SYSTEMS ENGINEERING RESEARCH CENTER

Measurable Requirements for Operational Resilience

WRT-1072

Ms. Sarah Standard, OUSD(R&E)

Dr. Peter Beling, Virginia Tech

NATIONAL SECURITY INSTITUTE
VIRGINIA TECH.

UNDER SECRETARY OF DEFENSE FOR RESEARCH AND ENGINEERING
USD R&E
DEPARTMENT OF DEFENSE

ANNUAL RESEARCH REVIEW 2022

Contents

Objective:

- Testable Requirements for Operational Resilience in Cyber

Opportunity:

- Apply methods from WRT-1022 & others from community on major program

Technical Approach:

- FOREST
- Mission Aware & CSRM
- Silverfish: Case study from WRT-1022
- Outline of Tasks for subject program
- Relation to initiatives in DTE&A

Research Team

Virginia Tech

- Peter Beling
- Tim Sherburne
- Scott Lucero

Stevens Institute of Technology

- Tom McDermott
- Megan Clifford

Related Prior SERC Projects

- WRT-1033: Transitioning Mission Aware Concepts and Methods to Evaluate Cost/Risk Decisions
  for Security Assurance Design
- ART-004: Methods to Evaluate Cost/Technical Risk and Opportunity Decisions for Security Assurance in Design
- RT-191” Risk-Based Approach to Cyber Vulnerability Assessment
- RT-172: Security Engineering
- RT-151: Security Engineering

Sponsor - DTE&A

Sarah Standard

Cybersecurity/Interoperability Technical Director, US Department of Defense (DoD)

A 1988 US Naval Academy (USNA) graduate and retired US Navy Information Professional Captain, Sarah earned her MA in Applied Mathematics from the University of Maryland, College Park, with applications in Numerical Analysis, Operations Research and Databases.

Sarah instructed calculus and cybersecurity courses at USNA from 2010-2014. In 2014 she began working for AVIAN, LLC where she developed and instructed a NAVAIR-specific cyber warfare course. In 2016, she transitioned to serve as the Cybersecurity and Interoperability Technical Director to now the Executive Director, for Developmental Test, Evaluation, and Assessments in the Office of the Under Secretary of Defense for Research and Engineering.

Distribution A - Cleared for Public Release by the Defense Office of Prepublication and Security Review, Case 23-S-0383, 10 November 2022

Motivation

- "… the Department will take necessary action to increase resilience – our ability to withstand, fight through and recover quickly from disruption."
  - National Defense Strategy 2022
- Measures of resilience and design tools are immature
- Research is needed to:
  - Decompose and measure effectiveness of system resilience requirements
  - Define and implement resilience patterns to meet resilience requirements
  - Incorporate resilience requirements into existing processes and tools

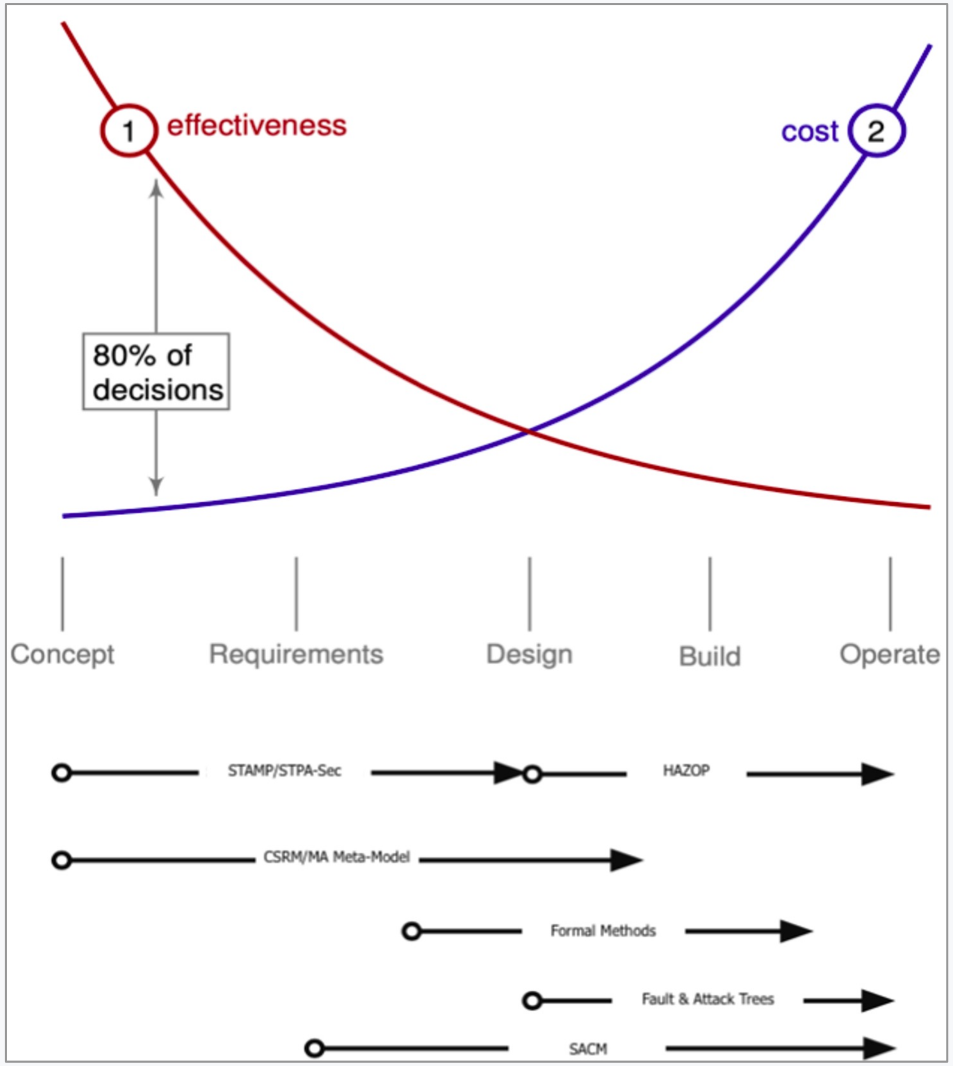
Project Overview

- 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

Build on Lessons Learned from Silverfish Case Study

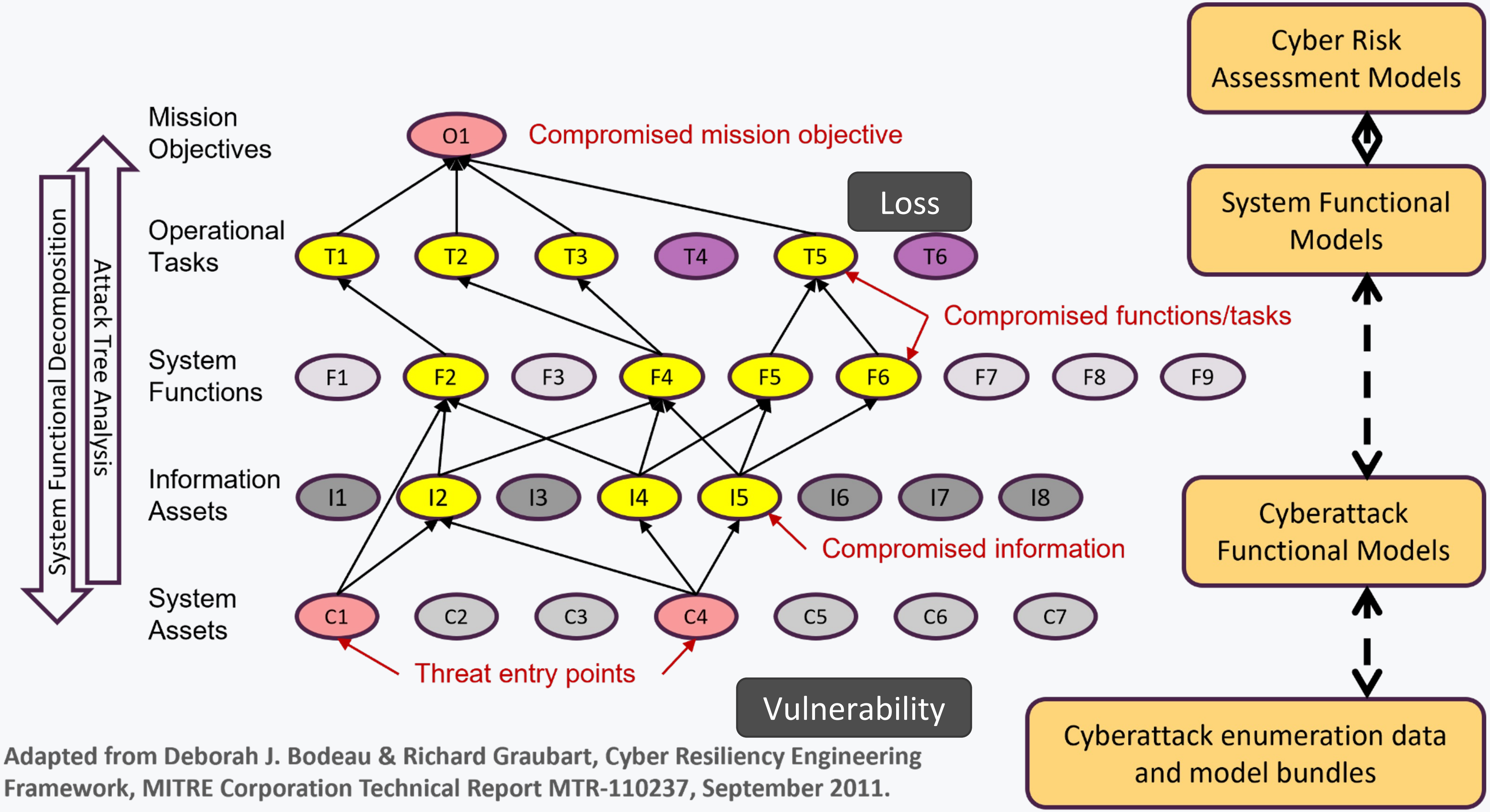
Approach: Resilience and Assurance Methodologies – Full System Life Cycle

- Need rigorous methods and tools usable in all stages of the SE process
  - From Mission Engineering to Developmental & Operational Test
- Earlier focus on loss causation and resilience
- Later focus on risk management and assurance
- Continuous evaluation of assurance-related quality attributes



Distribution A - Cleared for Public Release by the Defense Office of Prepublication and Security Review, Case 23-S-0383, 10 November 2022

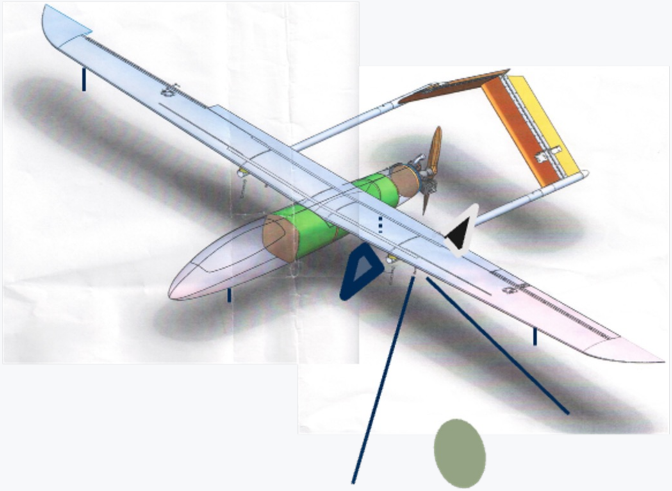
Functional Modeling in Cyber Resilience Engineering

