SERC RESEARCH REVIEW 2023 | NOVEMBER 15, 2023

Measuring Operational Resilience Pilot

WRT-1072

Sarah Standard
Cybersecurity/Interoperability Technical Director

PI: Peter Beling

NATIONAL SECURITY INSTITUTE
VIRGINIA TECH

Distribution A - Cleared for Public Release by the Defense Office of Prepublication and Security Review, Case 24-T-0180, 27 October, 2023

Contents

- Prior Work Summary
  - Resilience Definition
  - FOREST
  - SCRE Meta-Model
  - CRRM
- Results
  - Project Goals
  - CRRM Methodology via MBSE
  - GFI
    - MBSE-based Overview
    - MBSE Recommendation - Realization of Operational Use Cases
  - Adversity Chain
  - Measuring Resilience via Adversity Chain
    - Simulation Concepts

Distribution A - Cleared for Public Release by the Defense Office of Prepublication and Security Review, Case 24-T-0180, 27 October, 2023

SERC Research Team

Virginia Tech

- Peter Beling
- Tim Sherburne
- Scott Lucero

Stevens Institute of Technology

- Tom McDermott
- Megan Clifford

<u>Related Prior SERC Projects</u>

- **WRT-1022:** Measurable Requirements for Operational Resilience
- **WRT-1033:** Transitioning Mission Aware Concepts and Methods to Evaluate Cost/Risk Decisions for Security
- **ART-004:** Concept of Operations (CONOPS) Exploiting Cyber Vulnerabilities of Oil and Gas Pipelines Building the Systems Assurance Framework
- **RT-191:** Risk-Based Approach to Cyber Vulnerability Assessment
- **RT-172:** Security Engineering
- **RT-151:** Security Engineering

Distribution A - Cleared for Public Release by the Defense Office of Prepublication and Security Review, Case 24-T-0180, 27 October, 2023

Prior Work Summary

Distribution A - Cleared for Public Release by the Defense Office of Prepublication and Security Review, Case 24-T-0180, 27 October, 2023

Resilience

Challenge: What to Measure?

Ability to resist..

Ability to absorb…

Ability to recover from or adapt to…

…adversity that may cause harm, destruction, or loss of ability to perform required capability during operation.

This means: testing must intentionally introduce adversity that may cause harm, destruction, or loss of ability to perform mission-related functions during operation and measure the system's attributes, performance, and resulting effects.

Definitions (for this discussion)

Resilience: the ability of a system to provide required capability despite the influence of adversity (source: DoD Director, System Security Engineering)

Adversity: the events and conditions that can influence the system's behavior and outcomes (source: DoD Director, System Security Engineering)

Operational Resilience: the ability of systems to **resist**, **absorb**, and **recover from** or **adapt to** an adverse occurrence during operation that may cause harm, destruction, or loss of ability to perform mission-related functions (source DoD Instruction 8500.01)

Distribution A - Cleared for Public Release by the Defense Office of Prepublication and Security Review, Case 24-T-0180, 27 October, 2023

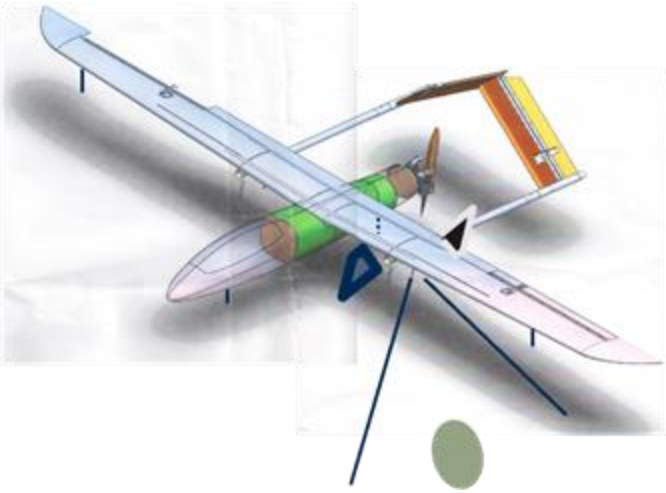
Toward Resilience

- To achieve resilience, use the same System Engineering processes as when considering Safety, Reliability and Survivability
- Design in Resilience
- Develop measurable cyber requirements alongside Performance, Safety and other “-ility” requirements
- Use common Mitigate and Recover capabilities, regardless of cause, where possible

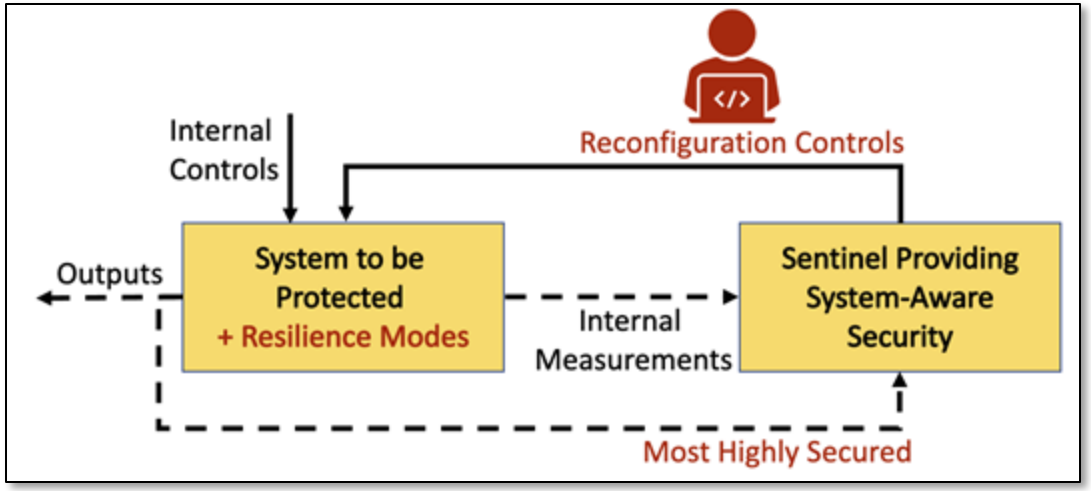
Distribution A - Cleared for Public Release by the Defense Office of Prepublication and Security Review, Case 24-T-0180, 27 October, 2023

Engineered Resilience Mechanisms

Resilience Mode - distinct and separate method of operation of a component, device, or system based upon a diverse redundancy or other design pattern.



Sentinel - pattern responsible for monitoring and reconfiguring a system using available Resilience Modes. The Sentinel functions are expected to be far more secure than the system being addressed for resilience.



Distribution A - Cleared for Public Release by the Defense Office of Prepublication and Security Review, Case 24-T-0180, 27 October, 2023

Requirements and Test for Resilience

- Resilience is a quality attribute
  - Rich notions of measurement
- Drive down to system requirements?
- Reason about the behavior of systems that have yet to be built?
- Integrated test
  - Technology
  - People
  - Processes
  - Decisions
- Testable requirements for engineered mechanisms

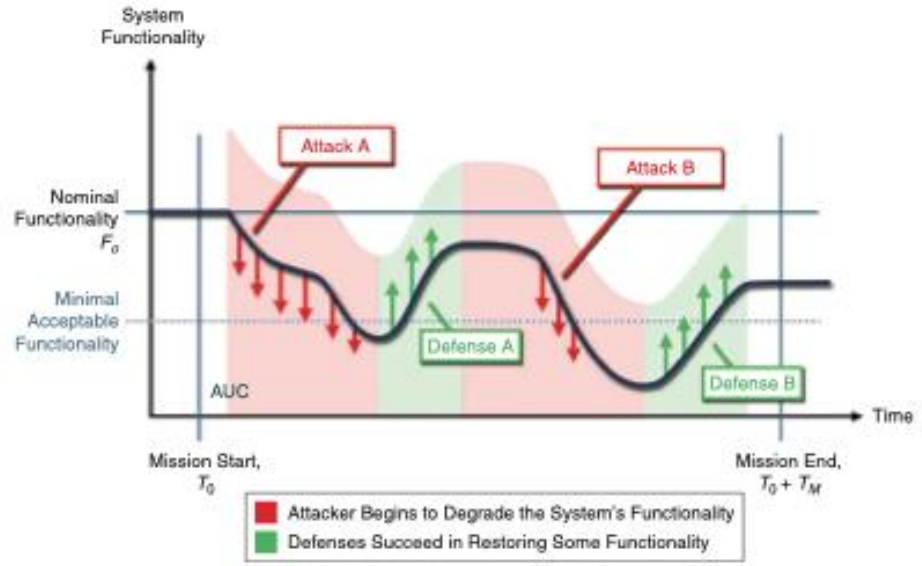


FIGURE 1. The stages of cyber resilience. AUC: area under the curve.

