SYSTEMS ENGINEERING RESEARCH CENTER

# Developmental Test and Evaluation and Cyberattack Resilient Systems

WRT-1022

Ms. Sarah Standard, OUSD(R&E)

Dr.  Peter Beling, Virginia Tech

NATIONAL SECURITY INSTITUTE
VIRGINIA TECH

ANNUAL RESEARCH REVIEW 2022

# Contents

- Motivation: Cyberspace Threats
- Resilience: Definitions and Challenge
- Toward a Solution
    - Measuring Anything Implies Defined Requirements
    - Cyber Survivability Attributes
    - Resilience Requires Engineering
    - Mission Based Cyber Risk Assessments
    - Requirements & Technical Performance Measures
    - Framework for Operational Resilience in Engineering and System Test (FOREST)
    - Resilience Requirements Templates
    - Case Study & Pilot Program

# Research Team

Virginia Tech

- Peter Beling
- Tim Sherburne

Stevens Institute of Technology

- Tom McDermott
- Megan Clifford

University of Virginia

- Barry Horowitz
- Cody Fleming

Related Prior SERC Projects

- WRT-1022: Developmental Test and Evaluation and Cyberattack Resilient Systems
- 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

Distribution A - Cleared for Public Release by the Defense Office of Prepublication and Security Review, Case 23-S-0384, 10 November 2022

# 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-0384, 10 November 2022

# Motivation: Cyberspace Threats

- Acquisition programs historically do not
  - Perform analysis for cyberspace threats as other threats in system engineering
  - Define system cyber performance (survivability or resilience) requirements
    - Only focus is on Risk Management Framework (RMF) activities
    - RMF controls are usually not in the performance specification or required to be tested against a representative cyberspace threat
    - Don't consider cyberspace threat to mission and mission defenders detection and recover needs when performing requirement analysis
  - Involve test organizations early to inform system engineering designs, prototypes, testing, and requests for proposals (RFPs)
  - Require cyber test and evaluation (T&E) by contractors
    - Programs only require contractors to support the program's RMF activities separately from engineering activities
  - Resource and perform adequate government cyber developmental T&E
    - Government cyber T&E occurs after the system design is completed, and often only during Operational T&E without resourcing or schedule to fix issues
- Snapshot, non-comprehensive, effect-restricted operational T&E routinely finds systems are not survivable or operationally resilient in a contested cyber environment
  - Over time, survivability and resilience degrade while cyber threats improve
    - Need sustainment cyber T&E that includes "hunting"

# 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 <u>and measure</u> the system's attributes, performance, and resulting effects.

It also means testing must take into account whether a "<u>defender's</u>" actions are required to resist, absorb, recover from or adapt to the adversity.

**Definitions** (for this discussion)

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

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

<u>Operational Resilience</u>: 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 23-S-0384, 10 November 2022

# Toward a Solution

- 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 23-S-0384, 10 November 2022

# Measuring Anything Implies Defined Requirements

- Typical cyber requirements are security controls that do not relate directly to mission capability or defender response
  - US DoD has the Joint Staff Cyber Survivability Endorsement (CSE) to the System Survivability Key Performance Parameter (SSD KPP)

    The SS KPP is mandatory for DoD joint systems
  - CSE requirements are ten (10) Cyber Survivability Attributes (CSAs) associated with a Cyber Survivability Risk Category (CSRC)
    - System Mission Type (Strategic, Operational, Tactical, Mission Support, Other)
    - Expected level of threat (Extreme, Advanced, Moderate, Limited, Nascent)
    - Dependency Level, i.e. interoperability (Extreme, High, Moderate, Low, Very Low)
    - Impact of Loss (Catastrophic, Severe, Moderate, Limited, Negligible)
  - Five CSRC levels (1-5)
    - Selected tailored CSAs are written with detailed system requirements Includes defender requirements

Distribution A - Cleared for Public Release by the Defense Office of Prepublication and Security Review, Case 23-S-0384, 10 November 2022

# Cyber Survivability Attributes

| SS KPP Pillars<br>(Mandatory) | Cyber Survivability Attributes (CSAs)<br>(All are to be considered; select those that are applicable) |
|---|---|
| **Prevent** | **CSA 01 - Control Access** |
| | **CSA 02 - Reduce Cyber Detectability** |
| | **CSA 03 - Secure Transmissions and Communications** |
| | **CSA 04 - Protect Information and Exploitation** |
| | **CSA 05 - Partition and Ensure Critical Functions at Mission Completion Performance Levels** |
| | **CSA 06 - Minimize and Harden Cyber Attack Surfaces** |
| **Mitigate** | **CSA 07 - Baseline & Monitor Systems, and Detect Anomalies** |
| | **CSA 08 - Manage System Performance if Degraded by Cyber Events** |
| **Recover** | **CSA 09 - Recover System Capabilities** |
| **Adapt for Prevent, Mitigate & Recover** | **CSA 10 - Actively Manage System's Configurations to Achieve and Maintain an Operationally Relevant Cyber Survivability Risk Posture (CSRP) … applicable to legacy systems that did not consider CSAs during development …** |

Resilience Starts Here

**Fundamental to CSE construct is selecting CSAs to achieve and maintain each Pillar --**
**# CSAs Expected for CSRC-5: 9-10, CSRC-4: 6-9, CSRC-3: 5-7, CSRC-2: 2-5, CSRC-1: 1-3**

Distribution A - Cleared for Public Release by the Defense Office of Prepublication and Security Review, Case 23-S-0384, 10 November 2022

