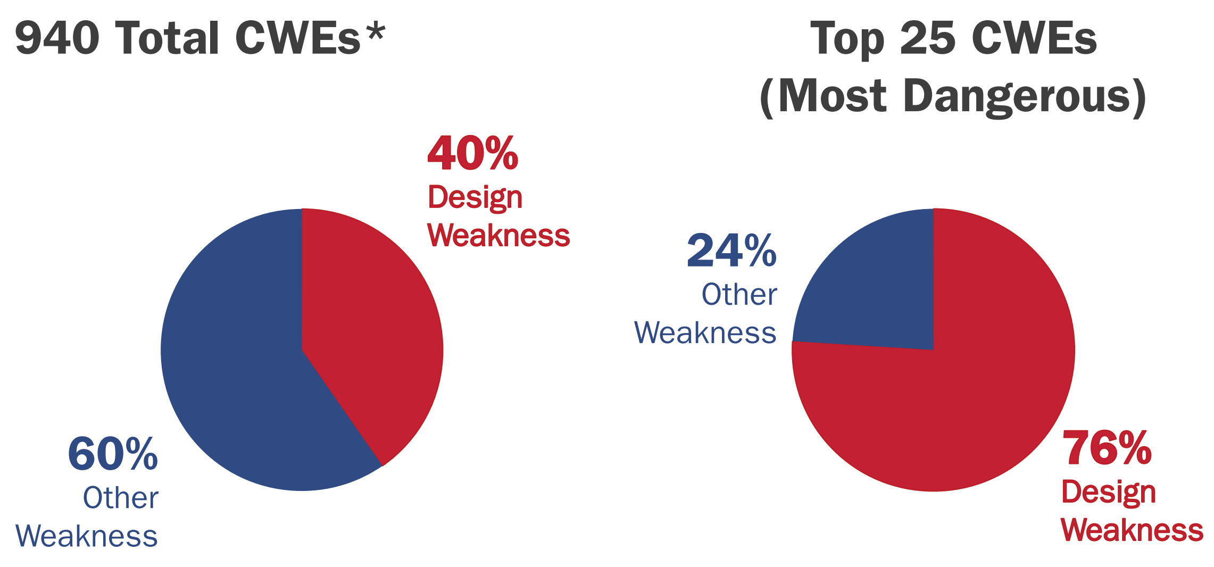
Security Engineering Risk Analysis (SERA)

> **“We wouldn't have to spend so much time, money, and effort on network security if we didn't have such bad software security.”**
>
> Bruce Schneier in Viega and McGraw, *Building Secure Software*, 2001

