Presented at:

NATO Systems Concepts and Integration (SCI) Specialists Meeting on “Cyber Physical Security of Defense Systems

Fort Walton Beach FL

8-9 May 2018

Naval Aviation Weapon System Cyber Risk Assessment Methodologies

8 May 2018

Presented to:

NATO Systems Concepts and Integration (SCI-300) Specialists Meeting

Presented by:

Steven B. Kern, Chief Engineer

Senior Scientific Technical Manager (SSTM)

NAVAIR Cyber Warfare Detachment

NAVAIR Public Release 2018-325. Distribution Statement A – “Approved for public release; distribution is unlimited”

Topics

- **Critical Questions for System Security Engineers**
- **Cyber Table Top (CTT)**
- **Cyber Risk Assessment (CRA)**
- **Cyber Attack Surface Enumeration (CASE)**
- **Cyber Risk Assessment to Mission (CRAM)**
- **Cyber Risk Assessment Nodal-based GUI (CRANG)**

Critical Questions

DESIGN/TEST/DELIVER

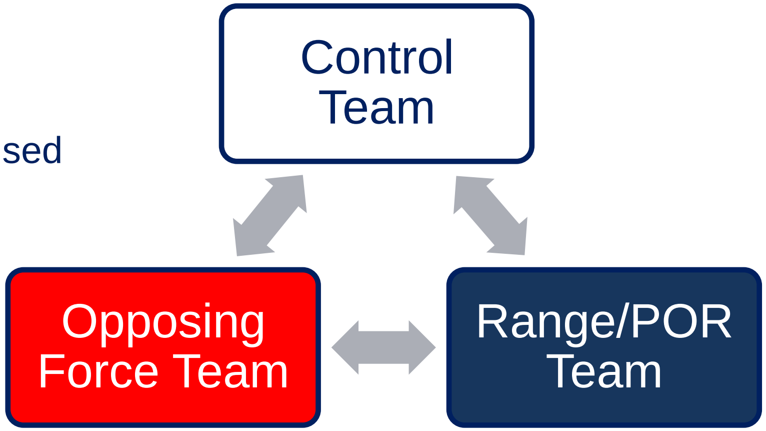
- How can I measure the cyber risk relative to all of the traditional safety of flight risks and mission risks?
- How and when can I prioritize a cyber risk vs. other risks during my program execution?
- How can I build in resilience against cyber attacks?
- How do I plan developmental and operational cyber tests?

EXPERIMENT/TRAIN/FIGHT

- How do I explain the weapon system adversarial cyber risk to an operator/maintainer/logistician?
- How do I provide an operator a way to detect when a weapon system is subject to a “cyber attack”?
- What is an acceptable level of operational cyber risk?
- What Techniques, Tactics and Procedures (TTPs) can an operator/maintainer/logistician execute to manage cyber risk to an acceptable level?

Cyber Table Top (CTT)

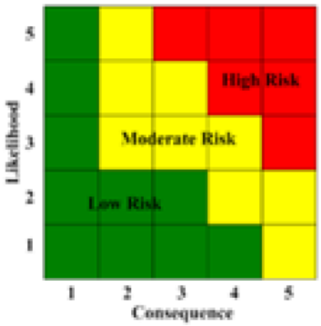
- **What is a CTT?**
  - A low technology, low cost, intellectually intensive exercise to introduce and explore the effects of cyber offensive operations on the capability of a system, SoS or FoS to execute a mission
- **Why is it used?**
  - Help identify, size and scope the cybersecurity test effort
  - Identify potential threat vectors, risks associated with threat vectors, potential threats from boundaries
  - Particularly useful for complicated SoS interactions
    - Can help prioritize where CRA efforts should be focused
- **What does it produce?**
  - Initial categorization of family of threats into 3 categories
    - Threats that must be tested against
    - Threats the require detailed analysis
    - Threats that will not be tested due to low risk or easy work around
  - Cybersecurity risk matrices
  - Recommendation for next actionable steps to increase resiliency to cybersecurity attacks



Control Team

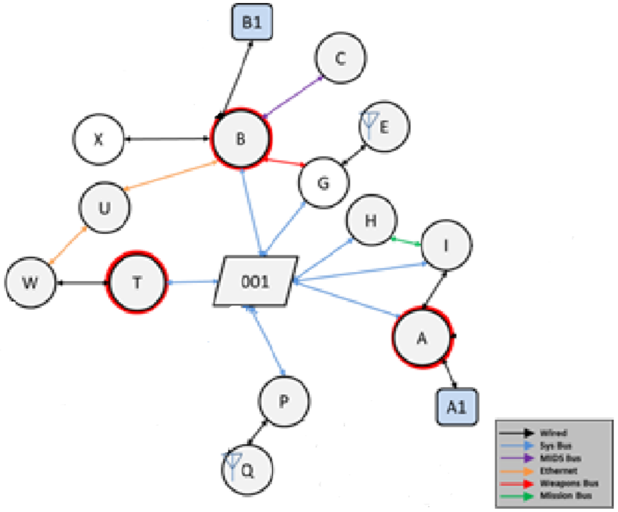
Opposing Force Team

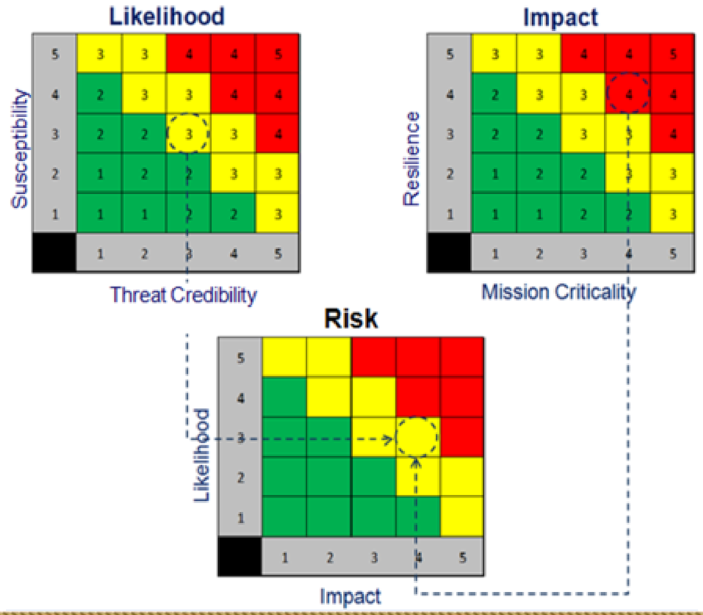
Range/POR Team



Cyber Risk Assessment (CRA)

- **What is a CRA?**
  - A systems engineering cyber attack tree based decomposition of a weapon system
    - Identify all entry points into the system
    - Identify target list (key components & functions that adversary would want to affect)
    - Create weighted attack paths from entry points to targets
- **Why is it used?**
  - Identify: potential threat vectors, risks associated with threat vectors, potential threats from boundary systems
  - Scope what vectors need to be validated via testing
- **What does it produce?**
  - CRA Report
    - Cybersecurity risk matrices





Likelihood

Susceptibility					
5	🟨 3	🟨 3	🟥 4	🟥 4	🟥 5
4	🟩 2	🟨 3	🟨 3	🟥 4	🟥 4
3	🟩 2	🟩 2	🟨 3	🟨 3	🟥 4
2	🟩 1	🟩 2	🟩 2	🟨 3	🟨 3
1	🟩 1	🟩 1	🟩 2	🟩 2	🟨 3
	1	2	3	4	5