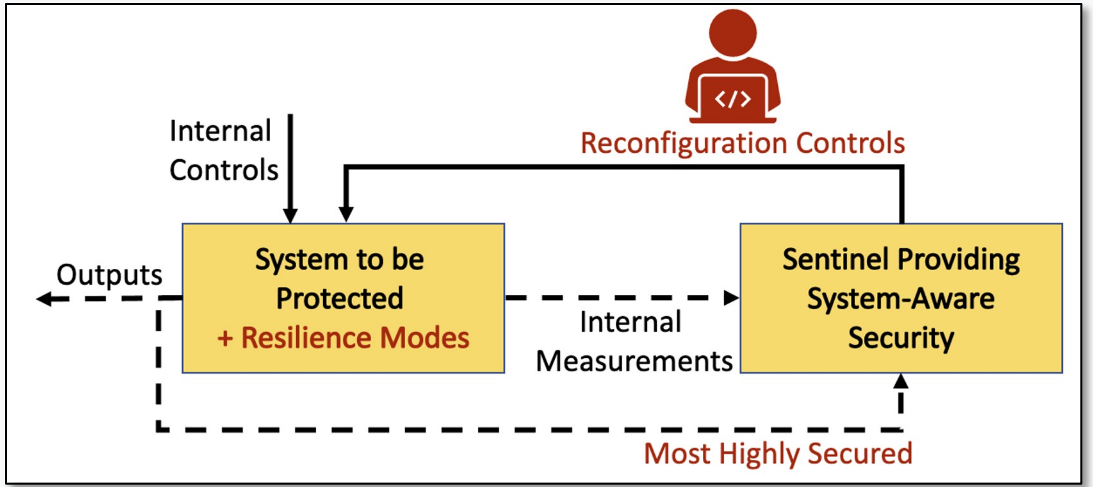


Adapted from Deborah J. Bodeau & Richard Graubart, Cyber Resiliency Engineering Framework, MITRE Corporation Technical Report MTR-110237, September 2011.

Engineered Resilience Mechanisms

- A **Resilience Mode** - distinct and separate method of operation of a component, device, or system based upon a diverse redundancy or other design pattern.
- A **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 23-S-0383, 10 November 2022

Resilience Modes and Detection Patterns - (UVA, Siemens, SIT)

Mode / Pattern	*Description*	*Attack model countered*
Trusted Kernel or Guard	Creates a small control system within the CPS that independently monitors and/or manages all resource access	Escalation, interruption attacks
Isolation	Creates an isolated runtime environment (sandbox) for the critical asset that is resistant against attacks.	Escalation, interruption attacks
Redundancy	Replicates the functionality of the critical asset in order to create multiple paths for high availability and fault tolerance in the case of individual function failures	Attacks that disable individual instances of critical assets and functionality.
Diversification	Produces functionally equivalent variations of binaries running in software critical assets. This is an enhancement of the redundancy countermeasure.	Coordinated attacks, zero-day attacks effective in identical binary copies of the critical assets.
Physically Unclonable Function	Secures the integrity and privacy of the messages in the system using a Physical Unclonable Function (PUF) that is hard to predict and duplicate.	Attacks that hijack the communication channels such as man-in-the-middle attacks.
Obfuscation	Obscures the real meaning of data/signals/flows by making them difficult for an attacker to understand. It can use random sources of noise from the environment of the critical assets to increase the entropy.	Attacks that require knowledge of the inner workings of the system, its functions, and its mission.
Parameter Assurance	Compares input data to a table of values in the system to check for large, unexpected deviations.	Attacks that manipulate data files or messages that are sent to the system.
Data Consistency Checking	Verifies the source of a parameter change.	Attacks that use operator specific data entry.
Limiting Circuits	Limits resource use (power, memory) to prevent overload	Power System Attack

Distribution A - Cleared for Public Release by the Defense Office of Prepublication and Security Review, Case 23-S-0383, 10 November 2022

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

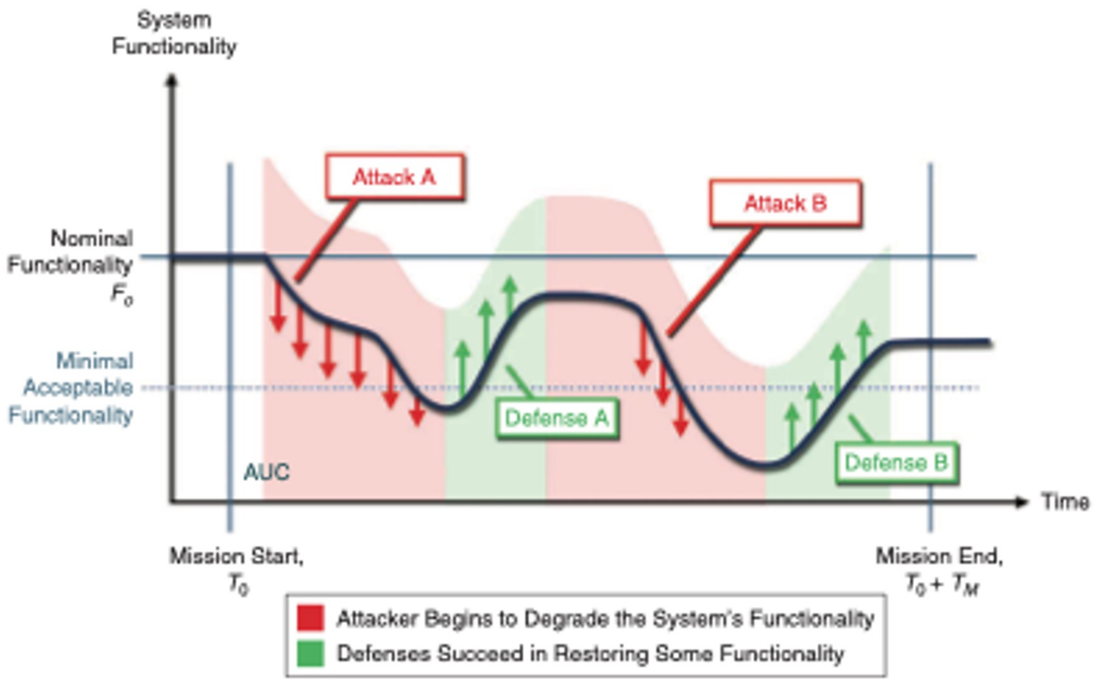
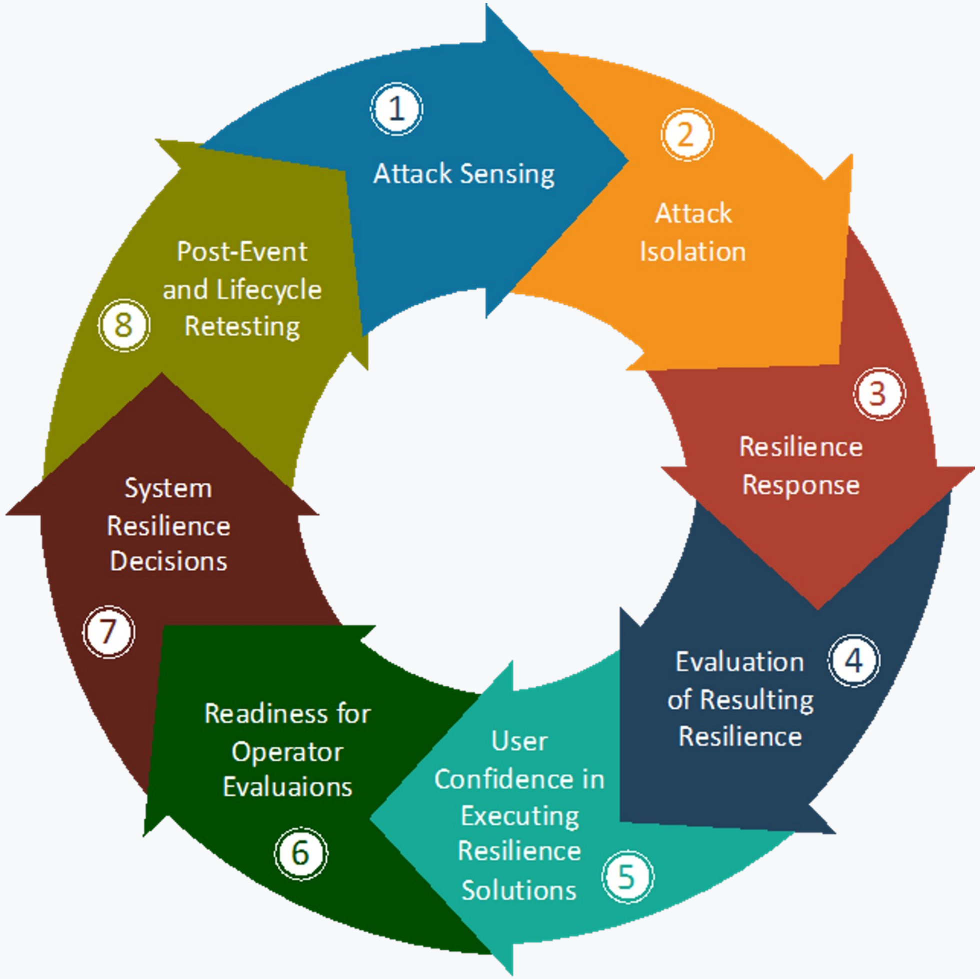


FIGURE 1. The stages of cyber resilience. AUC: area under the curve.