Source: Kott, A., & Linkov, I. (2021). To Improve Cyber Resilience, Measure It. *Computer*, *54*(2), 80-85.

Distribution A - Cleared for Public Release by the Defense Office of Prepublication and Security Review, Case 24-T-0180, 27 October, 2023

Framework for Operational Resilience in Engineering and System Test (FOREST)

Decomposition of how systems operate and respond under adversity:

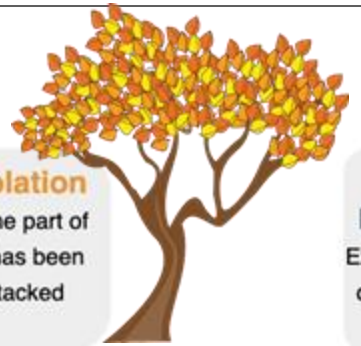
- Technology
- Processes
- Data
- Humans/operators
- Decisions

Distribution A - Cleared for Public Release by the Defense Office of Prepublication and Security Review, Case 24-T-0180, 27 October, 2023

FOREST and the Testable Resilience Efficacy Elements (TREEs)

1. Attack Sensing
Basis for discovering a successful cyber-attack and informing the system operators about the attack

2. Attack Isolation
Identification of the part of the system that has been successfully attacked



3. Resilience Response
Reconfiguration solution(s) for the attacks under consideration

4. Evaluation of Resulting Resilience
Explanations for the selection of solutions and anticipated performance

5. User Confidence in Executing Resilience Solutions
variability of situations that might confront the system under consideration

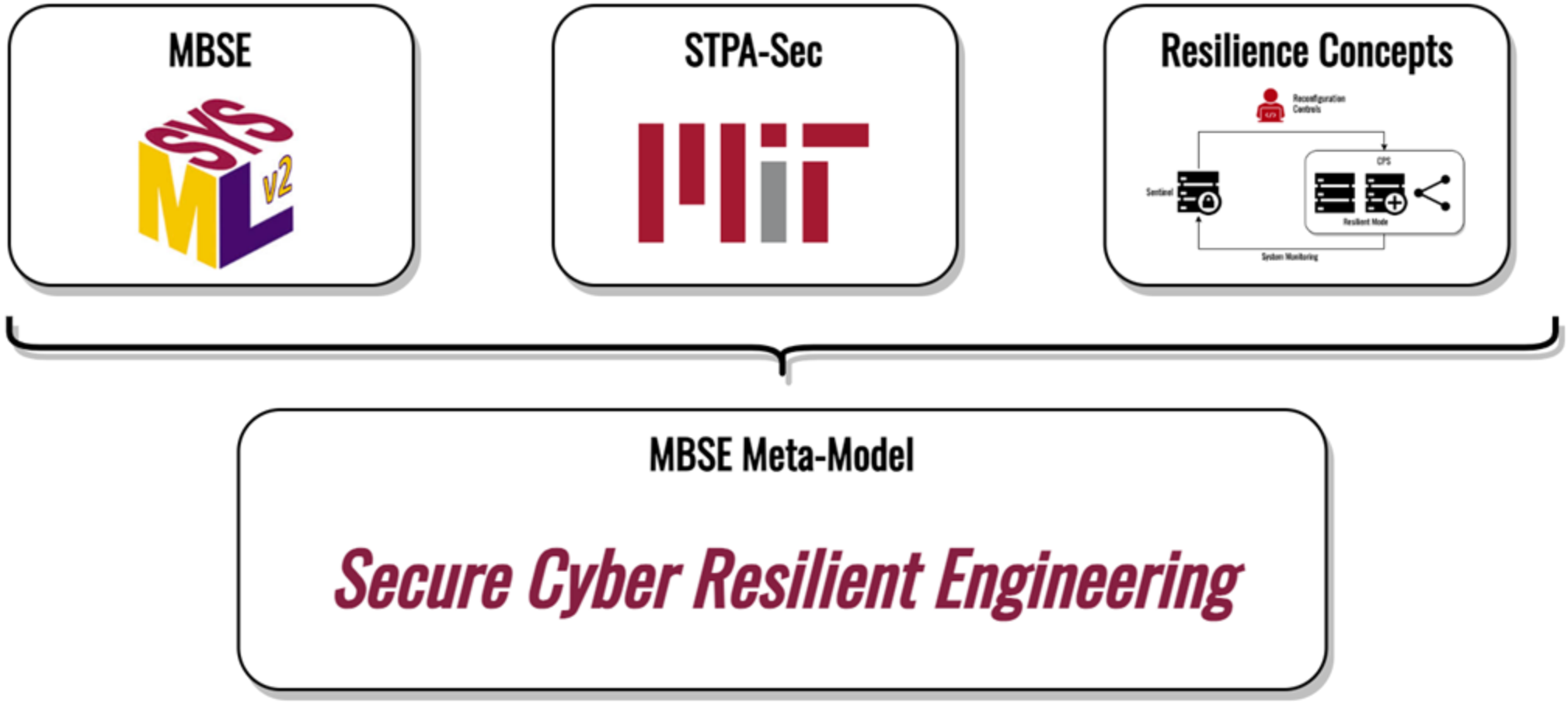
6. Readiness for Operator Evaluations
explanation of approach for addressing operator roles and anticipated performance

7. System Resilience Decisions
operational decision processes that will be required to achieve resilience as they relate to the military scenario being faced. This can provoke record keeping to understand the decisions made for resiliency, and can help feed future knowledge, requirements, and adjustments regarding system and mission capabilities.

8. Post-Event and Lifecycle Retesting
identification of information reporting and re-use of development test support capabilities to address system re-testing regarding potential improvements based upon results derived from executing resilience solutions in response to cyber-attacks.

Distribution A - Cleared for Public Release by the Defense Office of Prepublication and Security Review, Case 24-T-0180, 27 October, 2023

SCRE - Meta-Model Building Blocks



Distribution A - Cleared for Public Release by the Defense Office of Prepublication and Security Review, Case 24-T-0180, 27 October, 2023

STPA Overview

STPA is an iterative, methodical hazard analysis technique to identify causes of hazardous conditions intended to improve or promote system safety.

- In cyber-physical systems, security can be treated as analogous to safety.

Leveson, Thomas https://psas.scripts.mit.edu/home/get_file.php?name=STPA_handbook.pdf

STPA Outputs and Traceability

Figure 2.21 shows the traceability that is maintained between various STPA outputs.

