



System Security Engineering and Program Protection Case Study for the Materiel Solution Analysis Phase Tutorial

Melinda Reed

**Office of the Deputy Assistant Secretary of Defense
for Systems Engineering**

**15th Annual NDIA Systems Engineering Conference
San Diego, CA | October 22, 2012**



Agenda



- **Introduction**
- **Program Protection**
- **Criticality Analysis**
- **Threat Analysis**
- **Vulnerability Assessment**
- **Risk Assessment**
- **Countermeasures Selection**
- **Request for Proposal (RFP) and the PPP**



Learning Objectives



- **Discuss the Program Protection Plan (PPP) Analysis for Supply Chain and Malicious Insertion Threats for the Materiel Solution Analysis (MSA) Phase**
- **Show the risk based cost-benefit trade to select the Supply Chain and malicious insertion mitigations**
- **Describe basic supply chain and malicious insertion protections to incorporate in the MSA Phase PPP and RFP**
- **Recognize that supply chain and malicious insertion program protections are a shared government-industry responsibility**



Material Solution Analysis (MSA) Phase PPP Challenges



Ensuring that basic development, design and supply chain protections are established in the PPP and the RFP to prevent ,detect and respond to malicious attacks

Prevent – Countermeasures that reduce the exploitation of development, design and supply chain vulnerabilities

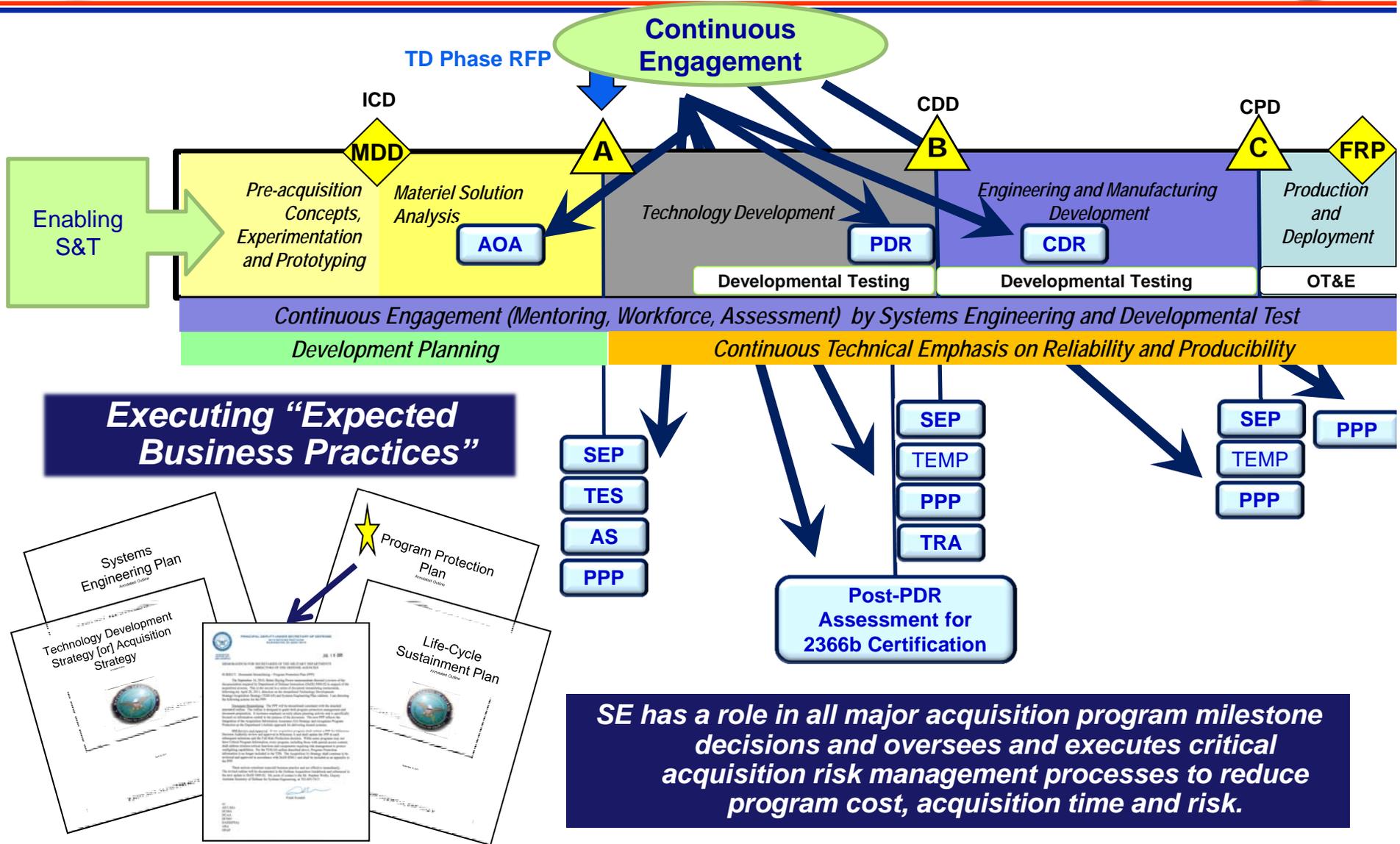
Detect – Countermeasure that monitor, alert and capture data about the attack

Respond – Countermeasures that analyze attacks and alter system or processes to mitigate the attack

***Milestone A Program Protection Plans
should contain all three types of mitigations as well as plans for more
detailed program protection analysis and updates to
inform system security engineering early in the design***



Acquisition Process Engagement





Ensuring Confidence in Defense Systems



- **Threat: Nation-state, terrorist, criminal, or rogue developer who:**
 - Gain control of systems through supply chain opportunities
 - Exploit vulnerabilities remotely
- **Vulnerabilities**
 - All systems, networks, and applications
 - Intentionally implanted logic
 - Unintentional vulnerabilities maliciously exploited (e.g., poor quality or fragile code)
- **Traditional Consequences: Loss of critical data and technology**
- **Emerging Consequences: Exploitation of manufacturing and supply chain**
- **Either can result in corruption; loss of confidence in critical warfighting capability**

Today's acquisition environment drives the increased emphasis:

<u>Then</u>		<u>Now</u>
Stand-alone systems	>>>	Networked systems
Some software functions	>>>	Software-intensive
Known supply base	>>>	Prime Integrator, hundreds of suppliers
CPI (technologies)	>>>	CPI and critical components



What Are We Protecting?

Program Protection Planning

DODI 5000.02 Enclosure Update

DoDI 5200.39
Change 1, dated Dec 2010

5200.mm

DoDI 5200.39

Technology

Components

Information

What: Leading-edge research and technology

Who Identifies: Technologists, System Engineers

ID Process: CPI Identification

Threat Assessment: Foreign collection threat informed by Intelligence and Counterintelligence assessments

Countermeasures: AT, Classification, Export Controls, Security, Foreign Disclosure, and CI activities

Focus: “Keep secret stuff in” by protecting any form of technology

What: Mission-critical elements and components

Who Identifies: System Engineers, Logisticians

ID Process: Criticality Analysis

Threat Assessment: DIA SCRM TAC

Countermeasures: SCRM, SSE, Anti-counterfeits, software assurance, Trusted Foundry, etc.

Focus: “Keep malicious stuff out” by protecting key mission components

What: Information about applications, processes, capabilities and end-items

Who Identifies: All

ID Process: CPI identification, criticality analysis, and classification guidance

Threat Assessment: Foreign collection threat informed by Intelligence and Counterintelligence assessments

Countermeasures: Information Assurance, Classification, Export Controls, Security, etc.

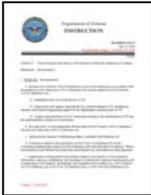
Focus: “Keep critical information from getting out” by protecting data

Protecting Warfighting Capability Throughout the Lifecycle

Note: Program Protection Planning Includes DoDI 8500 series



Program Protection Integrated in Policy and Guidance



- **Operation of the Defense Acquisition System**
 - DoDI 5000.02 – Regulatory Requirement for Program Protection Plan at MS B/C
 - Dec 2008 – References DoDI 5200.39



- **Critical Program Information (CPI) Protection Within the DoD**
 - DoDI 5200.39 – Assigns responsibility for Counterintelligence, Security, and System Engineering support for the ID and protection of CPI
 - Dec 2010 – Expands definition of CPI to include degradation of mission effectiveness
 - Technology, information, elements, or components



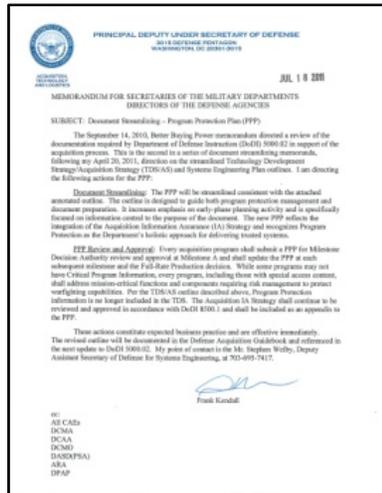
- **Supply Chain Risk Management to Improve the Integrity of Components Used in DoD Systems**
 - DTM 9-016 – Establishes policy and defense-in-breadth strategy for managing Supply Chain Risk to information and communications technology
 - Aug 2011
 - NEW** → Translating to Policy - DoDI 5200.mm, awaiting signature

GUIDANCE

- **Program Protection Plan Outline & Guidance, dated 18 Jul 2011**
 - Increases emphasis on early-phase planning activity focused on information central to program protection
- **Defense Acquisition Guidebook update**
 - Provides acquisition workforce with discretionary best practice that should be tailored to the needs of each program; Chapter 13, Program Protection, Chapter 4, System Engineering



New PPP Outline and Guidance



Signed by
Principal Deputy,
USD(AT&L) on
July 18, 2011

• What's in the Policy Memo?