Threat Credibility

Impact

Resilience					
5	🟨 3	🟨 3	🟥 4	🟥 4	🟥 5
4	🟩 2	🟨 3	🟨 3	🟥 4	🟥 4
3	🟩 2	🟩 2	🟨 3	🟨 3	🟥 4
2	🟩 1	🟩 2	🟩 2	🟨 3	🟨 3
1	🟩 1	🟩 1	🟩 2	🟩 2	🟨 3
	1	2	3	4	5

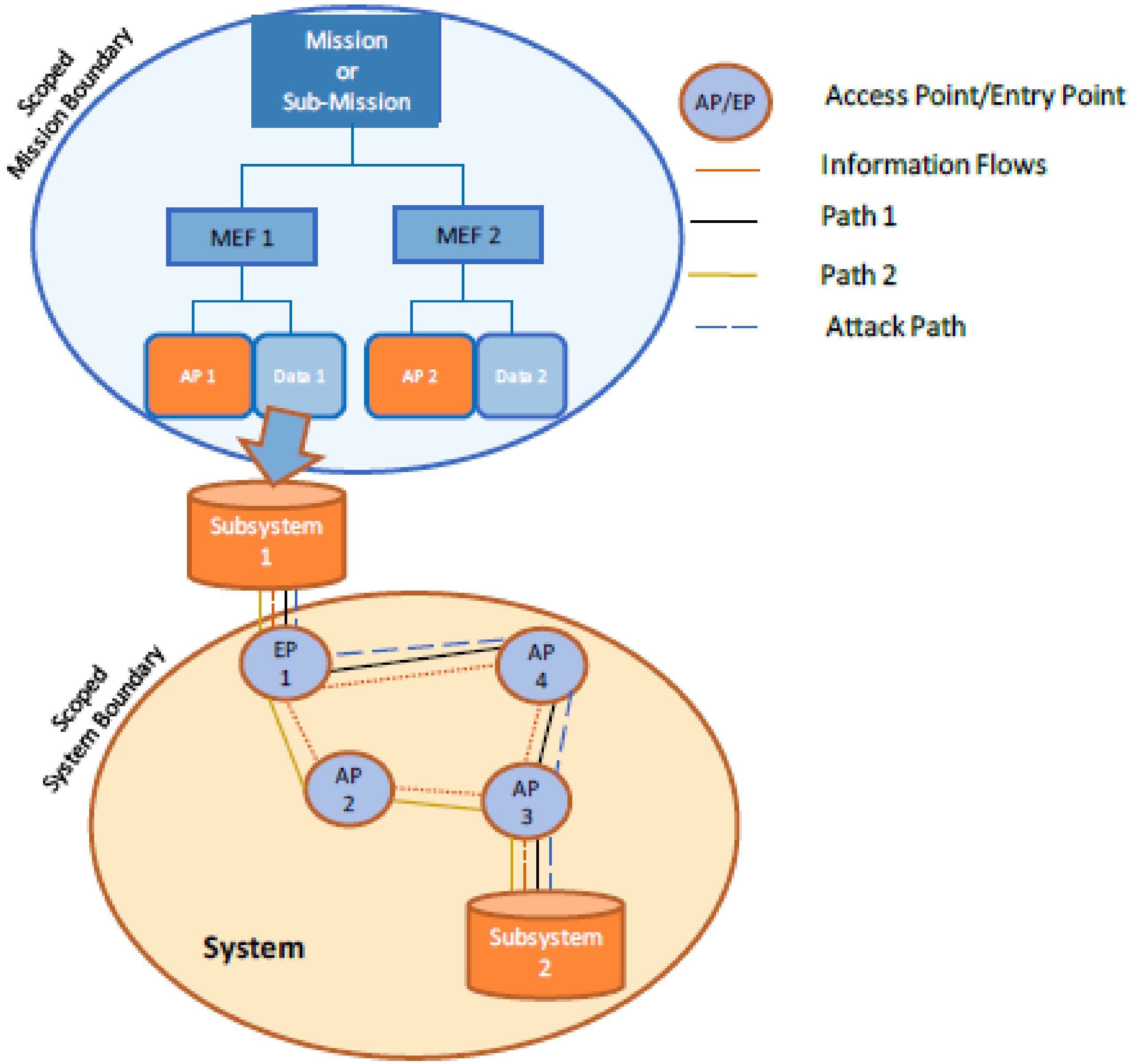
Mission Criticality

Risk

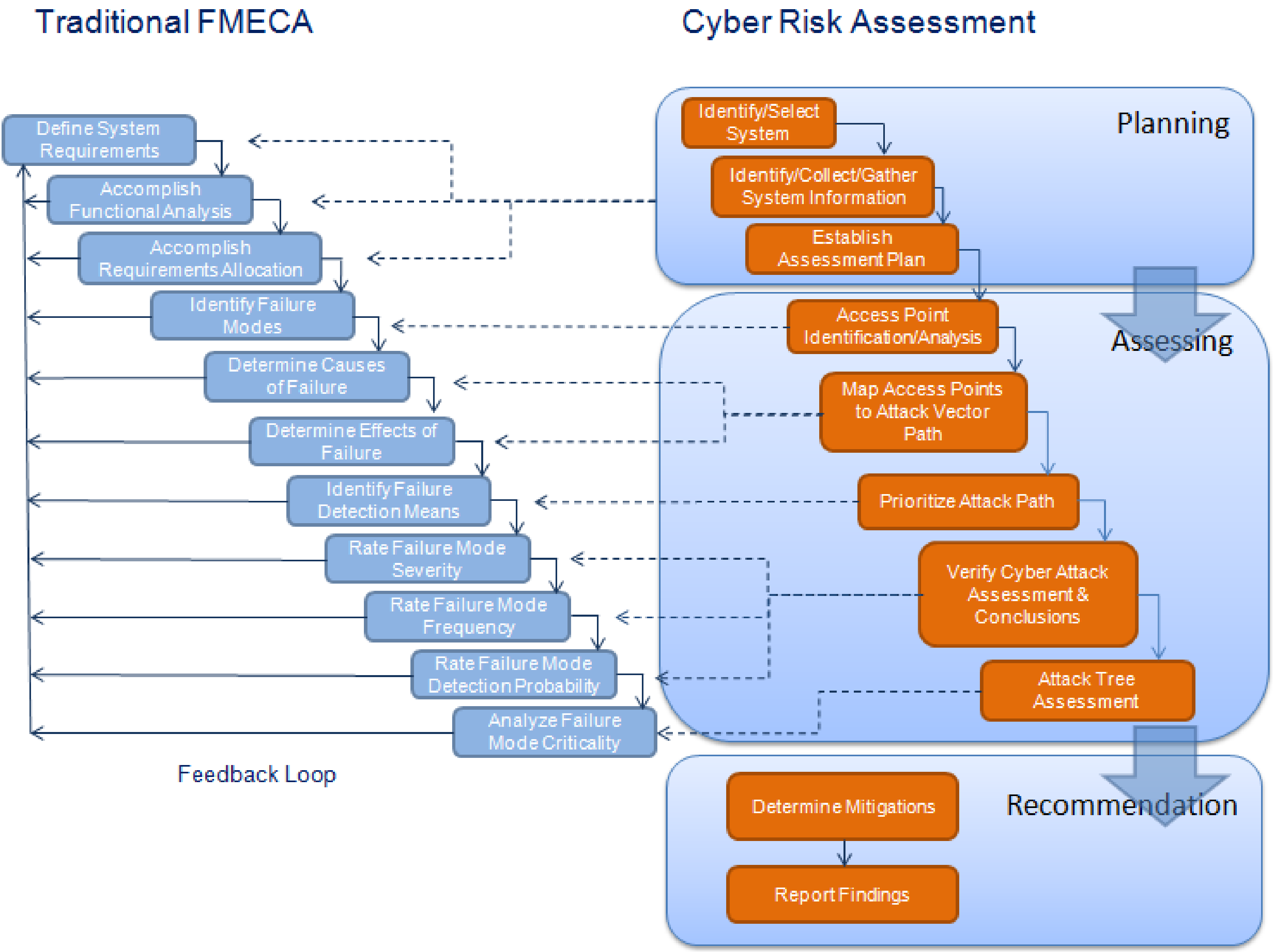
Likelihood					
5	🟨	🟨	🟥	🟥	🟥
4	🟩	🟨	🟨	🟥	🟥
3	🟩	🟩	🟨	🟨	🟥
2	🟩	🟩	🟩	🟨	🟨
1	🟩	🟩	🟩	🟩	🟨
	1	2	3	4	5