# CSA 7 and 8 Exemplars

- CSA 7 – Mitigate
  - Baseline and Monitor Systems and Detect Anomalies
    - System shall monitor, detect and report system health status and anomalies indicative of cyber events to the defender, maintainer, or operator
    - System shall report whether the actual system runtime configuration is the intended system runtime configuration
    - Operator/ defender can determine that the configuration of the system, when operating in all its states and modes and while transitioning between all its states and modes, accurately reflects the intended system configuration
    - System must provide defender / maintainers /operator reports of anomalies such as configuration changes, cyber-related event indicators, slowed processing, or loss of functionality within T = (# of seconds/minutes) [specified by sponsor].
- CSA 8 – Mitigate
  - Manage System Performance if Degraded by Cyber Events
    - System shall be sufficiently resilient to mitigate cyber-event effects through orderly, structured and prioritized system responses, in order to ensure minimum mission essential functionality requirements [specified] to complete the current mission or return for recovery; responds asymmetrically to cyber-events in real time
    - System "playbook" shall provide mission commander / defender intervention processes to prioritize critical system functions to maintain an acceptable level of performance under adverse conditions, including the ability to selectively disconnect/disable subsystems that are not critical as well as isolate the system from integrated platform systems

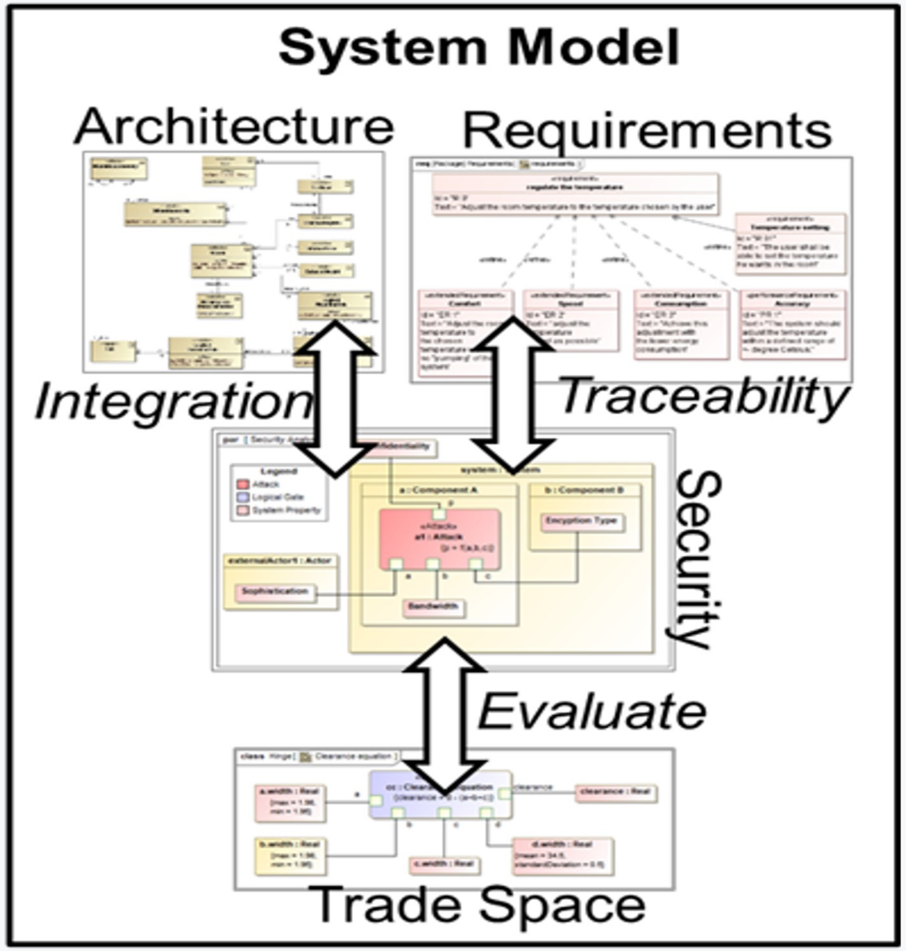
Distribution A - Cleared for Public Release by the Defense Office of Prepublication and Security Review, Case 23-S-0384, 10 November 2022

# CSA 9 and 10 Exemplars

- CSA 9 – Recover
  - Recover System Capabilities
    - After a cyber-event, the system shall be capable of being restored to full functionality from a trusted source; at a minimum, being restored to partial mission capability, between mission cycles or within [xx] hours [specified by sponsor]
    - System recovery shall prioritize cyber operational resiliency functions
- CSA 10 – Adapt
  - Actively Manage System's Configurations to Achieve and Maintain an Operationally Relevant Cyber Survivability Risk Posture (CSRP)
    - System must have a configuration management process, supported by automated capabilities and technology refresh options, to achieve and continuously maintain an objectively assessed and operationally-relevant risk posture
      - The process shall include inputs from operators, defenders and intel analysts to continuously assess changes in adversary threat, and include a machine readable Bill of Materials (BOM) of the system's GOTS/COTS HW, SW, FW including all dependencies on open source modules for a supply chain risk assessment prior to each milestone decision and supported release

Distribution A - Cleared for Public Release by the Defense Office of Prepublication and Security Review, Case 23-S-0384, 10 November 2022

# Resilience Requires Engineering



- CSAs are high level requirements
  - Engineers need lower level measurable requirements to demonstrate progress toward threshold during development
- Engineers must define performance specifications (P-spec) that articulate CSA as requirements for performance in cyberspace
  - No cookie cutter controls here!
  - Flow-down, map, and de-conflict security requirements (including technology and program protection) from the Cyber Survivability KPPs down to functional and technical/performance requirements
- Contractor must be required to decompose P-spec into lower levels and government must support scope with mission and threat context
  - Define Technical Performance Measures (TPMs) that trace to P-Spec
  - DoD uses Mission Based Cyber Risk Assessments (MBCRAs)

# Requirements & Technical Performance Measure

- Requirements should be
  - Measurable (quantifiable)
  - Unambiguous
  - Discreet
  - Bounded
  - Accurate/correct
  - Complete
  - Orthogonal
  - Well defined
  - Relevant and Traceable (to the mission)
  - Achievable (contractually)
  - Independently verifiable and repeatable (“testable”)

- Technical Performance Measures (TPMs) should be
  - Quantitative or qualitative
  - Unique to system functions
  - Relevant to Mission
  - Easily Measurable/Assessable
  - Robust to Varying Test Conditions
  - Orthogonal