- *“Every acquisition program shall submit a PPP for Milestone Decision Authority review and approval at Milestone A and shall update the PPP at each subsequent milestone and the Full-Rate Production decision.”*
- Existing acquisition Information Assurance Strategy
 - Appendix to PPP: Subject to a page count limit
- Expected business practice, effective immediately, and reflected in upcoming DoDI 5000.02 and DAG updates

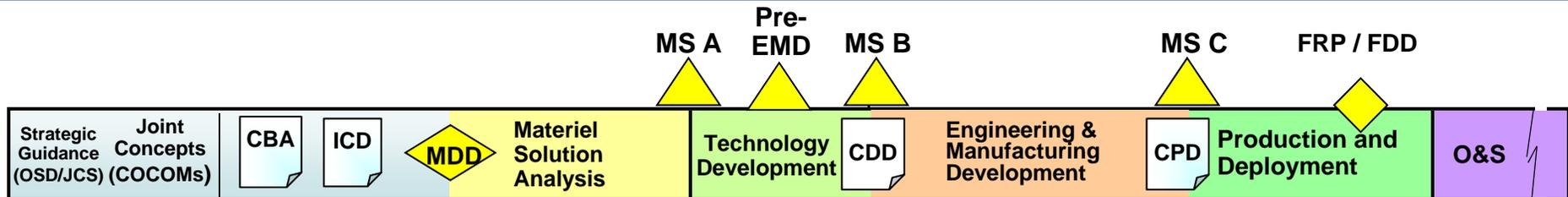
• What's in the Outline and Guidance?

- Plans for identifying and managing risk to CPI and critical functions and components
- Responsibilities for execution of comprehensive program protection
- Tables of actionable data, not paragraphs of boilerplate
- End-to-end system analysis and risk management
- Similar approach as TDS/AS and SEP Outline and Guidance

The PPP is the Single Focal Point for All Security Activities on the Program



PPP Development and Updates



A Program Protection Plan is required for Milestones A, B, C, and FRP; a draft is required for Pre-EMD

The PPP analysis consists of a Criticality Analysis (CA), Threat and Supplier Analysis (TA), Vulnerability Assessment (VA), Risk Assessment (RA), and a Cost-Benefit Trade-Off to select appropriate countermeasures to mitigate risks:

A PPP analysis is conducted iteratively, results are used to inform the Systems Engineering Technical Reviews (ASR, SRR, SFR, PDR, CDR, ...)

The PPP analysis becomes more detailed as the requirements are decomposed into system and subsystem specifications throughout the evolution of the design

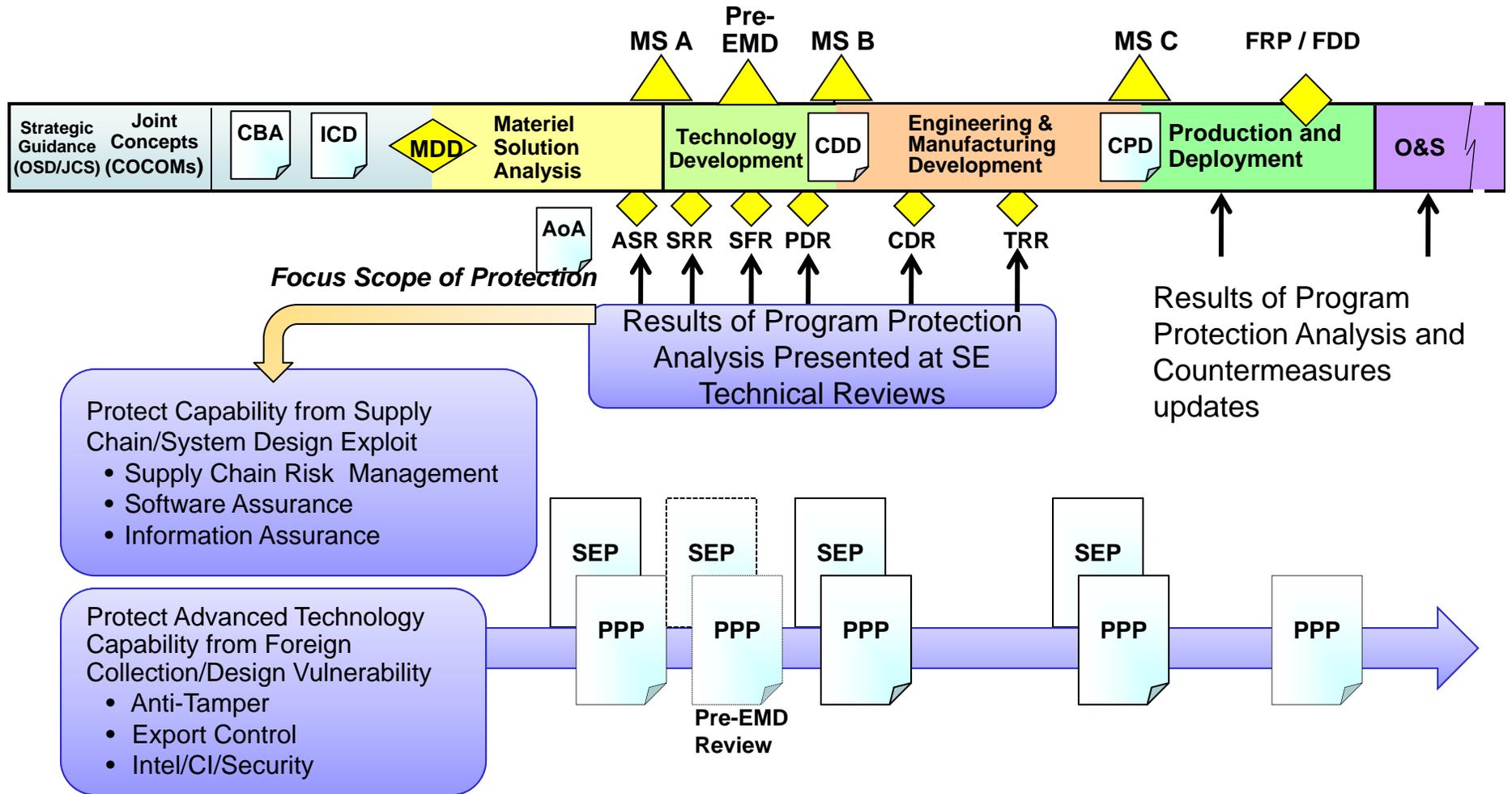
Program Office decisions resulting from the PPP analyses should be documented in the PPP

Critical Program Information (CPI) designation is used to provide additional protection (usually anti-tamper) of advanced technology to prevent loss of technology/ intellectual property and is determined through a special process

The results of the PPP analysis and CPI Identification are incorporated into the RFP via Statement of Work (SOW) and System Requirements Documents (SRD)