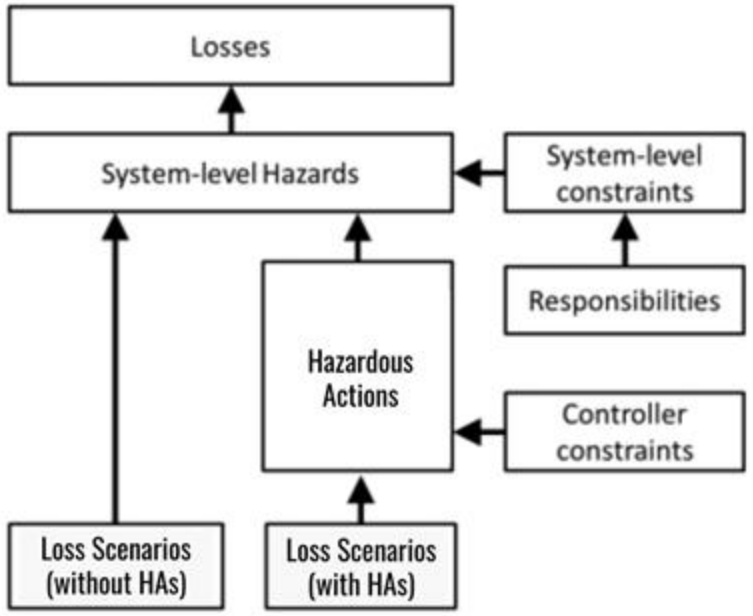
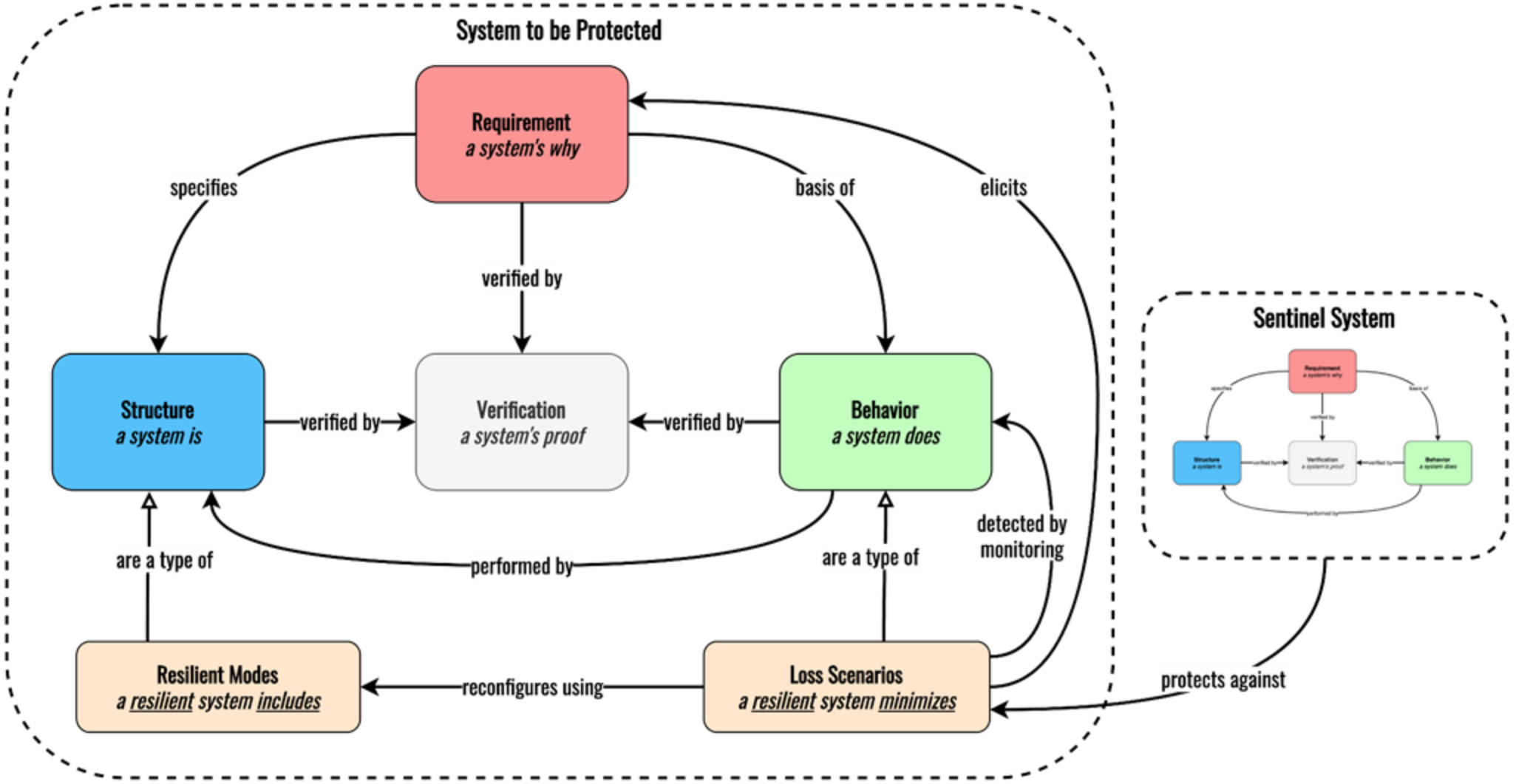


Figure 2.21: Traceability between STPA outputs

- A ***Loss*** involves something of value to stakeholders. Losses may include a loss of human life or human injury, property damage, environmental pollution, loss of mission, loss of reputation, loss or leak of sensitive information, or any other loss that is unacceptable to the stakeholders.
- A ***Hazard*** is a system state or set of conditions that, together with a particular set of worst-case environmental conditions, will lead to a loss.
- A ***Hazardous Action*** (HA) is a control action that, in a particular context and worst-case environment, will lead to a hazard.
- A ***Loss Scenario*** describes the causal factors that can lead to the hazardous actions and to hazards.

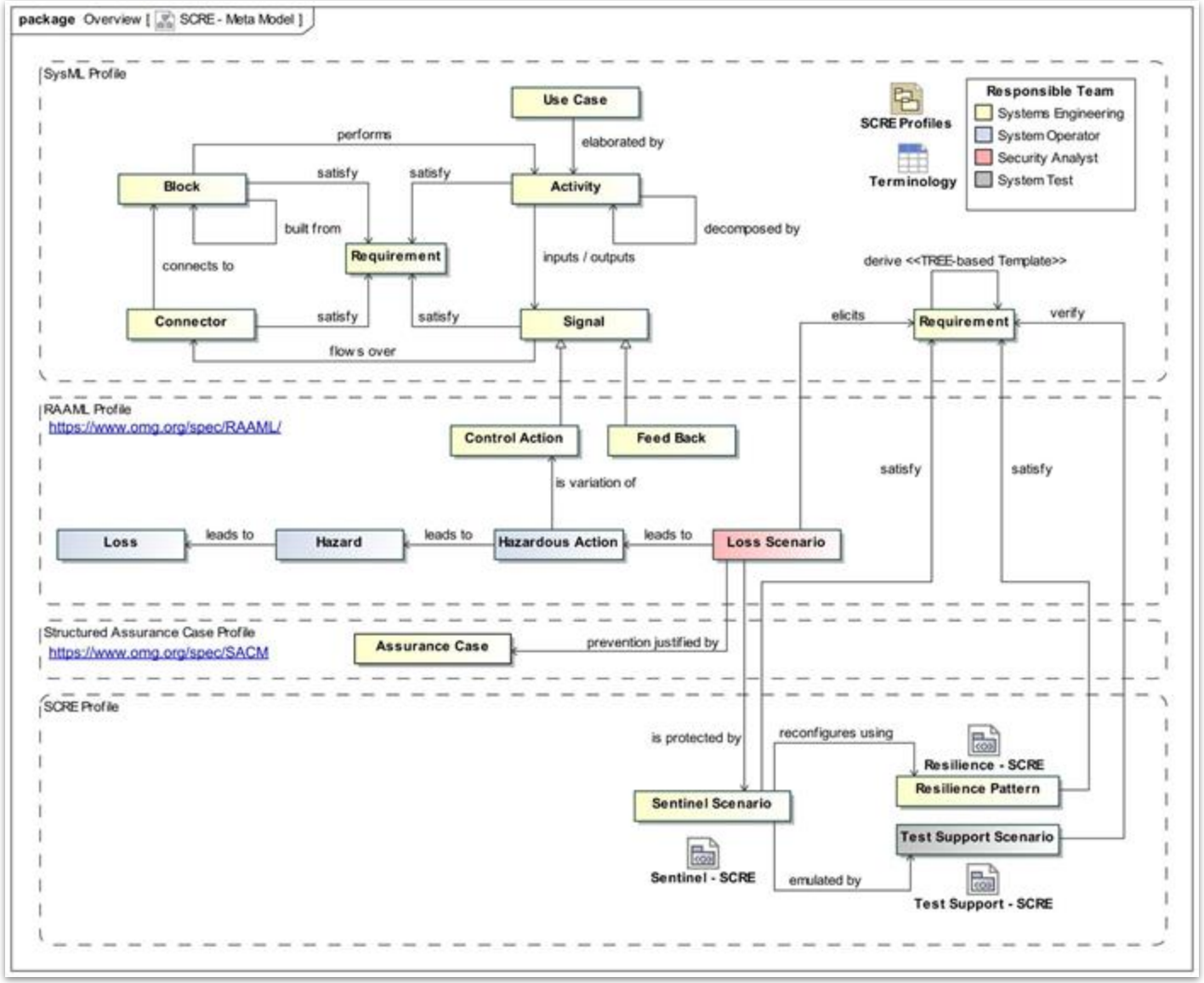
Distribution A - Cleared for Public Release by the Defense Office of Prepublication and Security Review, Case 24-T-0180, 27 October, 2023

