WPI

A Practical Educational Approach to Program Protection Planning

Don S. Gelosh, Ph.D., CSEP-Acq
Director, Systems Engineering

Corporate and Professional Education

540-349-3949

dsgelosh@wpi.edu

cpe.wpi.edu

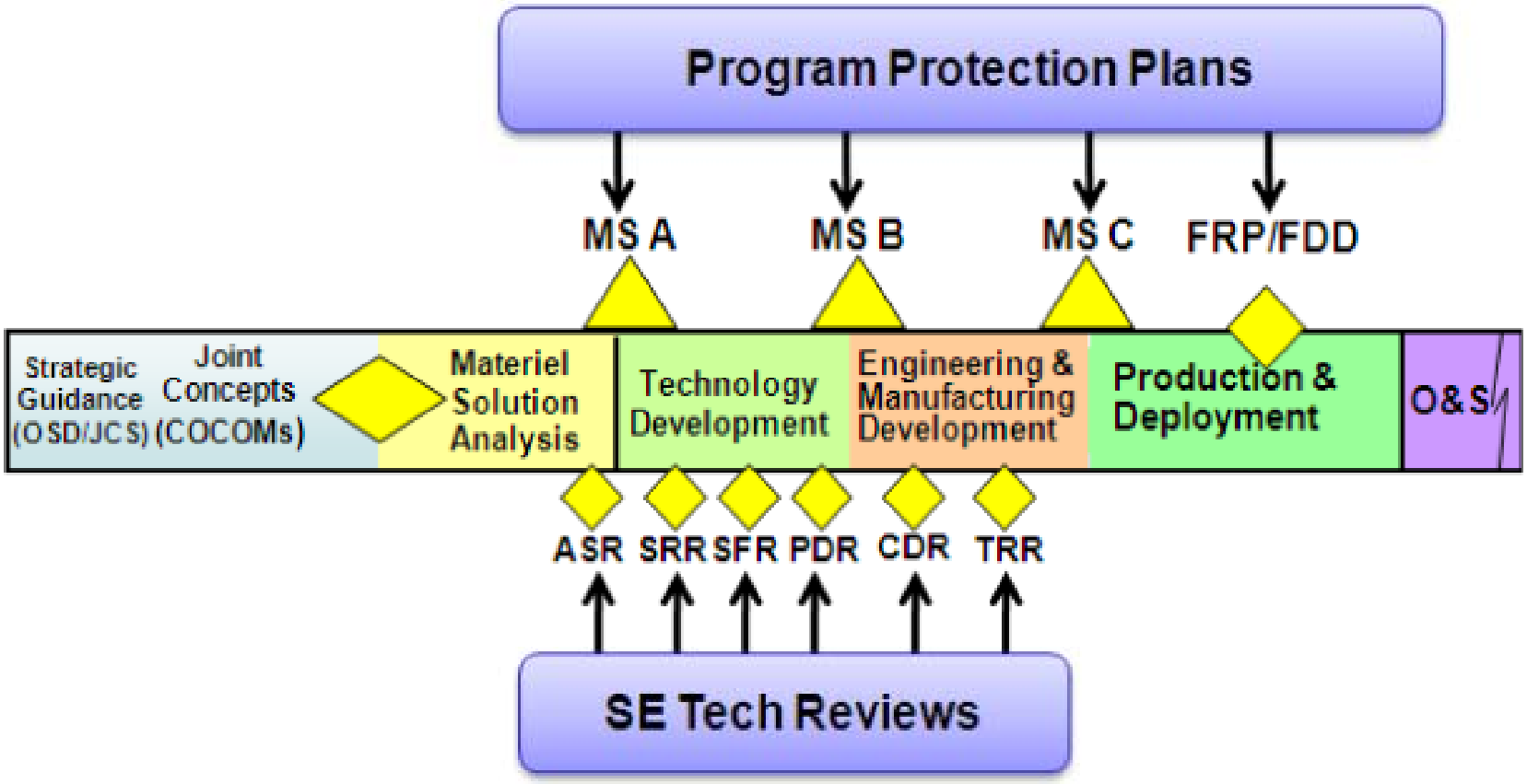
Background

- The US Department of Defense (DoD) now requires that all major defense acquisition programs have effective program protection planning in place.
- Program Protection Plans are required at each of the three major milestones (A, B and C) and the full rate production review.
- Program Protection Plans must encompass the entire system life cycle from the Material Development Decision to maintaining security during disposal of the system.
- This is a relatively new requirement so many defense contractors are struggling with exactly what the DoD policy and guidance specifies and are not necessarily putting together effective protection plans.
- Effective Program Protection Plans are crucial to developing, delivering and sustaining secure and trusted systems and networks.
- This presentation will describe a practical approach to educating systems engineers on Program Protection Planning.

Source Documents

- Operation of the Defense Acquisition System, DoDI 5000.02, December 8, 2008
- Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN), DoDI 5200.44, November 5, 2012
- Critical Program Information (CPI) Protection Within the Department of Defense, DoD Instruction 5200.39, 2008
- Report on Trusted Defense Systems in Response to National Defense Authorization Act, Section 254, DoD Congressional Report, 2009
- Supply Chain Risk Management (SCRM) to Improve the Integrity of Components Used in DoD Systems, Directive-Type Memorandum 09-016, 2010
- F. Kendall, “Document Streamlining–Program Protection Plan (PPP),” Principal Deputy Under Secretary of Defense for Acquisition, Technology, and Logistics, Washington, DC, 2011.

When Are the Plans Required*?