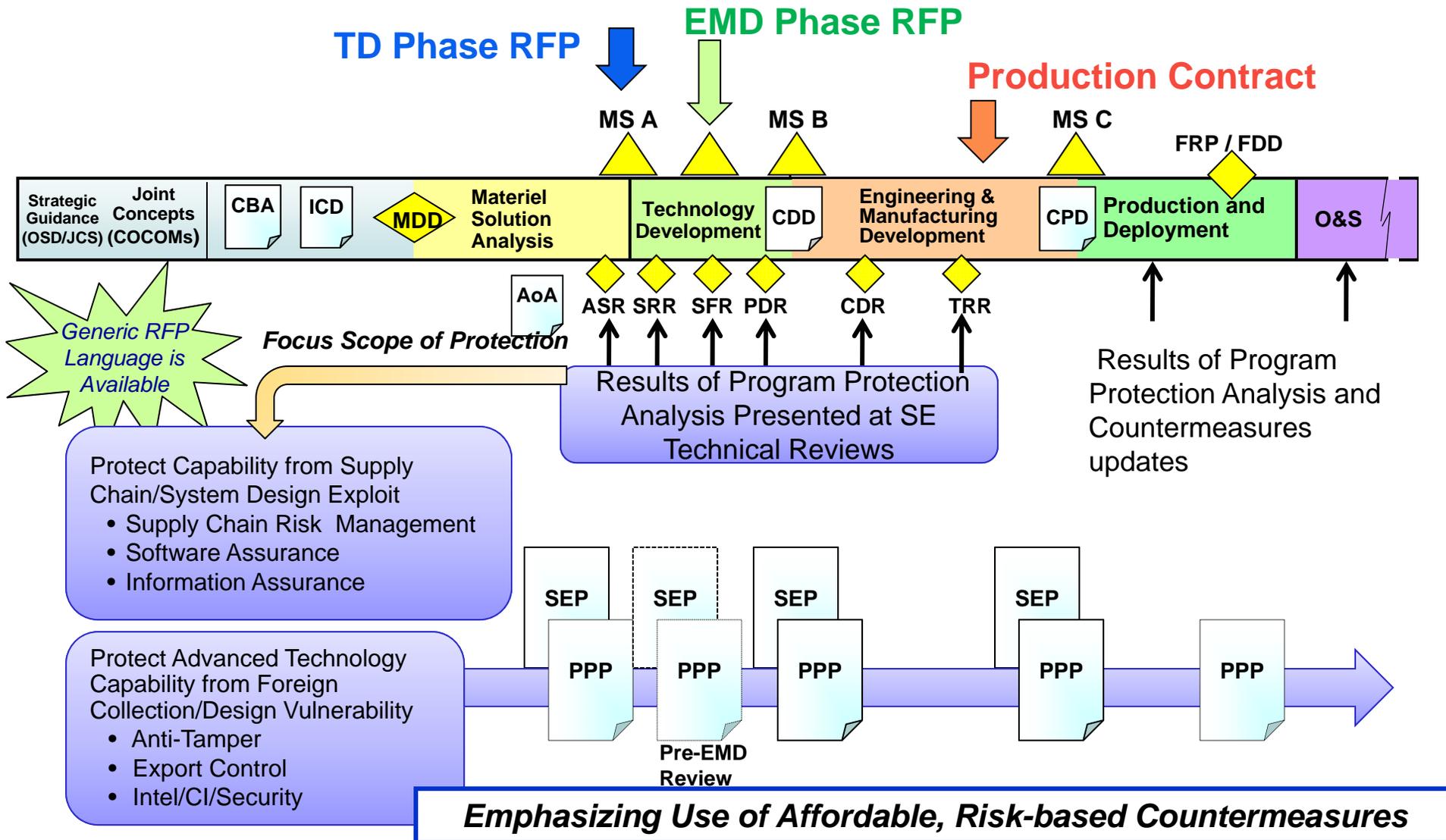


PPP Development and Updates





PPP Development and Updates





MSA Phase Engineering Analysis

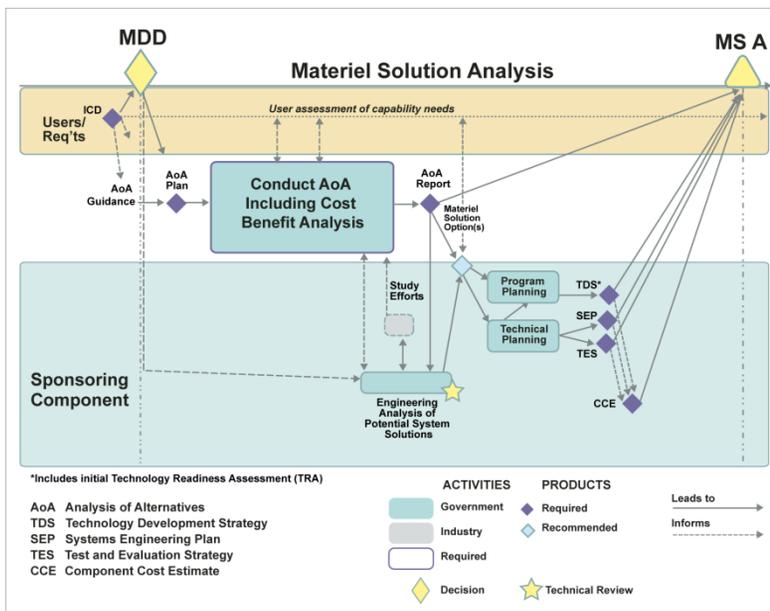


Fig 2-1 from Judith Dahmann and Mike Kelley "Systems Engineering During the Materiel Solution Analysis and Technology Development Phase." Washington, DC: Office of the Director, DDR&E, SE 2009. www.acq.osd.mil/sse

MSA Phase Engineering Analysis Objectives

- Confirm CONOPS and develop mission and functional threads
- Develop draft system requirements and notional system design
- Identify critical technology elements
- Determine external interfaces and interoperability
- Identify critical functions and CPI

Feeds key MS – A Requirements

- TDS, Acq Strategy, R&D Certified Cost Estimate, RFP, SEP, TES, PPP, RAM

Influences Draft CDD develop

- Balances capability, cost, schedule, risk and affordability

Requires an adequately resourced and experienced Program Office

- System and Domain Engineers
- Cost Analysts
- Mission and Operations Reps



Program Protection Analysis for Supply Chain and Software Assurance



Criticality Analysis Results

Mission	Critical Functions	Logic-Bearing Components (HW, SW, Firmware)	System Impact (I, II, III, IV)	Rationale
Mission 1	CF 1	Processor X	II	Redundancy
	CF 2	SW Module Y	I	Performance
Mission 2	CF 3	SW Algorithm A	II	Accuracy
	CF 4	FPGA 123	I	Performance

Vulnerability Assessment Results

Critical Components (HW, SW, Firmware)	Identified Vulnerabilities	Exploitability	System Impact (I, II, III, IV)
Processor X	Vulnerability 1 Vulnerability 4	Low Medium	II
SW Module Y	Vulnerability 1 Vulnerability 2 Vulnerability 3 Vulnerability 6	High Low Medium High	I
SW Algorithm A	None	Very Low	II
FPGA 123	Vulnerability 1 Vulnerability 23	Low Low	I

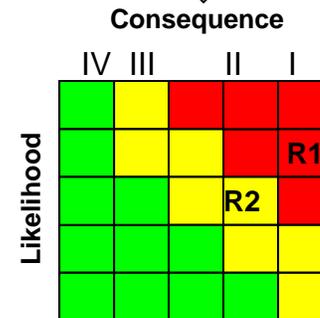
Threat Analysis Results

Supplier	Critical Components (HW, SW, Firmware)	Analysis Findings
Supplier 1	Processor X	Supplier Risk
	FPGA 123	Supplier Risk
Supplier 2	SW Algorithm A	Cleared Personnel
	SW Module Y	Cleared Personnel

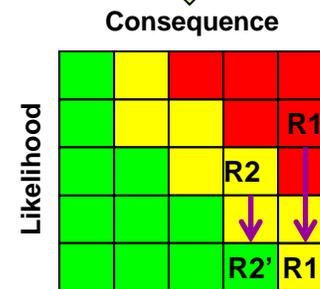
Consequence of Losing Mission Capability
Very High
High
Moderate
Low
Very Low

Likelihood of Losing Mission Capability
Near Certainty (VH)
Highly Likely (H)
Likely (M)
Low Likelihood (L)
Not Likely (VL)

Initial Risk Posture



Risk Mitigation Decisions



Risk Mitigation and Countermeasure Options



Criticality Analysis

Criticality Analysis Results

Mission	Critical Functions	Logic-Bearing Components (HW, SW, Firmware)	System Impact (I, II, III, IV)	Rationale
Mission 1	CF 1	Processor X	II	Redundancy
	CF 2	SW Module Y	I	Performance
Mission 2	CF 3	SW Algorithm A	II	Accuracy
	CF 4	FPGA 123	I	Performance

Consequence of Losing Mission Capability
Very High
High
Moderate
Low
Very Low

Vulnerability Assessment Results

Critical Components (HW, SW, Firmware)	Identified Vulnerabilities	Exploitability	System Impact (I, II, III, IV)
Processor X	Vulnerability 1 Vulnerability 4	Low Medium	II
SW Module Y	Vulnerability 1 Vulnerability 2 Vulnerability 3 Vulnerability 6	High Low Medium High	I
SW Algorithm A	None	Very Low	II
FPGA 123	Vulnerability 1 Vulnerability 23	Low Low	I

Likelihood of Losing Mission Capability
Near Certainty (VH)
Highly Likely (H)
Likely (M)
Low Likelihood (L)
Not Likely (VL)

Threat Analysis Results

Supplier	Critical Components (HW, SW, Firmware)	Analysis Findings
Supplier 1	Processor X	Supplier Risk
	FPGA 123	Supplier Risk
Supplier 2	SW Algorithm A	Cleared Personnel
	SW Module Y	Cleared Personnel

