34th Annual INCOSE international symposium
hybrid event
Dublin, Ireland
July 2 - 6, 2024

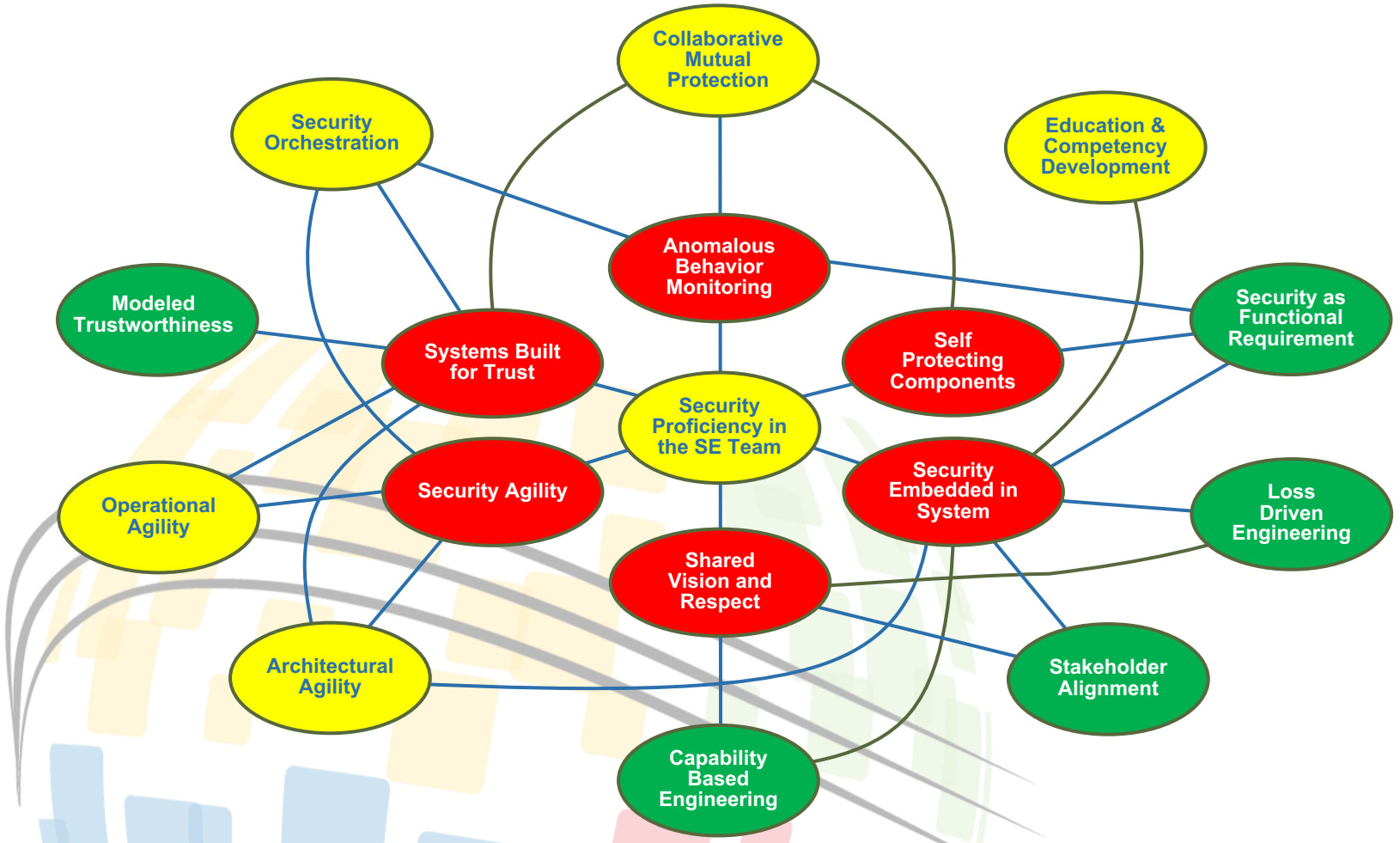
Enabling FuSE Security Objectives by Leveraging Cyber Survivability Methods

Introduction

- The FuSE Roadmap of Foundation Concepts for Security was published in 2021.
  - The paper outlined 6 Objectives and 11 Foundation Concepts that that define the key characteristics for a revised SE approach to Systems Security.
  - 5 of the 11 Foundation Concepts specifically address Systems Engineering processes.

- This paper studies several cybersecurity assessment and process guidebooks (from the T&E community) to identify processes and activities that could be used to form the foundation of a SE Security Process guidebook.

FuSE System Security Objectives and Foundation Concepts



Foundation Concepts Related to SE Processes

Foundation Concepts Related to Design, Academics, and Organization

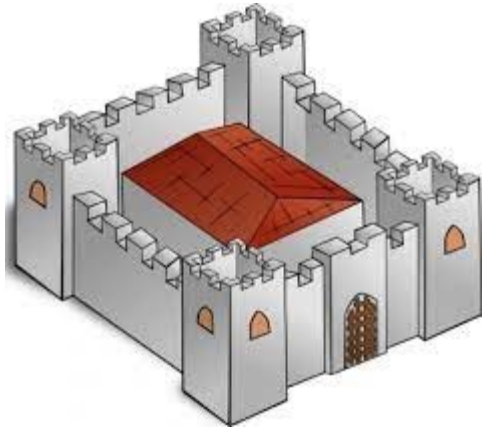
Fuse Security Objectives

INCOSE IS21 paper: Security in the Future of Systems Engineering (FuSE) a Roadmap of Foundation Concepts

Why is the FuSE Security Initiative Important?