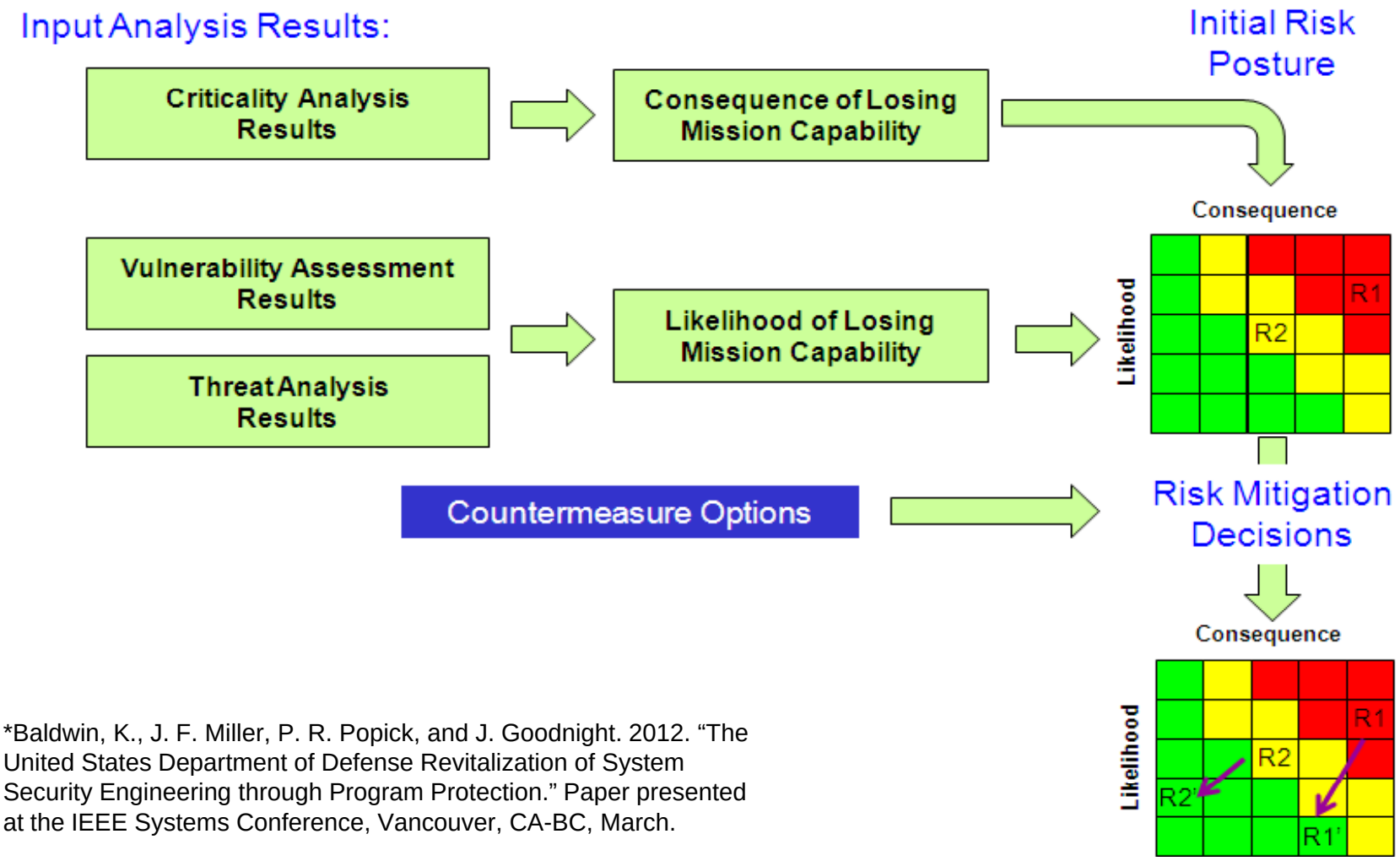


*Baldwin, K., J. F. Miller, P. R. Popick, and J. Goodnight. 2012. "The United States Department of Defense Revitalization of System Security Engineering through Program Protection." Paper presented at the IEEE Systems Conference, Vancouver, CA-BC, March.

A Practical Educational Approach

- A practical educational approach to Program Protection Planning (PPP) is to treat it as a structured way for companies to strategically plan for and manage security risk by identifying and quantifying:
  - Probability of Threats
  - System Vulnerabilities
  - Consequences
  - Suitable Countermeasures

How Do We Manage Risk*?



*Baldwin, K., J. F. Miller, P. R. Popick, and J. Goodnight. 2012. "The United States Department of Defense Revitalization of System Security Engineering through Program Protection." Paper presented at the IEEE Systems Conference, Vancouver, CA-BC, March.

A Practical Educational Approach

- Practical PPP education should also cover the following concepts in a practical way by exploring best practices as well as the underlying theories:
  - Supply Chain Risk Management
  - System Security Engineering
  - Anti-Counterfeit Parts
  - Anti-Tamper
  - Vendor Certifications
  - Cyber Security

Program Protection Planning Learning Outcomes

- Develop and implement efficient and effective Program Protection Plans.
- Strategically manage risk by identifying and quantifying the probability of threats, system vulnerabilities and their consequences and identifying suitable countermeasures.
- Critically evaluate valuate internal and external plans.