TPMs must

- Enable assessing implementation of system attributes
- Cover Data Needs

**Requirements & Metrics guide effective cyber testing**

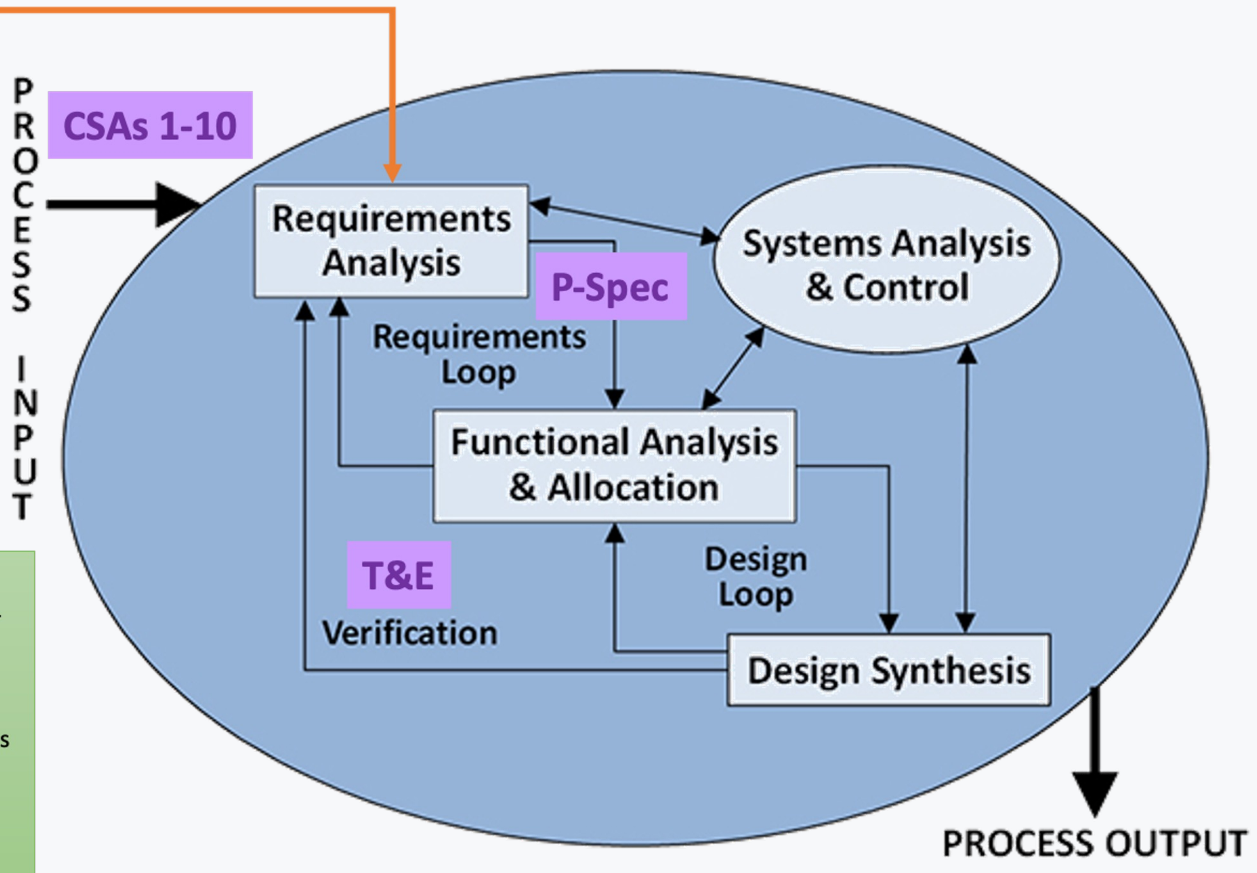
# What is a Mission Based Cyber Risk Assessment (MBCR

- The process of identifying, estimating, and prioritizing risks to DoD operational missions resulting from cyber effects on the system(s) being employed in support of the missions
- MBCRAs conducted early in the system lifecycle inform concept selection and design, later MBCRAs track system progress and inform specific test event planning
- MBCRA at a minimum should include these outcomes:
  - Characterize the attack surface and potential attack paths through the system
  - Identify potential vulnerabilities (susceptibilities)
  - Provide actionable, prioritized, human-understandable recommendations to address the identified potential vulnerabilities that are of concern (e.g., requirements, remediation, and/or mitigations)
  - Generate operationally representative cyberspace attack scenarios

# MBCRA in Systems Engineering Processes Model

**Requirements Analysis Process**

- Analyze capability and adversity driven by mission, operations, sustainment and environments
- Identify functional requirements
- Define performance and design constraint requirements