Risk Mitigation and Countermeasure Options

Initial Risk Posture

Consequence

	IV	III	II	I
Likelihood				

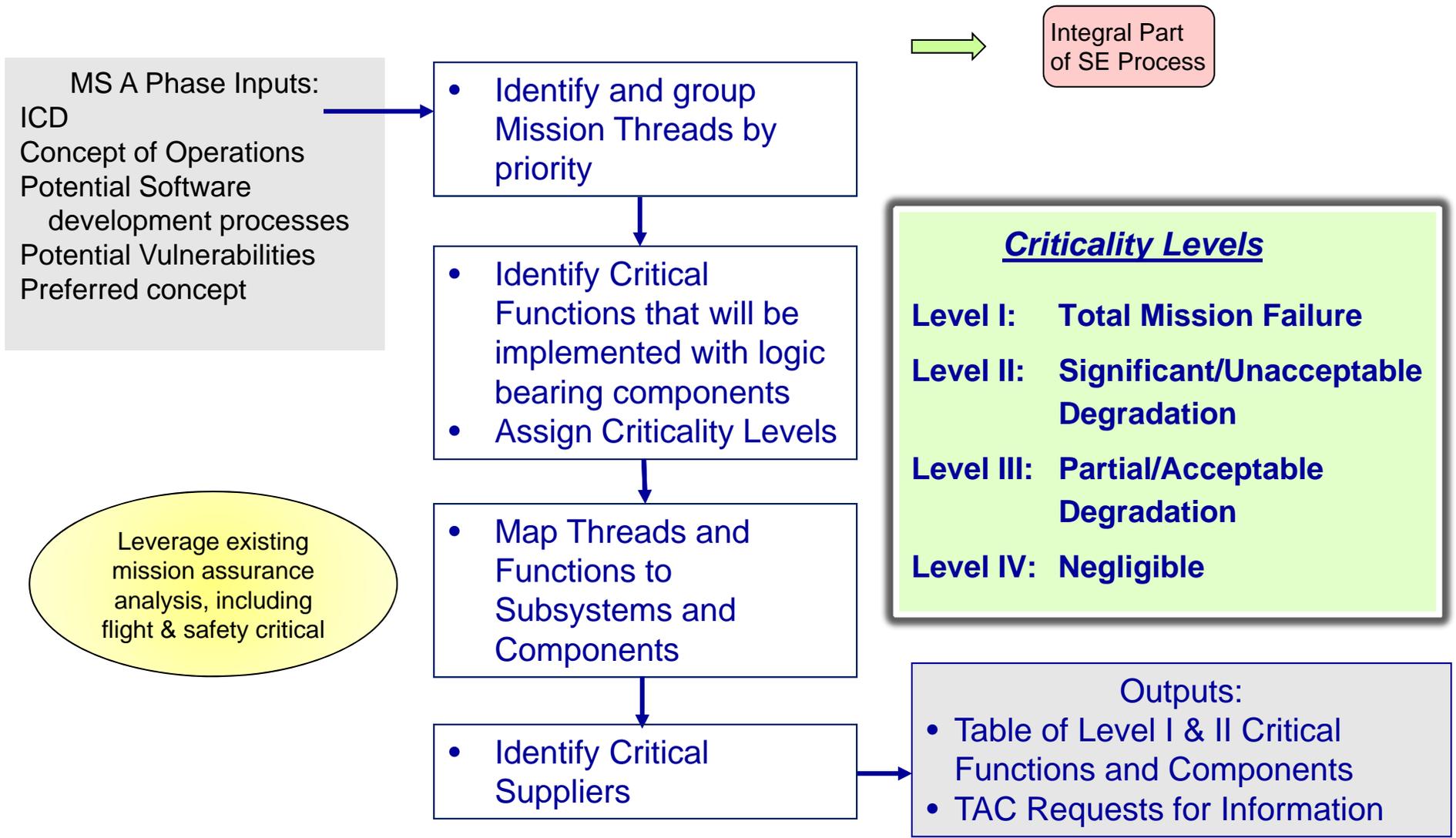
Risk Mitigation Decisions

Consequence

Likelihood				



Criticality Analysis Methodology





Criticality Analysis Exercise – Scenario Description



- In this Exercise, you will perform an initial Criticality Analysis. You will determine the Critical Functions of a system, but not the implementing Critical Components.
- You have been assigned to the program office for an acquisition program that has just completed its Analysis of Alternatives (AoA) and has begun the engineering analysis of the preferred concept .
- The preferred concept is a fixed wing unmanned aircraft system (UAS) to perform an ISR mission. The program office has begun defining and decomposing the preferred concept and assessing the critical enabling technologies.
- The ISR mission thread is the “kill chain” mission thread – to consider search, locate, and track of an enemy surface strike group and pass targeting information back to an airborne E-2D that, in turn, provides information to a carrier strike aircraft.



Criticality Analysis Exercise – Template for Results



- Divide into teams of 2 to develop an initial Criticality Analysis
- You have been provided with
 - A generic unmanned aerial vehicle operational view (OV-1)
 - A concept of operations
 - A copy of the chart shown below to record your results
- Determine and list 5 to 6 Critical Functions associated with the “kill chain” mission thread. Concentrate on functions that will be implemented with logic bearing hardware, firmware, and software. Assign Criticality Levels.

#	Critical Function	Level
1		
2		
3		
4		
5		
6		



Criticality Analysis Exercise – Results Discussion



- Brainstorm and consolidate the results provided by the whole group:

#	Critical Function	Level
1		
2		
3		
4		
5		
6		
7		
8		
9		
10		

Note: CA exercise results “exemplar” will be provided for use with future exercises



Threat Analysis

Criticality Analysis Results

Mission	Critical Functions	Logic-Bearing Components (HW, SW, Firmware)	System Impact (I, II, III, IV)	Rationale
Mission 1	CF 1	Processor X	II	Redundancy
	CF 2	SW Module Y	I	Performance
Mission 2	CF 3	SW Algorithm A	II	Accuracy
	CF 4	FPGA 123	I	Performance

Vulnerability Assessment Results

Critical Components (HW, SW, Firmware)	Identified Vulnerabilities	Exploitability	System Impact (I, II, III, IV)
Processor X	Vulnerability 1 Vulnerability 4	Low Medium	II
SW Module Y	Vulnerability 1 Vulnerability 2 Vulnerability 3 Vulnerability 6	High Low Medium High	I
SW Algorithm A	None	Very Low	II
FPGA 123	Vulnerability 1 Vulnerability 23	Low Low	I

Threat Analysis Results

Supplier	Critical Components (HW, SW, Firmware)	Analysis Findings
Supplier 1	Processor X	Supplier Risk
	FPGA 123	Supplier Risk
Supplier 2	SW Algorithm A	Cleared Personnel
	SW Module Y	Cleared Personnel

Consequence of Losing Mission Capability
Very High
High
Moderate
Low
Very Low

Likelihood of Losing Mission Capability
Near Certainty (VH)
Highly Likely (H)
Likely (M)
Low Likelihood (L)
Not Likely (VL)

Initial Risk Posture

Likelihood	Consequence			
	IV	III	II	I

Risk Mitigation Decisions

Likelihood	Consequence			
	IV	III	II	I

Risk Mitigation and Countermeasure Options



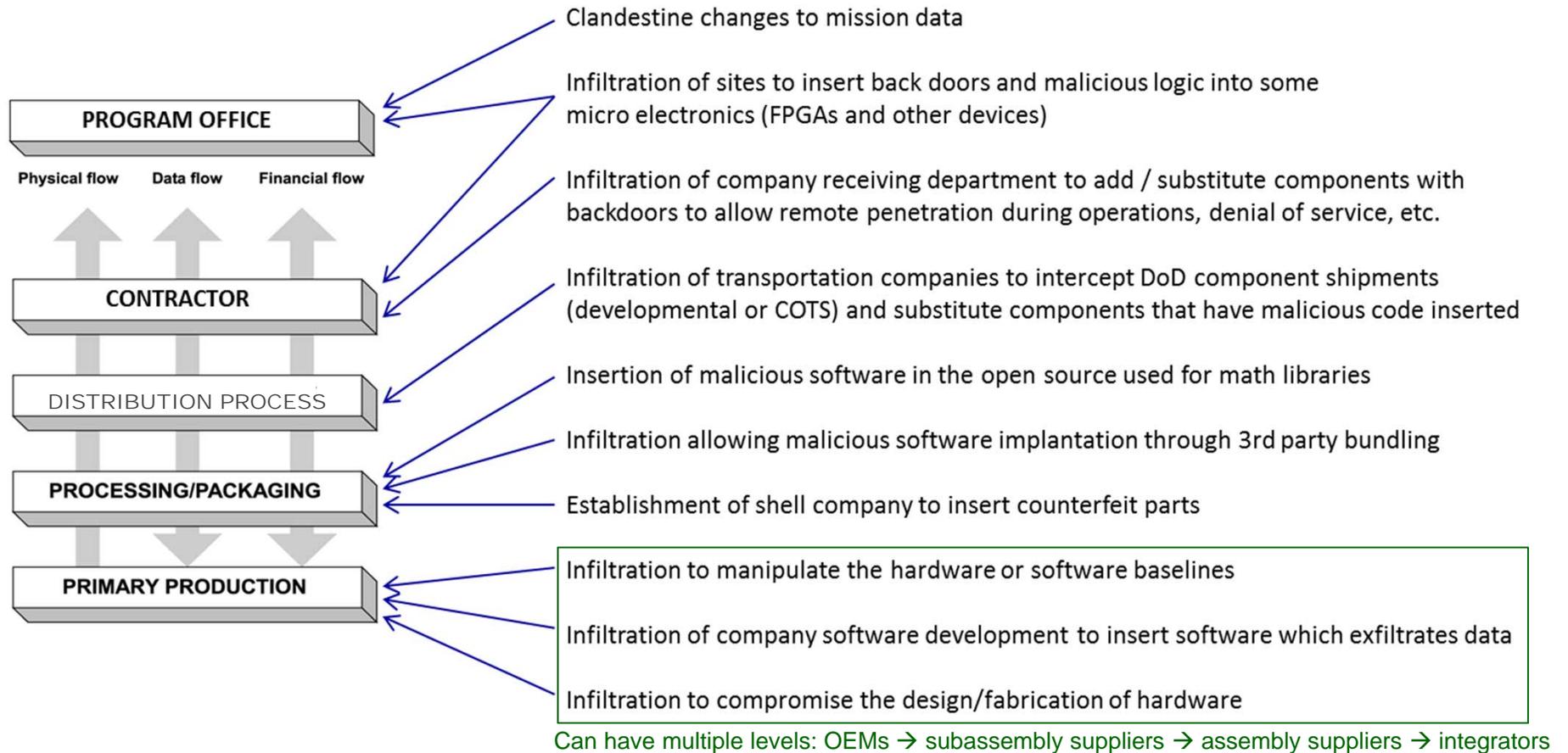
Generic Threats – Supply Chain Attacks



Coverage is for what part of the chain is infiltrated and what the malicious insertion accomplishes

Supply Chain

Attack Vectors





Generic Threats – Malicious System Exploitation Attacks



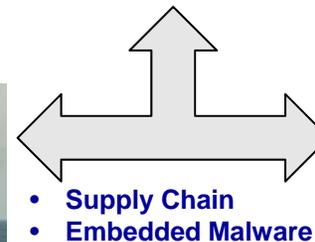
Attack Vectors for Malicious exploitation of fielded systems

Exploitation of system design vulnerabilities



- Configuration, Operational Practices**
- Supply Chain** (penetration, corruption)
- Malware** (downloaded, embedded)
- External Mission Load Compromise**
- DNS Based Threats** (cache poisoning)
- Applications** (built-in malware)
- E-mail Based Threats** (attachments)
- Data Leakage** (via social media)
- Password Misuse** (sharing)

- Denial of Service** (embedded malware)
- Kill Switch Activation** (embedded malware)
- Mission Critical Function Alteration** (embedded malware)
- Exfiltration** (by adversary)
- Network Threat Activity** (host discovery)
- Compromised Server Attacks** (on clients)
- Malicious Activity** (disruption, destruction)
- Auditing Circumvention** (evading detection)
- Web Based Threats** (disclosing sensitive info)
- Zero Day Vectors** (vulnerabilities without fixes)
- Improper File/Folder Access** (misconfiguration)