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

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

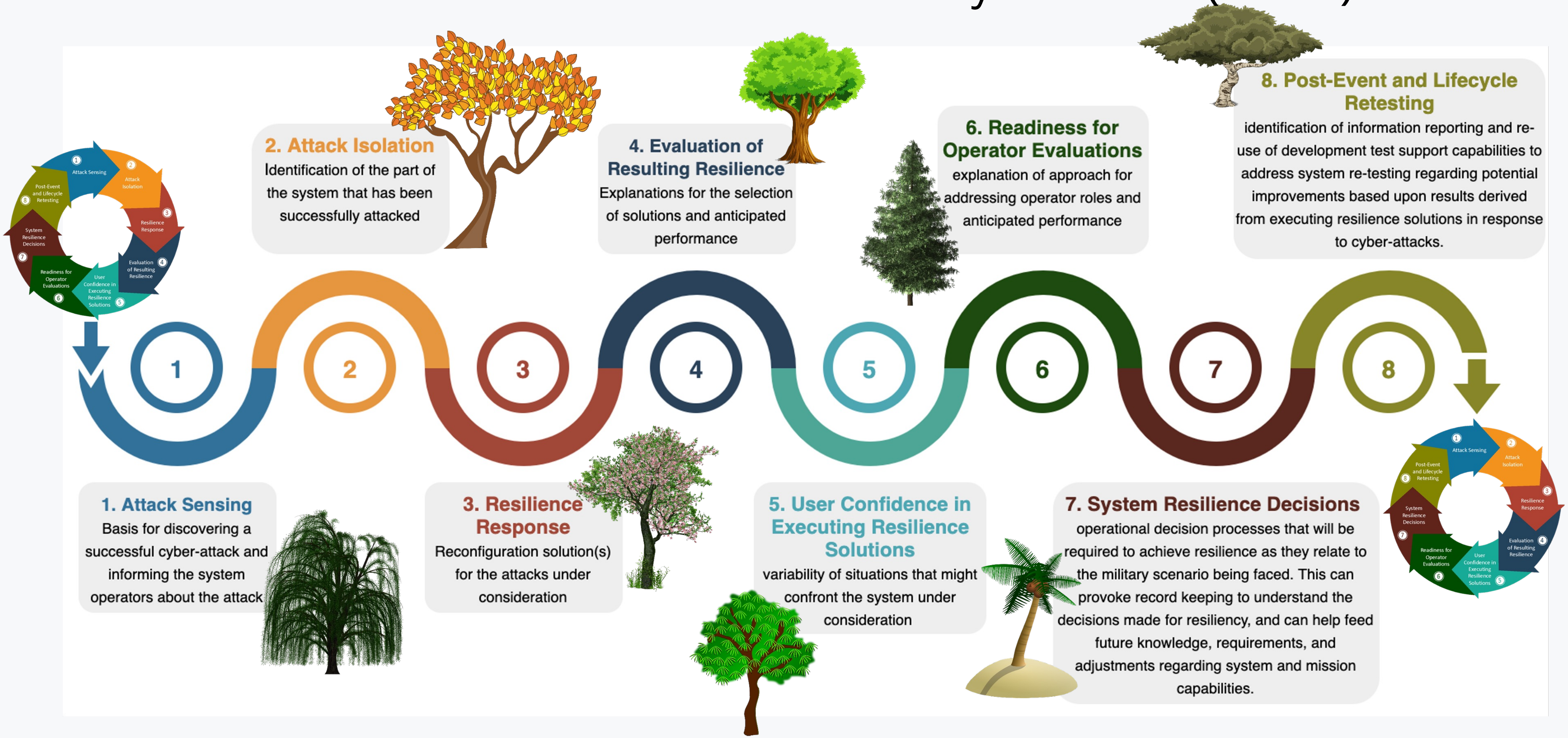

1
Attack Sensing
2
Attack Isolation
3
Resilience Response
4
Evaluation of Resulting Resilience
5
User Confidence in Executing Resilience Solutions
6
Readiness for Operator Evaluaions
7
System Resilience Decisions
8
Post-Event and Lifecycle Retesting

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 23-S-0383, 10 November 2022

FOREST and the Testable Resilience Efficacy Elements (TREEs)


1
Attack Sensing
2
Attack Isolation
3
Resilience Response
4
Evaluation of Resulting Resilience
5
User Confidence in Executing Resilience Solutions
6
Readiness for Operator Evaluations
7
System Resilience Decisions
8
Post-Event and Lifecycle Retesting
1
2
3
4
5
6
7
8

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

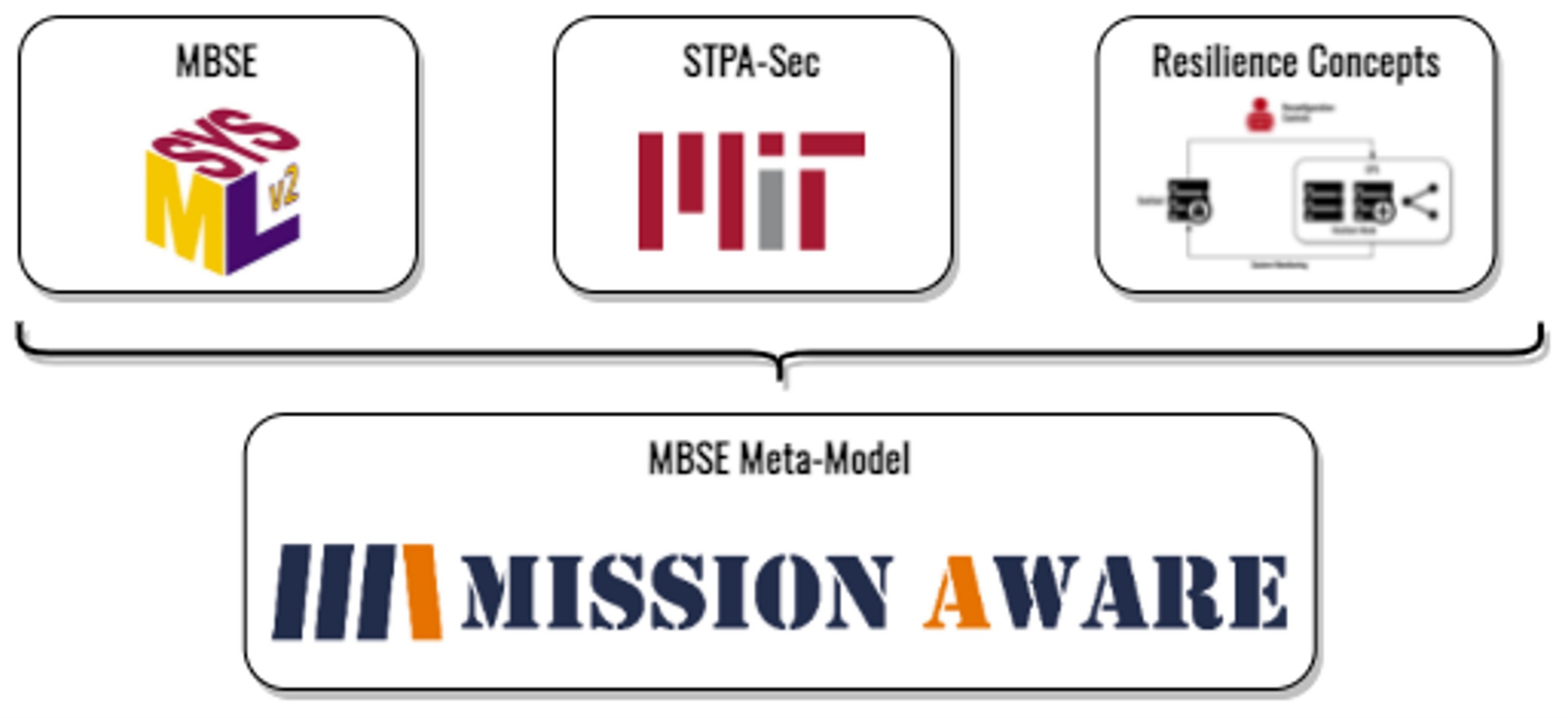
6. Readiness for Operator Evaluations
explanation of approach for addressing operator roles and anticipated performance

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.

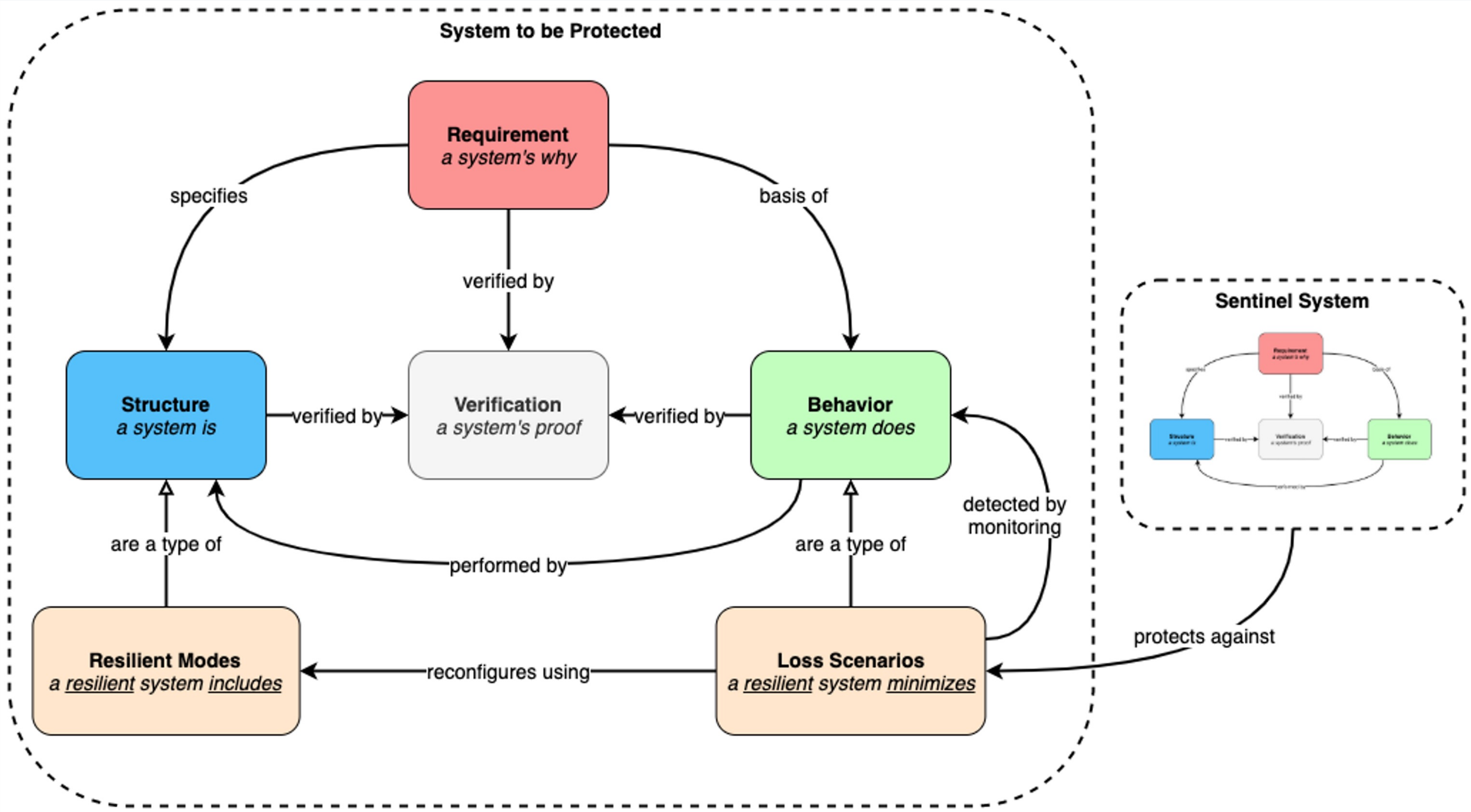
Distribution A - Cleared for Public Release by the Defense Office of Prepublication and Security Review, Case 23-S-0383, 10 November 2022

MA MBSE Meta-Model Building Blocks



Distribution A - Cleared for Public Release by the Defense Office of Prepublication and Security Review, Case 23-S-0383, 10 November 2022