- Develop and deliver sustainable trusted systems and networks using practical methods and best practices.
- Gain a competitive advantage and become an even greater asset to their organizations.

Example – Graduate Certificate in Program Protection Planning

Required Courses

- Concepts of Systems Engineering
- Engineering Dependable and Secure Systems
- Supply Chain Risk Management
- Practical Applications of Systems Security Engineering
- Protection Planning Across the Program Life Cycle

Electives

- Software Security Design and Analysis
- Network Security
- Operations Risk Management

Learning Outcomes for Concepts of Systems Engineering

- Understand and appreciate fundamental SE principles such as:
  - Requirements Development
  - Functional Analysis and Requirements Allocation
  - System Architecture and System Design
  - Integration, Verification and Validation
  - Trade Studies
  - Systems Analysis, Modeling and Simulation
  - Specialty Engineering
  - Risk Management
  - Technical Planning and Management

Learning Outcomes for Engineering Dependable and Secure Systems

- Understand how to design and build dependable systems that are:
  - Reliable, available, and secure
  - Able to deliver their intended capabilities despite hardware failures, software failures, network failures, external attack, and unexpected behavior
- Understand and appreciate:
  - Dependable system architectures
  - Resilience, security, and quality of service of networks
  - Dependability benchmarking
  - Software reliability
  - Autonomic and adaptable systems
  - Threat analysis and assessment.