- For reasons beyond the scope of this presentation, the process for assuring system security has become a regulatory activity, delegated to Network IT Security specialists with the primary objective of receiving an “authority to operate (ATO).”
- Systems are being designed and built first, then evaluated for their weaknesses and vulnerabilities.

Let’s build our system!



Now, how do we protect this mobile information processing system?

FuSE Security – a Different Way of Thinking

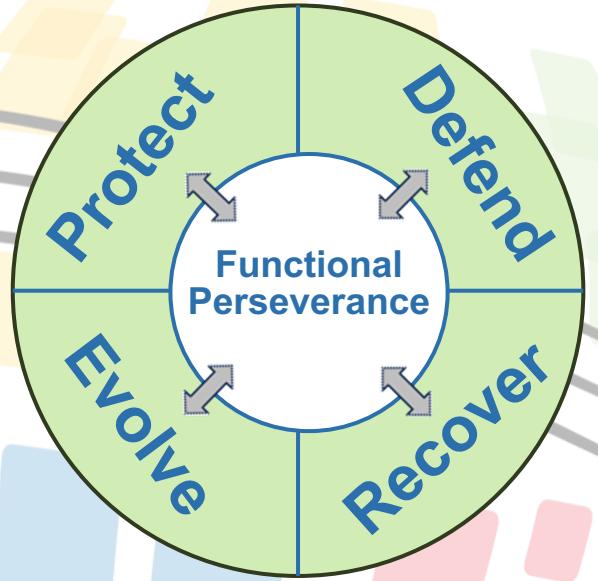
- A key objective of the FuSE Security Foundations Roadmap is to recognize that security (the ability to function in a hostile predatory environment) is part of the mission.

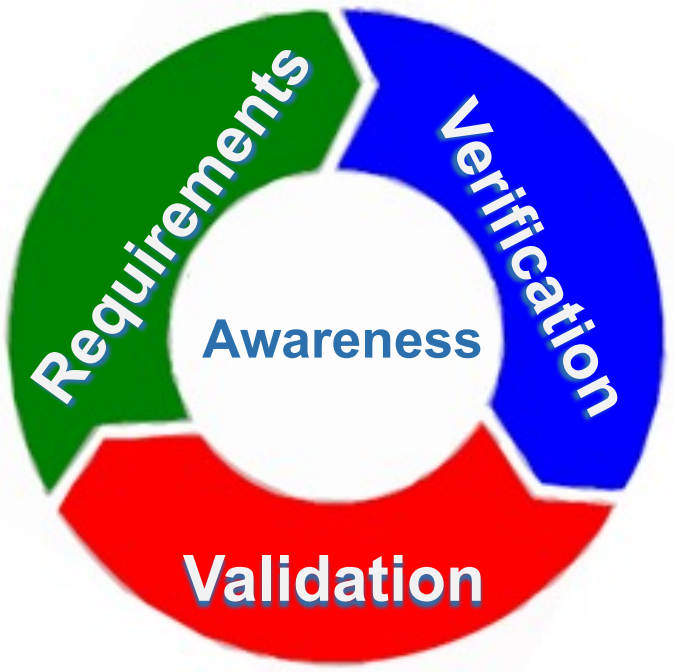
- Security capabilities and functions must be integrated into the architecture from the beginning, not designed as a separate subsystem or a “fence”.

- System security should be an integral part of the systems engineering lifecycle, the same as any other specialty engineering discipline!

FuSE Security – A New Perspective

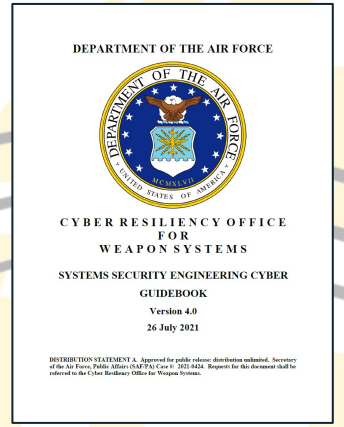
- **System Security WG Mission** - Make security as foundational to systems engineering as performance and safety.
- **Goal** – Functional perseverance in a hostile predatory environment.
- **Strategy** – Protect, Defend, Recover, Evolve



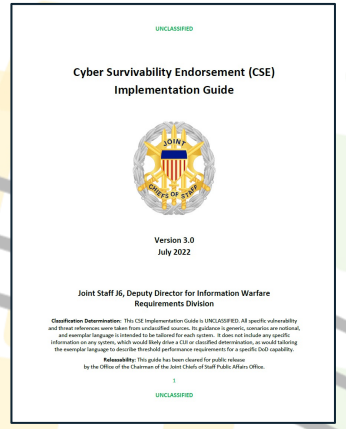


Where do we start?