Mission Aware Meta-Model: Top-Level



System to be Protected

Requirement
a system's why

specifies

basis of

verified by

Structure
a system is

verified by

Verification
a system's proof

verified by

Behavior
a system does

are a type of

performed by

are a type of

detected by monitoring

Resilient Modes
a resilient system includes

reconfigures using

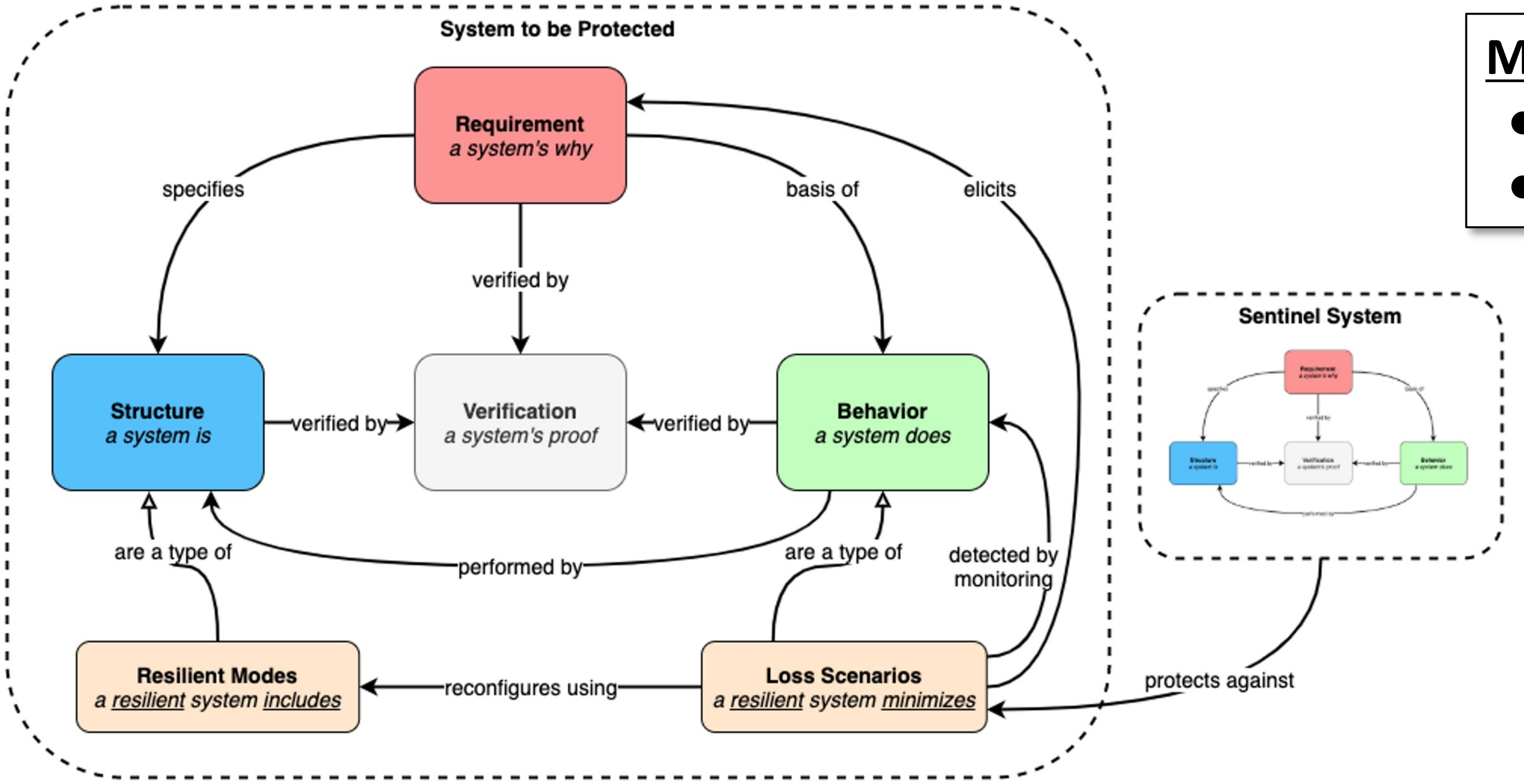
Loss Scenarios
a resilient system minimizes

Sentinel System

protects against

Distribution A - Cleared for Public Release by the Defense Office of Prepublication and Security Review, Case 23-S-0383, 10 November 2022

Systems Engineering Artifacts with FOREST Quality Attributes



FOREST: T.3:
a Loss Scenario reconfigures using Resilient Mode **Options** that provide *composability, availability,* and *safety*

FOREST: T.4:
A Resilient Mode is **Evaluated** for *availability, failure transparency, timeliness,* and *usability*
FOREST: T.5:
Operational **Confidence** in the Resilient Mode is rated for *learnability, predictability, repeatability* and *timeliness*
FOREST: T.6:
Operational **Readiness** for the Resilient Mode is rated by *adaptability, customizability,* and *timeliness*
FOREST: T.7:
Execution of the Resilient Mode is verified for *testability* and *timeliness*

FOREST: T.1:
a Loss Scenario is **Sensed** with *accuracy* and *timeliness*
FOREST: T.2:
a Loss Scenario is **Isolated** with *accuracy* and *timeliness*

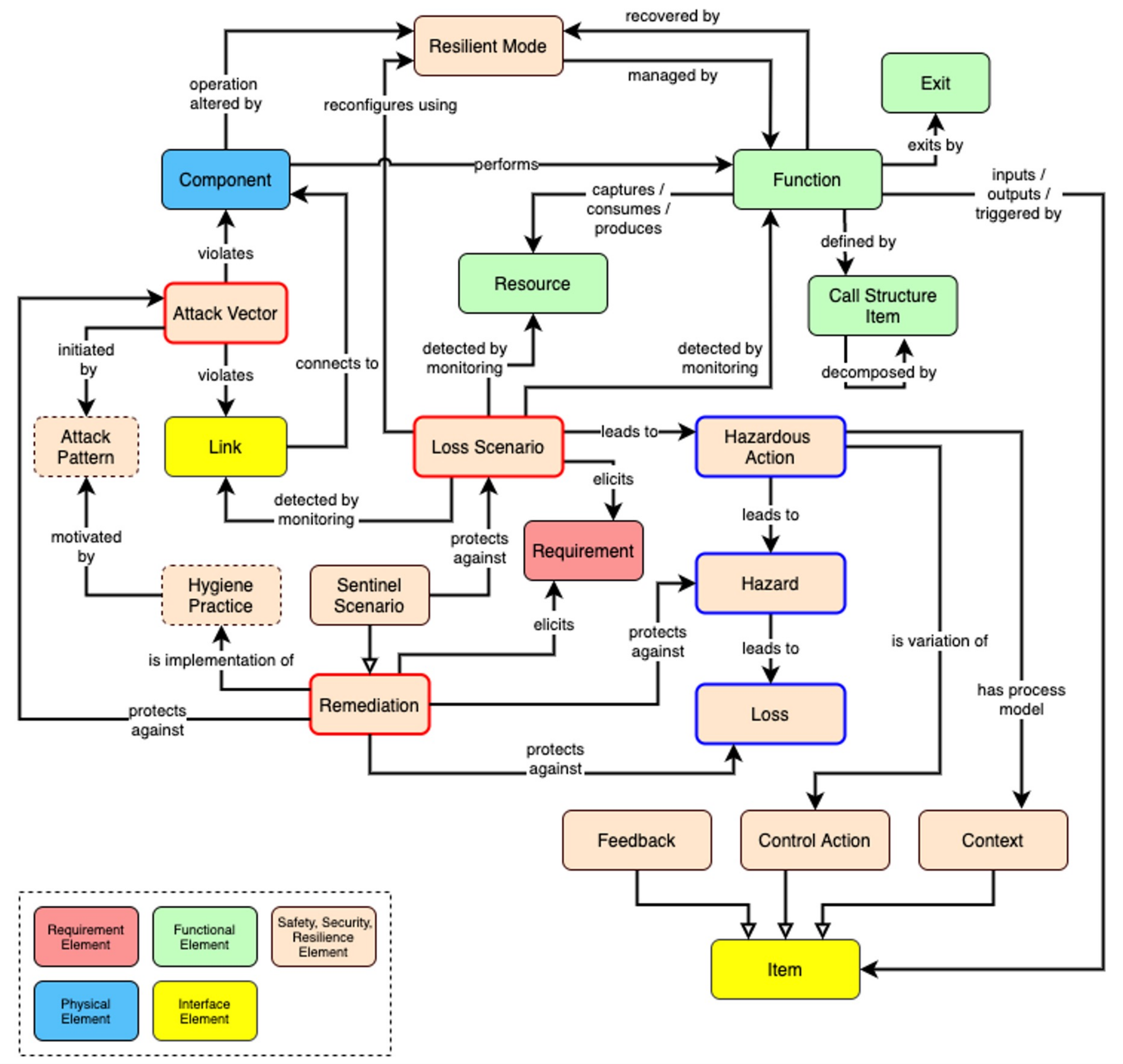
Mapping of Quality Attributes to:

- Loss Scenarios
- Resilient Modes

Understand Relationships to:

- Safety - Hazard Analysis
- Reliability Engineering

Mission Aware Meta-Model: Detail View



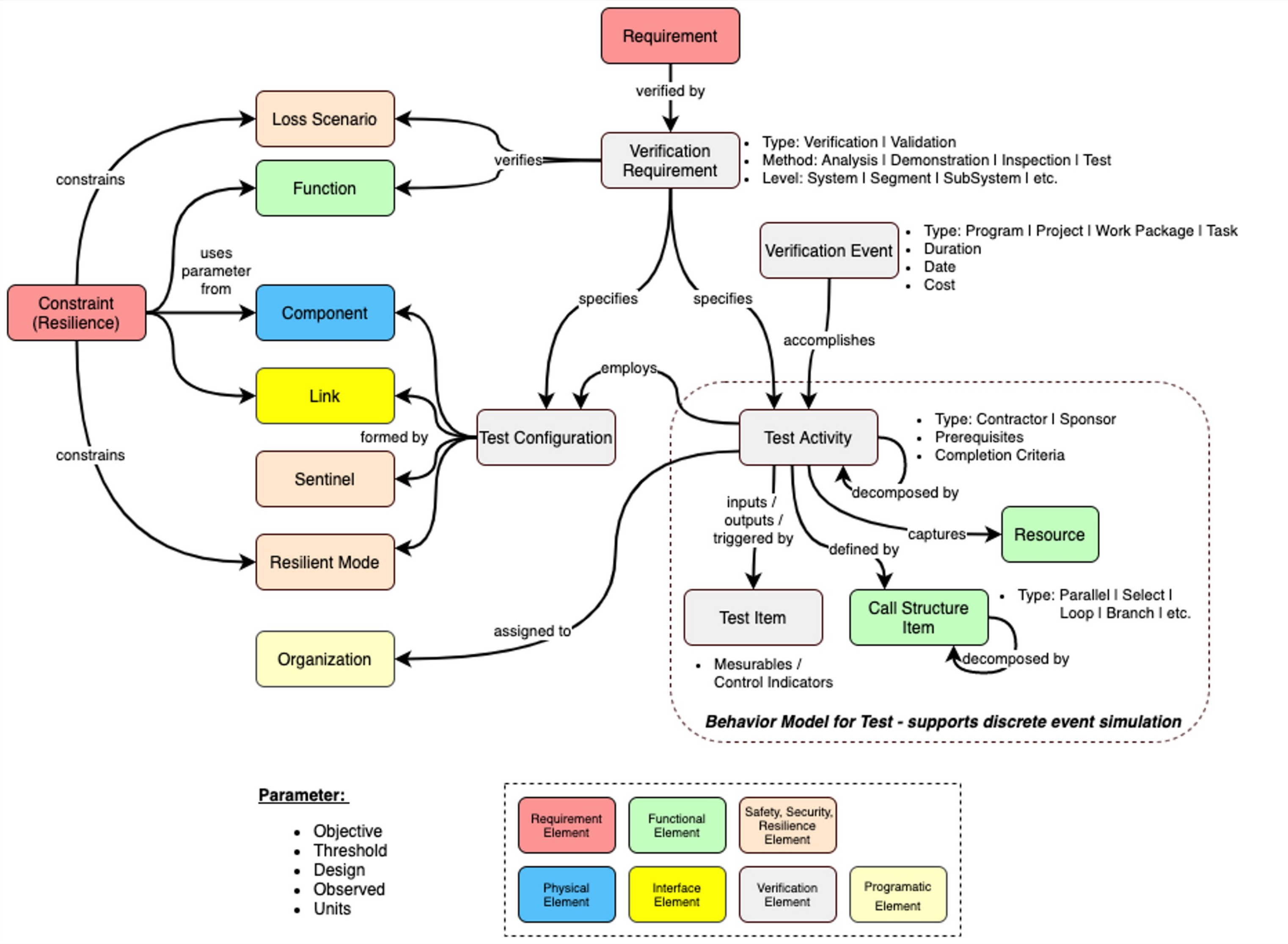
MISSION AWARE

CSRM Steps & Associated Meta-Model Entities:

1. System Description (Mission, Architecture, Behavior)
   - Use Case / Requirement
   - Component, Link
   - Function, Exit, Resource, Control-Action, Feedback, Context, Call Structure Item
2. Operational Risk Assessment
   - Loss, Hazard, Hazardous Action
3. Prioritized Resilience Solutions
   - Resilient Mode
4. Cyber Vulnerabilities Assessment
   - Loss-Scenario, Remediation, Elicited Requirements

Distribution A - Cleared for Public Release by the Defense Office of Prepublication and Security Review, Case 23-S-0383, 10 November 2022

Mission Aware Meta-Model: Verification & Test

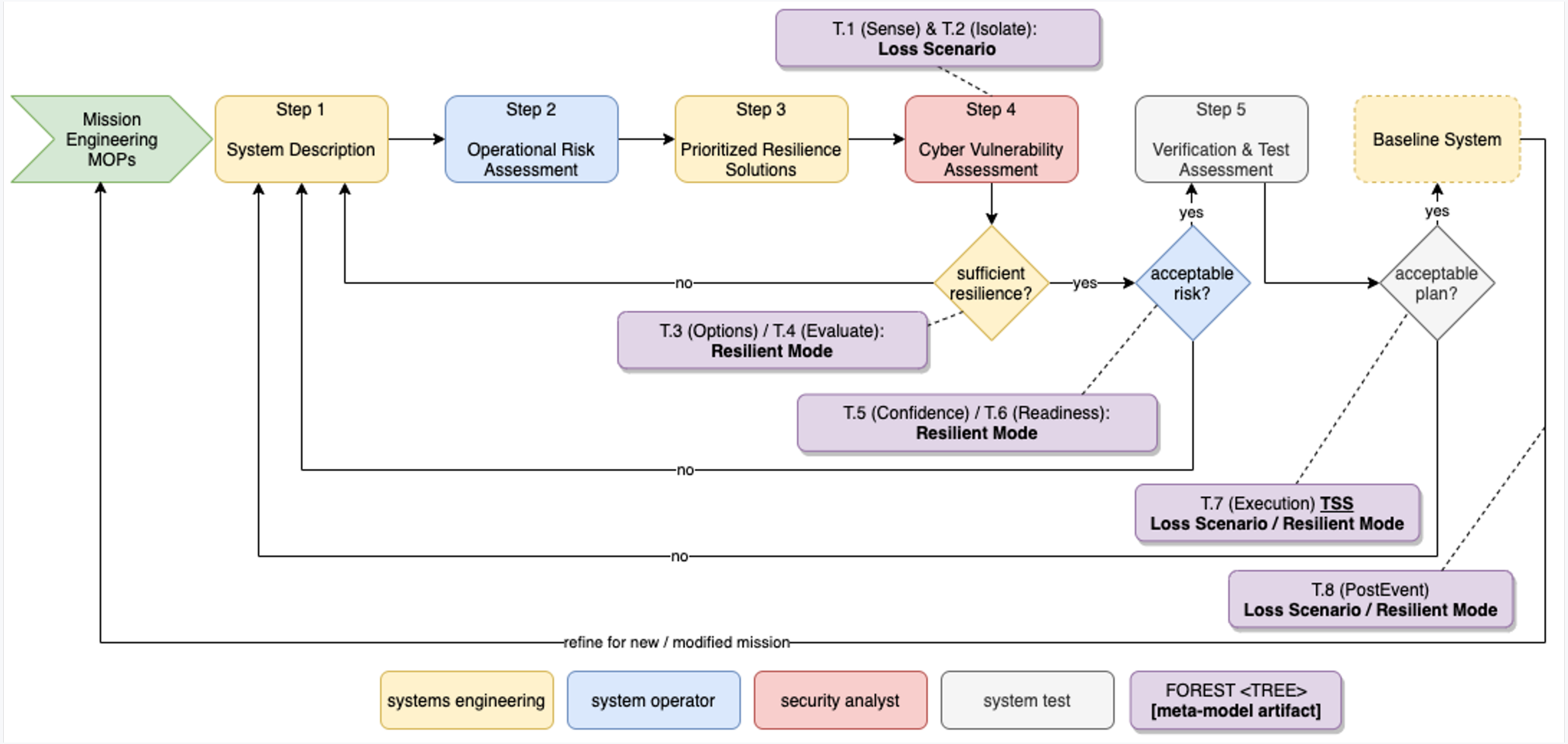


Verification & Test Meta-Model Details:

1. Verification Requirement
   - Function, Loss Scenario
2. Test Configuration
   - Component, Link, Resilient Mode, Sentinel
3. Verification Event / Test Activity
   - Test Plan / Strategy
   - Simulate Test Resource Utilization
   - Verify Resilience Constraints

Distribution A - Cleared for Public Release by the Defense Office of Prepublication and Security Review, Case 23-S-0383, 10 November 2022

Cyber Security Requirements Methodology (CSRM)



T.1 (Sense) & T.2 (Isolate):
Loss Scenario

Mission Engineering MOPs

Step 1
System Description

Step 2
Operational Risk Assessment

Step 3
Prioritized Resilience Solutions

Step 4
Cyber Vulnerability Assessment

Step 5
Verification & Test Assessment

Baseline System

sufficient resilience?

acceptable risk?

acceptable plan?

yes

no

T.3 (Options) / T.4 (Evaluate):
Resilient Mode

T.5 (Confidence) / T.6 (Readiness):
Resilient Mode

T.7 (Execution) **TSS**
Loss Scenario / Resilient Mode

T.8 (PostEvent)
Loss Scenario / Resilient Mode

refine for new / modified mission

systems engineering

system operator

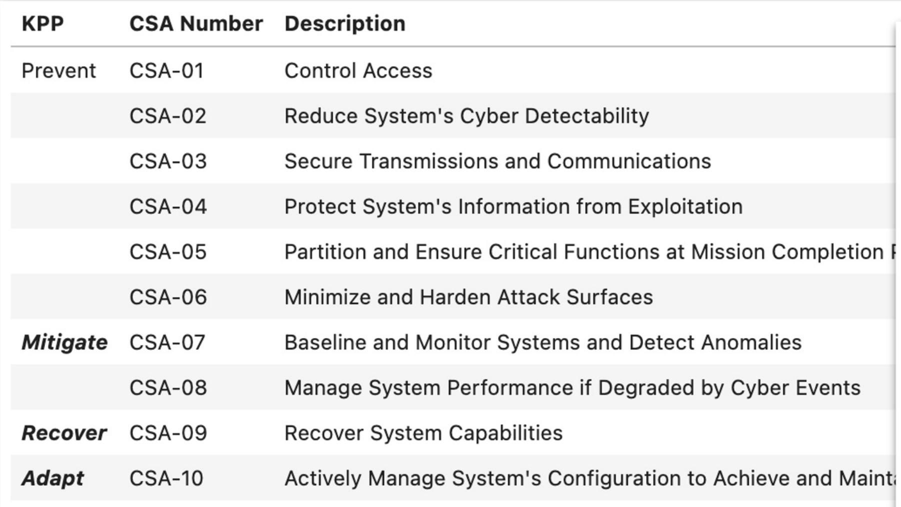
security analyst

system test

FOREST <TREE>
[meta-model artifact]