Learning Outcomes for Supply Chain Risk Management (SCRM)

- Understand and implement SCRM in a systems security engineering context.
- Understand how to mitigate the risk of counterfeit parts.
- Understand how to mitigate the risk of malicious insertion of code into software, firmware, non-volatile memory, or logic-bearing hardware.
- Understand threats and vulnerabilities to supply chain stakeholders, vendor certifications, and counterfeit parts.
- Understand how these topics impact SCRM throughout the DoD acquisition lifecycle.

Learning Outcomes for Practical Applications of System Security Engineering

- Understand the importance and implementation of System Security Engineering.
- Assess and evaluate threats, vulnerabilities, and countermeasures.
- Understand design and architectural trends and implement techniques in the areas of multilevel and multilateral security.
- Evaluate and implement security domains, physical protection, biometrics, emissions, and network defense.
- Understand the practical use and importance of cryptography, supply chain risk management, information assurance, software assurance and system assurance.

Learning Outcomes for Protection Planning Across the Program Life Cycle

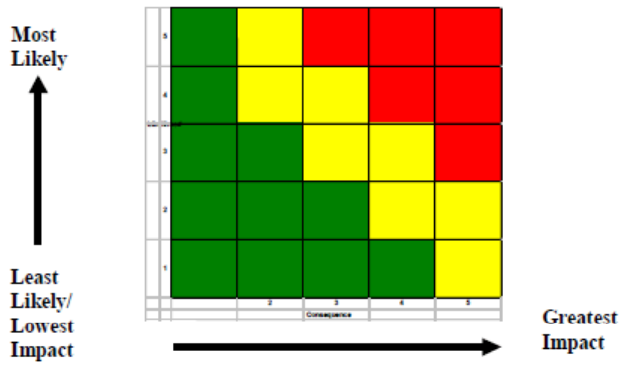
- Understand DoD's current policy and guidance for Program Protection Planning.
- Use Program Protection Planning theories and methods to inform systems security engineering tradeoffs among risks, costs and benefits across the various phases of a program's life cycle.
- Use criticality analysis techniques to identify mission critical functions and components.
- Use criticality analysis techniques to determine the consequences of losing mission capability.

Learning Outcomes for Protection Planning Across the Program Life Cycle

- Use threat analysis and vulnerability assessment to identify and manage the likelihood of losing mission capability.
- Assess security risk for the program by analyzing the consequences and likelihood of losing mission capability.
- Implement countermeasures to mitigate risk and neutralize threats and vulnerabilities.
- Implement these systems security engineering practices across the various phases of the program's life cycle.

Learning Outcomes for Operations Risk Management

- Understand decision making under uncertainty
- Understand classic methods from decision analysis by drawing upon management science and managerial decision-making, including negotiation and cognitive psychology
- Understand how to apply operations risk management to:
  - Quality Assurance
  - Supply Chains
  - Information Security
  - Environmental Management



Summary

- This presentation explored a practical educational approach to Program Protection Planning (PPP) by exploring best practices as well as the underlying theories.
- We proposed treating PPP as a structured way for companies to strategically plan for and manage security risk.
- We looked at identifying and quantifying the probability of threats, vulnerabilities and their consequences and identifying suitable countermeasures.
- We included concepts of anti-tamper, anti-counterfeit parts, supply chain risk management, vendor certifications, system security engineering and cyber security.

Questions?