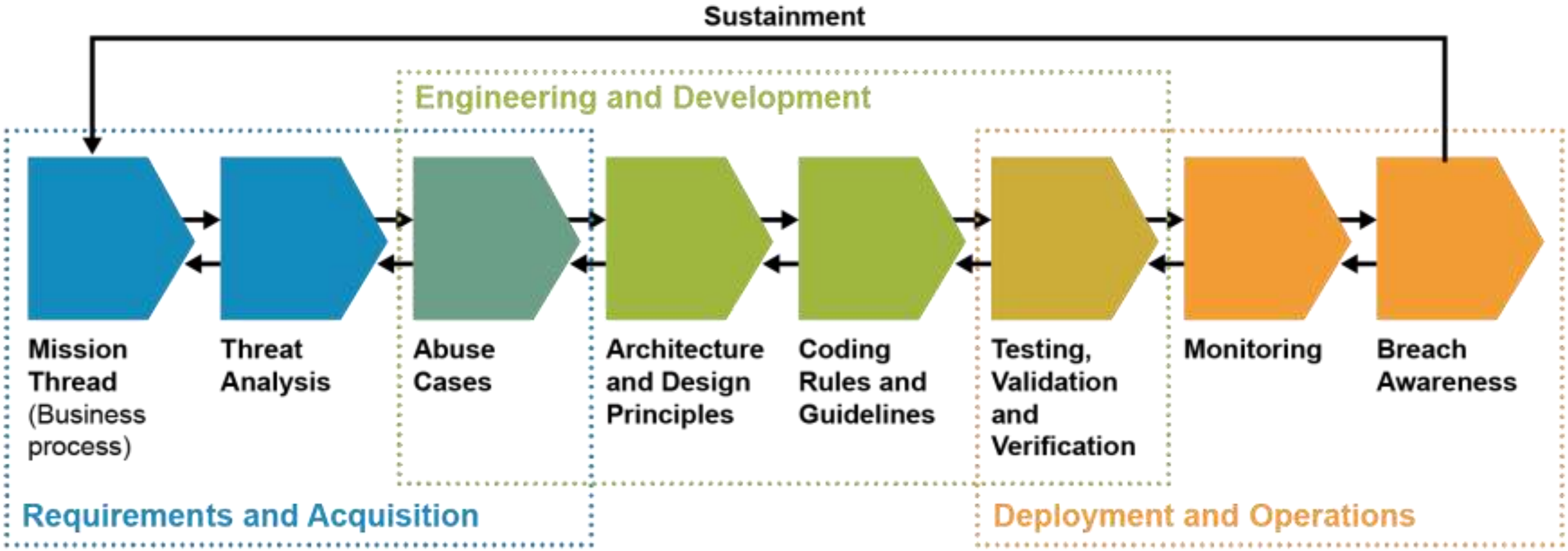
27% do not practice secure design.



30% do not use static analysis or manual code review during development.



47% do not perform acceptance tests for third-party code.



Sustainment

Engineering and Development

Mission Thread (Business process)