SCRE MBSE Meta-Model: Top-Level



Distribution A - Cleared for Public Release by the Defense Office of Prepublication and Security Review, Case 24-T-0180, 27 October, 2023

SCRE Meta-Model: Detail View

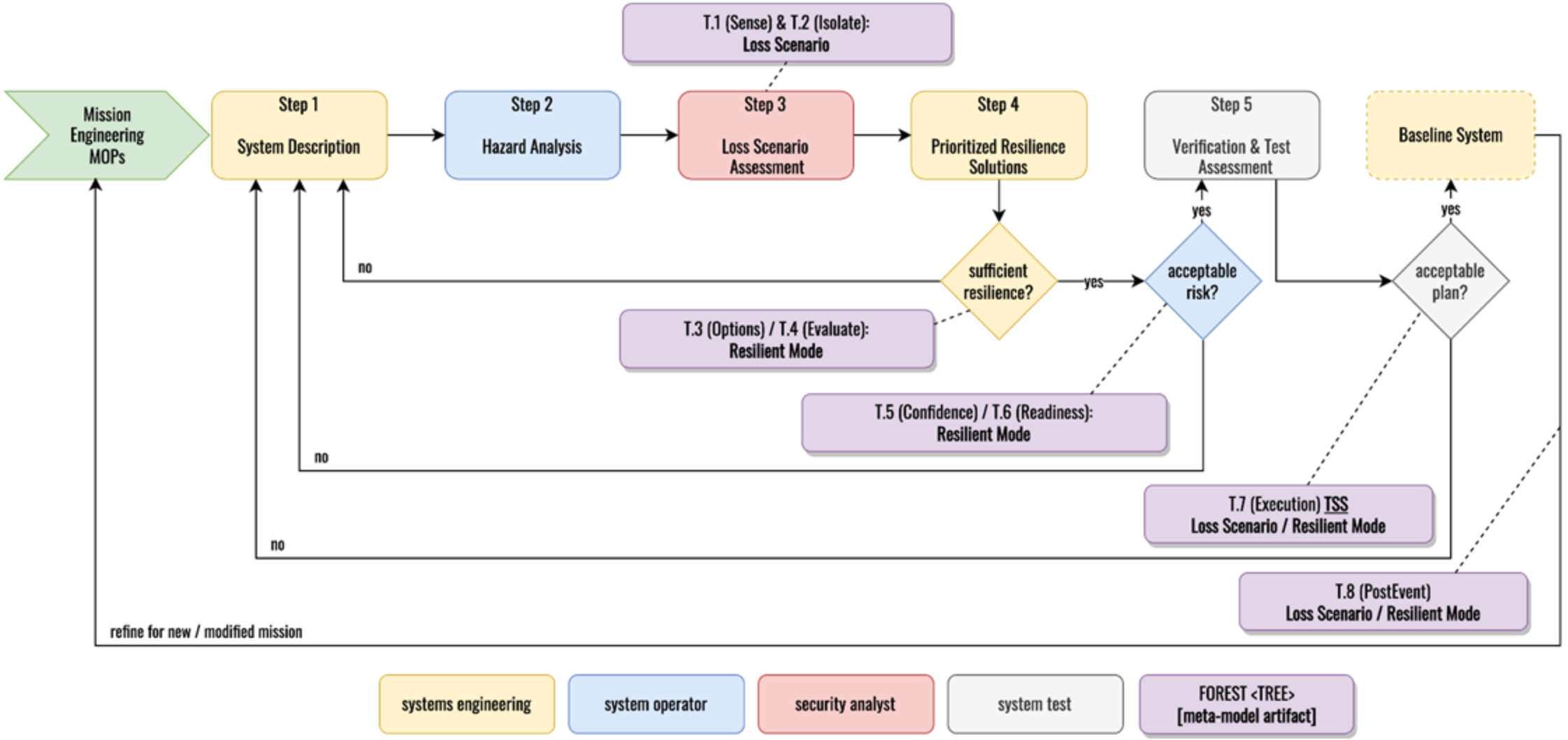


Meta-Model Artifact per SCRE Step

1A - Identify Operational **Use Cases** (Problem Framing).
1B – Define Activity Diagrams (**Block**, **Connector**, **Signal**) to realize Use Cases
1C – Define Control Structure (**Control Action, Feedback**) to support Use Cases
2 – Perform Hazard Analysis (**Loss, Hazard, Hazardous Action**) for Control Structure
3 – Identify **Loss Scenarios** for Control Structure & Risk Assessment
4 – Define Resilience Architecture (**Sentinel Scenario, Resilience Pattern, SCRE Requirements**) for Loss Scenarios to be 'protected against' (CSA: 7-10). Define **Assurance Cases** for Loss Scenarios to be 'prevented' (CSA: 1-6).
5 – Define Resilience Test & Evaluation (**Test Support Scenarios**) to verify SCRE Requirements

Distribution A - Cleared for Public Release by the Defense Office of Prepublication and Security Review, Case 24-T-0180, 27 October, 2023

Cyber Resilience Requirements Methodology (CRRM)



Distribution A - Cleared for Public Release by the Defense Office of Prepublication and Security Review, Case 24-T-0180, 27 October, 2023

Results

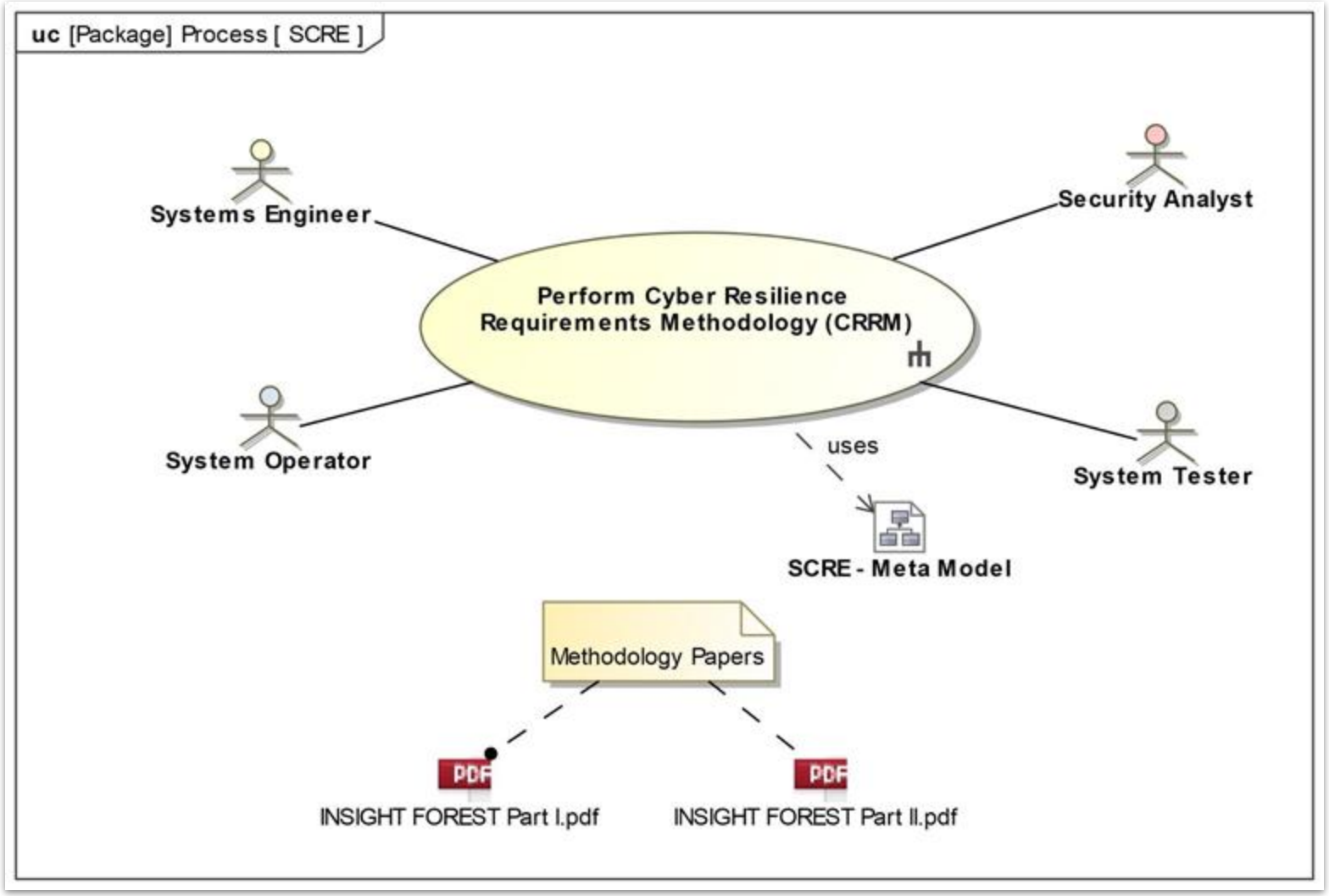
Distribution A - Cleared for Public Release by the Defense Office of Prepublication and Security Review, Case 24-T-0180, 27 October, 2023