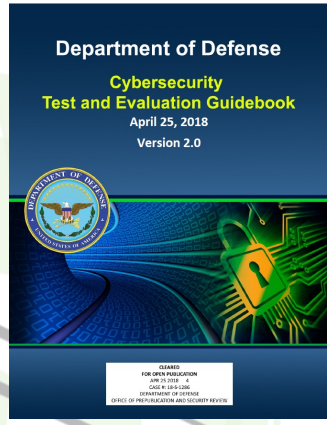
- Section 3.1.12 of the INCOSE SE Handbook describes the importance of integrated System Security Engineering into Systems Engineering, however, it provides almost no guidance on what that means or how to accomplish it!
- This paper reviews 6 specific Cyber T&E Guidebooks that address conduct of cyber security engineering, cyber risk assessment and cyber T&E to identify processes and methods that can be adopted or adapted as part of an INCOSE FuSE Systems Security work product.



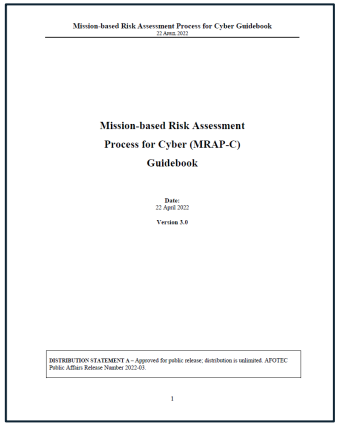
Systems Security Engineering (SSE) Cyber Guidebook



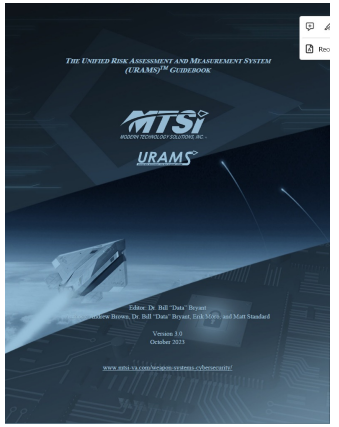
Cyber Survivability Endorsement (CSE) Implementation Guide



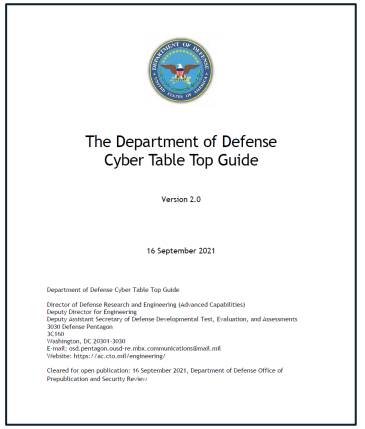
Cybersecurity Test and Evaluation Guidebook 2.0



Mission-based Risk Assessment Process for Cyber (MRAP-C) Guidebook



Unified Risk Assessment and Measurement System (URAMS) Guidebook

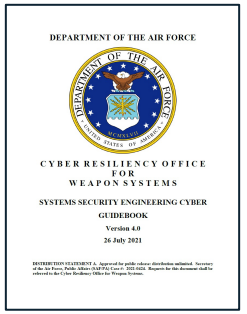


Cyber Table Top Guidebook

Cyber Security is not a “DoD only” problem!

- While all 6 guidelines are from US DoD, FuSE Security applies to all countries, all industries, both government and commercial.
- These US DoD documents were selected because they were:
  - The most complete.
  - The most mature.
  - The most available.
- The task will be to derive industry agnostic processes that can be equally applied by both commercial and government/defense projects.

Systems Security Engineering (SSE) Cyber Guidebook


DEPARTMENT OF THE AIR FORCE

CYBER RESILIENCY OFFICE FOR WEAPON SYSTEMS

SYSTEMS SECURITY ENGINEERING CYBER GUIDEBOOK

Version 4.0

26 July 2021

- Introduces the role of the SSE, responsible for ensuring that cyber survivability engineering processes are performed throughout the engineering lifecycle.
- It describe the cyber security specific activities that need to be performed in the context of standard SE Technical Processes (Mission Analysis, Requirements Management, Architecture Development, etc.)
- The SSE is not a cyber security specialist. It is a Systems Engineering role.

Pre-Acquisition

- Review and understand the customer and stakeholder requirements, capabilities, and desired effects
- Identify the Mission Environment(s)
- Conduct Functional Thread and Criticality Analysis
- Conduct Threat and Vulnerability Analysis

Acquisition

- Develop initial system security requirements
- Ensure requirements for cyber survivability are documented in applicable system specifications
- Ensure requirements for cyber survivability analysis and associated deliverables are included in the Statement of Work

Program Execution

- Conduct SSE through SE (decomposing and allocating system cyber survivability requirements to lower-level subsystems)
- Ensure program reviews & technical reviews include design compliance with cyber survivability requirements
- Ensure program protection activities and system design are on track