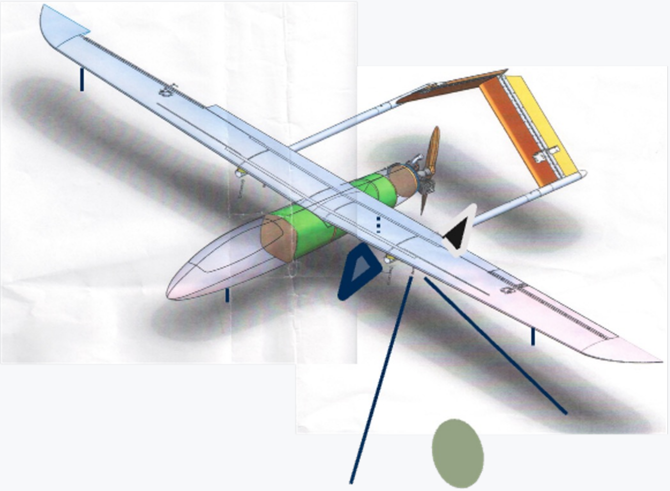
## MBCRA Informs Engineering and Test

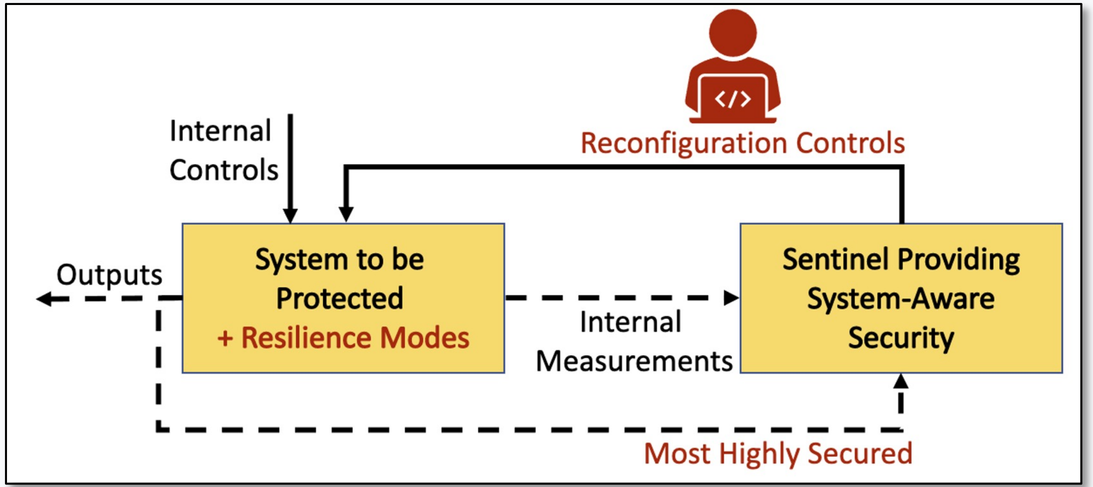
- Identify the mission essential functions and the MBCRA in-scope system critical components
- Map mission dependence at the component, system, and mission thread level
- Determine how the expected threat adversary could access the system and exploit mission critical functions
- Characterize and prioritize attacks for testing based on mission criticality
- Generate attack scenarios for test
- Recommend remediation or mitigations

Distribution A - Cleared for Public Release by the Defense Office of Prepublication and Security Review, Case 23-S-0384, 10 November 2022

# 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.





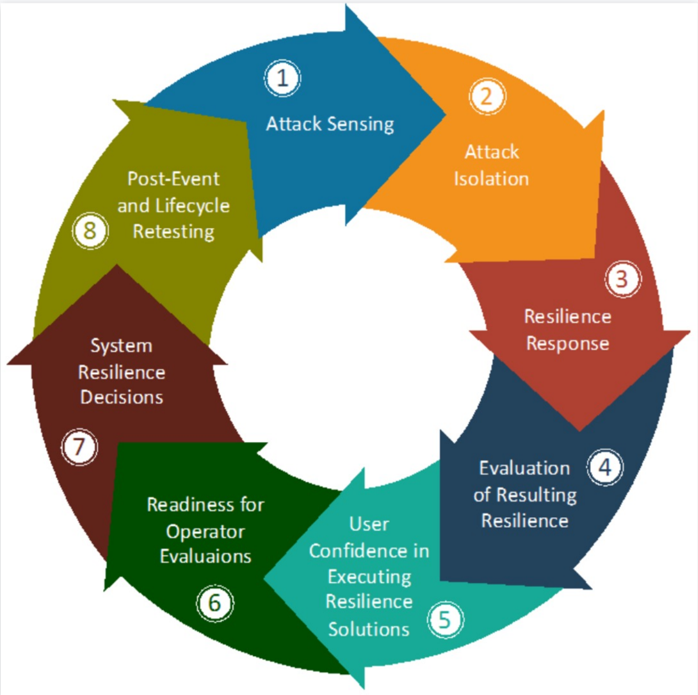
Distribution A - Cleared for Public Release by the Defense Office of Prepublication and Security Review, Case 23-S-0384, 10 November 2022

# Framework for Operational Resilience in Engineering and Systems Test (FOREST)

- To be effective in resilience engineering, we must be able to reason about:
- system functions, tasks and missions
- how systems operate as they undergo adversity and response
- the role of defenders
  - 8-TREE (Testable Requirements Elicitation Elements) in FOREST that relate to the evaluation of resilient systems during tests
  - Provides early validation that operational designs are addressing corresponding T&E needs for assuring that mission and system objectives are being satisfied
  - Focused on supporting operator and defender post cyberspace attack or amidst a cyber event

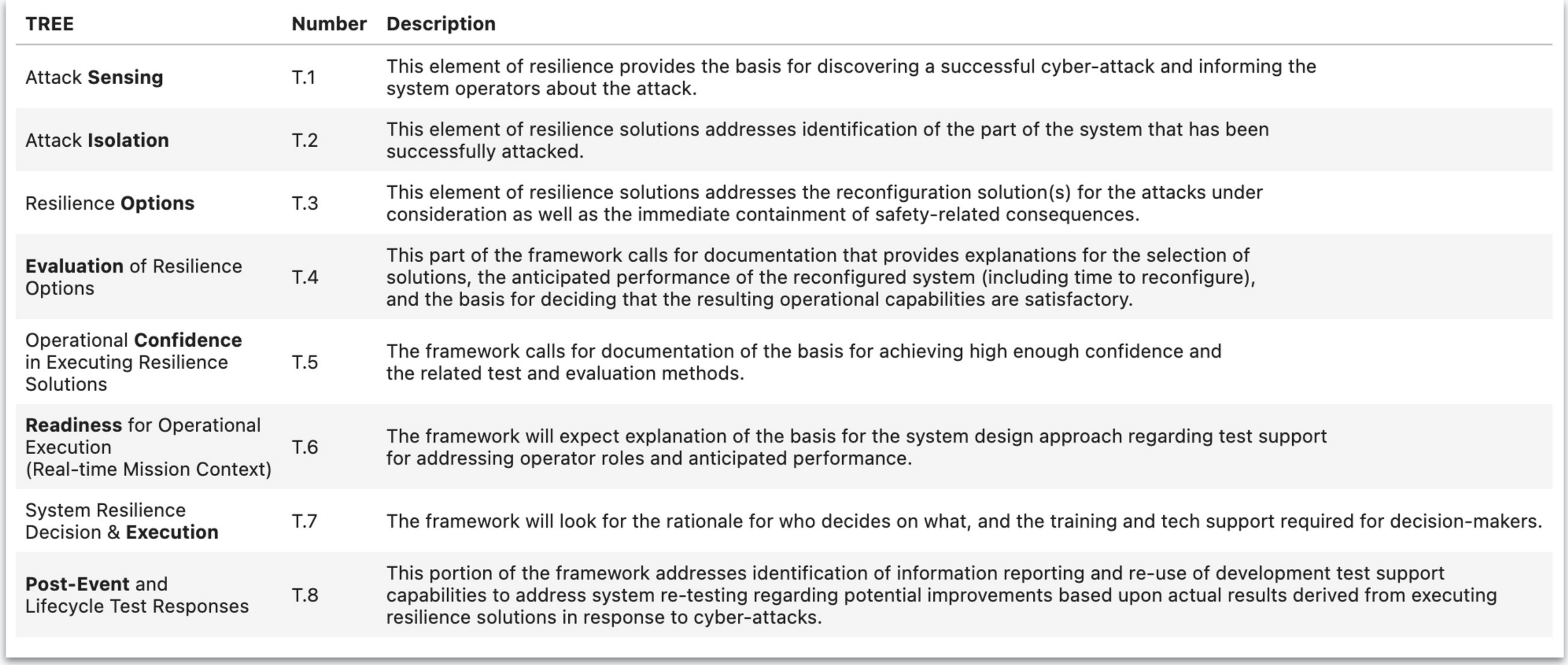
- A work in progress… pilot project ongoing