Project Goals

- Apply the Framework for Operational Resilience in Engineering and System Test (FOREST) and related resilience approaches to a DoD acquisition program
  - Identify critical functionality losses that require operational resilience
  - Decompose mission resilience requirements, assess identified systems functions using Systems-Theoretic Process Analysis – Security (STPA-Sec)
  - Define measurable and testable metrics for resilience
  - Define and implement resilience patterns to meet resilience requirements
  - Assess the robustness of resilience designs
  - ***Recommend improvements to engineering processes and tools, FOREST framework, overall engineering policy and guidance***

Distribution A - Cleared for Public Release by the Defense Office of Prepublication and Security Review, Case 24-T-0180, 27 October, 2023

CRRM Methodology via MBSE



Perform CRRM

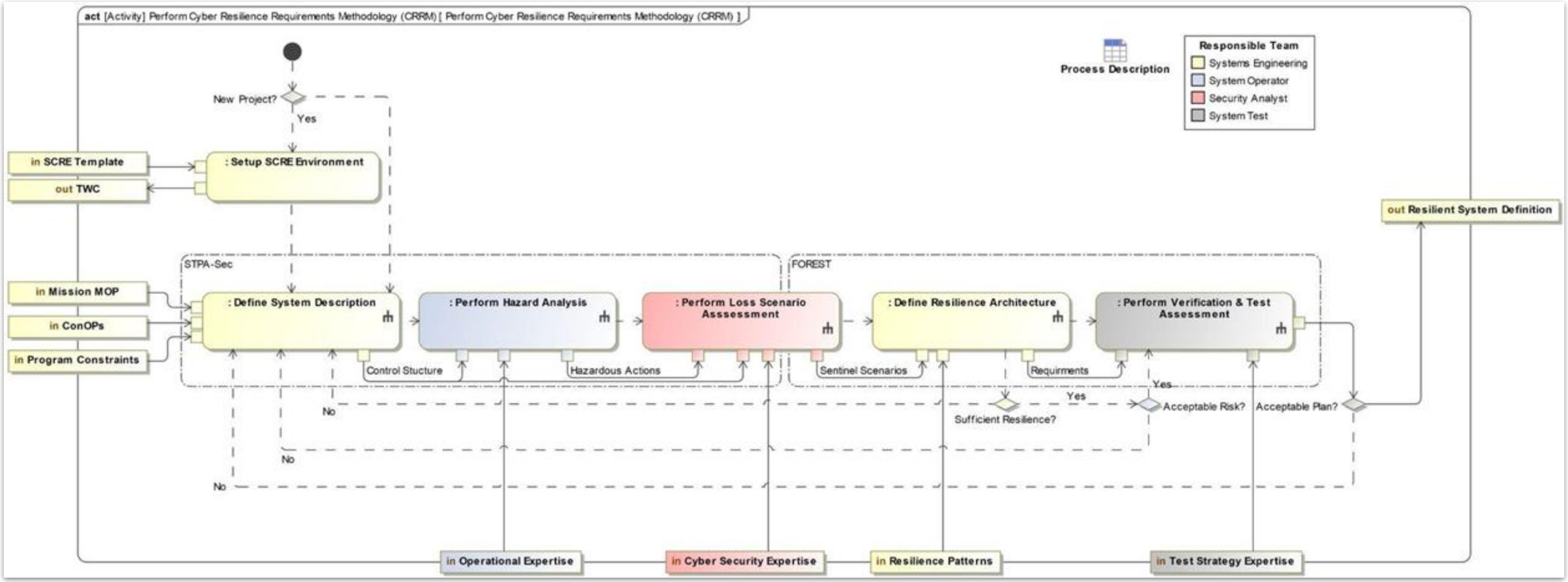
- 4 Actor Perspectives
- Steps Reference Relevant Meta-Model Artifacts

Distribution A - Cleared for Public Release by the Defense Office of Prepublication and Security Review, Case 24-T-0180, 27 October, 2023

CRRM Methodology via MBSE

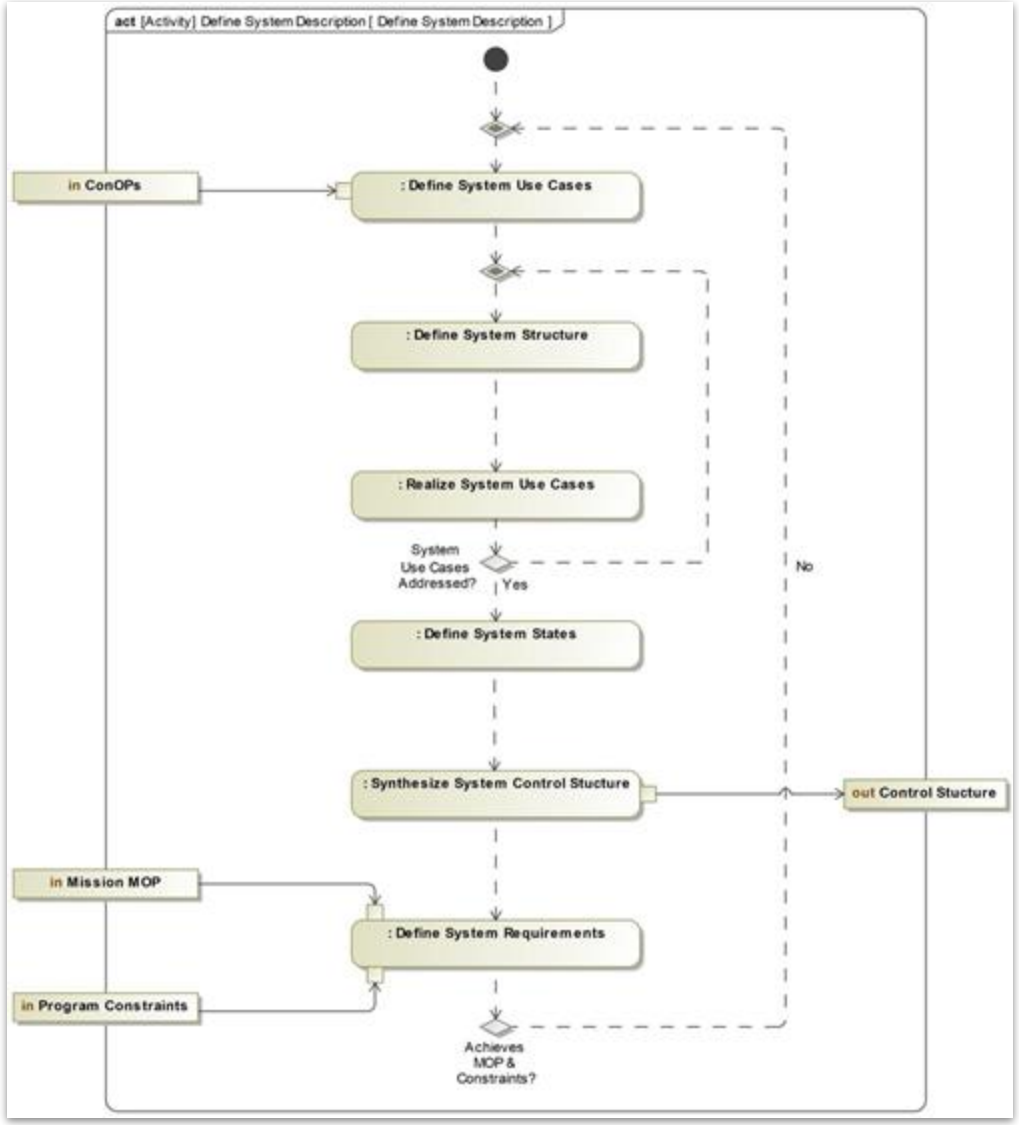
Top-Level CRRM Activity Diagram

- Responsible Team Color Coding
- Environment Setup using Templates and TWC
- Includes STPA-Sec & FOREST Activities
- Identifies Key Inputs / Outputs



Distribution A - Cleared for Public Release by the Defense Office of Prepublication and Security Review, Case 24-T-0180, 27 October, 2023

CRRM Methodology via MBSE



System Description Activity Detail

- Based on ConOPs, Define and Realize key System Use Cases
- Synthesize System Control Structure from Use Case Realizations (Activity Diagrams)
  - Key output is System Control Structure for next step (STPA Hazard Analysis)
- Iteratively define System Requirements that satisfy mission and programmatic constraints
  (cost, weight, power budget, link capacity, schedule, etc.)