Importance of Good Design

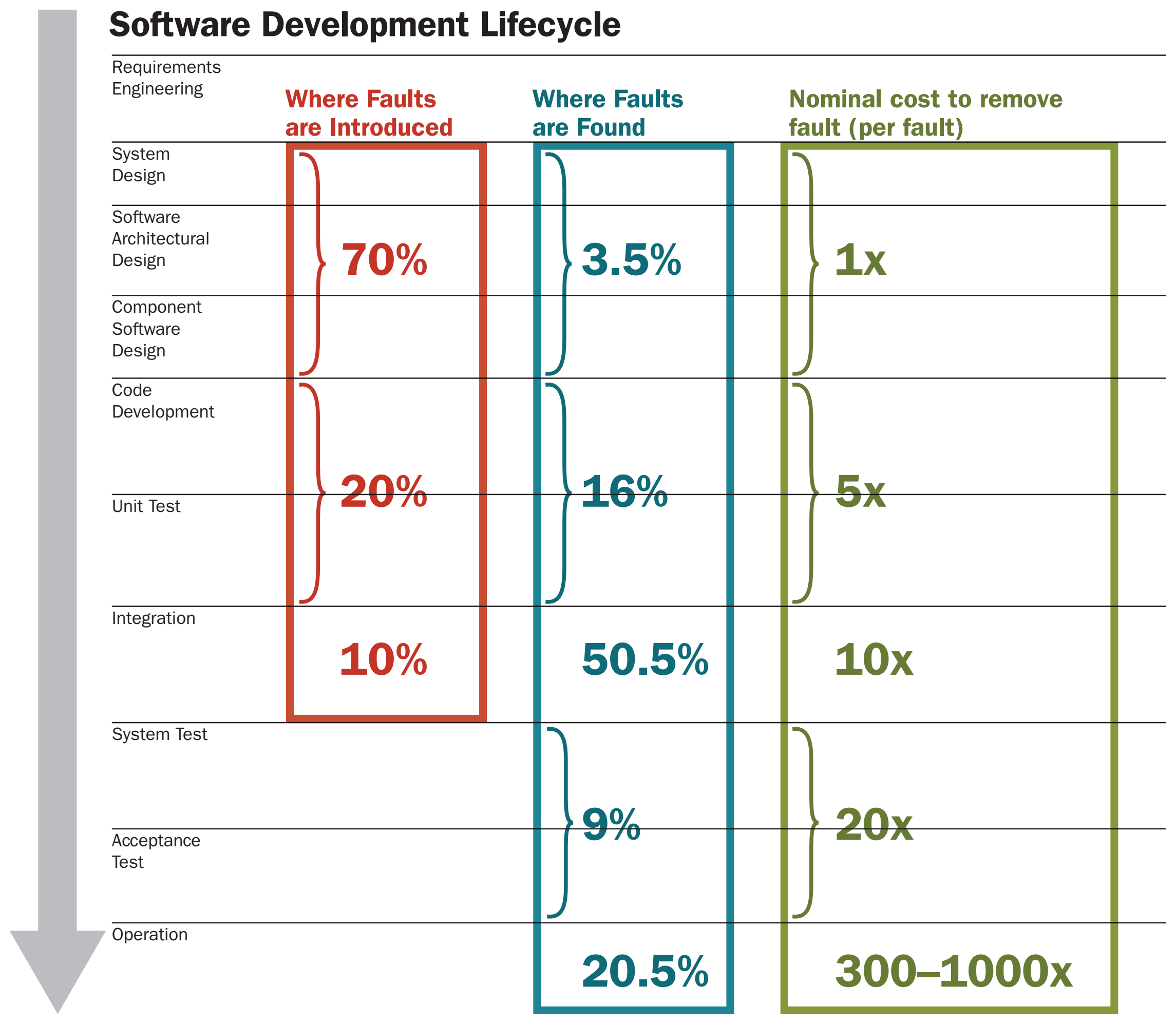


*MITRE’s Common Weakness Enumeration (CWE)
Source: http://cwe.mitre.org/ as of Feb 9, 2014

Software Faults: Introduction, Discovery, and Cost

Faults account for 30–50% percent of total software project costs.

- Most faults are introduced before coding (~70%).
- Most faults are discovered at system integration or later (~80%).



Errors during requirements engineering are costly!

- Defects cost up to 200 times more once fielded than if caught in requirements engineering
- Reworking defects consumes >50% of project effort
- >50% of defects are introduced in requirements engineering

