Systems Engineering and System Security Engineering Requirements Analysis and Trade-Off Roles and Responsibilities

Melinda Reed

Office of the Deputy Assistant Secretary of Defense for Systems Engineering

18th Annual NDIA Systems Engineering Conference

Springfield, VA | October 28, 2015

Incorporating SSE Into SE

- **System Security Engineering (SSE) is an element of system engineering that applies scientific and engineering principles to identify security vulnerabilities and minimize or contain risks associated with these vulnerabilities [DoDI 5200.44]**

- **In order to properly consider system security as a design consideration:**
  - SSE efforts must have a repeatable process for analyzing and integrating SSE specialties to implement a comprehensive protection scheme
  - Results of the analysis should also consider cost, schedule and technical constraints to inform SE trade-offs

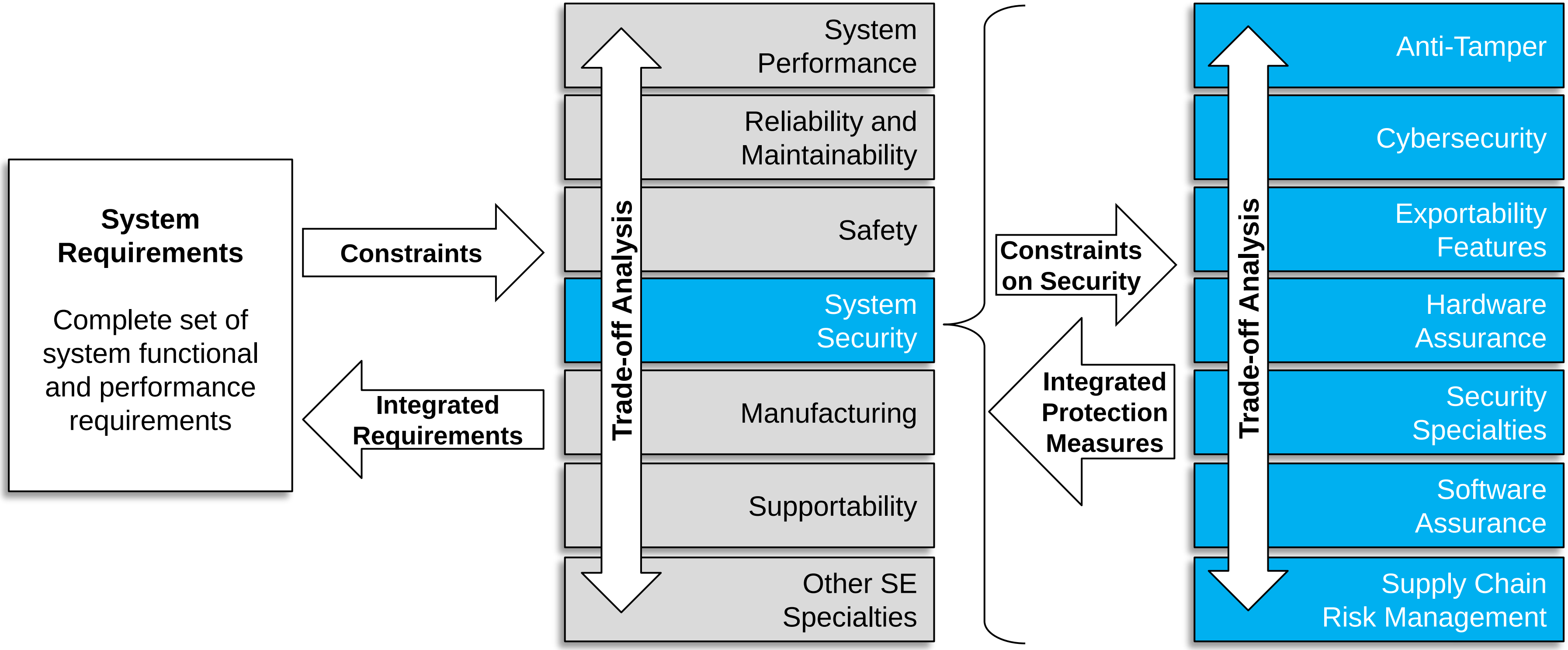
- **To integrate system security engineering into SE activities:**
  - Structure SSE responsibilities in the context of SE activities to align with SE efforts
  - Ensure System Engineering considers SSE in their design decisions, to include understanding threats and vulnerabilities to the program and system.
  - Utilize SE tools and methods for system security trade-off analyses