Threat Analysis

Abuse Cases

Architecture and Design Principles

Coding Rules and Guidelines

Testing, Validation and Verification

Monitoring

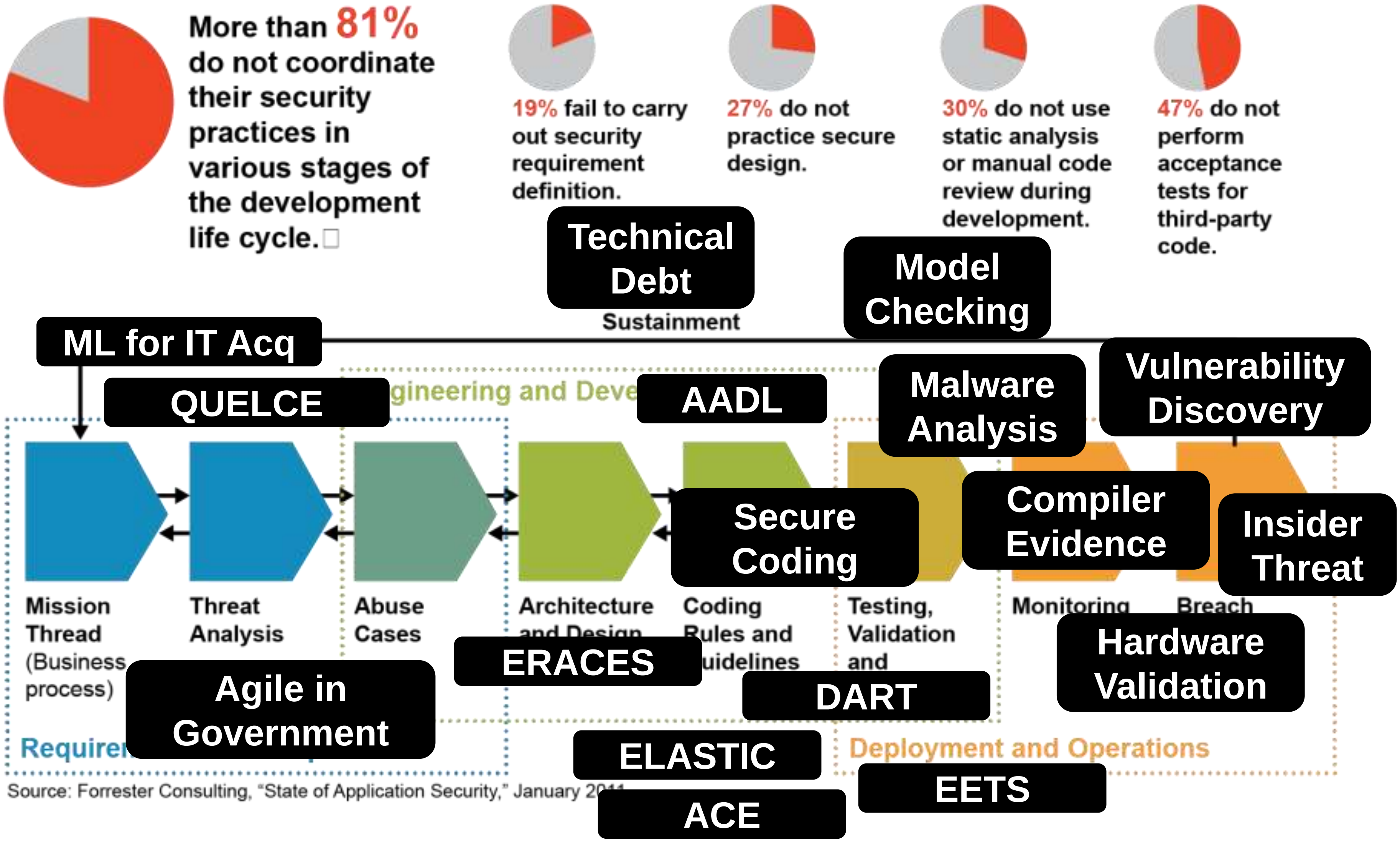
Breach Awareness

Requirements and Acquisition

Deployment and Operations

Source: Forrester Consulting, "State of Application Security," January 2011

Lifecycle View



More than 81% do not coordinate their security practices in various stages of the development life cycle.

19% fail to carry out security requirement definition.

27% do not practice secure design.

30% do not use static analysis or manual code review during development.

47% do not perform acceptance tests for third-party code.

Source: Forrester Consulting, "State of Application Security," January 2011

Technical Debt

Model Checking

ML for IT Acq

QUELCE

AADL

Malware Analysis

Vulnerability Discovery

Secure Coding

Compiler Evidence

Insider Threat

ERACES

Agile in Government

DART

Hardware Validation

ELASTIC

EETS

ACE

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.

Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the United States Department of Defense.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN “AS-IS” BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

DM-0002871