Impact

Mission and System Boundaries



Comparison of FMECA & CRA


Traditional FMECA
Cyber Risk Assessment
Define System Requirements
Accomplish Functional Analysis
Accomplish Requirements Allocation
Identify Failure Modes
Determine Causes of Failure
Determine Effects of Failure
Identify Failure Detection Means
Rate Failure Mode Severity
Rate Failure Mode Frequency
Rate Failure Mode Detection Probability
Analyze Failure Mode Criticality
Feedback Loop
Planning
Identify/Select System
Identify/Collect/Gather System Information
Establish Assessment Plan
Assessing
Access Point Identification/Analysis
Map Access Points to Attack Vector Path
Prioritize Attack Path
Verify Cyber Attack Assessment & Conclusions
Attack Tree Assessment
Recommendation
Determine Mitigations
Report Findings

CRA Information Requirements

Information requirements fall into three categories: information about the mission, information about the system, and nature of the threat (cyber intelligence reporting or applied threat actor capability model).

Information about the mission

- Mission(s) supported, mission-essential functions (MEFs), operational objectives
- CONOPS/CONEMPS for the System
- Interviews with operators, logisticians, and maintainers
- Cyber Table Top (CTT) Operational Scenarios/Mission Threads, and Results

Information about the system

- DoD Architecture Framework (DoDAF) Views
  - *OV-1 High-Level Operational Concept Graphic*
  - *OV-3 Operational Information Exchange (Resource Flow) Matrix*
  - *OV-4 Operational Relationships Chart*
  - *OV-5 Operational Activity Model*
  - *SV-5a Operational Activity to Systems Function System and Mission Criticality Assessment Output*
- System data (interfaces, architecture, utilization, environment, contexts, etc.)
- Existing security policies and procedures
- Acquisition lifecycle status and Systems Engineering Technical Review (SETR) event point, along with the body of documentation used to support the events
- Cyberspace threat information (initial assessment based on the system's doctrinal and mission utility)
- Program Protection Plan (PPP)
- TSN Criticality Assessment, if available
- Supply-chain information , if available
- RMF Assessment and Authorization (A&A) or legacy Certification and Accreditation (C&A) information from the Enterprise Mission Assurance Support Service (eMASS) and other sources
- Defense in Depth Architecture Diagrams
- Block wiring diagrams (H/W, functional, etc.)
- System interface documentation (Interface Control Document (ICD) Interface Requirements Document (IRD), Configuration Definition Document(s) etc.)
- H/W and Software (S/W) information
- H/W and S/W configurations
- Technical or maintenance documentation
- Information collected/processed/stored by system and sensors during mission (example: EO images from EO sensor, IR images from IR sensor)
- Traditional FMECA and Mission Essential Subsystem Matrix (MESM) information or results

Nature of the threat

- Capstone Threat Assessment (CTA), System Threat Assessment Report (STAR) or Validated Online Lifecycle Threat (VOLT) (future replacement for STAR)
- Critical Intelligence Parameters (CIPs)

CRA Key Roles

- **CRA Leader – (**typically the Program Office Chief Engineer): The CRA Lead must work with the system owners and stakeholders to understand the program acquisition strategy, identify the purpose for the assessment, and develop the communications strategy. During the assessment process, they are responsible for the planning, scheduling, execution, and oversight of all assessment activities.
- **System Architecture Lead** (typically the Program Office System Security Engineer): A full understanding of the system architecture is required to properly perform the risk assessment. In order to support this understanding, the System Architecture Lead will identify and assist with the collection of required source information, technical data, and system information. They will characterize the systems, subsystems, and/or components and will assist the team in the development of system models that have not been provided.
- **Cyber Warfare Lead** (Highly trained/experienced hacker)**:** The Cyber Warfare Lead contributes to the assessment by characterizing the missions, assisting in the development of mission models and decomposition of the MEFs, and identifying or validating the data and information types used or created by the mission. Additional tasks include mapping the access points to the MEFs; evaluating the network, known weaknesses, and access points; and determining vulnerabilities that formulate attack scenarios and objectives.
- **Threat Information Lead** (Cyber Intelligence Analyst): The Threat Information Lead analyzes cyber threat characteristics and Tactics, Techniques, and Procedures (TTP) in order to characterize the threats to the mission and system. They prioritize the threats and determine the threat scope. Summarized adversarial cyber-attack capabilities are analyzed and decomposed from an adversarial perspective, and threat-related inputs and conclusions for the final report are generated.
- **Knowledge Manager**: The Knowledge Manager will administer the collection, storage, and distribution of data to support the CRA, along with the management of Requests for Information (RFIs), ensuring the data requirements are addressed and information is accessible at the identified storage locations. The Knowledge Manager will assist the team in executing the communications strategy and completing output products, such as the CRA Report.
- **Supporting Team**: These skillsets may include experts in areas such as RMF, Test and Evaluation (T&E), Maintenance, Logistics, administrative, financial, legal, and contracts.

DSB Cyber Threat Model

DEFENSE SCIENCE BOARD REPORT
Resilient Military Systems and the Advanced Cyber Threat Jan 2013

Tier VI organizations employ full-spectrum techniques, including humans (e.g., spies engaged in bribery and blackmail) and close-access means (physical or electronic) to gain system penetration, and have the resources to conduct many operations concurrently

Tier V actors are able to insert malicious software or modified hardware into computer and network systems at various points during their lifecycle for later exploit (e.g., a “cyber time bomb”).

Tier IV is characterized by larger, well-organized teams, either state or criminal. Tiers V and VI encompass actors who can go beyond malicious software inserted through Internet access, and instead, create vulnerabilities in otherwise well-protected systems.

Tier III and IV actors employ a broad range of software capabilities to penetrate cyber systems and effect exploits through Internet access. A major distinction between Tiers III and IV is scale