Distribution Statement A – Approved for public release by DOPSR on 10/19/2015, SR Case # 16-S-0128 applies. Distribution is unlimited.

SE and SSE Trade-off Analyses Concept

Systems Engineering Specialties

System Security Engineering Specialties



System Requirements

Complete set of system functional and performance requirements

Constraints

Integrated Requirements

Trade-off Analysis

System Performance

Reliability and Maintainability

Safety

System Security

Manufacturing

Supportability

Other SE Specialties

Constraints on Security

Integrated Protection Measures

Trade-off Analysis

Anti-Tamper

Cybersecurity

Exportability Features

Hardware Assurance

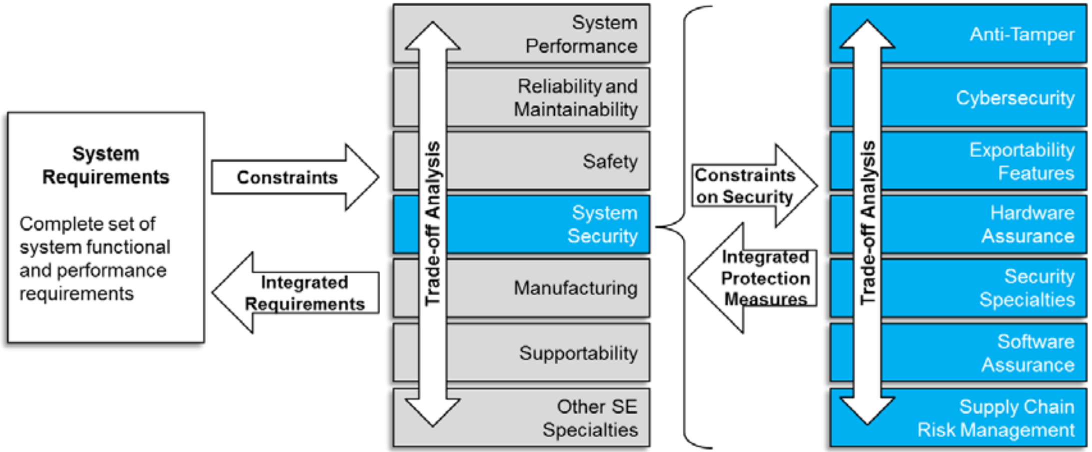
Security Specialties

Software Assurance

Supply Chain Risk Management

Roles Supporting SSE Trade-off Analyses

- **Systems Engineer:** Synthesizes and balances the requirements from each SE specialty (one of these specialties is SSE).
- **System Security Engineer:** Synthesizes and balances contributions from across security disciplines to achieve comprehensive system protection with the constraints of cost, schedule, and performance while maintaining an acceptable level of risk. These security disciplines include
  - *SSE specialties:* anti-tamper, cybersecurity, hardware assurance, software assurance, and supply chain risk management
  - *Security specialties:* personnel security, industrial security, physical security, and information security
- **System Security Engineering Specialists:** Identify the system security vulnerabilities and the needed system security protection measures within the scope of a particular system security engineering specialty.
- **Security Specialists:** Define security requirements and processes within a particular security specialty.



Distribution Statement A – Approved for public release by DOPSR on 10/19/2015, SR Case # 16-S-0128 applies. Distribution is unlimited.