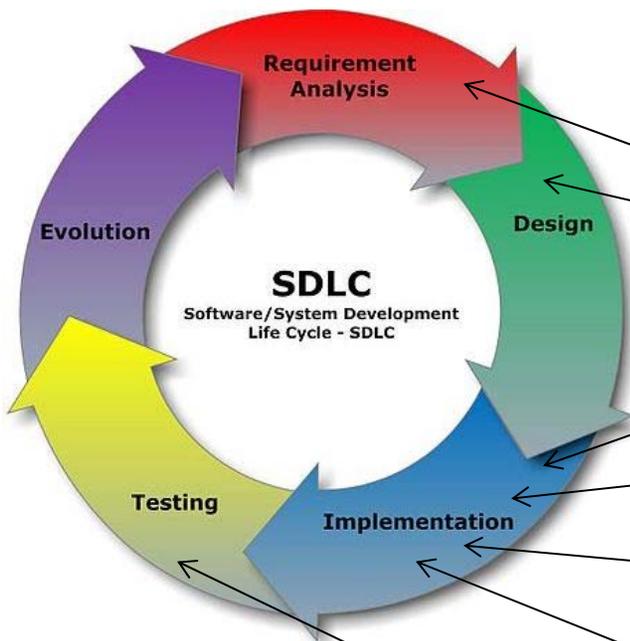




Generic Threats – Malicious Insertion in Software Development Life Cycle



Coverage is for what part of SDLC is targeted and how malicious insertion is accomplished



Attack Vectors for Malicious Code Insertion

- Hidden in software's design (or even requirements)
- Appended to legitimate software code
- Added to linked library functions
- Added to installation programs, plug-ins, device drivers, or other support programs
- Integrated into development tools (e.g., compiler generates malicious code)
- Inserted via tools during system test



Threat Analysis – Methodology for Potential Supplier Threats



- **Input**
 - List of Critical Functions and their (potential) implementing Critical Components
- **For each Level I and selected Level II Critical Function**
 - Determine COTS or custom development, Hardware, Software, Firmware
 - Develop a list of potential suppliers of critical functions
 - On shore, Off Shore, Reuse (Gov't or Commercial)
 - Match potential suppliers to critical components
 - Include supplier location
 - For reuse include program / system source and OEM location
- **Build potential supply chain diagrams or tables for use in Vulnerability Assessment (See Architecture Handout)**
- **Request supplier threat information for Level I/II critical-function component suppliers**
- **Output**
 - Supply chain diagrams and threat request information
 - Assume a Likely [M(3)] to Highly Likely [H(4)] threat likelihood for suppliers that have limited supply alternatives, can not be switched (for other reasons), or have no information request results



Vulnerability Assessment



Criticality Analysis Results

Mission	Critical Functions	Logic-Bearing Components (HW, SW, Firmware)	System Impact (I, II, III, IV)	Rationale
Mission 1	CF 1	Processor X	II	Redundancy
	CF 2	SW Module Y	I	Performance
Mission 2	CF 3	SW Algorithm A	II	Accuracy
	CF 4	FPGA 123	I	Performance



Consequence of Losing Mission Capability
Very High
High
Moderate
Low
Very Low

Vulnerability Assessment Results

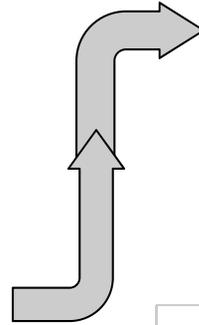
Critical Components (HW, SW, Firmware)	Identified Vulnerabilities	Exploitability	System Impact (I, II, III, IV)
Processor X	Vulnerability 1	Low	II
	Vulnerability 4	Medium	
SW Module Y	Vulnerability 1	High	I
	Vulnerability 2	Low	
	Vulnerability 3	Medium	
	Vulnerability 6	High	
SW Algorithm A	None	Very Low	II
FPGA 123	Vulnerability 1	Low	I
	Vulnerability 23	Low	



Likelihood of Losing Mission Capability
Near Certainty (VH)
Highly Likely (H)
Likely (M)
Low Likelihood (L)
Not Likely (VL)

Threat Analysis Results

Supplier	Critical Components (HW, SW, Firmware)	Analysis Findings
Supplier 1	Processor X	Supplier Risk
	FPGA 123	Supplier Risk
Supplier 2	SW Algorithm A	Cleared Personnel
	SW Module Y	Cleared Personnel



Initial Risk Posture

Consequence

	IV	III	II	I
Likelihood				

Risk Mitigation Decisions

Consequence

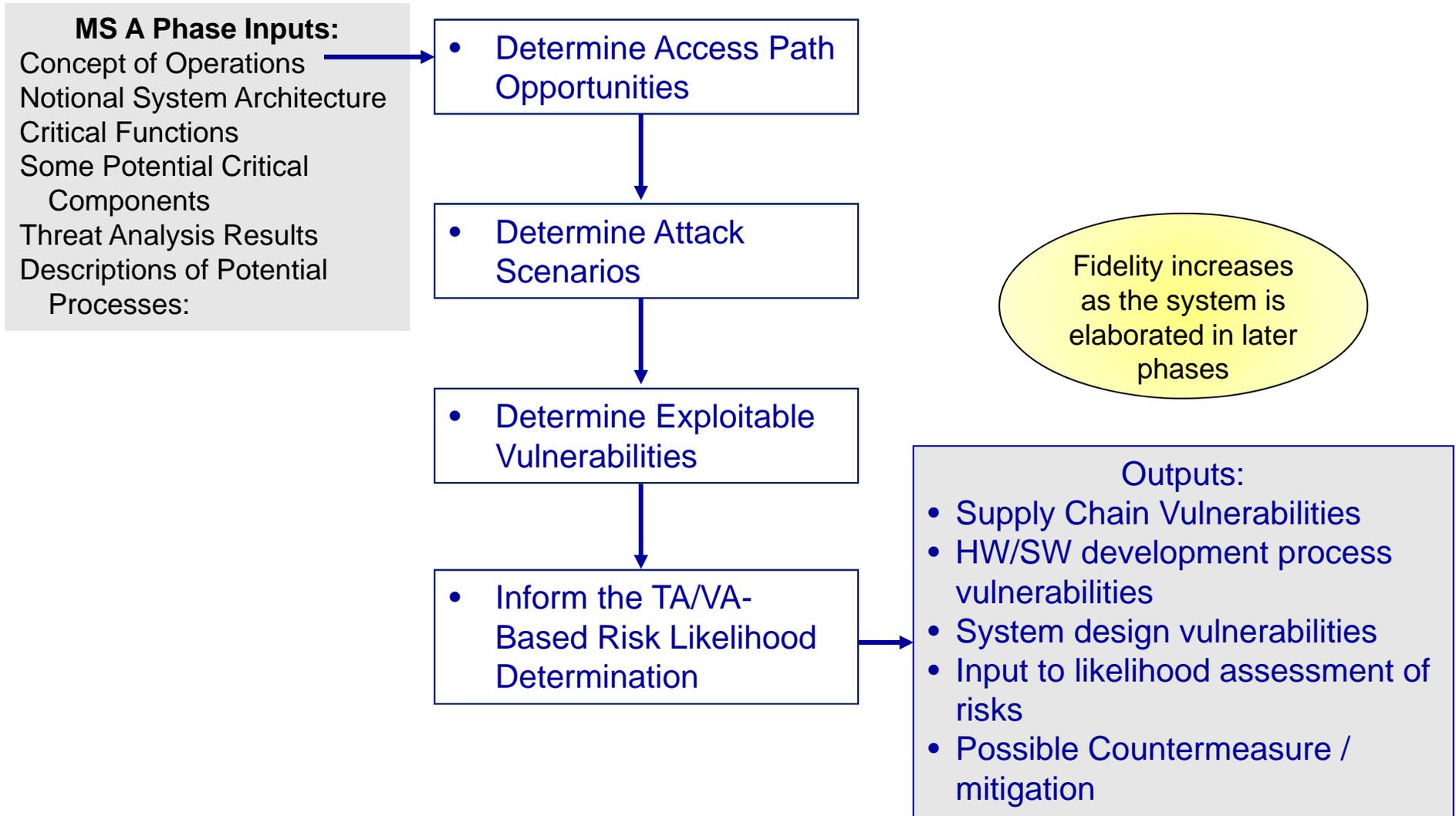
	IV	III	II	I
Likelihood				

Risk Mitigation and Countermeasure Options



Vulnerability Assessment Methodology

Vulnerability Assessment





Vulnerability Assessment Exercise Part I



Continuing along on the UAS for maritime surveillance we are going to look at potential supply chains, including software and firmware COTS, and the software development process for tracking and search functions from the preceding criticality analysis.

The end objective is to identify and quantify the potential vulnerabilities so that cost effective “countermeasures” can be incorporated into the system requirements or the statement of work prior to issuing the RFP

Brain storm a list of the possible vulnerabilities to each of the potential supply chain and the software development process chains provided. Also consider UAV specific vulnerabilities

You have been provided with

1. Criticality Analysis Results *in Exemplars*
2. Architecture Handout
 - Generic supply chain and malicious threat vectors
 - A notional architecture that is used to support requirements analysis
 - Two potential supply chains diagrams
 - Two possible software development life cycles



Vulnerability Assessment Exercise Part I Output Template



Supply Chain 1

Supply Chain Vulnerability	Software Development Vulnerability

Supply Chain 2

Supply Chain Vulnerability	Software Development Vulnerability



Vulnerability Assessment Exercise Part II with Heuristic Questions



Continuing along on the UAS for maritime surveillance we are going to look at potential supply chains, including software and firmware COTS, and the software development process for two of the components from the Vulnerability Assessment Part I

The objective of this exercise is to identify and quantify additional potential vulnerabilities for two of the components

1. For two given potential critical components (one from each of the potential supply/development chains provided), answer the questions on the following two charts
2. Add domain specific questions or any questions that you developed during vulnerability brainstorming that are not addressed in the following two charts

You have been provided with

- Two selected potential critical components
- A set of generic supply chain and software assurance vulnerability questions
- Results of participants' brain storming domain specific vulnerabilities



Vulnerability Assessment Exercise Part II



☐ Supply chain vulnerabilities to consider (put a “Y” or N next to each question)

CC1 CC2

1. Does the Contractor have a process to establish trusted suppliers ?
2. Require suppliers to have similar processes for the above questions?
3. Has the prime contractor vetted suppliers of critical function components (HW/SW/Firmware) based upon the security of their processes?
4. Are secure shipping methods used to ship How are components shipped from one supplier to another
5. Does receiving supplier have processes to verify critical function components received from suppliers to ensure that components are free from malicious insertion (e.g. seals, inspection, secure shipping, testing, etc.)?
6. Does the supplier have controls in place to ensure technical manuals are printed by a trusted supplier who limits access to the technical material?
7. Does the supplier have controls to limit access to critical components?
8. Can the contractor identify everyone that has access to critical components?
9. Are Blind Buys Used to Contract for Critical Function Components?
10. Are Specific Test Requirements Established for Critical Components?
11. Does the Developer Require Secure Design and Fabrication or Manufacturing Standards for Critical Components?