# 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

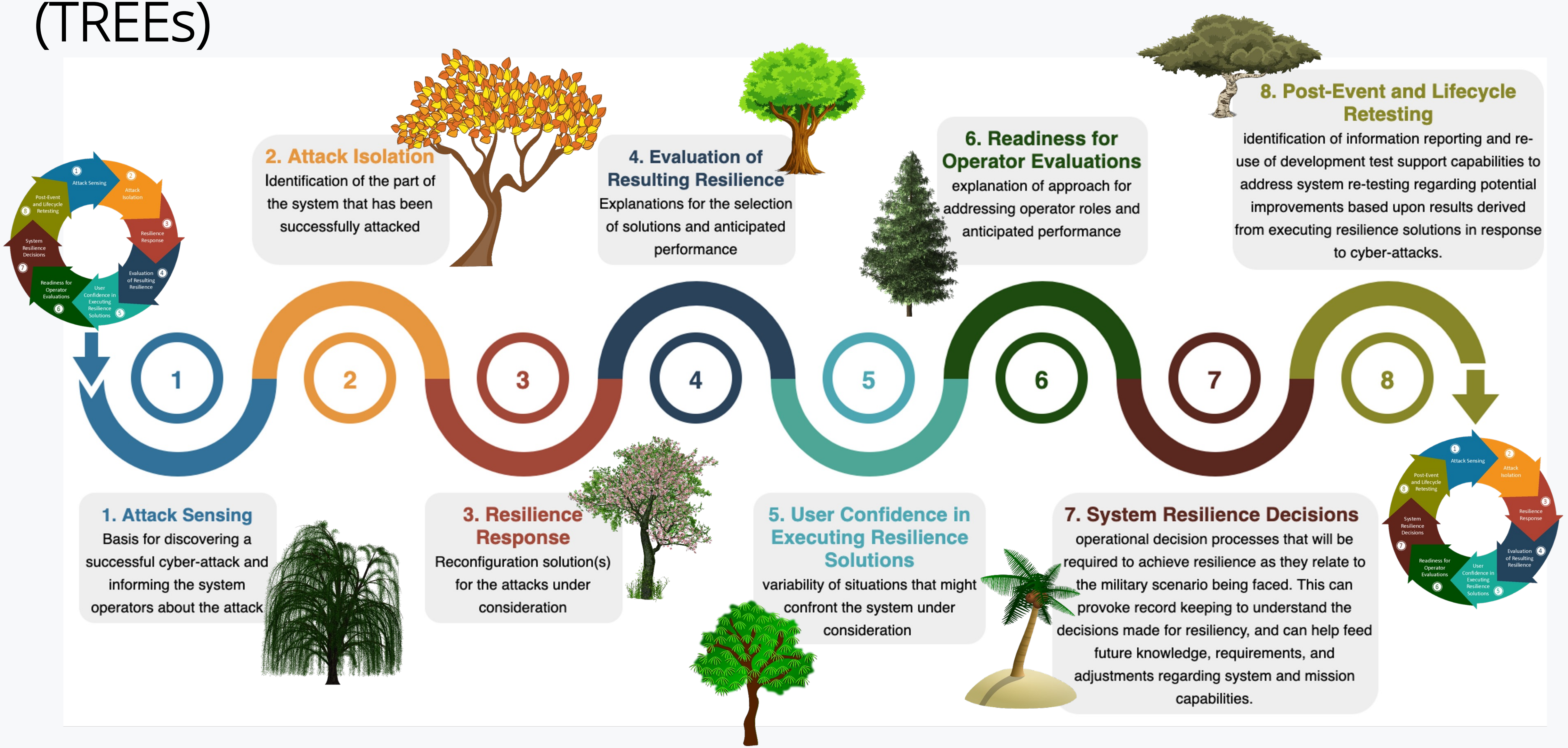
Decomposition of how systems operate as they undergo adversity and response:

- Technology
- Humans / Operators
- Decision Orientation



| TREE | Number | Description |
|---|---|---|
| Attack **Sensing** | T.1 | This element of resilience provides the basis for discovering a successful cyber-attack and informing the system operators about the attack. |
| Attack **Isolation** | T.2 | This element of resilience solutions addresses identification of the part of the system that has been successfully attacked. |
| Resilience **Options** | T.3 | This element of resilience solutions addresses the reconfiguration solution(s) for the attacks under consideration as well as the immediate containment of safety-related consequences. |
| **Evaluation** of Resilience Options | T.4 | This part of the framework calls for documentation that provides explanations for the selection of solutions, the anticipated performance of the reconfigured system (including time to reconfigure), and the basis for deciding that the resulting operational capabilities are satisfactory. |
| Operational **Confidence** in Executing Resilience Solutions | T.5 | The framework calls for documentation of the basis for achieving high enough confidence and the related test and evaluation methods. |
| **Readiness** for Operational Execution (Real-time Mission Context) | T.6 | The framework will expect explanation of the basis for the system design approach regarding test support for addressing operator roles and anticipated performance. |
| System Resilience Decision & **Execution** | T.7 | The framework will look for the rationale for who decides on what, and the training and tech support required for decision-makers. |
| **Post-Event** and Lifecycle Test Responses | T.8 | This portion of the framework addresses identification of information reporting and re-use of development test support capabilities to address system re-testing regarding potential improvements based upon actual results derived from executing resilience solutions in response to cyber-attacks. |

# FOREST and the Testable Resilience Efficacy Elements (TREEs)


Attack Sensing
Attack Isolation
Resilience Response
Evaluation of Resulting Resilience
User Confidence in Executing Resilience Solutions
Readiness for Operator Evaluations
System Resilience Decisions
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.

# T&E Considerations for each TREE

T1: Sensing

- Timing and Accuracy of Sensing

T2: Isolation

- Accuracy of performing the automated parts of Isolation
- Value of follow on diagnostics as compared to the delay times

T3: Options

- Number of Resilient options per Loss Scenario

T4: Evaluation

- Technical Availability of Resilient Modes
- Operator judgement of Usability and Failure Transparency for Resilient Modes

T5: Confidence

- Resilient Mode self-test mechanisms
- Training modules for Resilient Modes
- Operator consistency in Resilient Mode selection and timing

T6: Readiness

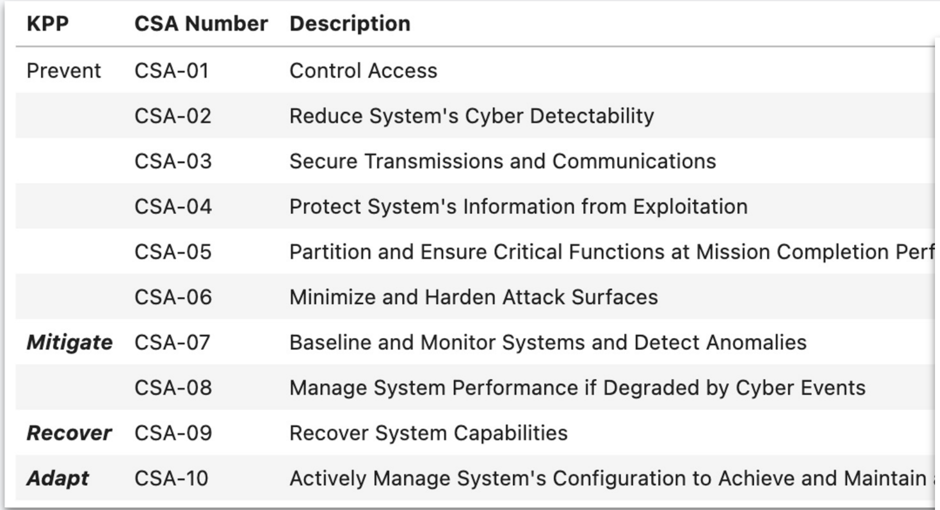
- Operational Availability of Resilience Mode
- Mission Survivability with Resilience Mode
- Mission Adaptability for Resilience Mode

T7: Execution

- Test Support System to Emulate Loss Scenarios and Exercise Associated Resilient Modes
  - Test Coverage of Resilient Modes
  - System Stability with Resilient Modes

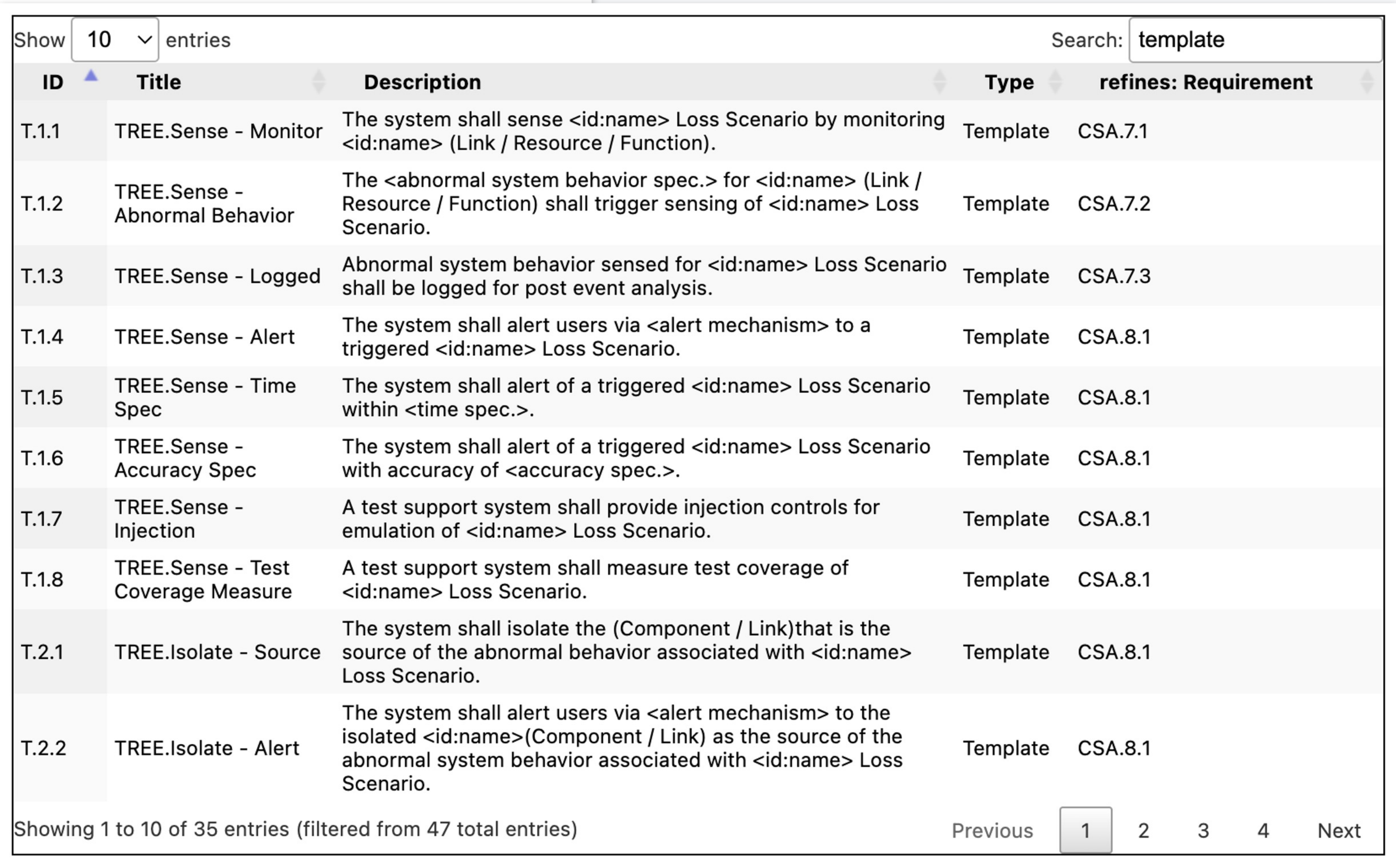
Distribution A - Cleared for Public Release by the Defense Office of Prepublication and Security Review, Case 23-S-0384, 10 November 2022