Responsibilities For Each Role Related to Program Protection

- **Systems Engineer**
  - Integrates Program Protection into the program’s systems engineering processes
  - Conducts trade-off analyses with respect to system security and other design considerations
  - Collaborates with the system security engineer on any system security requirements adjustments
  - Incorporates system security requirements into the system performance specification, technical baselines, and solicitation documents
  - Ensures the PPP accurately reflects the systems engineering constraints and decisions

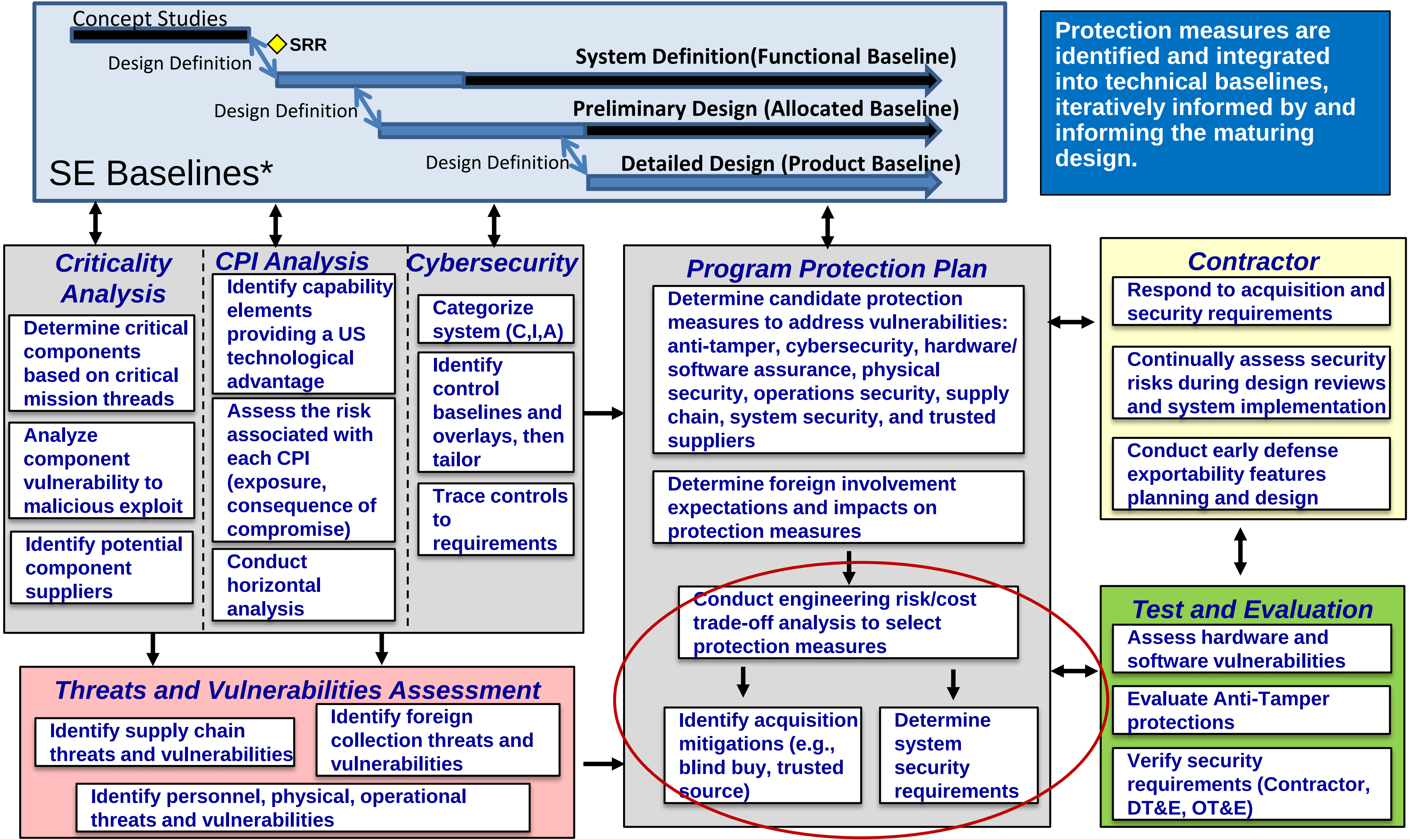
Distribution Statement A – Approved for public release by DOPSR on 10/19/2015, SR Case # 16-S-0128 applies. Distribution is unlimited.