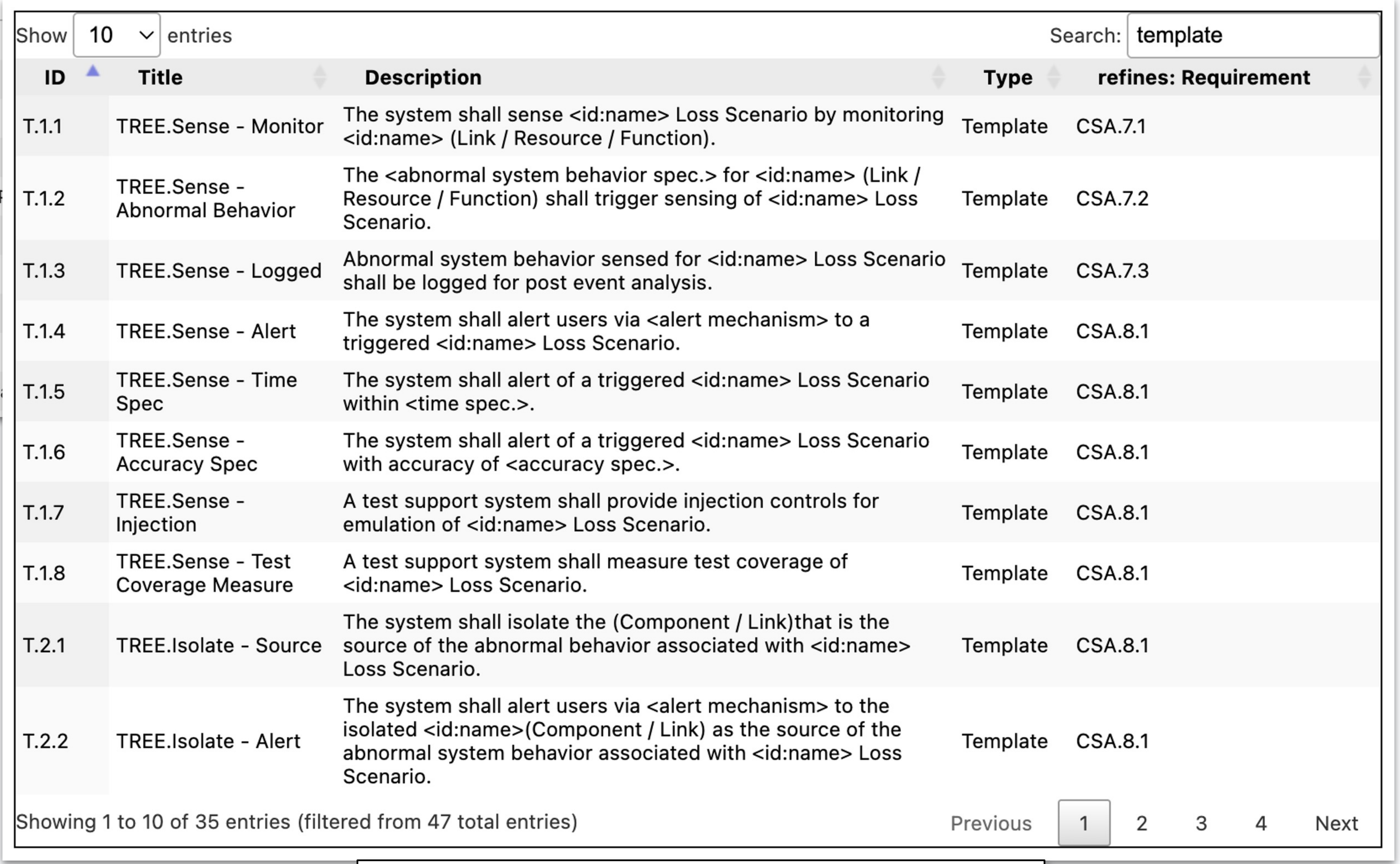
Resilience Requirement Templates

NATIONAL SECURITY INSTITUTE
VIRGINIA TECH.



KPP	CSA Number	Description
Prevent	CSA-01	Control Access
	CSA-02	Reduce System's Cyber Detectability
	CSA-03	Secure Transmissions and Communications
	CSA-04	Protect System's Information from Exploitation
	CSA-05	Partition and Ensure Critical Functions at Mission Completion P
	CSA-06	Minimize and Harden Attack Surfaces
Mitigate	CSA-07	Baseline and Monitor Systems and Detect Anomalies
	CSA-08	Manage System Performance if Degraded by Cyber Events
Recover	CSA-09	Recover System Capabilities
Adapt	CSA-10	Actively Manage System's Configuration to Achieve and Maint

Cyber Survivability Attributes - DoD Joint Staff



Show 10 entries

Search: template

ID	Title	Description	Type	refines: Requirement
T.1.1	TREE.Sense - Monitor	The system shall sense <id:name> Loss Scenario by monitoring <id:name> (Link / Resource / Function).	Template	CSA.7.1
T.1.2	TREE.Sense - Abnormal Behavior	The <abnormal system behavior spec.> for <id:name> (Link / Resource / Function) shall trigger sensing of <id:name> Loss Scenario.	Template	CSA.7.2
T.1.3	TREE.Sense - Logged	Abnormal system behavior sensed for <id:name> Loss Scenario shall be logged for post event analysis.	Template	CSA.7.3
T.1.4	TREE.Sense - Alert	The system shall alert users via <alert mechanism> to a triggered <id:name> Loss Scenario.	Template	CSA.8.1
T.1.5	TREE.Sense - Time Spec	The system shall alert of a triggered <id:name> Loss Scenario within <time spec.>.	Template	CSA.8.1
T.1.6	TREE.Sense - Accuracy Spec	The system shall alert of a triggered <id:name> Loss Scenario with accuracy of <accuracy spec.>.	Template	CSA.8.1
T.1.7	TREE.Sense - Injection	A test support system shall provide injection controls for emulation of <id:name> Loss Scenario.	Template	CSA.8.1
T.1.8	TREE.Sense - Test Coverage Measure	A test support system shall measure test coverage of <id:name> Loss Scenario.	Template	CSA.8.1
T.2.1	TREE.Isolate - Source	The system shall isolate the (Component / Link)that is the source of the abnormal behavior associated with <id:name> Loss Scenario.	Template	CSA.8.1
T.2.2	TREE.Isolate - Alert	The system shall alert users via <alert mechanism> to the isolated <id:name>(Component / Link) as the source of the abnormal system behavior associated with <id:name> Loss Scenario.	Template	CSA.8.1

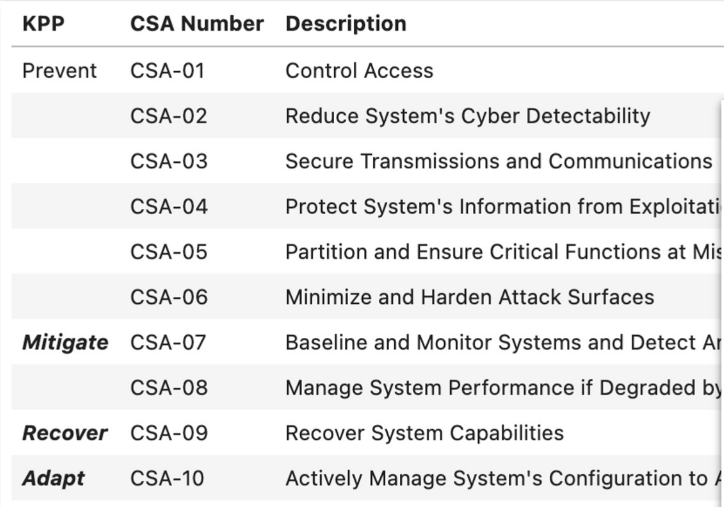
Showing 1 to 10 of 35 entries (filtered from 47 total entries)

Previous 1 2 3 4 Next

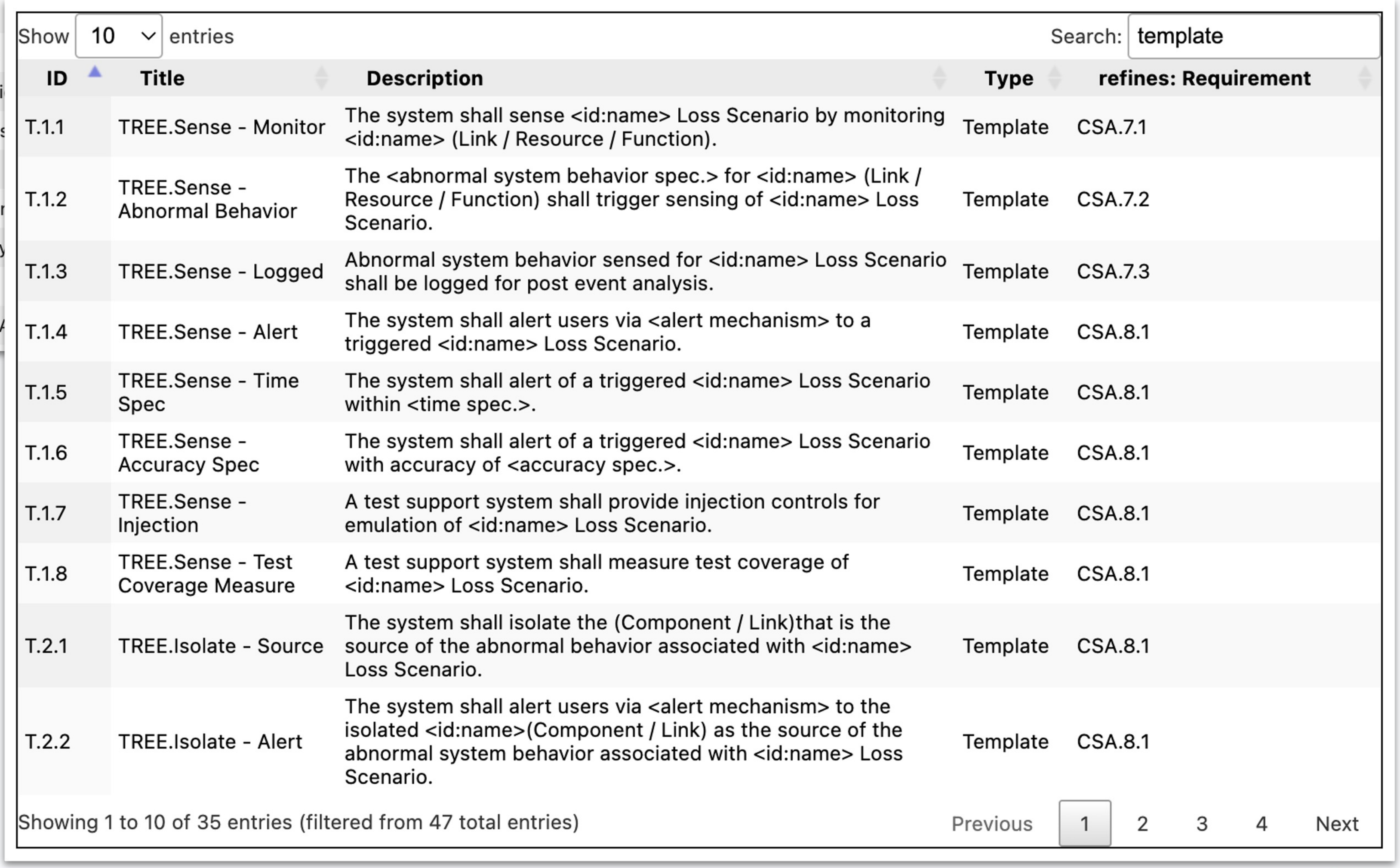
TREE-based Requirement Templates

Distribution A - Cleared for Public Release by the Defense Office of Prepublication and Security Review, Case 23-S-0383, 10 November 2022

Resilience Requirement Templates



KPP	CSA Number	Description
Prevent	CSA-01	Control Access
	CSA-02	Reduce System's Cyber Detectability
	CSA-03	Secure Transmissions and Communications
	CSA-04	Protect System's Information from Exploitati
	CSA-05	Partition and Ensure Critical Functions at Mis
	CSA-06	Minimize and Harden Attack Surfaces
Mitigate	CSA-07	Baseline and Monitor Systems and Detect Ar
	CSA-08	Manage System Performance if Degraded by
Recover	CSA-09	Recover System Capabilities
Adapt	CSA-10	Actively Manage System's Configuration to A