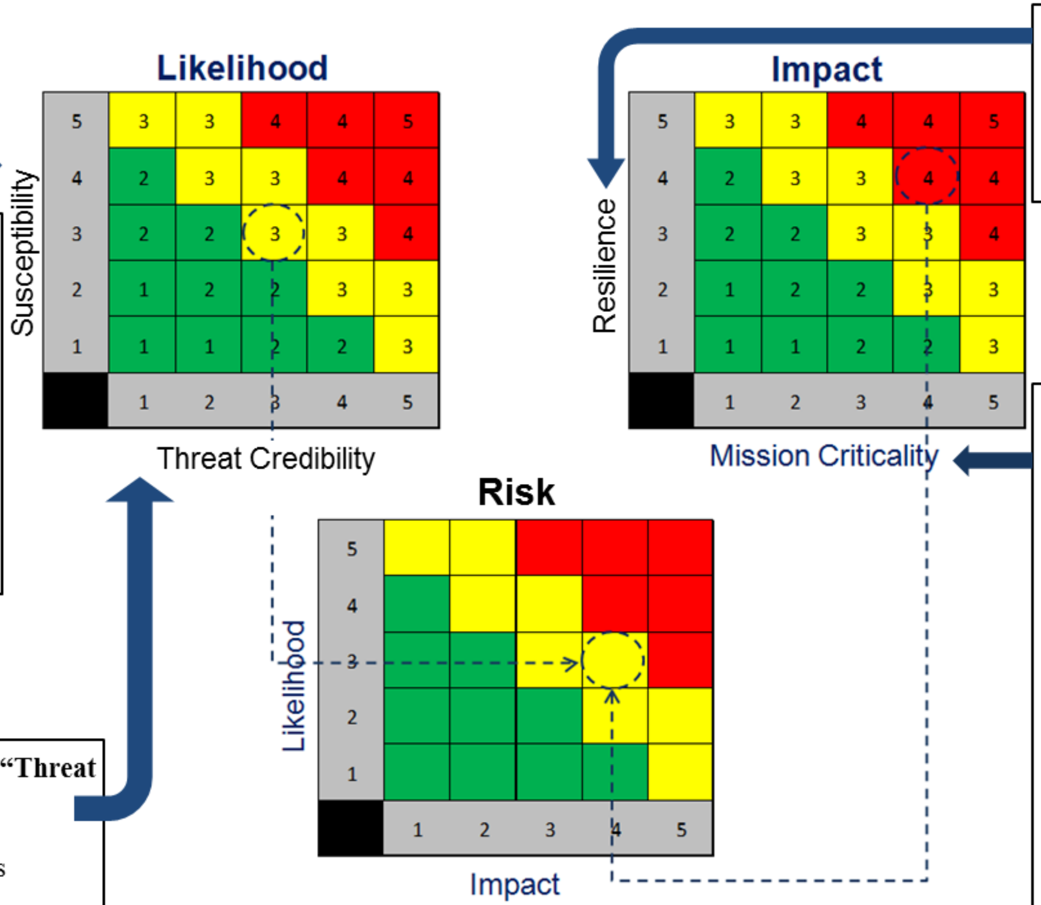
Tier II Actors have some ability to develop their own malicious code and their actions may be characterized by pursuit of specific objectives such as the theft of business or financial data. Low-tier actors can employ some very sophisticated tools and techniques developed and exposed by others.

Tier I practitioners, using malicious code developed by others, are commonly referred to as “script kiddies” and are driven as much by the desire to brag about their success in executing an “attack” as they are to cause specific damage.

Cyber Risk Assessment (CRA) Scoring

Susceptibility

- Availability of Details (*includes protocols/standards / ubiquity of software*)
- Supply Chain Exposure
- Accessibility/Reachability
- Usage Window/Frequency of Use
- Security Controls
- Hygiene



Likelihood

Susceptibility					
5	3	3	4	4	5
4	2	3	3	4	4
3	2	2	3	3	4
2	1	2	2	3	3
1	1	1	2	2	3
	1	2	3	4	5

Threat Credibility

Impact

Resilience					
5	3	3	4	4	5
4	2	3	3	4	4
3	2	2	3	3	4
2	1	2	2	3	3
1	1	1	2	2	3
	1	2	3	4	5

Mission Criticality

Risk

Likelihood					
5	🟨	🟨	🟥	🟥	🟥
4	🟩	🟨	🟨	🟥	🟥
3	🟩	🟩	🟨	🟨	🟥
2	🟩	🟩	🟩	🟨	🟨
1	🟩	🟩	🟩	🟩	🟨
	1	2	3	4	5

Impact

Resilience

- Non-Persistence
- Redundancy (incl. Backup/Restore)
- Heterogeneity
- Distributive Allocation

Mission Criticality

- ***<u>MSN -> Sys -> Comp -> Data/...</u>***
- Necessity/Dependency within the context of Mission Essential Function (MEF)
  - Each for C, I and A assessment of mission system asset (scoped)
- Criticality of MEF within context of Mission (scoped)

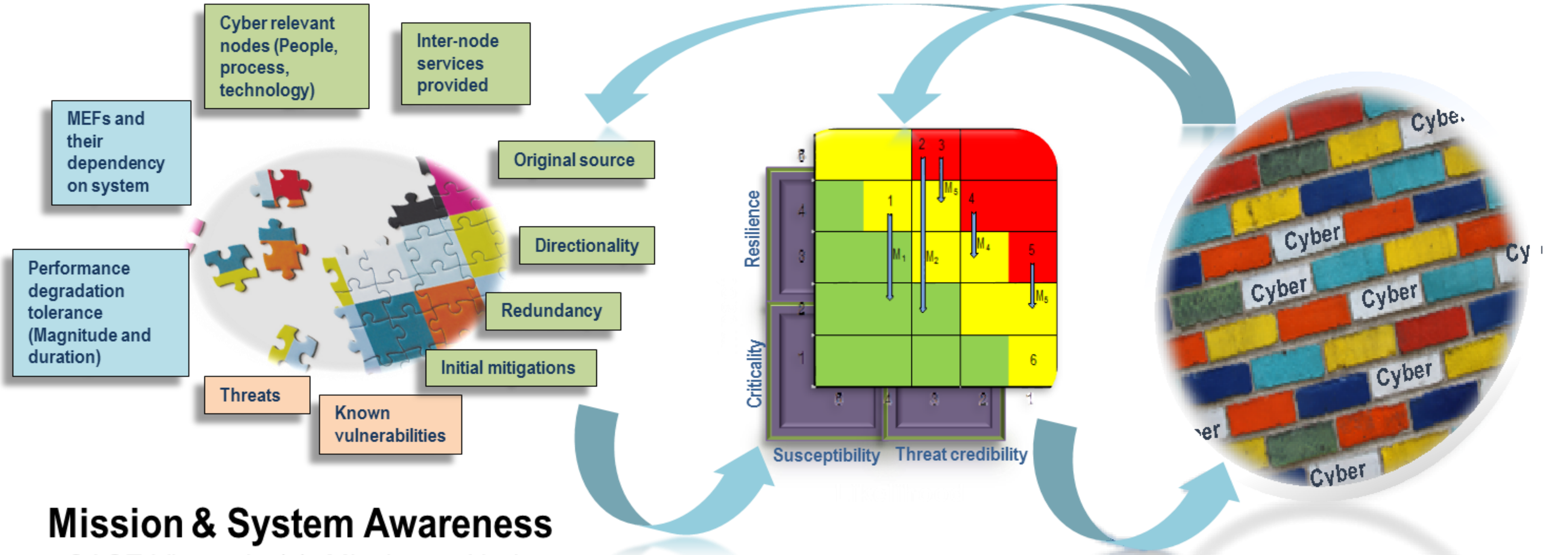
➢ Mission criticality answers the question: "How vital to mission success is the data, information, service being attacked?"