Responsibilities For Each Role Related to Program Protection

- **System Security Engineer**
  - Leads SSE team in evaluating and balancing contributions to produce a coherent security capability across the system and the acquisition.
  - Leads Program Protection analyses for CPI, TSN, and program information
  - Collaborates with SSE specialists and security specialists to assess vulnerabilities, identify protections
  - Conducts trade-off analyses to integrate protection measures from across SSE specialties and security specialties
  - Translates protection measures into system security requirements, and adjusts them based upon constraints/decisions relayed from the systems engineer
  - Collaborates with the systems engineer to integrate the system security requirements into appropriate SE artifacts
  - Leading the development of the PPP
- **System Security Engineering Specialists**
  - Assist the system security engineer with program protection analyses
  - Identify protection measures within their specialty
  - Collaborate with the system security engineer to adjust protection measures based on constraints/decisions relayed from the system security engineer

Distribution Statement A – Approved for public release by DOPSR on 10/19/2015, SR Case # 16-S-0128 applies. Distribution is unlimited.

SSE Trade-off Analyses in the Context of Program Protection



Concept Studies

SRR

Design Definition

System Definition(Functional Baseline)

Design Definition

Preliminary Design (Allocated Baseline)

Design Definition

Detailed Design (Product Baseline)

SE Baselines*

Protection measures are identified and integrated into technical baselines, iteratively informed by and informing the maturing design.

Criticality Analysis

- Determine critical components based on critical mission threads
- Analyze component vulnerability to malicious exploit
- Identify potential component suppliers

CPI Analysis

- Identify capability elements providing a US technological advantage
- Assess the risk associated with each CPI (exposure, consequence of compromise)
- Conduct horizontal analysis

Cybersecurity

- Categorize system (C,I,A)
- Identify control baselines and overlays, then tailor
- Trace controls to requirements

Program Protection Plan

- Determine candidate protection measures to address vulnerabilities: anti-tamper, cybersecurity, hardware/ software assurance, physical security, operations security, supply chain, system security, and trusted suppliers
- Determine foreign involvement expectations and impacts on protection measures
- Conduct engineering risk/cost trade-off analysis to select protection measures
- Identify acquisition mitigations (e.g., blind buy, trusted source)
- Determine system security requirements

Contractor

- Respond to acquisition and security requirements
- Continually assess security risks during design reviews and system implementation
- Conduct early defense exportability features planning and design

Test and Evaluation

- Assess hardware and software vulnerabilities
- Evaluate Anti-Tamper protections
- Verify security requirements (Contractor, DT&E, OT&E)

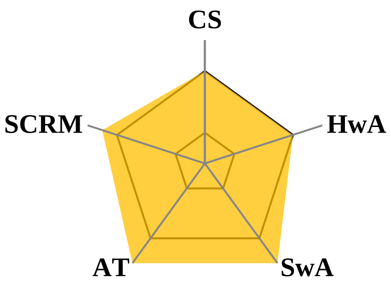
Threats and Vulnerabilities Assessment

- Identify supply chain threats and vulnerabilities
- Identify foreign collection threats and vulnerabilities
- Identify personnel, physical, operational threats and vulnerabilities