Show 10 entries

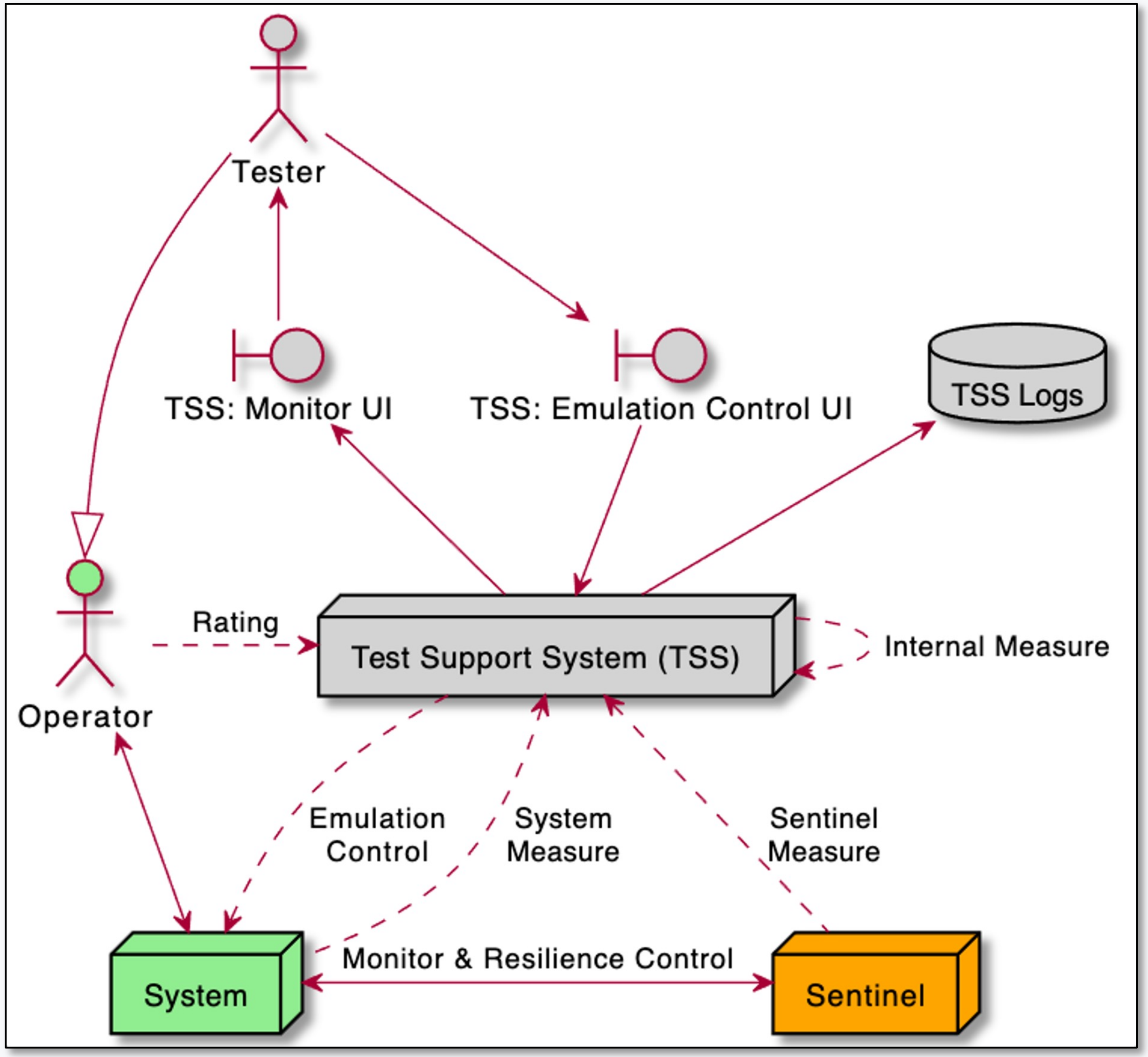
Search: template

ID	Title	Description	Type	refines: Requirement
T.1.1	TREE.Sense - Monitor	The system shall sense <id:name> Loss Scenario by monitoring <id:name> (Link / Resource / Function).	Template	CSA.7.1
T.1.2	TREE.Sense - Abnormal Behavior	The <abnormal system behavior spec.> for <id:name> (Link / Resource / Function) shall trigger sensing of <id:name> Loss Scenario.	Template	CSA.7.2
T.1.3	TREE.Sense - Logged	Abnormal system behavior sensed for <id:name> Loss Scenario shall be logged for post event analysis.	Template	CSA.7.3
T.1.4	TREE.Sense - Alert	The system shall alert users via <alert mechanism> to a triggered <id:name> Loss Scenario.	Template	CSA.8.1
T.1.5	TREE.Sense - Time Spec	The system shall alert of a triggered <id:name> Loss Scenario within <time spec.>.	Template	CSA.8.1
T.1.6	TREE.Sense - Accuracy Spec	The system shall alert of a triggered <id:name> Loss Scenario with accuracy of <accuracy spec.>.	Template	CSA.8.1
T.1.7	TREE.Sense - Injection	A test support system shall provide injection controls for emulation of <id:name> Loss Scenario.	Template	CSA.8.1
T.1.8	TREE.Sense - Test Coverage Measure	A test support system shall measure test coverage of <id:name> Loss Scenario.	Template	CSA.8.1
T.2.1	TREE.Isolate - Source	The system shall isolate the (Component / Link)that is the source of the abnormal behavior associated with <id:name> Loss Scenario.	Template	CSA.8.1
T.2.2	TREE.Isolate - Alert	The system shall alert users via <alert mechanism> to the isolated <id:name>(Component / Link) as the source of the abnormal system behavior associated with <id:name> Loss Scenario.	Template	CSA.8.1

Showing 1 to 10 of 35 entries (filtered from 47 total entries)

These requirements do not measure resilience, but they measure components to inform an **Evaluation** of resilience when combined with other test data

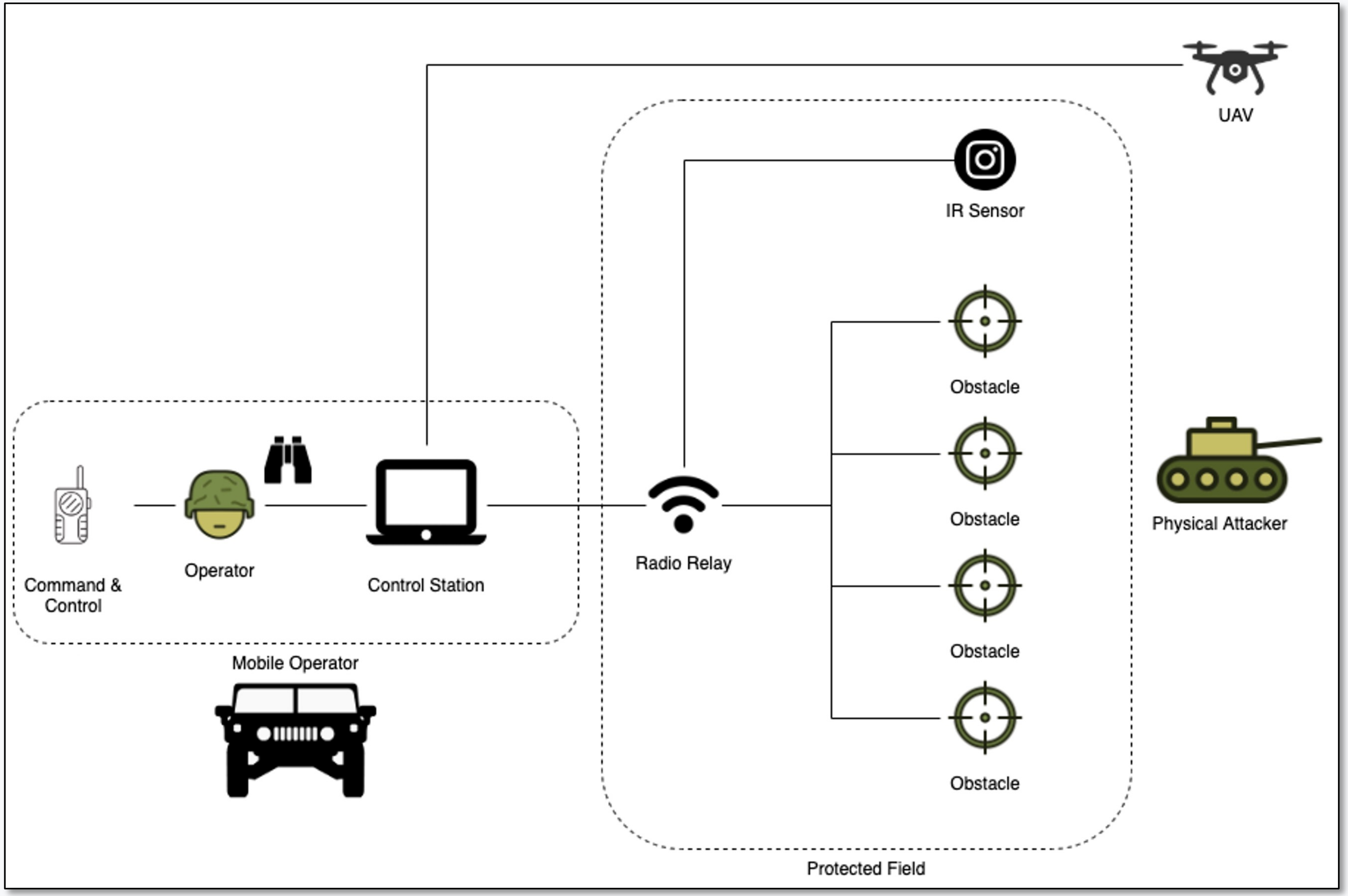
Cyber Resilience Test - Reference Architecture



- Many standard tests can be done through manipulation of the external environment

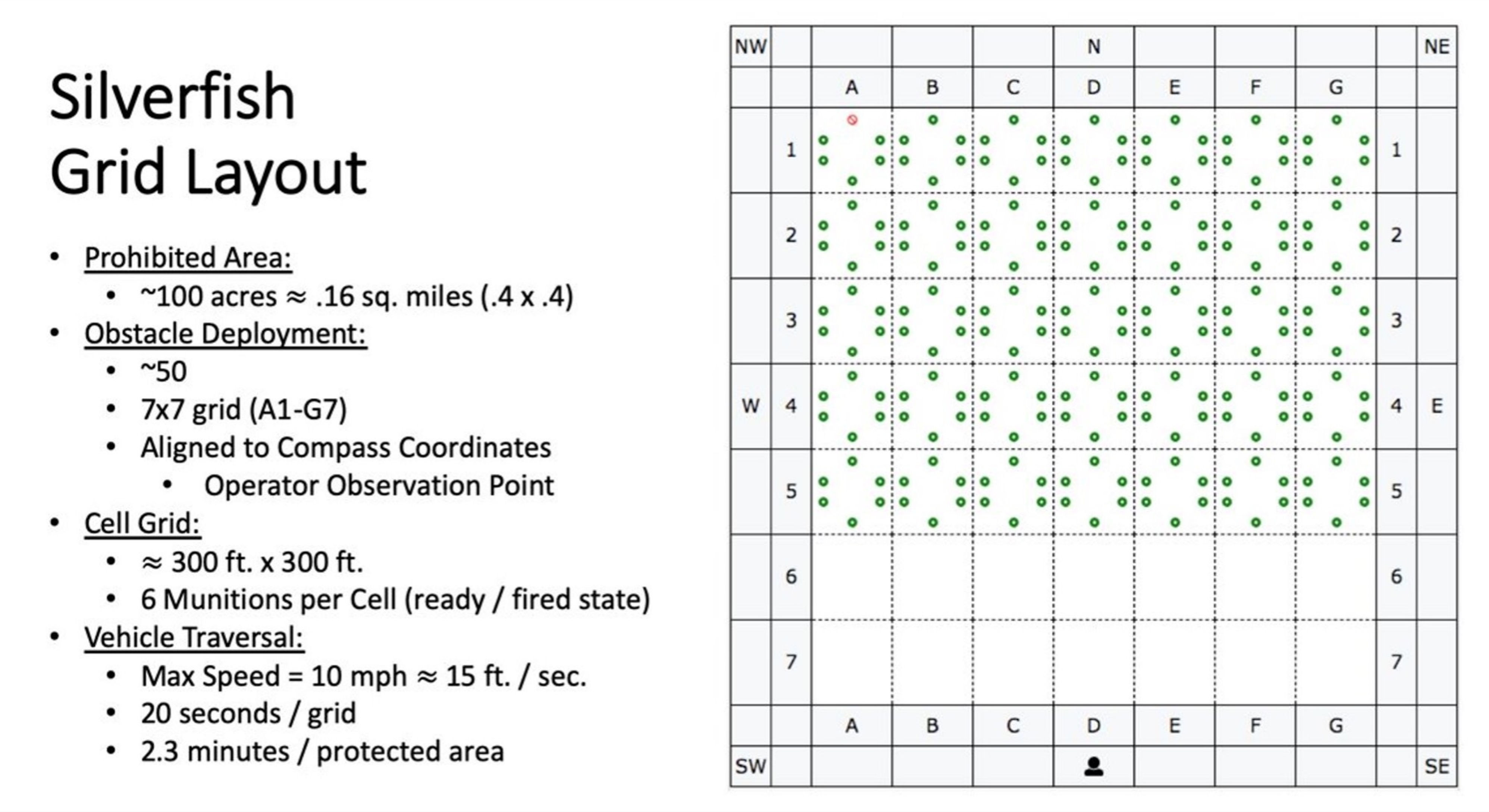
- Resilience tests require manipulation of the system's internal states