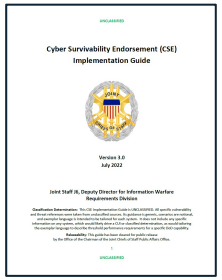
Capability Based Engineering

Stakeholder Alignment

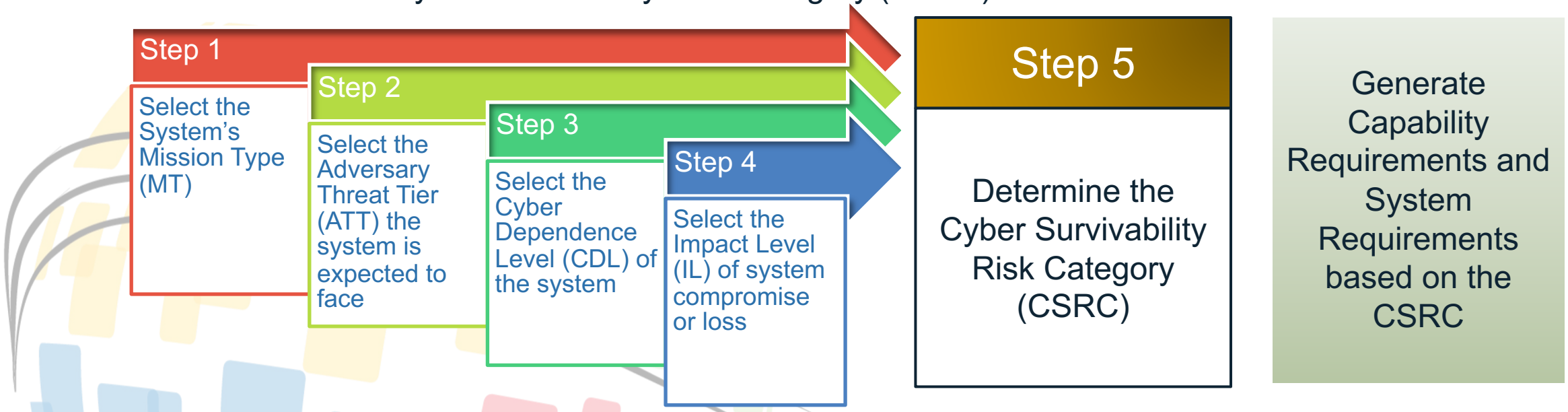
Loss Driven Engineering

Security as Functional Requirement

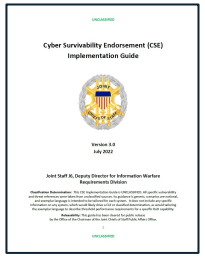
Cyber Survivability Endorsement (CSE) Implementation Guide



- A risk-management framework to develop mission impact-focused cyber survivability requirements.
- It is a five-step process that enables programs to articulate the cybersecurity and cyber resiliency threshold performance requirements for ensuring a system's minimum viable capabilities can be achieved at an operationally acceptable mission assurance level.
- Defines a set of Cyber Survivability Attributes (CSA) with associated security requirements based on the Determine the Cyber Survivability Risk Category (CSRC).

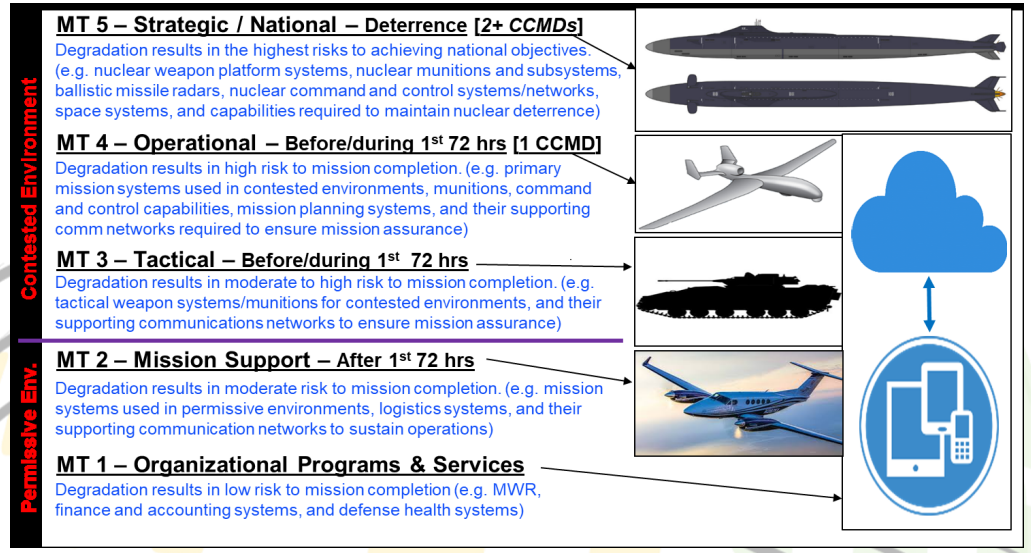


CSE Implementation Guide



- In addition to a description of the 5-step process, the CSEIG:
  - Provides guidance for the development of cyber survivability capability requirements and systems requirements, with examples.
  - Provides a classification/taxonomy and definitions for key cyber survivability characteristics.

Mission Type



Adversary Threat Tier

ATT 5 – Extreme: (e.g., Russia SVR, APT-29). Uses a range of initial exploitation techniques that vary in sophistication, coupled with 'stealthy' intrusion tradecraft to cause denial, degradation, deception, disruption, and destruction of mission capabilities. Uses custom tools, compromised accounts, and system misconfiguration to blend in with normal/unmonitored traffic to move undetected in victim networks. Demonstrated capability to target cloud resources and supply chain (e.g., SolarWinds).