Threat Credibility (formerly "Threat Means")

- Primary
  - Adversary's Capabilities
  - Adversary's Attraction

This last matrix ends in a *Cyber Risk product*

Cyber Risk Management Fundamentals



Cyber relevant nodes (People, process, technology)

Inter-node services provided

MEFs and their dependency on system

Original source

Directionality

Performance degradation tolerance (Magnitude and duration)

Redundancy

Initial mitigations

Threats

Known vulnerabilities

Mission & System Awareness

CASE Viewpoint(s), Mission-to-Node Mapping and Threats/Vulnerability Formulation

Analysis & Assessment

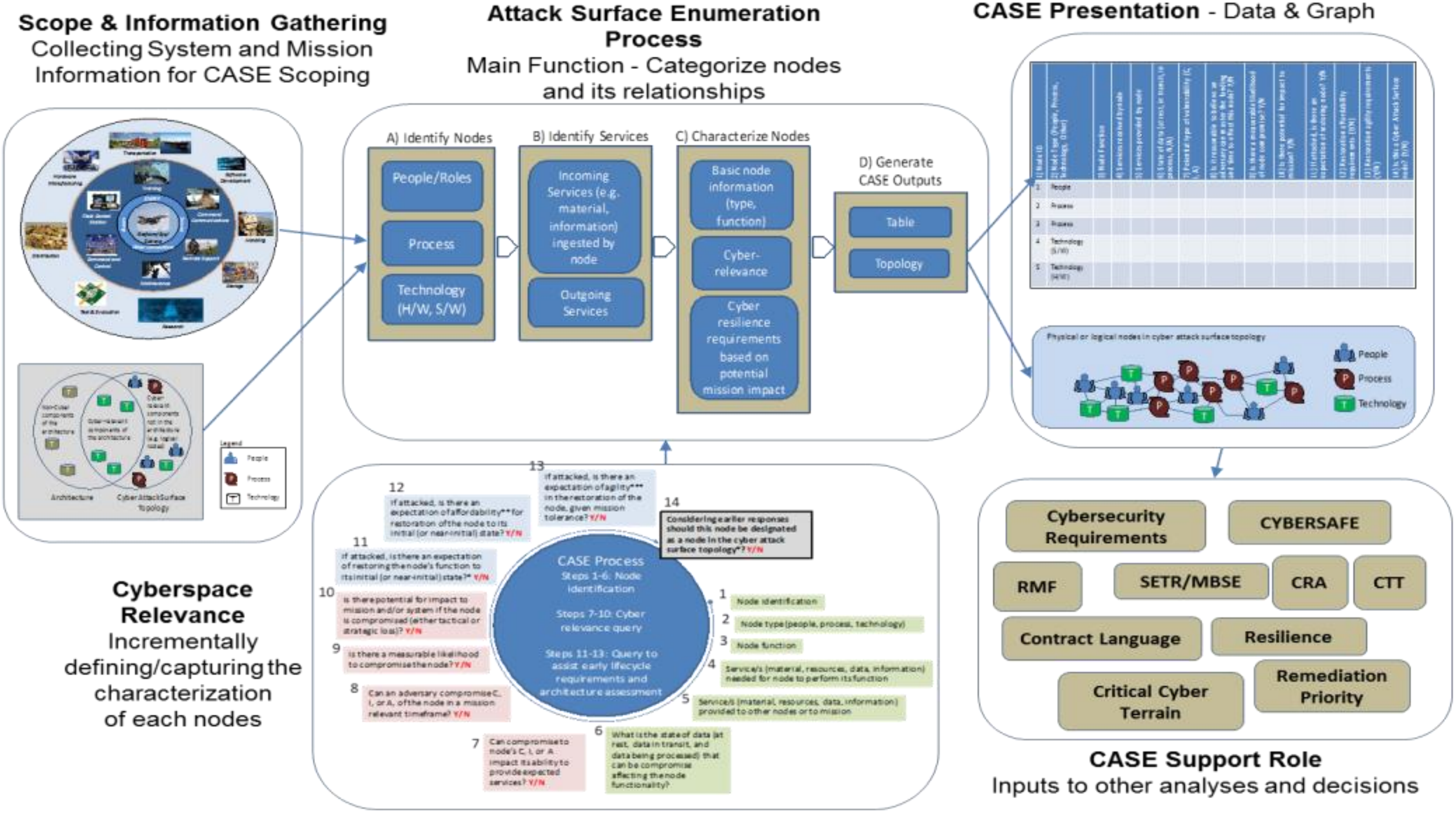
Determining System’s Cyber Risk Posture: Access Point Criticality, Susceptibility, Resilience, and Threat Credibility

Mitigation/Remediation

Mitigation optimization, decision analysis (e.g. ORC) , and implementation (Cyber and non-cyber). Continuous monitoring and reassessments

Cyber Attack Surface Enumeration (CASE)

CASE Framework



Scope & Information Gathering
Collecting System and Mission Information for CASE Scoping

Cyberspace Relevance
Incrementally defining/capturing the characterization of each nodes

Attack Surface Enumeration Process
Main Function - Categorize nodes and its relationships

CASE Process
Steps 1-6: Node identification
Steps 7-10: Cyber relevance query
Steps 11-13: Query to assist early lifecycle requirements and architecture assessment

1 Node identification

2 Node type (people, process, technology)

3 Node function

4 Service/s (material, resources, data, information) needed for node to perform its function

5 Service/s (material, resources, data, information) provided to other nodes or to mission

6 What is the state of data (at rest, data in transit, and data being processed) that can be compromise affecting the node functionality?

7 Can compromise to node's C, I, or A impact its ability to provide expected services? Y/N

8 Can an adversary compromise C, I, or A, of the node in a mission relevant timeframe? Y/N

9 Is there a measurable likelihood to compromise the node? Y/N

10 Is there potential for impact to mission and/or system if the node is compromised (either tactical or strategic loss)? Y/N

11 If attacked, is there an expectation of restoring the node's function to its initial (or near-initial) state?* Y/N

12 If attacked, is there an expectation of affordability** for restoration of the node to its initial (or near-initial) state? Y/N

13 If attacked, is there an expectation of agility*** in the restoration of the node, given mission tolerance? Y/N

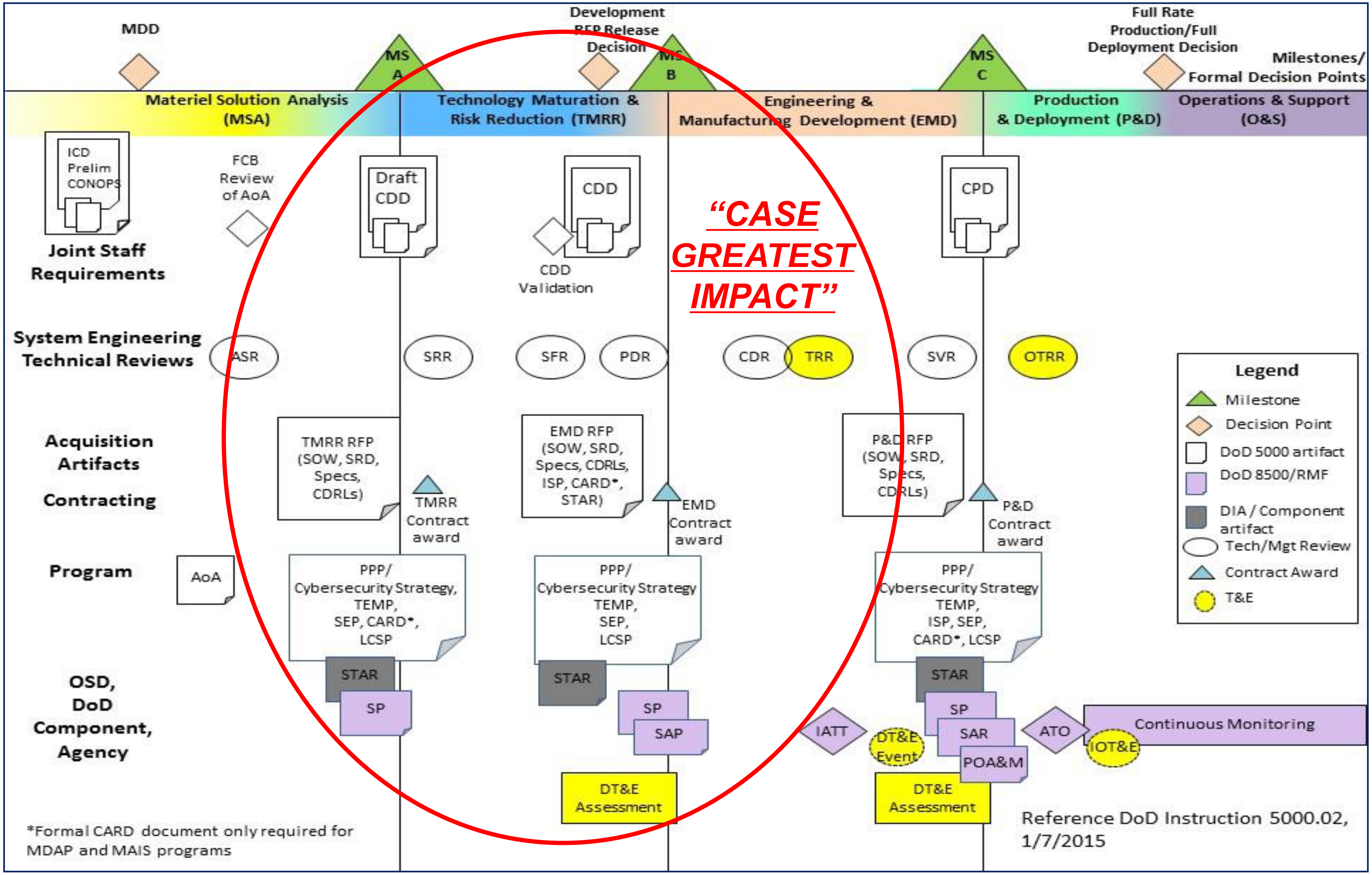
14 Considering earlier responses should this node be designated as a node in the cyber attack surface topology*? Y/N