Integration of SSE Protection Measures Through Trade-off Analyses

1. Begin with initial inputs from SSE Specialists

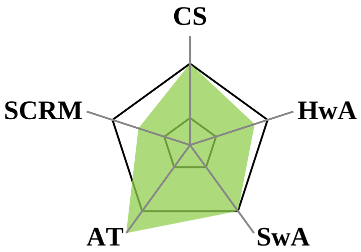
SSE Specialty Inputs



2. Conduct analyses to integrate inputs

3. Identify preferred system security solution

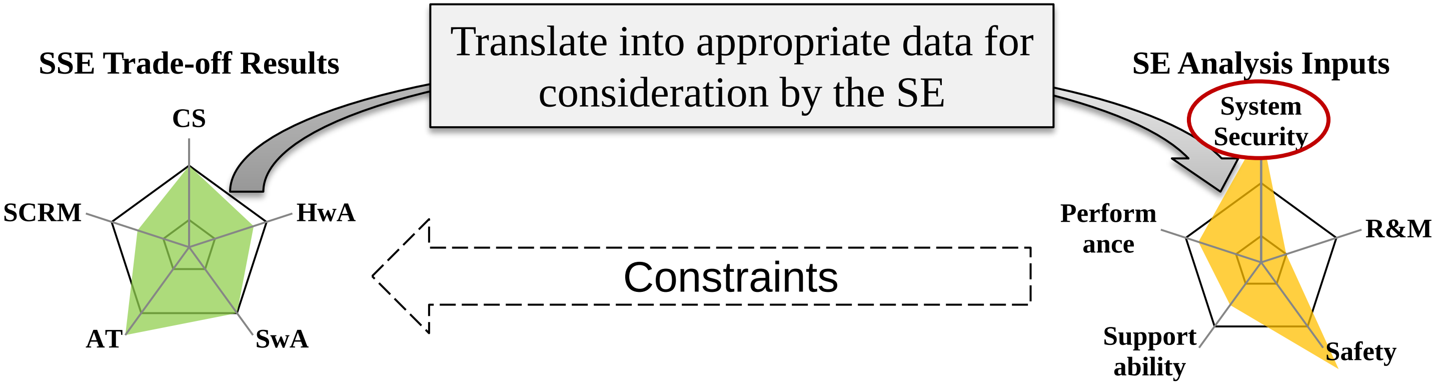
SSE Trade-off Results



- **Goal of integrating SSE protection measures**
  - Achieve comprehensive protection within the constraints (cost, performance, schedule, etc.)
- **Through conducting trade-off analyses the system security engineer should be able to identify and resolve:**
  - Conflicts among the protection measures
  - Gaps in the overall protection scheme
  - Redundancy among protection measures

Distribution Statement A – Approved for public release by DOPSR on 10/19/2015, SR Case # 16-S-0128 applies. Distribution is unlimited.

SSE Results Incorporated into SE Analyses

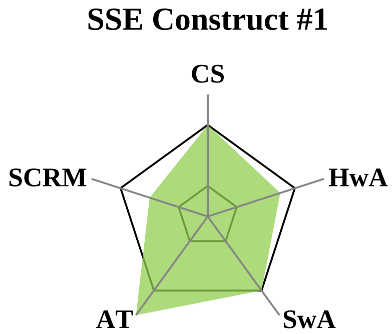


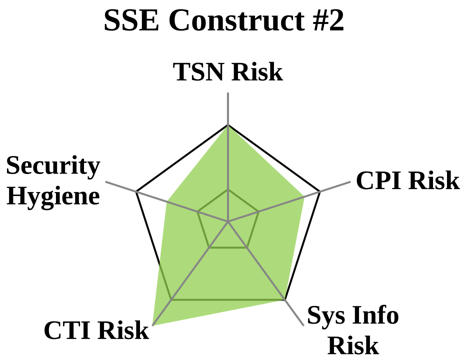
- **Employing SE methods/tools for SSE enables the ability to incorporate SSE results into broader SE analyses and decisions**
  - Supports the typical SE approach of iteratively conducting analyses to refine the system

Distribution Statement A – Approved for public release by DOPSR on 10/19/2015, SR Case # 16-S-0128 applies. Distribution is unlimited.