ATT 4 – Advanced: (e.g., Russia GRU, APT-28; China APT-41). Conducts complex, long-term cyber attack operations combining multiple intelligence sources to obtain access to high-value networks. After gaining access, combines well known TTPs to move laterally, evade defenses and collect additional info. Uses tools to conduct widespread, distributed and anonymized 'brute force' access to cloud services. Develops detailed target technical knowledge for more damaging attacks.

ATT 3 – Moderate: Sophisticated, persistent, and well-resourced adversaries at nation-state level. Capable of advanced cyber tradecraft to use publicly available tools, develop/use customized malware, and acquire access to some ATT-4/ATT-5 tools to stealthily implant malware/vulnerabilities, conduct wide-ranging intelligence collection operations, gain access to more isolated networks, and in some cases, create limited effects against defense critical infrastructure networks.

ATT 2 – Limited: Capable of limited advanced cyber tradecraft using publicly available and customized tools to exploit known and unknown vulnerabilities. Able to identify -- and target-for espionage or attack -- easily accessible unencrypted networks running common operating systems using publicly available tools. Possesses some limited strategic planning.

ATT 1 – Nascent: Little-to-no organized cyber capabilities, with no knowledge of a network's underlying systems beyond publicly connected open-source information. Willing to exploit known vulnerabilities.

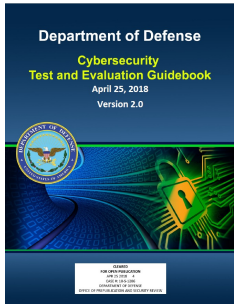
Capability Based Engineering

Stakeholder Alignment

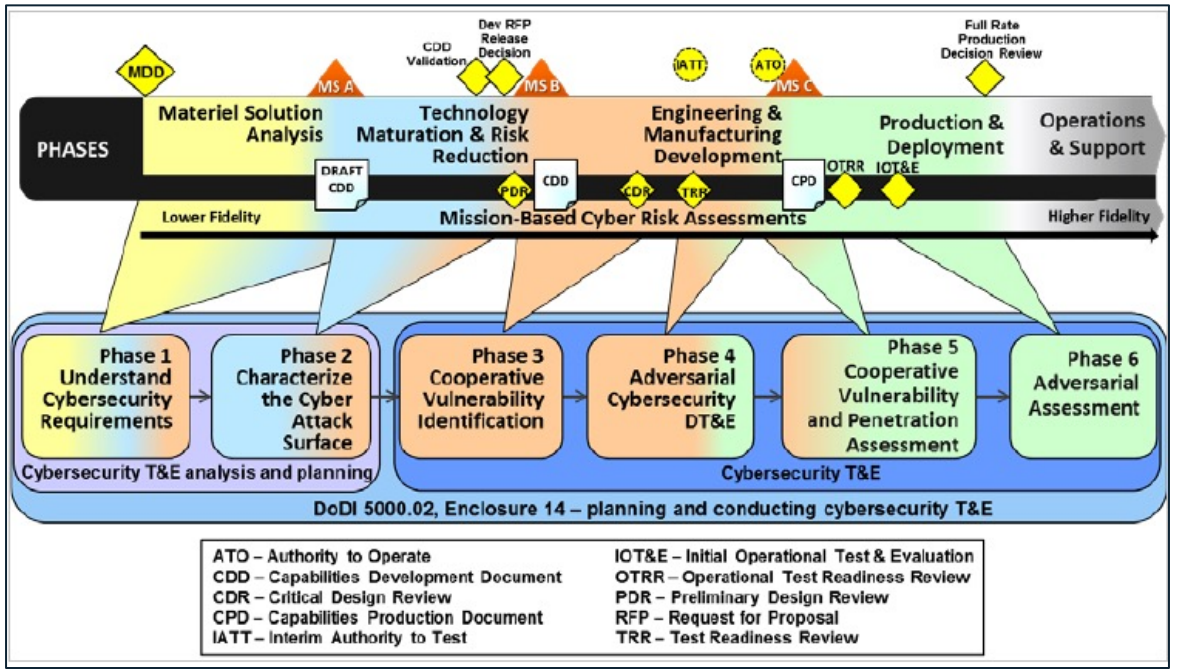
Loss Driven Engineering

Security as Functional Requirement

Cybersecurity Test and Evaluation Guidebook 2.0



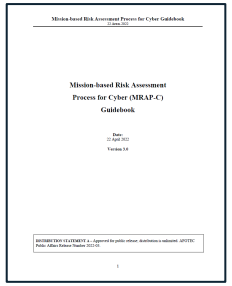
- The Cybersecurity T&E Guidebook describes the 6-Phase Cybersecurity T&E process.
- The primary objective of the process is to ensure that major cyber vulnerabilities have been addressed in the system design, prior to entering cyber operational test and evaluation.
- Phases 1, 2 and 3 describe the system engineering activities, artifacts and data required to plan and execute a Cyber Security T&E exercise.
- It also describes the collaborations that should be occurring between the SE and T&E teams.