CASE Presentation - Data & Graph

(1) Node ID	(2) Node Type (People, Process, Technology, Other)	(3) Node Function	(4) Services received by node	(5) Services provided by node	(6) State of data (at rest, in transit, in process, N/A)	(7) Potential type of vulnerability (C, I, A)	(8) [illegible]	(9) [illegible]	(10) [illegible]	(11) [illegible]	(12) [illegible]	(13) [illegible]	(14) Is this a Cyber Attack Surface node? (Y/N)
1	People												
2	Process												
3	Process												
4	Technology (S/W)												
5	Technology (H/W)												

CASE Support Role
Inputs to other analyses and decisions

Cyber Attack Surface Enumeration (CASE)



MDD

MS A

Development RFP Release Decision

MS B

MS C

Full Rate Production/Full Deployment Decision

Milestones/ Formal Decision Points

Materiel Solution Analysis (MSA)

Technology Maturation & Risk Reduction (TMRR)

Engineering & Manufacturing Development (EMD)

Production & Deployment (P&D)

Operations & Support (O&S)

ICD Prelim CONOPS

Joint Staff Requirements

FCB Review of AoA

Draft CDD

CDD

CDD Validation

CPD

“CASE GREATEST IMPACT”

System Engineering Technical Reviews

ASR

SRR

SFR

PDR

CDR

TRR

SVR

OTRR

Acquisition Artifacts

Contracting

TMRR RFP (SOW, SRD, Specs, CDRLs)

TMRR Contract award

EMD RFP (SOW, SRD, Specs, CDRLs, ISP, CARD*, STAR)

EMD Contract award

P&D RFP (SOW, SRD, Specs, CDRLs)

P&D Contract award

Program

AoA

PPP/ Cybersecurity Strategy, TEMP, SEP, CARD*, LCSP

PPP/ Cybersecurity Strategy TEMP, SEP, LCSP

PPP/ Cybersecurity Strategy TEMP, ISP, SEP, CARD*, LCSP

OSD, DoD Component, Agency

STAR

SP

STAR

SP

SAP

DT&E Assessment

IATT

DT&E Event

STAR

SP

SAR

POA&M

DT&E Assessment

ATO

Continuous Monitoring

IOT&E

Legend

Milestone

Decision Point

DoD 5000 artifact

DoD 8500/RMF

DIA / Component artifact

Tech/Mgt Review

Contract Award

T&E

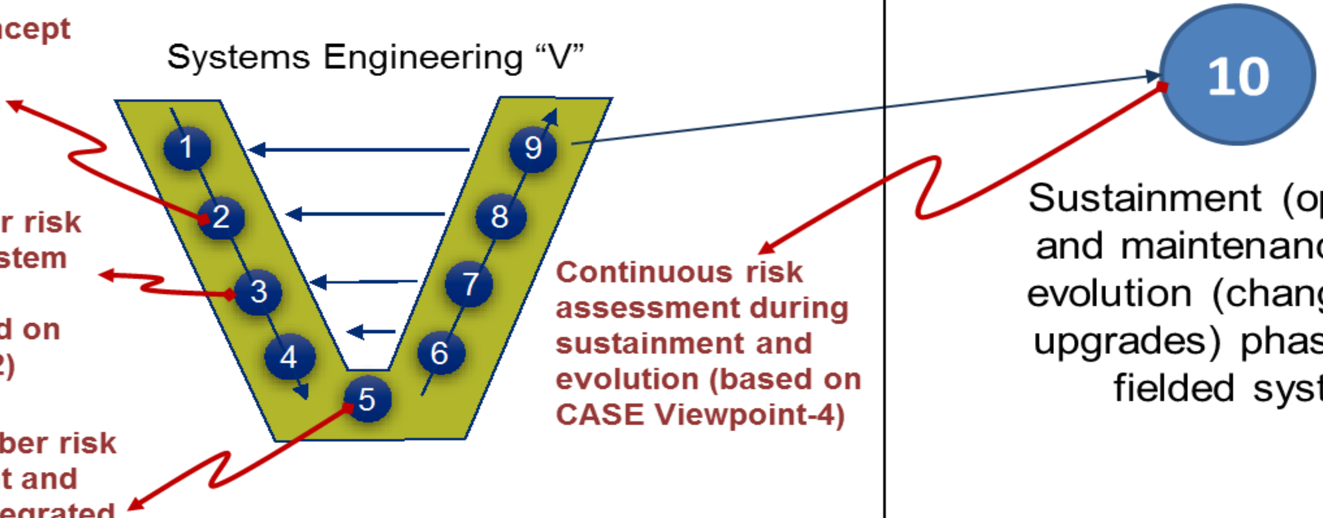
*Formal CARD document only required for MDAP and MAIS programs

Reference DoD Instruction 5000.02, 1/7/2015

Cyber Attack Surface Enumeration (CASE)

A Cyber Resilient Design

Developmental Systems



Early cyber risk assessment at concept level mitigations (based on CASE Viewpoint-1)

Intermediate cyber risk assessment at system architecture level mitigations (based on CASE Viewpoint-2)

Detailed cyber risk assessment and detailed integrated design level mitigations (based on CASE Viewpoint-3)

Continuous risk assessment during sustainment and evolution (based on CASE Viewpoint-4)