Vulnerability Assessment Exercise Part II



- UAV and design specific vulnerabilities to consider from Part I brainstorming (put a “Y” or “N” next to each question)

CC1 CC2

- 1.
- 2.
- 3.
- 4.
- 5.
- 6.
- 7.
- 8.



Vulnerability Assessment Exercise Heuristic Questions Discussions



Walk through one or two student Vulnerability Assessment Responses for each of the potential supply chains

Brainstorm possible countermeasures to the vulnerabilities identified

Discuss iterative design interactions and then provide a solution exemplar as a basis for next exercise



Initial Risk Assessment

Input Analysis Results:

Criticality Analysis Results

Mission	Critical Functions	Logic-Bearing Components (HW, SW, Firmware)	System Impact (I, II, III, IV)	Rationale
Mission 1	CF 1	Processor X	II	Redundancy
	CF 2	SW Module Y	I	Performance
Mission 2	CF 3	SW Algorithm A	II	Accuracy
	CF 4	FPGA 123	I	Performance

Vulnerability Assessment Results

Critical Components (HW, SW, Firmware)	Identified Vulnerabilities	Exploitability	System Impact (I, II, III, IV)
Processor X	Vulnerability 1 Vulnerability 4	Low Medium	II
SW Module Y	Vulnerability 1 Vulnerability 2 Vulnerability 3 Vulnerability 6	High Low Medium High	I
SW Algorithm A	None	Very Low	II
FPGA 123	Vulnerability 1 Vulnerability 23	Low Low	I

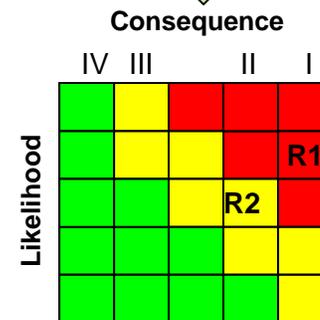
Threat Analysis Results

Supplier	Critical Components (HW, SW, Firmware)	Analysis Findings
Supplier 1	Processor X	Supplier Risk
	FPGA 123	Supplier Risk
Supplier 2	SW Algorithm A	Cleared Personnel
	SW Module Y	Cleared Personnel

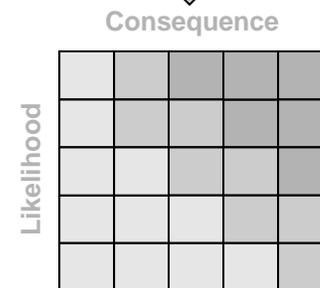
Consequence of Losing Mission Capability
Very High
High
Moderate
Low
Very Low

Likelihood of Losing Mission Capability
Near Certainty (VH)
Highly Likely (H)
Likely (M)
Low Likelihood (L)
Not Likely (VL)

Initial Risk Posture



Risk Mitigation Decisions



Risk Mitigation and Countermeasure Options



Risk Assessment Methodology



The Criticality Level (resulting from the CA) yields a consequence rating as shown:

The critical component associated with risk R1 is a Level I component.

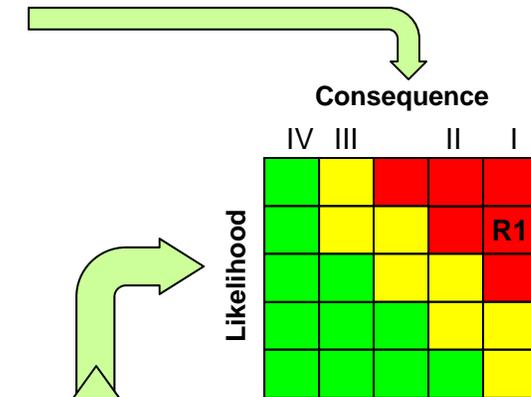
Consequence of Losing Mission Capability
Very High
High
Moderate
Low
Very Low

The overall likelihood rating is determined by combining the likelihood information from both the TA and the VA.

The illustrated critical component risk R1 has an overall highly likely (H = 4) rating

Likelihood of Losing Mission Capability
Near Certainty (VH)
Highly Likely (H)
Likely (M)
Low Likelihood (L)
Not Likely (VL)

Initial Risk Posture



The overall risk rating for R1 (designated by row-column) is: **4-5**



Risk Assessment – Exercise Overview



- In this Exercise, you will perform a risk assessment to determine a risk rating for selected critical components
- Use the CA results to determine the consequence rating
- Use the TA and VA results to determine the likelihood rating
 - Use the exemplar critical components and their associated TA and VA exercise results
 - Calculate the likelihood using the supply chain, software development, and domain-specific information for each critical component
 - Use these assessments to determine the overall risk likelihood
- Develop an overall risk rating assessment that places the critical component risk in the risk cube
- You have been provided with
 - Two selected critical components
 - VA exercise results (exemplars)
 - Copies of the output templates shown on the next slide, but with previous exemplars filled in



Risk Assessment Exercise – Templates for Results



Overall Likelihood

Component	Threat Assessment Likelihood	Supply Chain VA Likelihood	Software Development VA Likelihood	Overall Likelihood
Critical Component 1				
Critical Component 2				

Risk Rating

Component	Overall Likelihood	Consequence (from Criticality Analysis)	Risk Rating
Critical Component 1			
Critical Component 2			



Risk Assessment – Likelihood Guidance



- One approach for translating the vulnerability assessment into a risk likelihood input is to use an equal weighted scoring model that calculates the percentage of “No” answers in the groupings of “Y-N” questions from the VA.
- We will use this method for the exercise:

Number of “No” Responses	Risk Likelihood
All “NO”	Near Certainty (VH - 5)
$\geq 75\%$ NO	High Likely (H - 4)
$\geq 25\%$ No	Likely (M - 3)
$\leq 25\%$ No	Low Likelihood (L - 2)
$\leq 10\%$ No	Not Likely (NL - 1)

- Use the table above to determine the risk likelihood for each critical component
 - Develop likelihood calculations for supply chain, software, and domain-specific
- Approaches to combining the Supply Chain Vulnerability Assessment and the Software Vulnerability Assessment
 - Do separate calculations to determine two vulnerability likelihoods and then use the most severe among the threat and the two vulnerabilities as the overall likelihood input
 - ✓ Do separate calculations and average to get a single likelihood calculation
 - Domain specific judgment on weightings to get a single likelihood



Countermeasures Selection

Input Analysis Results:

Criticality Analysis Results

Mission	Critical Functions	Logic-Bearing Components (HW, SW, Firmware)	System Impact (I, II, III, IV)	Rationale
Mission 1	CF 1	Processor X	II	Redundancy
	CF 2	SW Module Y	I	Performance
Mission 2	CF 3	SW Algorithm A	II	Accuracy
	CF 4	FPGA 123	I	Performance

Vulnerability Assessment Results

Critical Components (HW, SW, Firmware)	Identified Vulnerabilities	Exploitability	System Impact (I, II, III, IV)
Processor X	Vulnerability 1 Vulnerability 4	Low Medium	II
SW Module Y	Vulnerability 1 Vulnerability 2 Vulnerability 3 Vulnerability 6	High Low Medium High	I
SW Algorithm A	None	Very Low	II
FPGA 123	Vulnerability 1 Vulnerability 23	Low Low	I

Threat Analysis Results

Supplier	Critical Components (HW, SW, Firmware)	Analysis Findings
Supplier 1	Processor X	Supplier Risk
	FPGA 123	Supplier Risk
Supplier 2	SW Algorithm A	Cleared Personnel
	SW Module Y	Cleared Personnel

Consequence of Losing Mission Capability
Very High
High
Moderate
Low
Very Low

Likelihood of Losing Mission Capability
Near Certainty (VH)
Highly Likely (H)
Likely (M)
Low Likelihood (L)
Not Likely (VL)

Initial Risk Posture

Consequence

Likelihood				

Risk Mitigation Decisions

Consequence

Likelihood				

Risk Mitigation and Countermeasure Options



Countermeasures Based on the Vulnerability Assessment



- There are two aspects of countermeasures selection associated with the Vulnerability Assessment results
 - 1) How much should be invested in countermeasures; i.e., how many of them do you need and/or how high a cost should be tolerated? This question is tied to the overall risk rating (H-M-L) which, in turn, is tied to the number of “No” answers in VA Exercise Part II.
 - 2) What types of countermeasures are needed. This question is tied to the specific vulnerabilities identified in the VA Exercises and captured in the domain-specific questions of Part II.