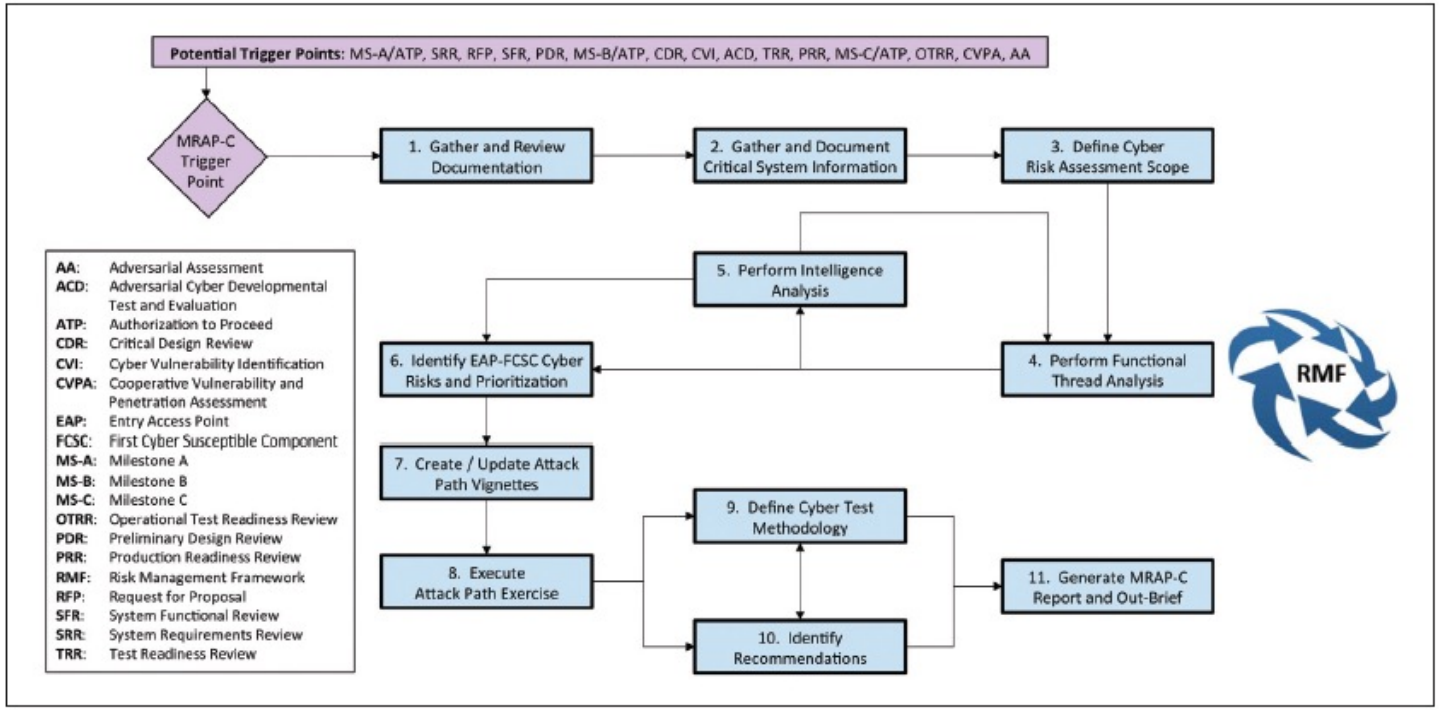
Stakeholder Alignment

Security as Functional Requirement

Mission-based Risk Assessment Process for Cyber (MRAP-C) Guidebook


Mission-based Risk Assessment Process for Cyber (MRAP-C) Guidebook

- Developed by the USAF based on analysis of 20 different mission based cyber risk assessment (MBCRA) methodologies, taking best practices from each.
- MRAP-C provides early risk analysis to inform cyber requirements and design considerations as well as to generate a cyber-evaluation methodology to support test community strategies.
- Performed multiple times throughout the program (during concept/CONOPS development, logical architecture development, and detailed design.)



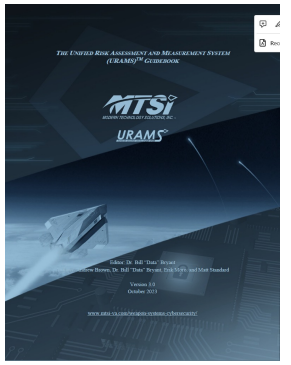
Capability Based Engineering

Stakeholder Alignment

Loss Driven Engineering

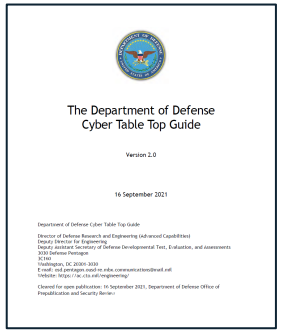
Security as Functional Requirement

Unified Risk Assessment and Measurement System (URAMS) Guidebook



- URAMS is an MBCRA process based on Systems Theoretic Process Analysis for Security (STPA-Sec).
- Its scope is broader than MRAP-C and not only performs a risk assessment, but also includes:
  - A more rigorous scoring methodology.
  - An approach for assessing mission failure at the mission level based on the risk probabilities of individual events.
  - An approach for using the results for program decision-making.
  - An approach for model based implementation in SysML.
- Introduces Structured Assurance Cases as means to evaluate the achievement of a security objective.
- 4-Step Process:
  - **Step 1: Problem Framing** - Define the system purpose and goal, identify losses, identify sys-tem-level hazards, and identify system-level security constraints.
  - **Step 2: Model the Control Structure** – Create the control structure relationship, assign control actions based on responsibilities, and define feedback.
  - **Step 3: Identify Hazardous Control Actions and Constraints** – Identify hazardous control ac-tions, and define controller constraints.
  - **Step 4: Identify Risk Scenarios** – Use hazardous control actions to develop loss scenarios, use hazardous control actions (HCA) to develop loss scenarios, and identify risk scenarios.