Legacy Systems

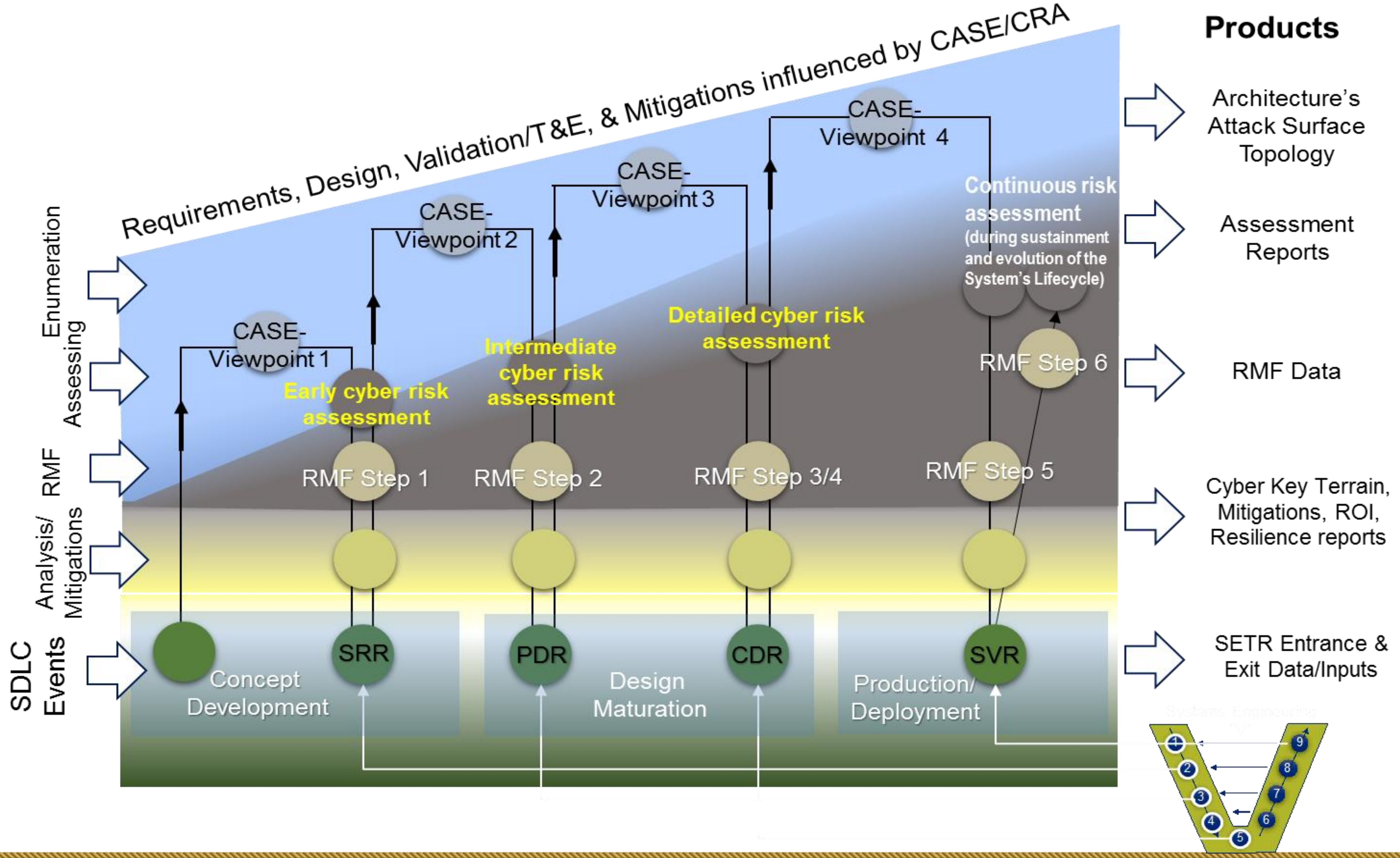
Sustainment (operation and maintenance) and evolution (changes and upgrades) phase of an fielded system

CASE informs cybersecurity and resilience decisions within the design process at each step of the system engineering approach

CASE enables post-design cyber assessment and mitigations

Cyber Attack Surface Enumeration (CASE)

Integrated Risk Management Processes



Requirements, Design, Validation/T&E, & Mitigations influenced by CASE/CRA

Enumeration

Assessing

RMF

Analysis/ Mitigations

SDLC Events

CASE-Viewpoint 1

CASE-Viewpoint 2

CASE-Viewpoint 3

CASE-Viewpoint 4

Early cyber risk assessment

Intermediate cyber risk assessment

Detailed cyber risk assessment

Continuous risk assessment (during sustainment and evolution of the System's Lifecycle)

RMF Step 1

RMF Step 2

RMF Step 3/4

RMF Step 5

RMF Step 6

SRR

PDR

CDR

SVR

Concept Development

Design Maturation

Production/ Deployment

Products

Architecture's Attack Surface Topology

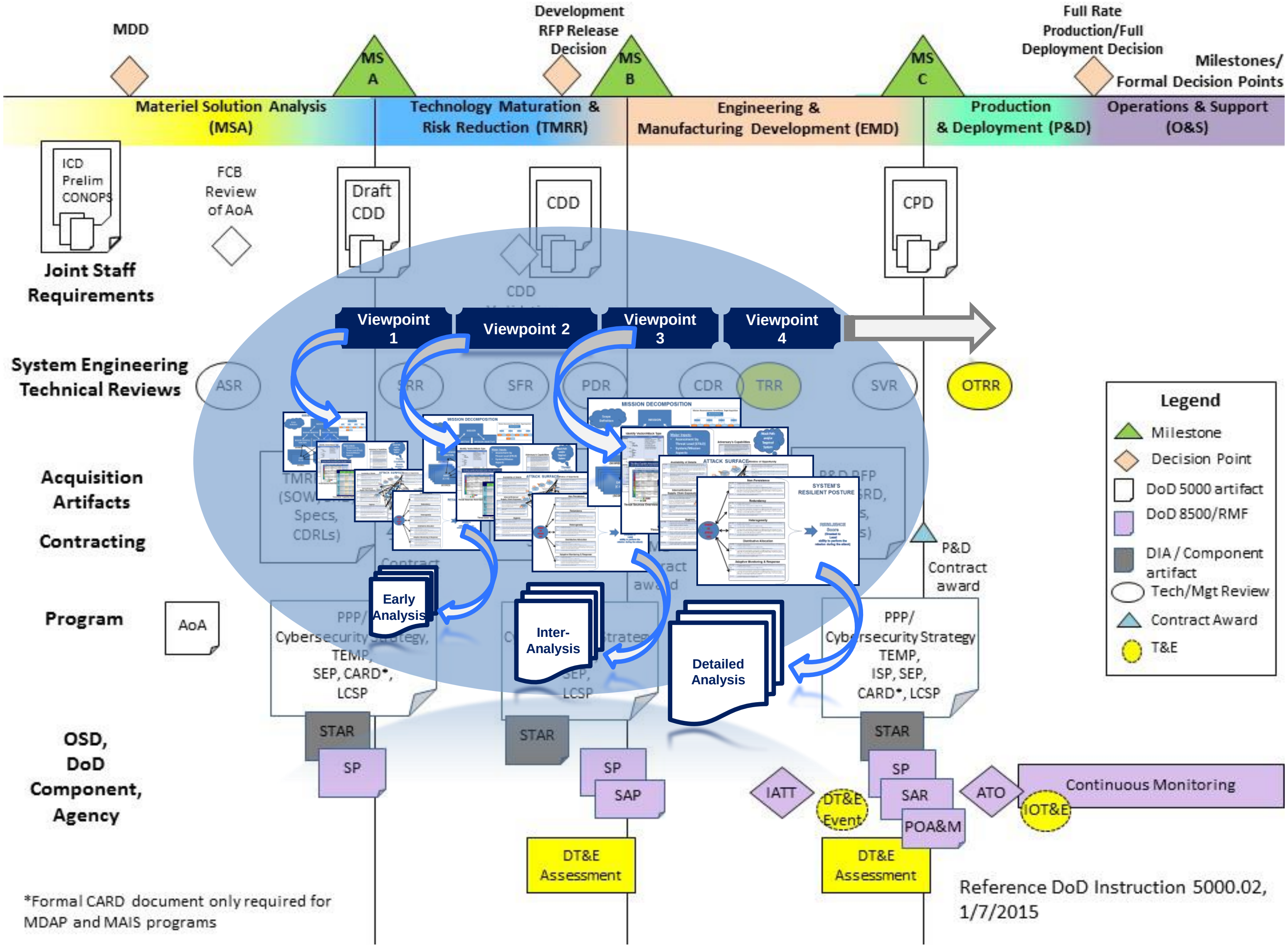
Assessment Reports

RMF Data

Cyber Key Terrain, Mitigations, ROI, Resilience reports

SETR Entrance & Exit Data/Inputs

Cyber Attack Surface Enumeration (CASE)