Examples of Possible Countermeasures



Risk Cost

-1	M
-2	H
-1	L
-2	L
-1	M
-2	H
-2	M
-1	L

- Possible acquisition process countermeasures for critical functions with risk lowering impact and order of magnitude cost
 - A supplier management plan
 - supplier selection criteria to reduce supply chain risks
 - Identification functionally equivalent alternate components and sources
 - Evaluates and maintains a list of suppliers and alternates suppliers with respect to the criteria established
 - An anonymity plan that
 - Protects the baseline design, test and supply chain data
 - Use blinds buys for component procurement
 - Secure design and coding standards that address the most common vulnerabilities identified in CWE or the CERT.
 - The use of secure design and coding standards are part of the criteria used for design and code inspections
 - The use of a static analyzer to identify and mitigate vulnerabilities
 - Inspection of code for vulnerabilities and malware
 - Access control that
 - Limits access
 - Logs access and notes specific information changed and accessed
 - Require inspection and approval of changes
 - A Government provided supply chain threat briefing
- **Values assigned to risk reduction and cost are for example. Program based team's must develop estimates for their environment for reducing risk likelihood and cost to implement.**



Examples of Possible Countermeasures



- Possible system design countermeasures for critical functions with risk lowering impact and order of magnitude cost

Risk Cost

-2	H
-1	M
-1	L
-2	L
-2	M
-2	M
-2	H

- A separation kernel –
 - hardware and/or firmware and/or software mechanisms whose primary function is to establish, isolate and separate multiple partitions and control information flow between the subjects and exported resources allocated to those partitions
- Fault detection with degraded mode recovery
- Authentication with least privilege for interfacing with critical functions
- Wrappers for COTS, legacy and developmental software to enforce strong typing and context checking.
- Wrappers for COTS, legacy and developmental software to identify and log invalid interface parameters
- physical and logical diversity where redundancy or additional supply chain protections are required
- An on-board monitoring function that checks for configuration integrity and unauthorized access.
 - Examples include honey pots which capture information about attackers, scanners and sniffers that check for signatures of attackers, and monitoring clients which check for current patches and valid configurations



Cost-Benefit-Risk Trade Study Exercise



- List the critical components that require risk reduction
- For each critical component
 - Determine which countermeasures to evaluate
 - Estimate the implementation cost impacts
 - Estimate the risk reduction achieved by each countermeasure

Component	Risk Rating	Countermeasures	Cost impact	Risk reduction	Residual Risk Rating

- Select Countermeasures for Implementation
- Determine Residual Risk Rating for future PPP assessments
 - Determine updated risk rating after implementation of countermeasures
 - Repeat the CA, TA, VA to support a new RA to refine this rating
 - Further countermeasures may be needed



Residual Risk

Criticality Analysis Results

Mission	Critical Functions	Logic-Bearing Components (HW, SW, Firmware)	System Impact (I, II, III, IV)	Rationale
Mission 1	CF 1	Processor X	II	Redundancy
	CF 2	SW Module Y	I	Performance
Mission 2	CF 3	SW Algorithm A	II	Accuracy
	CF 4	FPGA 123	I	Performance

Vulnerability Assessment Results

Critical Components (HW, SW, Firmware)	Identified Vulnerabilities	Exploitability	System Impact (I, II, III, IV)
Processor X	Vulnerability 1 Vulnerability 4	Low Medium	II
SW Module Y	Vulnerability 1 Vulnerability 2 Vulnerability 3 Vulnerability 6	High Low Medium High	I
SW Algorithm A	None	Very Low	II
FPGA 123	Vulnerability 1 Vulnerability 23	Low Low	I

Threat Analysis Results

Supplier	Critical Components (HW, SW, Firmware)	Analysis Findings
Supplier 1	Processor X	Supplier Risk
	FPGA 123	Supplier Risk
Supplier 2	SW Algorithm A	Cleared Personnel
	SW Module Y	Cleared Personnel

Consequence of Losing Mission Capability
Very High
High
Moderate
Low
Very Low

Likelihood of Losing Mission Capability
Near Certainty (VH)
Highly Likely (H)
Likely (M)
Low Likelihood (L)
Not Likely (VL)

Initial Risk Posture

	Consequence			
	IV	III	II	I
Likelihood				R1
		R2		

Risk Mitigation Decisions

	Consequence			
	IV	III	II	I
Likelihood				R1
			R2	
			↓	↓
			R2'	R1'

Risk Mitigation and Countermeasure Options



RFP Sections

RFP Package

- Section A: Solicitation Contract Form
- Section B: Supplies or services and prices/costs
- **Section C: Description/specifications/work statement**
 - System Requirements Document (SRD - SPEC)
 - Statement of Work (SOW)
 - Contract Deliverable Requirements List (CDRLs)
- Section D: Packaging and marking
- Section E: Inspection and Acceptance
- Section F: Deliveries or performance
- Section G: Contract administration data
- Section H: Special contract requirements
- Section I: Contract Clauses
- Section J: List of Documents, Exhibits, and other Attachments
- Section K: Representations, Certification, and Other Statements of Offerors
- **Section L: Instructions, conditions, and notice to offerors**
- **Section M: Evaluation factors for award**

- **Incorporate Process Protections**
Statement of Work (SOW),
Statement of Objectives (SOO),
Performance Work Statement (PWS), or equivalent
- **Incorporate Design Protections**
System Requirements Document (SRD), Specification, or equivalent
- **Contract Deliverable Requirements List (CDRL) and Data Item Description (DID)**

- **Description of program protection processes for Level I/II critical components**
 - Sections L and M



Potential basic development, design and supply chain protections (1 of 4)



- **The contractor shall:**

- Create and update the program protection analysis at each of the SETRs to:
 - Identify mission critical functions and associated components
 - Identify technology exploitation, fielded system compromise, development and supply chain malicious insertion vulnerabilities
 - Utilize threat assessments
 - Develop program protection risks
 - Identify risk reduction countermeasures (mitigations) based upon a cost-benefit trade study
- Maintain multi-level visibility into the supply chain of the critical function components .
- Extend these responsibilities to sub-tier suppliers of critical function components
- Incorporate government provided intelligence
- Establish secure design and coding standards



Potential basic development, design and supply chain protections (2 of 4)



- **For Level I Mission Critical Functions/Critical Components the system shall establish basic protection requirements unless justified by a cost benefit analysis. Supply Chain and Development basic protections shall include:**
 - Supplier Management Plan that
 - Includes supplier selection criteria to reduce supply chain risks
 - Identifies functionally equivalent alternate components and sources
 - Evaluates and maintains a list of suppliers and alternates suppliers with respect to the criteria established
 - An anonymity plan that
 - Protects the baseline design, test and supply chain data
 - Use blinds buys for component procurement
 - Additional access controls that
 - Further limits access beyond normal program control
 - Logs access
 - Establishes data collection for post attack forensic analysis
 - Require inspection and approval of changes
 - Black hat attack testing of system, development environment and supply chain
 - Red team testing
 - Material and non material attack / compromise response process development



Potential basic development, design and supply chain protections (3 of 4)



- **For Level I Mission Critical Functions/Critical Components the system shall establish basic protection requirements unless justified by a cost benefit analysis. Design requirements basic protections shall include:**
 - Establish least privilege using distrustful decomposition (privilege reduction) or similar approach to move level I critical functions into separate mutually untrusting programs*
 - Physical and logical diversification of components for critical functions which require redundancy to meet reliability or safety requirements
 - Physical and logical diversification with voting to establish trustworthiness of selected level I critical function components
 - Wrappers for COTS, legacy and developmental software to enforce strong typing, context checking and other interface validation methods for interfaces with critical functions.
 - Wrappers for COTS, legacy and developmental software to identify and log invalid interface data using secure logging approaches
- **Basic protection security requirements and designs shall be discussed in each of the Systems Engineering Technical Reviews**

*See SEI -2009-TR-010



Potential basic development, design and supply chain protections (4 of 4)



To evaluate each contractors implementation of the basic program protections

- **Section L of the RFP should include:**
 - **The contractor shall describe for level I mission critical functions / components the approach to :**
 - Supplier management and the use of an anonymity plans
 - Maintenance of multi-level visibility into the supply chain of the critical function components
 - PPP analysis to determine and mitigate program protection risks
 - Establish and update secure design and coding standards
 - Use of secure design patterns and least privilege for critical functions
 - Use of physical and logical diversification for critical function components
- **Section M of the RFM should include**
 - **The above section L statement in the evaluation criteria**



Program Protection Plan Contents



Sections

1. Introduction
2. Program Protection Summary
3. Critical Program Information (CPI) and Critical Functions
4. Horizontal Protection
5. Threats, Vulnerabilities, and Countermeasures
6. Other System Security-Related Plans and Documents
7. Program Protection Risks
8. Foreign Involvement
9. Processes for Management and Implementation of PPP
10. Processes for Monitoring and Reporting CPI Compromise
11. Program Protection Costs

Appendices

- A. Security Classification Guide
 - B. Counterintelligence Support Plan
 - C. Criticality Analysis
 - See CA Brief
 - D. Anti-Tamper Plan (If Applicable)
 - See AT Guidance
 - E. Information Assurance Strategy
 - See IA Strategy Guidance
- If it is desired to attach other documents to the PPP, call them “Supporting Documents”
 - These will not be included in the package routed up the chain for signature
 - PPP Appendix that require other signatures must be approved prior to PPP approval
 - Includes SCG, CISP, AT Plan, IA Strategy

Tailor Your Plan to Your Program; Classify Tables Appropriately



MSA Phase Key Points



- ❑ It is both possible and necessary to perform meaningful system security engineering prior to Milestone A
 - Mission critical system functions and some potential implementing components can be identified
 - Known generic attack vectors mapped against the system CONOPS and notional architecture can be used to inform a vulnerability assessment that uncovers potential exploitable vulnerabilities

- ❑ A risk based cost benefit trade-off is a mechanism to select the protection requirements to incorporate into the TD Phase RFP SOW and SRD

- ❑ The SOW should indicate that further program protection analysis is a Government-Industry shared responsibility throughout the remainder of the lifecycle as the system is refined and details are determined



Learning Objectives



- **Discuss the MSA Phase Program Protection Plan(PPP) Analysis for Supply Chain and Malicious Insertion Threats**
- **Show the risk based cost-benefit trade to select the mitigations**
- **Describe basic protections to incorporate in the MSA Phase PPP and RFP**
- **Recognize that supply chain and malicious insertion program protections are a shared government-industry responsibility**



Tutorial Thoughts



- 1. What did you like most?**
- 2. What most needs improvement?**
- 3. What specific changes do you recommend?**



For Additional Information



Contact the Program Protection Team:

Melinda Reed
melinda.reed@osd.mil

Paul Popick
paul.popick.ctr@osd.mil



Questions?