Silverfish Case Study



Distribution A - Cleared for Public Release by the Defense Office of Prepublication and Security Review, Case 23-S-0383, 10 November 2022

Silverfish User Interface

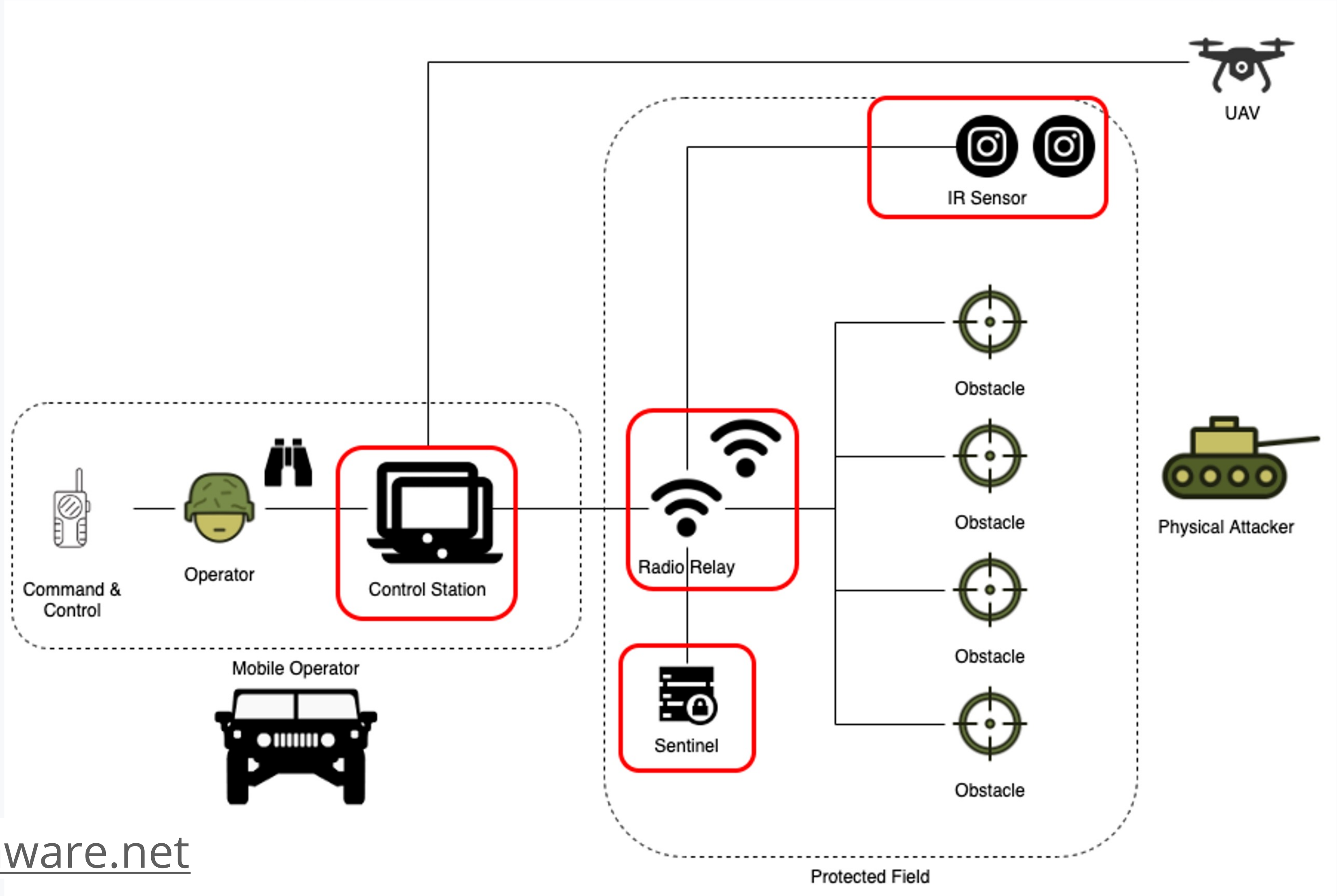


Silverfish Grid Layout

- Prohibited Area:
  - ~100 acres ≈ .16 sq. miles (.4 x .4)
- Obstacle Deployment:
  - ~50
  - 7x7 grid (A1-G7)
  - Aligned to Compass Coordinates
    - Operator Observation Point
- Cell Grid:
  - ≈ 300 ft. x 300 ft.
  - 6 Munitions per Cell (ready / fired state)
- Vehicle Traversal:
  - Max Speed = 10 mph ≈ 15 ft. / sec.
  - 20 seconds / grid
  - 2.3 minutes / protected area

Distribution A - Cleared for Public Release by the Defense Office of Prepublication and Security Review, Case 23-S-0383, 10 November 2022

Silverfish Architecture – Resilient Modes



https://mission-aware.net

Distribution A - Cleared for Public Release by the Defense Office of Prepublication and Security Review, Case 23-S-0383, 10 November 2022

WRT-1072: ongoing Pilot on Major Program

- Decompose and translate weapon system's mission resilience requirements and performance; define measurable and testable metrics
  - Flow-down, map, and de-conflict security requirements from the CSAs down to functional and technical / performance requirements
  - Validate system's mission resilience requirements decomposition process and measurable and testable metrics development approach
- Define and implement resilience patterns that meet resilience requirements
  - Categorize resilience based on the functional design and performance requirements
  - Define and demonstrate resilience design and development approach through digital modeling and engineering
- Assess resilience designs
  - Demonstrate mission-based cyber risk assessments, digital engineering, modeling, dynamic simulation approaches, and automated analytics
  - Maturity review and recommendations for MBSE/simulation capabilities to effectively categorize resiliency requirements and simulate cyber offensive/defensive capabilities

Identify best practices, methods, and tools

Distribution A - Cleared for Public Release by the Defense Office of Prepublication and Security Review, Case 23-S-0383, 10 November 2022

Milestones

Milestone	Date
□ Technical exchanges with team & community	Ongoing
▪ Program Office	
▪ MITRE	
▪ SS – OUSD(R&E)	
▪ Joint Staff J6	
▪ JHU APL	
□ Select engagement with broad cyber resilience community	
□ Derivation of requirements, measure & metrics using FOREST	March 2023
□ Technical Approaches to identification of solutions	July 2023
□ Identify best practices, methods, and tools; reporting	November 2023

Shifting the Traditional Testing Paradigm to a "Testing Continuum"

Capability And Outcome Focused Testing

"Shift left" – Incorporates Mission Context Early
Alignment with mission threads /GRA – "effects" chains
Mission-focused cyber testing for Operational Resilience
Prioritize critical functionality

Incorporate Mission Context early to improve design, development, and testing, and identify system performance aspects most critical to success in combat; Keep the "end in mind" of desired capability; "Test like we fight" accounting for CONOPS evolution – capability effects evolving to mission/system effects; Focus Cyber contribution on Operational Resilience vs. selective vulnerability mitigation.

Agile, Scalable Framework

Improved focus on decisions space
Focused best design
Modernized SW Test
Adapting/Evolving Systems (AI/ML)

An "agile, scalable" model-based evaluation framework is responsive to Decision Space updates/evolution as tech matures, CONOPS evolve, and Acq Milestones progress; Enables clear alignment of Test (Data) to Evaluation (Information) in the Decision Space; Includes model validation and accreditation data gathering within the framework.

Enhanced Test Design

Leverage Integrated Test
Statistical Analyses
Integrated model libraries
Authoritative Data

Establishes clear linkage of early engineering and technology validation testing with desired operational testing outcomes; Enables effective "iterative" testing for the continuum of decision space; Develops responsive human to system integration for evolving and adapting systems; Use of STAT techniques essential in focusing test design considerations for complex systems.

Live, Virtual, Constructive (LVC) Environment

"Integrated M&S VV&A
Consistent threat and environment updates
Federated System-of-System Models
Authoritative Digital Models – complex systems

M&S increases in visibility as a critical component of overall test programs, including increased use of complex LVC capabilities and stronger integration of M&S VV&A activities into the evaluation framework. Early investment & validation of Live, Virtual, and Constructive (LVC) environments supports assessment of system performance against increasingly complex threats that cannot be replicated in live testing, as well as increases confidence in system effectiveness.

Model Based Environment

Management of data complexity / KM
Automated test and analysis
Authoritative Data / Transparency
Digital Twins

Model based environment enables development of "digital thread" from early Capability Model to deployed Digital Twin; Increases application of automated test and analysis; Aids development of new "model-test-validate" paradigm; Supports integration of SoS level capabilities with required Model Validation Levels (MVL) assessment framework. Knowledge Management infrastructure critical for managing data complexity.

"Digital" Workforce

Transformation - adaptive, evolving
Focused domain "credentialing"
MBSE/MBTE
Iterative SW/DevSecOps

Increased set of skills and model-based context required to address iterative development and testing; Ubiquitous coupling and alignment with SE community; Focuses on targeted "credentialing" to ensure relevant, up-to-date context for evolving model-based domain; Adaptation and evolution of the Engineering and T&E workforce ensures the successful implementation of these concepts within this new T&E continuum.

Q & A

NATIONAL SECURITY INSTITUTE
VIRGINIA TECH

SYSTEMS ENGINEERING RESEARCH CENTER

THANK YOU

| Stay connected with us online.

Distribution A - Cleared for Public Release by the Defense Office of Prepublication and Security Review, Case 23-S-0383, 10 November 2022