*Formal CARD document only required for MDAP and MAIS programs

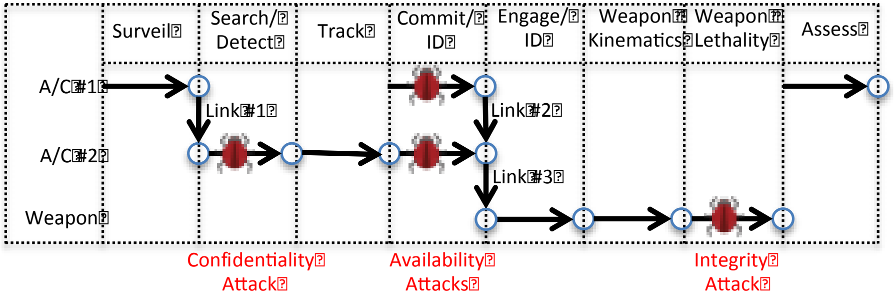
Reference DoD Instruction 5000.02, 1/7/2015

Cyber Risk Assessment to Mission (CRAM)

Kill Chain analyses are currently used/accepted to assess Navy mission thread effectiveness

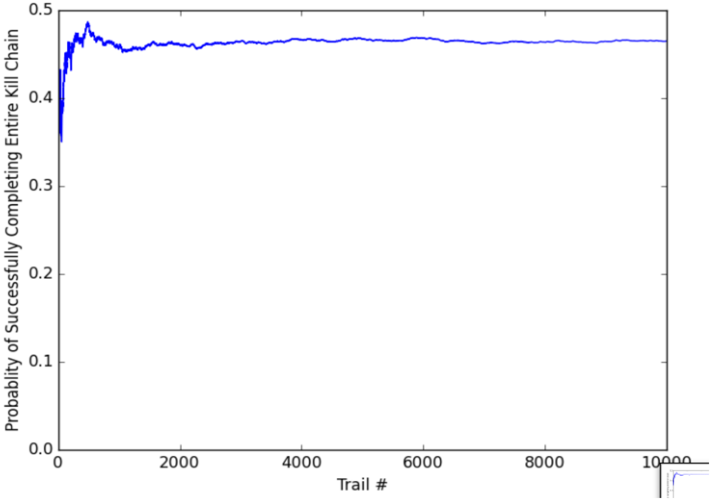
- **Assessed by Subject Matter Experts (SMEs)**
- **Supported by Warfare Analysis Methods**
  - *Deterministic*
  - *Stochastic Markov Chain Monte Carlo (MCMC) method, providing a tool for the warfare analyst to incorporate cyber-attack effects from CRAs to quantify the MOEs and MOPs.*
- **Cyber attacks can be introduced at any point in the kill-chain**
  - *Choice of cyber attacks depends on phase of Warfare (Shaping, Deterring, Seizing Initiative, Dominating, Stabilizing, Enabling Civil Authority)*
- **Probability of a Cyber attack = Likelihood score from a CRA**
  - *Adversarial Capability and Intent*
  - *Warfare System Susceptibility*

Notional Kill-Chain



Ps=10% **Ps=50%** **Ps=30%**

Monte-Carlo Result

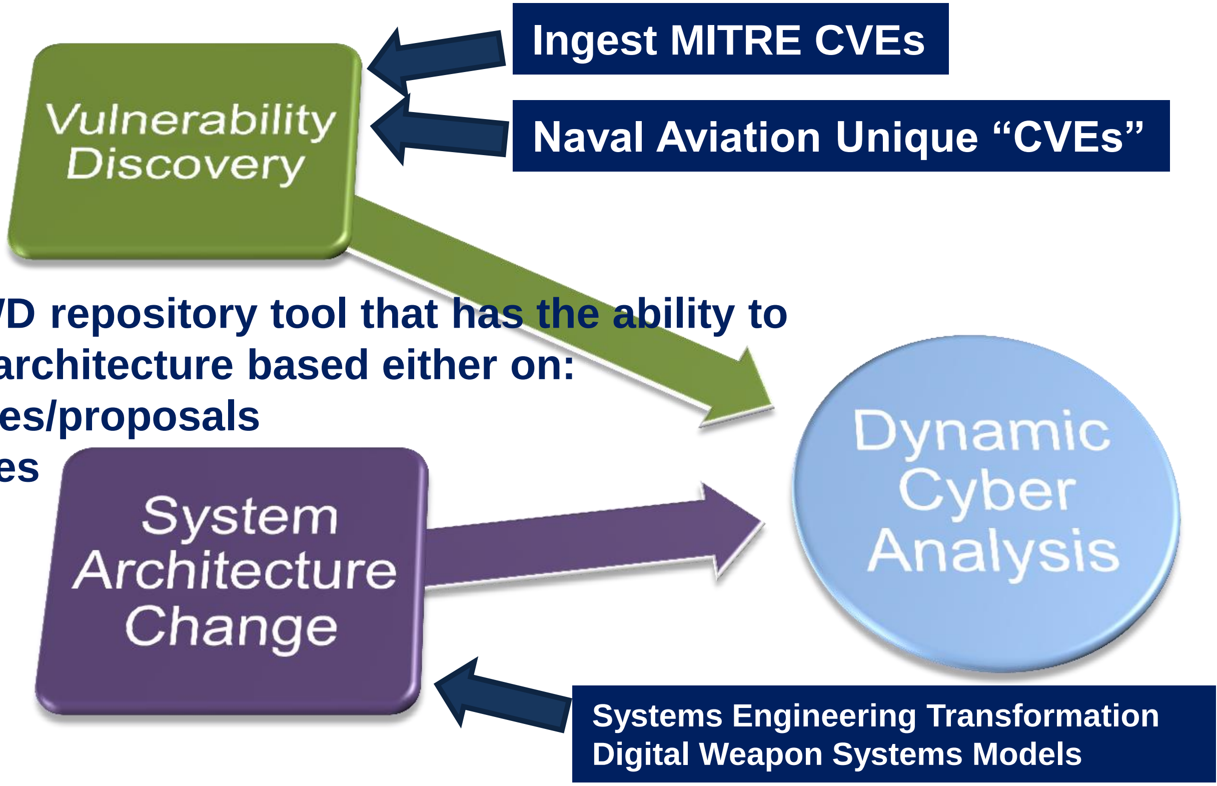


Cyber Risk Assessment Nodal-based GUI (CRANG)

CRANG

VISION

- Create a common NAVAIR/CWD repository tool that has the ability to dynamically assess systems architecture based either on:
  - new configuration changes/proposals
  - newly found vulnerabilities


Ingest MITRE CVEs
Naval Aviation Unique "CVEs"
Vulnerability Discovery
Dynamic Cyber Analysis
System Architecture Change
Systems Engineering Transformation Digital Weapon Systems Models

GOALS

- Easy to use platform for PMA's to deliver system architecture to the CWD
- Provide NAVAIR with same-day analysis of all recorded systems or "systems of systems" in response to newly found New-Day vulnerabilities
- Repository capable of providing immediate vulnerability assessments of configuration changes to software or hardware

Summary

- Adversarial threat-driven Cyber Table Top (CTT) and Cyber Risk Assessment (CRA) methods developed
- CASE developed as a tool for early incorporation into the Systems Engineering and Acquisition processes
- CRAM method to assess risk via kill-chain analysis
- CRANG provides a vulnerability repository for weapon systems

QUESTIONS / DISCUSSION