Appendix



DoDI 5200.mm Trusted Systems and Networks



- **Key Policy Objectives**
 - Manage risk of mission-critical function and component compromise throughout lifecycle of key systems
 - Criticality Analysis is the systems engineering process for focusing activities
 - Mitigations: Supply chain risk management, software assurance, secure design
 - Use all-source intelligence analysis to inform procurement decisions
 - Codify trusted foundry requirement for DoD-unique ASICs
 - Document planning and accomplishments in PPP and IA Strategy
- **Key OSD and Component Responsibilities**
 - Ensure and coordinate protection of mission critical functions and components across the program lifecycle
 - Advance state of the art in software assurance methodology and tools
 - Investigate “trust” implications for non-ASIC microelectronics
 - Analyze suspected and confirmed supply chain exploits across DoD
 - Tasks the Heads of the Components to establish TSN focal points,
 - Tasks DoD with developing a strategy for trust in FPGAs
- **Status**
 - Instruction is currently awaiting signature



Criticality Analysis Considerations (1/2)



- ❑ **Use Mission Threads to Identify Critical Functions**
 - Based on likelihood of mission failure if the function is corrupted or disabled
 - Derived during pre-Milestone A, revised as needed for successive development milestones
- ❑ **Group Mission Capabilities by Relative Importance, As Applicable**
 - Training or reporting functions may not be as important as core mission capabilities
- ❑ **Map Critical Functions to System's Critical Components**
 - Based on likelihood of mission failure if the component is corrupted or disabled
 - Includes Critical Subsystems, Configuration Items, and Components
- ❑ **Map Critical Subsystems, CIs, and sub-CIs (Components) to Information and Communications Technologies (ICT's)**
 - Logic-bearing components have been singled out as often implementing critical functions and as susceptible to lifecycle corruption
- ❑ **Assign Criticality Levels to the Identified CIs or Components, Criteria May Include:**
 - Frequency of component use across mission threads
 - Presence of redundancy – triple-redundant designs can indicate critical functions.



Identifying Mission Critical Functions



Criticality Analysis Considerations (2/2)

Criticality Analysis



❑ Identify Any CIs or Components That Do Not Directly Implement Critical Functions, But Either Have Unmediated Communications Access (i.e., An Open Access Channel) to One or More Critical Functions or Protect a Critical Function

- Which components give or receive information to/from the critical components?
- A non-critical component may communicate with a critical function in a way that exposes the critical function to attack. In some cases, the architecture may need to include defensive functions or other countermeasures to protect the critical functions



❑ Identify Critical Conditions/Information Required to Initialize the System to Complete Mission-Essential Functions

- What information is needed to successfully execute capabilities?
- How is this information obtained, provided, or accessed by the system?
- How quickly must information be received to be useful?
- Does the sequence in which the system initializes itself (power, software load, etc.) have an impact on performance?



❑ Repeat Process as System is Refined or Modified

- Design changes may result in adding or removing specific CIs and sub-CIs from the list of critical functions and components
- Key Decision Points: Systems Engineering Technical Reviews, Acquisition Milestone Decisions



Tutorial Reference Catalog of Attack Vectors (1 of 3)



Attack Vector Name	Description
Reverse engineering of lost / stolen / captured components	The adversary disassembles a stolen or captured system to learn technical details about its operation and/or vulnerabilities that may be exploited
Compromise design and/or fabrication of hardware components	APT is able to compromise not merely the distribution, but the design and manufacturing of critical organization hardware at selected suppliers
Adversary intercepts hardware in distribution channel	Adversary intercepts hardware from legitimate suppliers and modifies it or replaces it with faulty hardware
Malicious software update	An attacker uses deceptive methods to cause a user or an automated process to download and install malicious code believed to be valid/authentic
Counterfeit web sites used to distribute malicious software updates	Adversary creates a duplicate of a legitimate web site, which users access and unwittingly download malicious software upgrades, patches, etc.
Components/spares no longer available	Adversaries offer necessary replacement parts, but with malware incorporated
Man-in-the-middle (MITM) supply chain	Adversary eavesdrops on sessions between organization and external supplier to gain insight into organization's supply chain needs that they can later exploit
Malicious software implantation through 3rd party bundling	The inclusion of insecure 3rd party components in a product or code-base, possibly packaging a malicious component in a product before shipping to customer.
Adversary gains unauthorized access by exploiting a software vulnerability	The adversary exploits known or unknown (0-day) software vulnerabilities to bypass security controls and gain unauthorized access
Adversary gains unauthorized access using stolen credentials	The adversary uses stolen user account information or PKI credentials to log into the system
Adversary initiates a botnet attack to disrupt network services	A botnet can be directed to spam a designated target system over a range of ports and protocols, resulting in a Distributed Denial of Service (DDoS) attack



Tutorial Reference Catalog of Attack Vectors (2 of 3)



Attack Vector Name	Description
Ex-filtration via removable media	Clandestine transfer of sensitive data to removable media, e.g., printed reports, CD, thumbdrive, etc., which is physically carried outside the security perimeter
Ex-filtration via external network	Clandestine ex-filtration of sensitive data, encrypted and transferred to a remote system outside the security perimeter using a variety of data formats
Derivation of Critical Program Information from unclassified sources	Aggregation of unclassified and/or unprotected data used to derive sensitive data
Unauthorized / unrestricted copying	Unauthorized copies of sensitive data are made and stored within the security perimeter, for future exfiltration, without document control or accountability
Clandestine changes to software or mission data	Clandestine alteration of software or data so that a system operates in a manner that compromises mission effectiveness or safety
Use of public domain info to identify and target suppliers	Suppliers are targeted for cyber and/or social engineering attack based on adversary's supply chain awareness
Netflow data used to identify critical internal workflows	Adversary analyzes netflow traffic data to identify and target key network workflows, IT resources, and/or personnel
Shell company established to export critical technologies	Adversary sets up a dummy company for the purpose of acquiring products that contain restricted or export-controlled technologies for shipment overseas
Software defects hidden/obscured by code complexity	Highly complex code can obscure software defects, even by static source code analysis tools
Use of counterfeit parts of foreign or unknown origin	Insertion of counterfeit parts of foreign origin into products destined for the U.S. having potential to degrade or sabotage performance and reliability of systems
Hardware/Software baseline manipulations	An adversary in the employ of a solution provider subverts computers and networks through subtle hardware or software manipulations



Tutorial Reference Catalog of Attack Vectors (3 of 3)



Attack Vector Name	Description
Hiding backdoors and features for unauthorized remote access	An adversary in the employ of a software supplier deliberately hides backdoors and features for unauthorized remote access and use
Foreign hardware incorporated into computing environment	Hardware incorporated into the computing environment that was manufactured overseas or acquired from a foreign-owned domestically controlled company
Foreign software incorporated into computing environment	Software incorporated into the computing environment that was developed overseas or acquired from a foreign-owned domestically controlled company
Malicious Code Pre-installed	Malicious code (e.g., viruses, logic bombs, self-modifying code, spyware, trojans) is pre-installed on components being integrated into the computing environment
Disruption of Critical Product or Service	Failure or disruption in the production or distribution of a critical product or service
Malicious or Unqualified Service Provider	Reliance upon a malicious or unqualified service-provider for the performance of technical services
Installation of Unintentional Vulnerabilities	Installation of hardware or software that contains unintentional vulnerabilities



Vulnerability Assessment Considerations (1/2)



Where and Under What Conditions was the System Designed?

- Who made significant system-wide design decisions?
- Who has had access to design information?
- How are requirements and specifications for critical components communicated to suppliers?
- How much do suppliers know about how critical their products are to the overall system?



Where and Under What Conditions were Critical Components Developed?

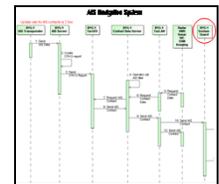
- For custom components, who made significant design decisions?
- Who has had access to design information?
- Where are critical components fabricated or manufactured?
- Who has had access to fabrication or manufacturing processes?
- What testing of critical components has been conducted? How and where?
- How are critical components shipped?
- How has custody of critical components been managed?



System Requirements



Data Flow Diagrams



How and Where are Components Assembled and Integrated into Completed Systems?

- What final system testing is conducted?

Assessing Vulnerability of Critical Components



Vulnerability Assessment Considerations (2/2)



❑ Where and under what conditions was critical software or firmware developed?

- How were software requirements developed and communicated?
- Who designed the algorithms implemented in software?
- Who designed and developed the software?
- What design and code review or inspection processes have been employed?
- Who has had access to the software code base? How has access to the code base been controlled?
- What software tools (compilers, debuggers, hardware emulators, test harnesses, etc.) have been employed in developing the software?
- What libraries of separately developed software modules have been used?
- Are software developers able to work remotely; for example, from home?
- How is the configuration of software and firmware managed?
- What controls are there over the software build process?
- How and where has the software been tested? What test criteria have been applied?



❑ How are software updates distributed and loaded in the field?

- What verification techniques are used to ensure complete and effective updates?



❑ How are other system maintenance operations conducted?

- How are line-replaceable subsystems managed?
- Are depot operations established?
- What plans are there to ensure reliable sources of replacement parts?