# 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 Exploitation |
| | CSA-05 | Partition and Ensure Critical Functions at Mission Completion Perf |
| | 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 Maintain |

**Cyber Survivability Attributes - DoD Joint Staff**



Show 10 entries        Search: template

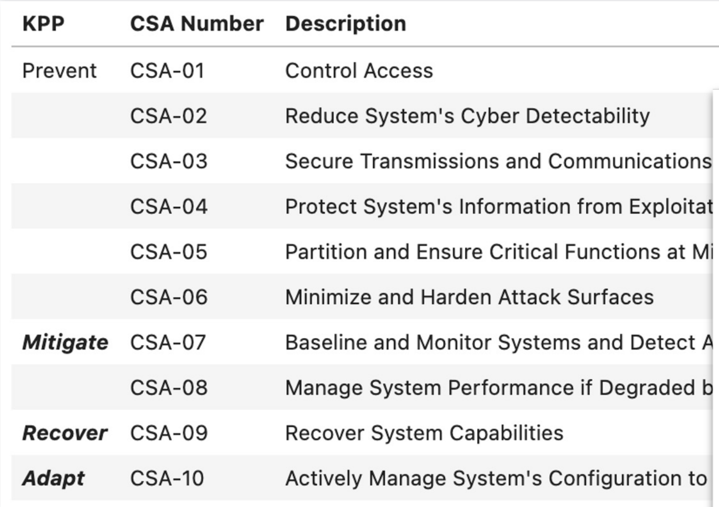
| ID | Title | Description | Type | refines: Requirement |
|---|---|---|---|---|
| T.1.1 | TREE.Sense - Monitor | The system shall sense <id:name> Loss Scenario by monitoring <id:name> (Link / Resource / Function). | Template | CSA.7.1 |
| T.1.2 | TREE.Sense - Abnormal Behavior | The <abnormal system 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)