Cyber Table Top (CTT) Guidebook


The Department of Defense
Cyber Table Top Guide

Version 2.0

16 September 2021

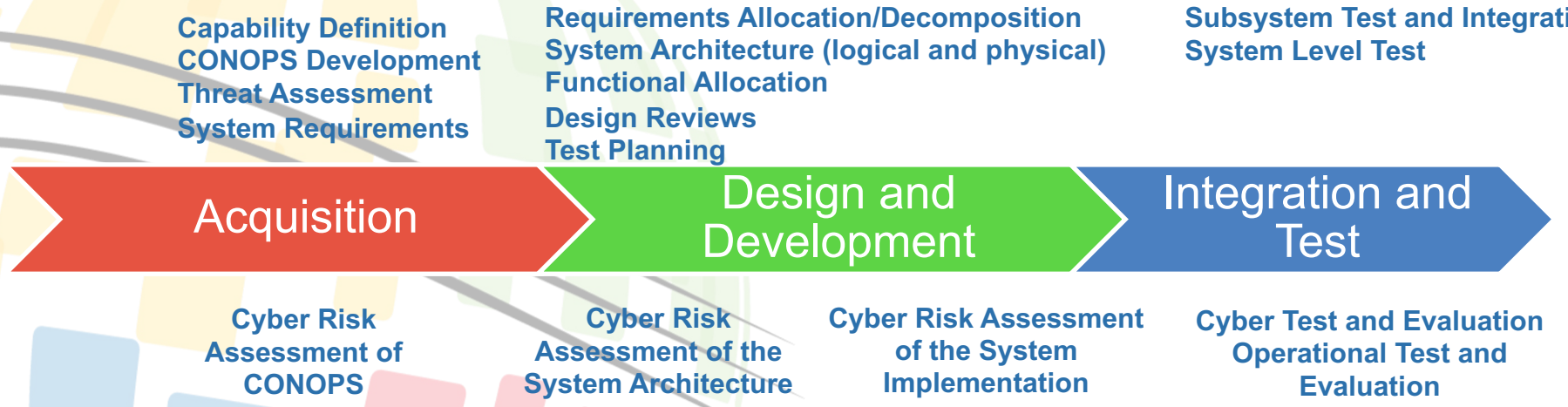
- A 4-step assessment process executed as a war game.
- It involves operational users, system developers and cyber warfare experts as the opposing force (OPFOR).
  - The operational team describes what the users and the system will do in each phase of the mission.
  - The cyber warfare experts in the OPFOR team identify where they could attack.
- The output of the exercise is a “Cyber Security” Failure Modes and Effects Analysis (Cyber-FMEA).
- As with other MBCRA processes, the CTT describes the inputs that should be provided by systems engineering.

Modeled Trustworthiness – The Fifth Element!

- While this Foundation Concept was not specially supported by any of the reviewed T&E guidebooks, it will be an integral part of any resulting SE Security Process.
- The intent of this Foundation Concept is to prove a level of system security through evidence-based assurance.
- It will be enabled through model based systems engineering (MBSE):
  - The SE artifacts and data required by T&E should come from models (conceptual, logical and physical architectures.)
  - The risks and vulnerabilities identified by cyber security assessments should be included in the architecture models with traceability to associated security mitigations.
- Additional profile extensions or new viewpoints in the Unified Architecture Framework (UAF) may be required to fully implement this Foundation Concept.

What can we take away from the Cyber T&E Guidebooks?

- Each guidebook process:
  - Begins early in the system lifecycle during concept development.
  - Emphasizes understanding the mission, the threat and which systems, functions and information are mission critical.
  - Conducts Mission Based Cyber Risk Assessments during each major lifecycle phase.
  - Describes artifacts and design information needed from Systems Engineering.
  - Includes process descriptions and guidance to perform many of the cyber risk assessment activities.



What can we take away from the Cyber T&E Guidebooks?

SSE Cyber Guidebook	•Defines security specific SE roles and responsibilities as part of the overall SE lifecycle.
CSE Implementation Guide	•Taxonomies and frameworks can help the non-cyber specialist describe and communicate characteristics of the mission, critical assets and the threat.
MRAP-C Guidebook	•Describes a structured mission-based risk assessment process that begins early in the project lifecycle. •Provided detailed guidance/instruction for each process step.
URAMS Guidebook	•Applies new methodologies (STPA-SEC, Assurance Cases) •Includes guidance for MBSE implementation. •Provides a mathematical approach for calculating mission risk.
CTT Guidebook	•Describes a wargame based approach that results in a “Cyber FMEA.” •Shows the importance and value of all stakeholders in the assessment process.