Topics for Further Consideration

- **Most appropriate construct for assessing system security options. Potential concepts to consider include:**





- **Standard scale of measuring aspects of system security to enable comparison**

- **Translation of preferred SSE solution into useful data that can be utilized in SE trade-off analyses**
  - An effective, reliable, and repeatable method for properly representing system security for systems engineering

Wrap Up

- DoD is emphasizing the importance of SSE within systems engineering and its contribution to the design of systems

- Utilizing systems engineering approaches, methods, and tools for SSE brings rigor to system security analyses and supports the integration of SSE into SE

- The ability to effectively measure SSE and the SSE specialties individually is the next step toward fully enabling the integration of SSE into SE

Distribution Statement A – Approved for public release by DOPSR on 10/19/2015, SR Case # 16-S-0128 applies. Distribution is unlimited.

Systems Engineering: Critical to Defense Acquisition

Defense Innovation Marketplace

http://www.defenseinnovationmarketplace.mil

DASD, Systems Engineering

http://www.acq.osd.mil/se

For Additional Information

Melinda Reed

ODASD, Systems Engineering
571-372-6562 | Melinda.K.Reed4.civ@mail.mil

JeanPaul LeSaint

Engility Corporation
571-372-6554 | JeanPaul.R.LeSaint.ctr@mail.mil

Matthew Perticone

Engility Corporation

571-372-6555 | Matthew.Perticone.ctr@mail.mil

Distribution Statement A – Approved for public release by DOPSR on 10/19/2015, SR Case # 16-S-0128 applies. Distribution is unlimited.

Security Engineering Specialties Quick Reference

- **Cybersecurity**: Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation. (*National Security Presidential Directive-54/Homeland Security Presidential Directive-23, "Cybersecurity Policy," January 8, 2008*)

- **Hardware Assurance (HwA):** The level of confidence that hardware, e.g., electronic components such as integrated circuits and printed circuit boards, functions as intended and is free of vulnerabilities, either intentionally or unintentionally designed or inserted as part of the system's hardware throughout the lifecycle.

- **Software assurance (SwA):** The "Level of confidence that software is free from vulnerabilities, either intentionally designed into the software or accidentally inserted at anytime during its lifecycle and that the software functions in the intended manner." (*Public law 112-239-Jan 2013*).

- **Anti-tamper (AT):** Systems engineering activities intended to prevent or delay exploitation of CPI in U.S. defense systems in domestic and export configurations to impede countermeasure development, unintended technology transfer, or alteration of a system due to reverse engineering. (*DoDI 5200.39*)

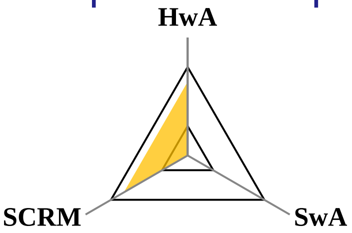
- **Supply Chain Risk Management (SCRM):** The risk that an adversary may sabotage, maliciously introduce unwanted function, or otherwise subvert the design integrity, manufacturing, production, distribution, installation, operation or maintenance of a covered system so as to surveil, deny, disrupt, or otherwise degrade the function, use, or operation of such system (*National Defense Authorization Act for FY2011, Section 806)*

- **Defense Exportability Features (DEF):** To develop and incorporate technology protection features into a system or subsystem during its research and development phase. (*National Defense Authorization Act for FY2011, Section 243)*

Distribution Statement A – Approved for public release by DOPSR on 10/19/2015, SR Case # 16-S-0128 applies. Distribution is unlimited.