Distribution A - Cleared for Public Release by the Defense Office of Prepublication and Security Review, Case 24-T-0180, 27 October, 2023

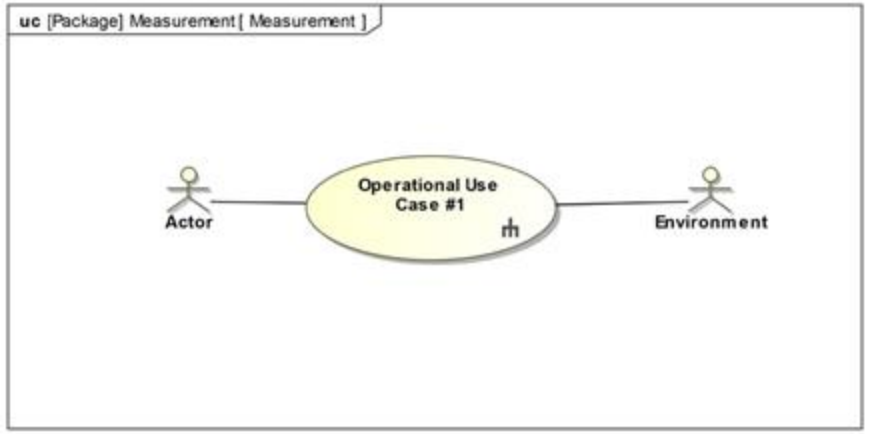
GFI - MBSE Overview

- Government Furnished Information (GFI) input to contractors
  - Pilot Program - GFI was Cameo MBSE
    - Contractor to follow STPA
- Allocated Baseline from Contractors
  - Indications of how GFI was used

- Recommendations
  - Detailed Process Description
    - CRRM with Meta-Model Artifacts
  - Operational Use Case Realization (Activity Diagrams)

Distribution A - Cleared for Public Release by the Defense Office of Prepublication and Security Review, Case 24-T-0180, 27 October, 2023

GFI MBSE Recommendation - Operational Use Case Realization

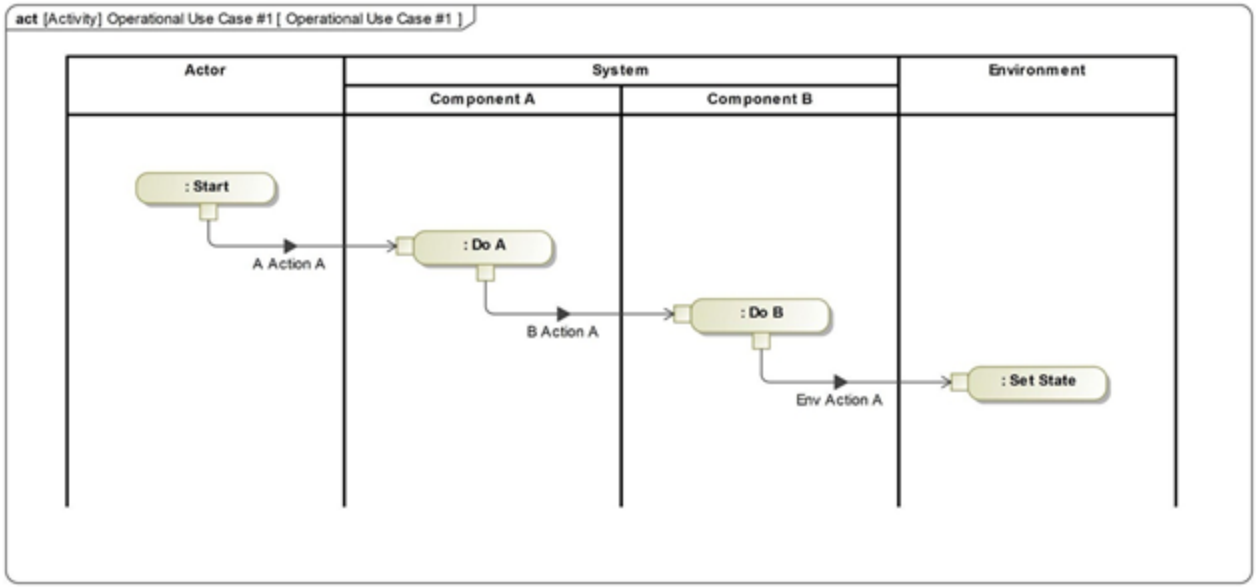


Operational Use Case Realization:

- Include relevant external and internal subsystems
- Identify message flow between subsystems

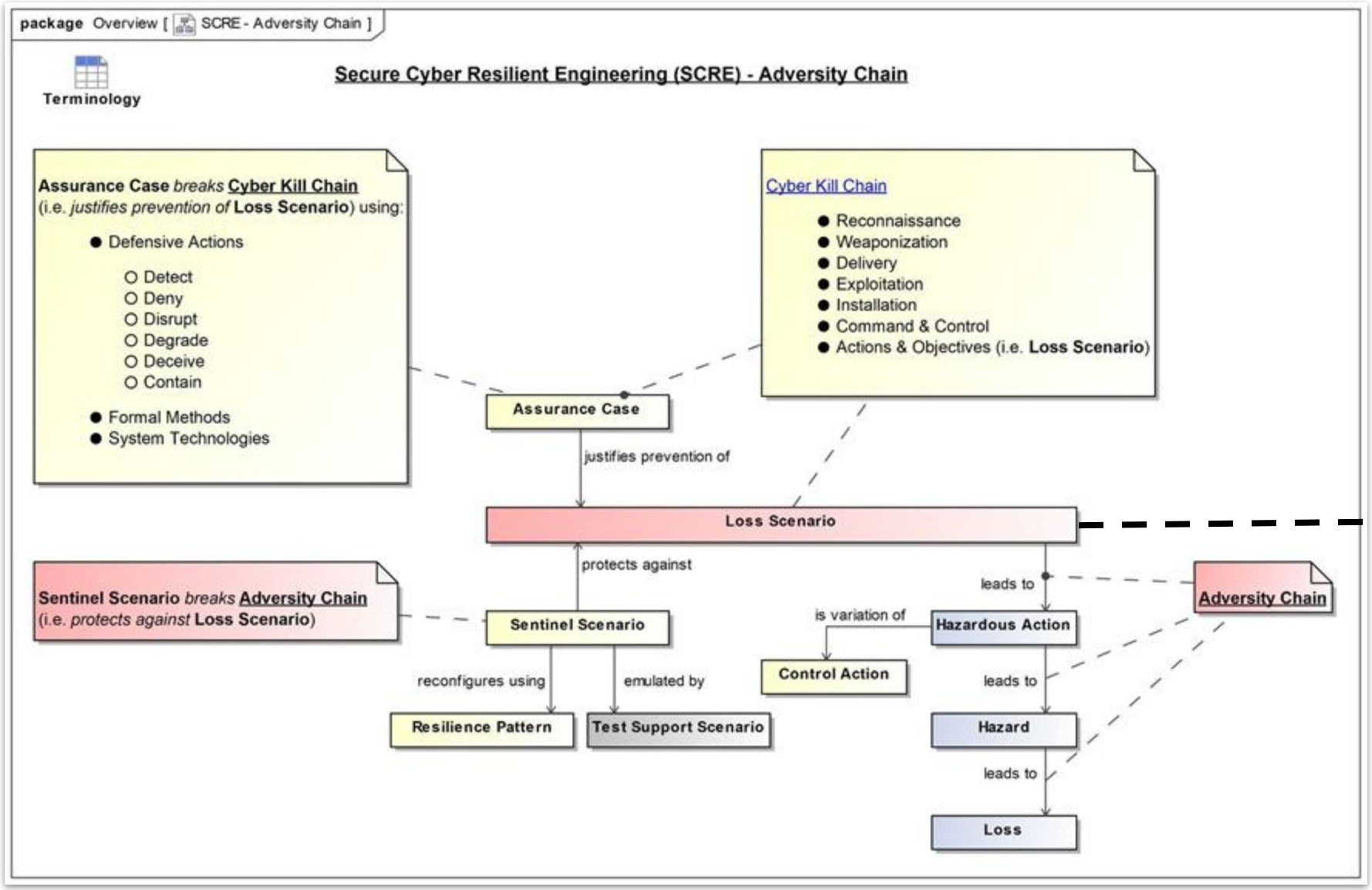
Enables:

- Synthesis of STPA Control Structure - identify hierarchy of control, and message flow type (control action or feedback)
- Identification of "normal" activity ordering - and associated identification of STPA Hazardous Actions (happens too soon, too late, out-of-order)



Distribution A - Cleared for Public Release by the Defense Office of Prepublication and Security Review, Case 24-T-0180, 27 October, 2023

SCRE - Adversity Chain



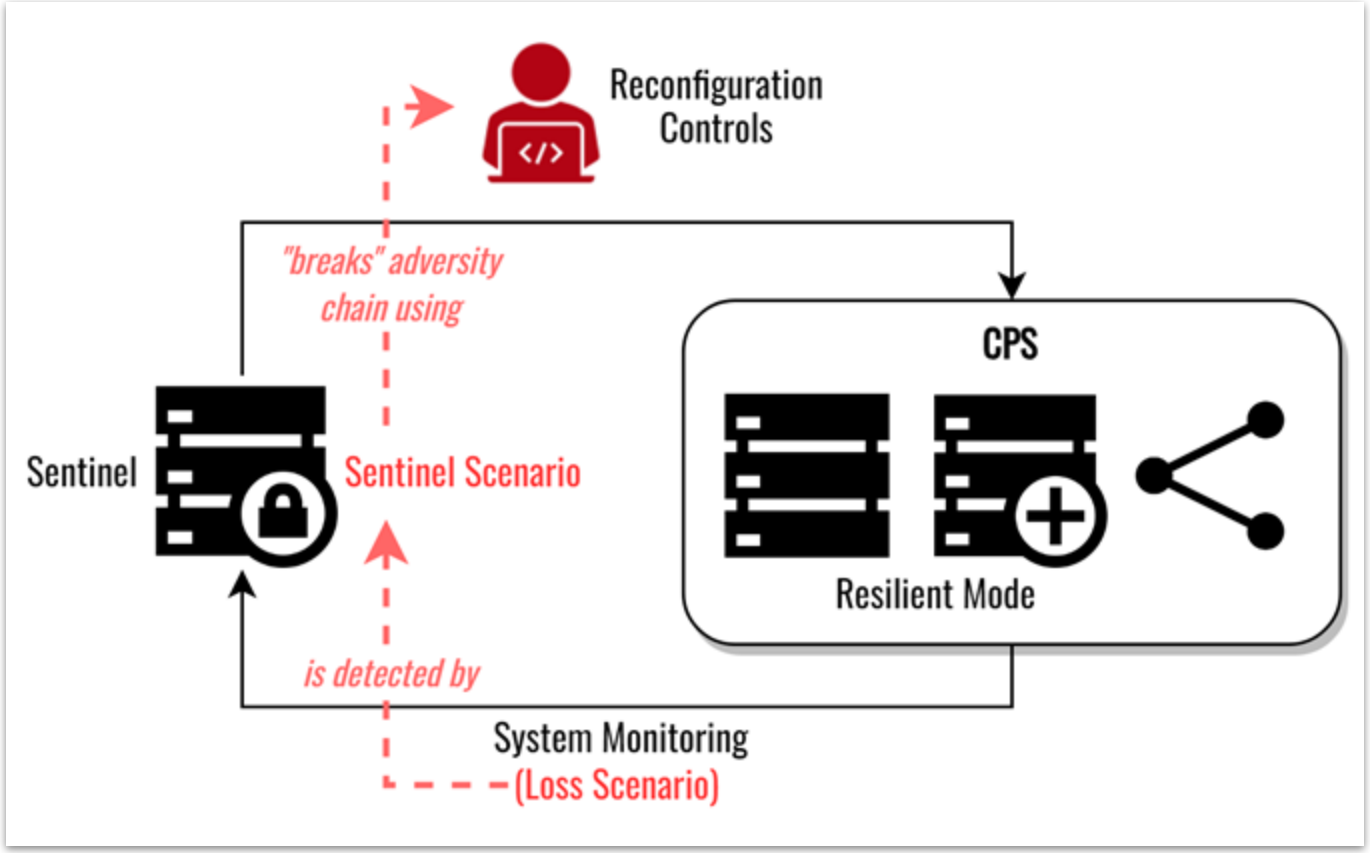
Kill Chain Progression
(Defensive Mechanisms)

Adversity Chain Progression
(Resilience Mechanisms)

Distribution A - Cleared for Public Release by the Defense Office of Prepublication and Security Review, Case 24-T-0180, 27 October, 2023

SCRE - Adversity Chain

Observe the System rather than the Adversary



Can specify and test:

- Time to detect
- Characteristics of resilience modes
- Human-autonomy control roles
- Information / communications

Distribution A - Cleared for Public Release by the Defense Office of Prepublication and Security Review, Case 24-T-0180, 27 October, 2023

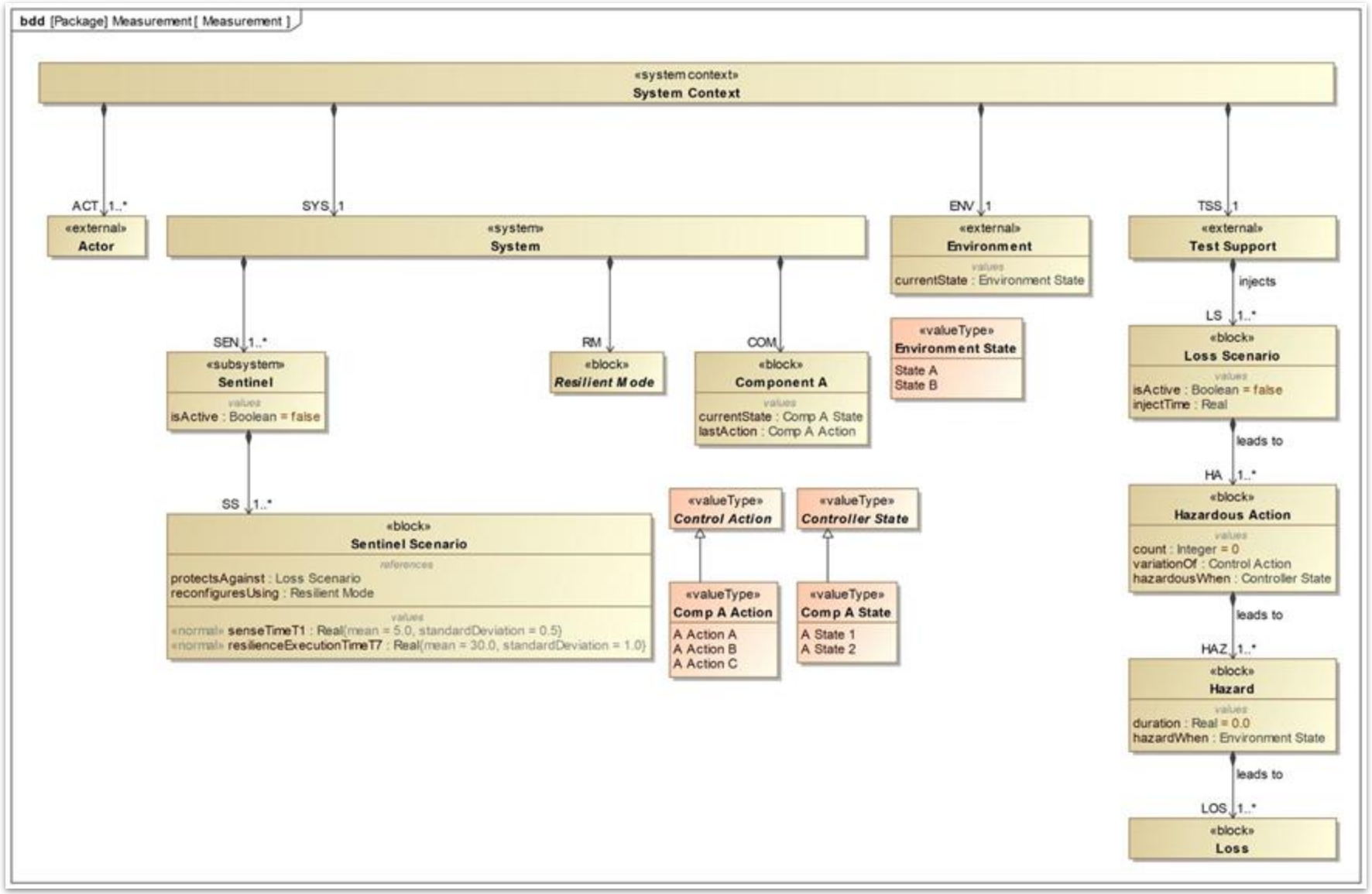
Measuring Resilience via Adversity Chain