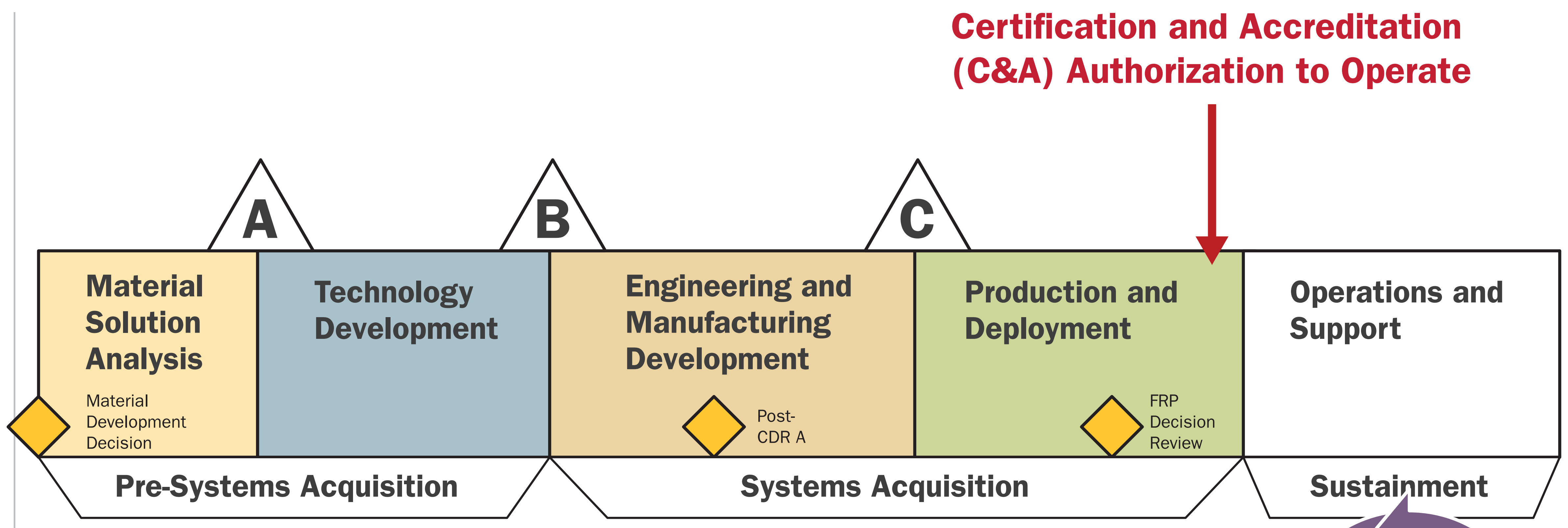
Goal: Reduce Security Design Risk

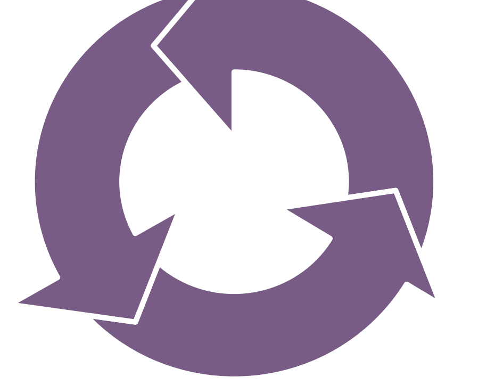
Security design weaknesses

- Are not addressed by security controls or static analysis tools and
- Cannot be easily addressed during operations (e.g., by patching systems)

Applying SERA during requirements specification

- Provides early detection of design weaknesses for remediation
- Reduces residual security risk during operations

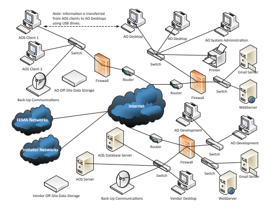
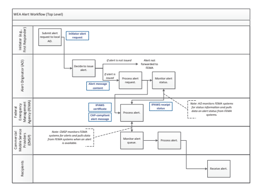
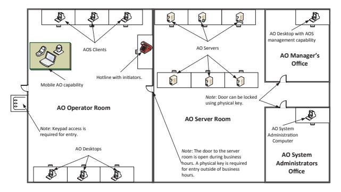

Certification and Accreditation
(C&A) Authorization to Operate
A
B
C
Material Solution Analysis
Material Development Decision
Technology Development
Engineering and Manufacturing Development
Post-CDR A
Production and Deployment
FRP Decision Review
Operations and Support
Pre-Systems Acquisition
Systems Acquisition
Sustainment



Security Engineering Risk Analysis

1. Establish operational context.

Modeling Techniques

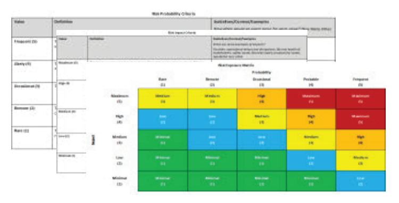




2. Identify risk.

Risk Identification Worksheet

3. Analyze risk.

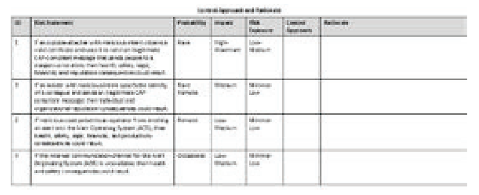
Risk Evaluation Criteria



Risk Analysis Worksheet

4. Develop control plan.

Control Approach Worksheet



Control Plan Worksheet

Software Engineering Institute | Carnegie Mellon University

Contact: Carol Woody cwoody@cert.org