Trade-off Example #1

1. SSE Specialists Inputs

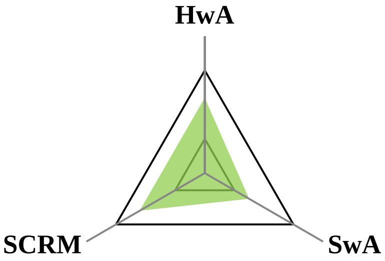


- ***SCRM #1:*** For Level 1 and Level 2 critical components, conduct functional verification testing on a sample set to verify that there are no malicious features present
- ***SCRM #2:*** Acquire all hardware components from the original equipment manufacturer (OEM) or an authorized distributor.
- ***HwA #1:*** For COTS components, use the OEM or an authorized distributor
- ***HwA #2:*** For GOTS components, use DLA qualified parts, manufacturers, and distributors
- ***HwA #3:*** Acquire all DoD-unique ASICs from a DMEA approved vendor

2. Trade Analyses

- ***REDUNDANCY:*** Acquisition from OEM requirements (SCRM #1, HwA #2) are redundant
- ***CONFLICTS:*** Sourcing and verification requirements are conflicting, but can be synthesized to more effectively secure the acquisition of all hardware components
- ***GAPS:*** Requirements do not effectively address the software

3. Identify Preferred SSE Solution

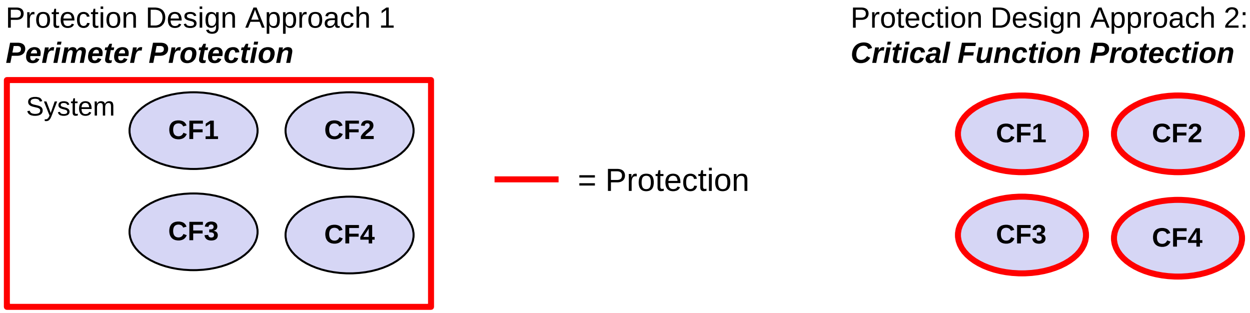


- ***SSE #1:*** For DoD-unique ASICs, acquire from DMEA approved vendor
- ***SSE #2:*** For GOTS components, use DLA qualified parts, manufacturers, and distributors and conduct visual, non-destructive inspection or analysis of Level I/II components.
- ***SSE #3:*** For COTS components, acquire from OEM or authorized distributor when available.
- ***SSE#4:*** For Level I/II COTS HW critical components, conduct side-channel analysis or conduct functional verification inspection to verify no malicious features exist.
- ***SSE#5:*** Conduct static analysis, design inspections and code inspections to enforce secure design and coding standards

Trade-Off Example #2

Goal: Determine the most cost-effective system security design alternative that achieves desired performance and protection

1. **Input:** Two design alternatives



Protection Design Approach 1
Perimeter Protection
System
CF1
CF2
CF3
CF4
= Protection
Protection Design Approach 2:
Critical Function Protection
CF1
CF2
CF3
CF4

2. **Trade-Off Analysis:** The System Security Engineer may utilize modeling, simulation, and analysis to determine:
   - Cost associated with each alternative
   - The effectiveness of preventing attacks
   - The impact of the design on system performance and other design considerations

3. **Identify Preferred SSE Solution:** Based on the cost, protection effectiveness, and impact of design, the System Security Engineer would determine the most appropriate protection design approach. The approach would then be proposed to the Systems Engineer.

Benefits: Because of the data gathered during modeling, simulation, and analysis, the SSE is able to identify the most-cost effective system security design alternative that achieves performance