We may not agree with the exact content, but the overall approach and the types of guidance provide a starting framework for an INCOSE Security Engineering Guidebook.

Challenges and Opportunities

- **Challenge #1:** Security threats evolve more quickly than most other threats.
  - An effective systems security process must include a process that maintains awareness of the security threat over the system lifecycle and provides a system security capability that can evolve with the changing threat.

- **Challenge #2:** If system security is not a requirement in the contract/systems specification, addressing them in the design may be considered out of scope.
  - There is an opportunity for systems engineering to provide comments and feedback during requests for information (RFI) or in response to draft RFPs or new commercial product kickoffs.

Challenges and Opportunities

- **Challenge #3:** The security threat can attack through the supply chain, through maintenance operations, during training and other non-operational postures.
  - A comprehensive systems security technical process will need to address the entire system lifecycle from concept development through sustainment.

- **Challenge #4:** The intent of Modeling Trust is to prove a level of system security through evidence-based assurance.
  - Model-based systems engineering (MBSE) improves rigor and completeness in traceability from requirements through implementation and test using the models as the authoritative source of truth.

Summary and Conclusions

- **We analyzed six guidebooks for performing security engineering and found that all six included processes, methods and activities that closely align to FuSE Security objectives and foundation concepts including:**
  - Developing security capability and system requirements
  - Beginning the system risk assessment early in the program during CONOPS development at the operational level and continuing through logical architecture development and implementation.
  - Conduct of mission analysis and identification of critical systems, functions and information.
  - The need for stakeholder alignment between program management, systems engineering and operational test and evaluation.

- **We can no longer design systems and then ask if they are vulnerable.**
  - We must begin by recognizing the mission-critical functions and assets that must be protected and design solutions to prevent, mitigate, recover, and adapt.
  - Attainment of the ATO is not the objective. The requirement should be to produce systems that can operate and survive in a hostile environment.

Secure-by-design approaches typically describe a shift in focus from finding and patching vulnerabilities to eliminating the design flaws in the software architecture that enable those vulnerabilities.

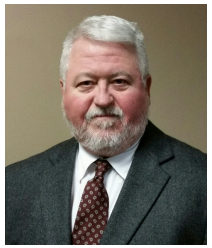
Summary and Conclusions

- **Systems engineering must make system security as "*foundational a perspective in systems design as system performance and safety are today.*"**
  - That means including security requirements in the systems specifications, reviewing design compliance during design reviews, and developing statements of work that require contract deliverables that provide the analysis of the security functions and their effectiveness.

- **Achieving cyber survivability is broader than systems engineering and requires focus and collaboration between acquisition program offices, system design teams, and cyber OT&E organizations.**

- **The complexity of the problem will require the rigor and capabilities of advanced modeling tools and modeling languages to provide the necessary traceability for evidence-based assurance and to support the evolution and adaption of security solutions as the threat evolves.**

About the Authors



Barry Papke is the MBSE Special Project Lead for CATIA Magic. He has thirty-five years of systems engineering and operations analysis experience in the aerospace and defense industry across the entire systems engineering lifecycle from concept development through integration, test and post-delivery support. Throughout his career, he has been actively involved in application of model-based methods including requirements management, enterprise architecture, cost estimation, system design, and operations analysis. He is a member of the INCOSE Agile and Security Working Groups and the MBSE Initiative.

Ron Kratzke has over 30 years of experience in complex systems management and systems engineering. His early career was as a U.S. Navy Surface Warfare officer specializing in the operation, maintenance, and management of Navy nuclear power plants and shipboard combat systems. Following his navy career, Mr. Kratzke provided system engineering design support on advanced systems for a number of government organizations including: the Department of Defense, Department of Homeland Security, Defense Advanced Research Projects Agency, Defense Threat Reduction Agency, and the Joint Program Executive Office for Chemical and Biological Defense. He is currently managing the systems engineering team in North America for Dassault Systems.

Martin (Trae) Span III is currently a PhD Candidate in Systems Engineering at Colorado State University. He is also commissioned as a Major in the United States Air Force (USAF). He has served the USAF as a Developmental Test Engineer responsible for planning and executing complex weapon system test and evaluation. Additionally, he has served as Deputy Director for the US Air Force Academy systems engineering program teaching multiple courses in systems engineering and project management. He serves as a developmental engineer and holds the Department of Defense certifications in systems engineering, science and technology management, test and evaluation, and program management. His PhD work is focused on cyber-security requirements elicitation for complex cyber-physical systems

Nataliya (Natasha) Shevchenko. Nataliya Shevchenko is a senior member of the technical staff within the CERT Division of the Carnegie Mellon University Software Engineering Institute (CMU SEI). She specializes in systems engineering, model-based system engineering (MBSE), and threat modeling methods. She has a breadth of experience across the software development lifecycle for more than 20 years. Prior to joining CMU SEI, Shevchenko worked in the teleconferencing, freight and rail, and financial services critical infrastructures. She holds MS degrees in Software Engineering from Carnegie Mellon University and both BS/MS degrees in Mathematics from Donetsk State University in Ukraine.

34th Annual INCOSE international symposium

hybrid event

Dublin, Ireland
July 2 - 6, 2024

www.incose.org/symp2024
#INCOSEIS