- Mission Success is *equivalent* to avoiding STPA Losses
- Avoiding STPA Losses *is accomplished by* Sentinel Scenarios that successfully **break** Adversity Chain
  - Success in **breaking** Adversity Chain is *measured* by:
    - Minimizing *time* for FOREST TREE-based **recovery** (to resilient mode of operation) - thereby:
      - Minimizing *count* of Hazardous Actions
      - Minimizing *time* in Hazard States

- Model Simulation
  - Trade space analysis to *optimize* ***recovery*** requirements within the context of mission and system constraints
    (cost, weight, power budget, link capacity, schedule, etc.)
  - Monte Carlo analysis to *demonstrate* ***minimization*** (with / without Resilient Mode) of Hazardous Actions and Hazards within constraints of recovery requirements

Distribution A - Cleared for Public Release by the Defense Office of Prepublication and Security Review, Case 24-T-0180, 27 October, 2023

Adversity Chain Measurements



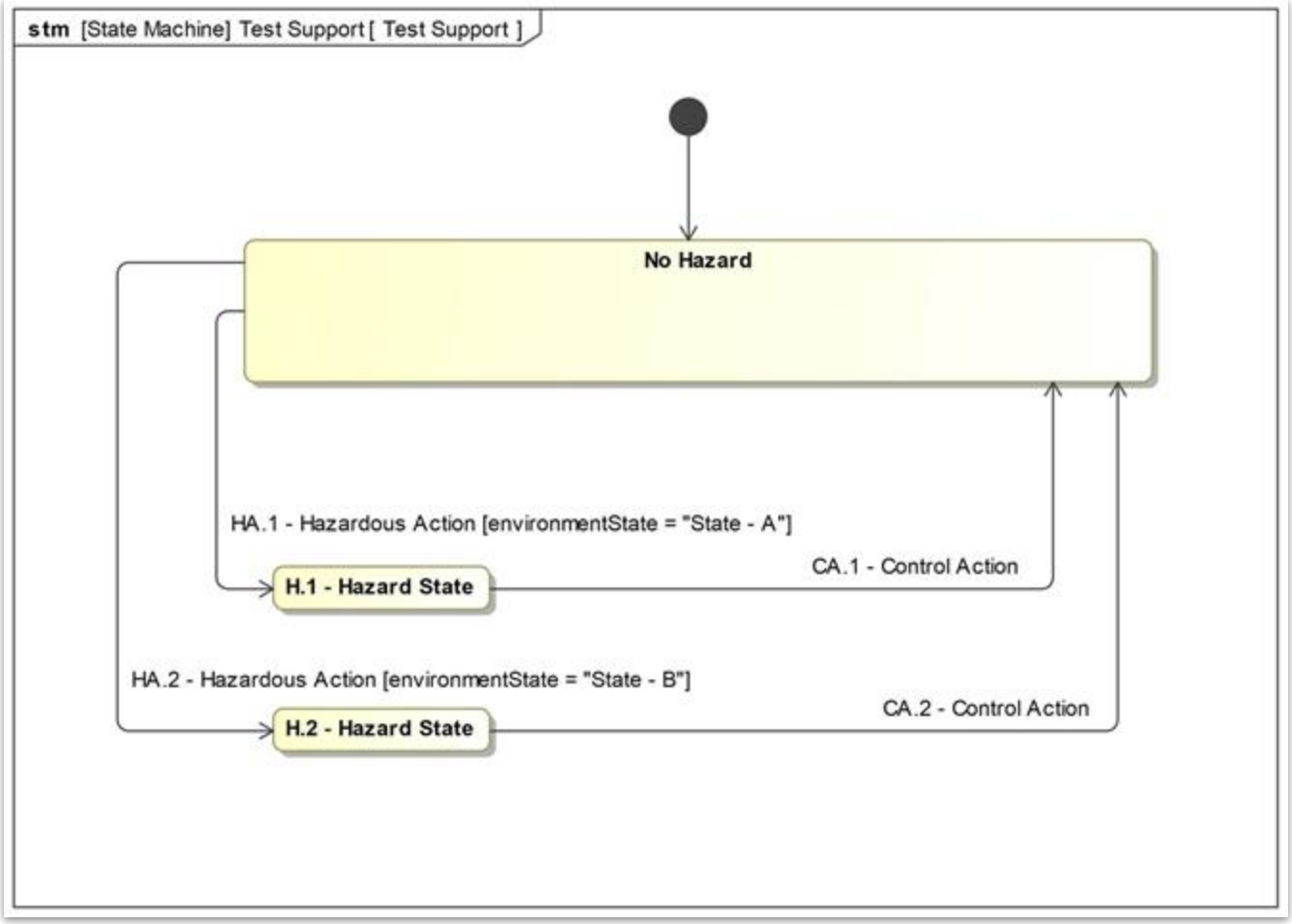
Test Support System *injects* Loss Scenario

Sentinel Scenario sets distribution for FOREST TREE-based recovery times

Sentinel detects and monitors *count* of Hazardous Actions and *duration* of Hazard State with and without Resilient Mode

Distribution A - Cleared for Public Release by the Defense Office of Prepublication and Security Review, Case 24-T-0180, 27 October, 2023

Adversity Chain Measurements



Sentinel Monitoring determines *count* of Hazardous Actions based on:

- Patterns of monitoring (e.g. control action consistency) for deviations from normal behavior
- Current state of Controllers

Sentinel Monitoring determines *duration* of Hazard State based on:

- Current state of Environment when Hazardous Action detected
- Control Actions which transition from a Hazard state and/or changes in Environmental state

Distribution A - Cleared for Public Release by the Defense Office of Prepublication and Security Review, Case 24-T-0180, 27 October, 2023

References

- McDermott, T., Clifford, M. M., Sherburne, T., Horowitz, B., & Beling, P. A. (2022). Framework for Operational Resilience in Engineering and System Test (FOREST) Part I: Methodology–Responding to “Security as a Functional Requirement”. INSIGHT, 25(2), 30-37.

- McDermott, T., Clifford, M. M., Sherburne, T., Horowitz, B., & Beling, P. A. (2022). Framework for Operational Resilience in Engineering and System Test (FOREST) Part II: Case Study–Responding to “Security as a Functional Requirement”. INSIGHT, 25(2), 38-43.

- Fleming, C. H., Elks, C., Bakirtzis, G., Adams, S., Carter, B., Beling, P., & Horowitz, B. (2021). Cyberphysical security through resiliency: A systems-centric approach. Computer, 54(6), 36-45.

- SCRE Cameo Meta-Model Profile & Case Study Models
  - https://github.com/stars/tsherburne/lists/scre

Distribution A - Cleared for Public Release by the Defense Office of Prepublication and Security Review, Case 24-T-0180, 27 October, 2023

Thank you

Stay connected with SERC Online:

Email the presenter: Peter Beling

beling@vt.edu

Email the research team: VT National Security Institute

beling@vt.edu

Distribution A - Cleared for Public Release by the Defense Office of Prepublication and Security Review, Case 24-T-0180, 27 October, 2023