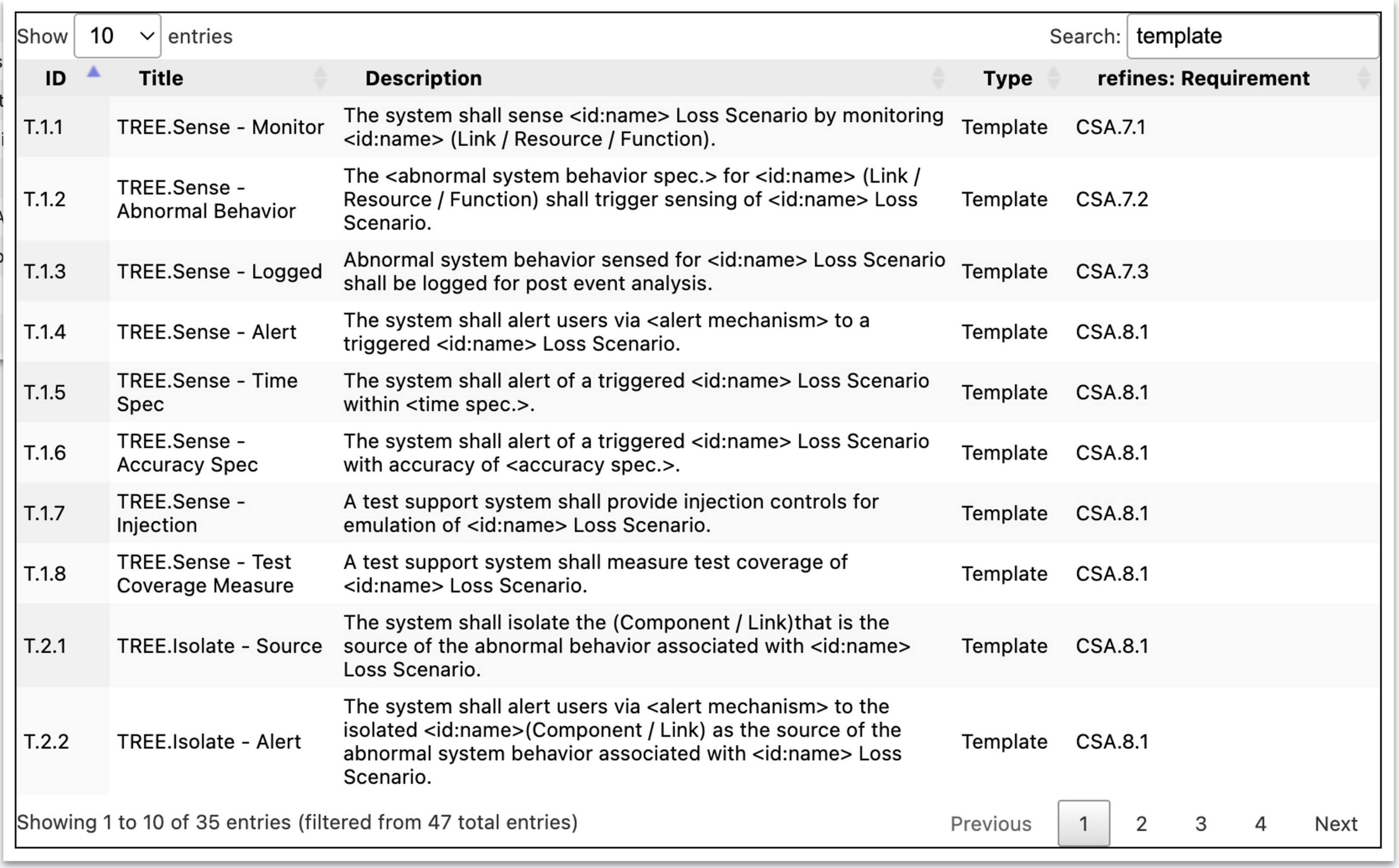
Previous 1 2 3 4 Next

**TREE-based Requirement Templates**

# 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 Exploitat |
| | CSA-05 | Partition and Ensure Critical Functions at Mi |
| | CSA-06 | Minimize and Harden Attack Surfaces |
| ***Mitigate*** | CSA-07 | Baseline and Monitor Systems and Detect A |
| | CSA-08 | Manage System Performance if Degraded b |
| ***Recover*** | CSA-09 | Recover System Capabilities |
| ***Adapt*** | CSA-10 | Actively Manage System's Configuration to |



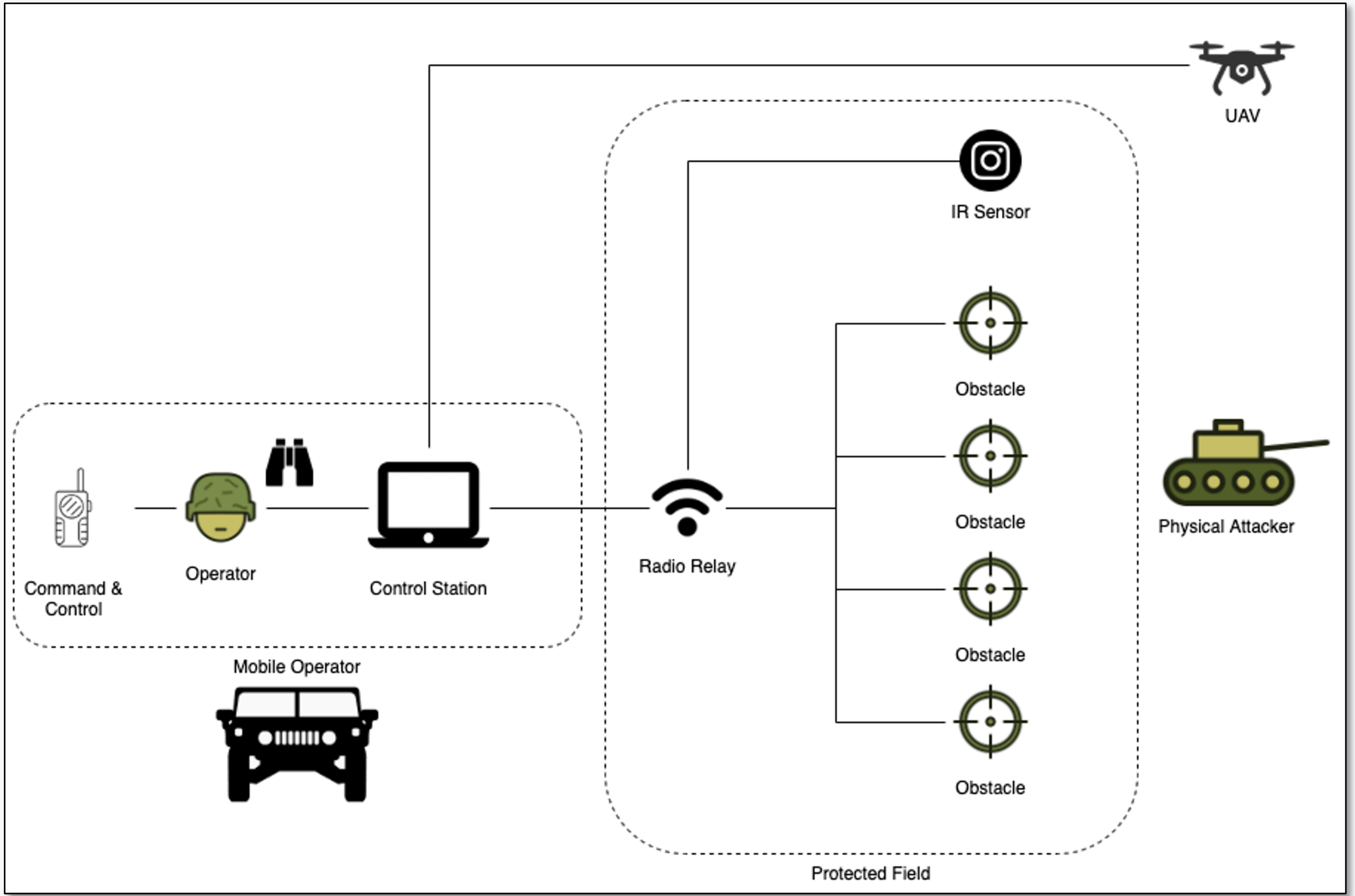
| ID | Title | Description | Type | refines: Requirement |
|---|---|---|---|---|
| T.1.1 | TREE.Sense - Monitor | The system shall sense <id:name> Loss Scenario by monitoring <id:name> (Link / Resource / Function). | Template | CSA.7.1 |
| T.1.2 | TREE.Sense - Abnormal Behavior | The <abnormal system 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

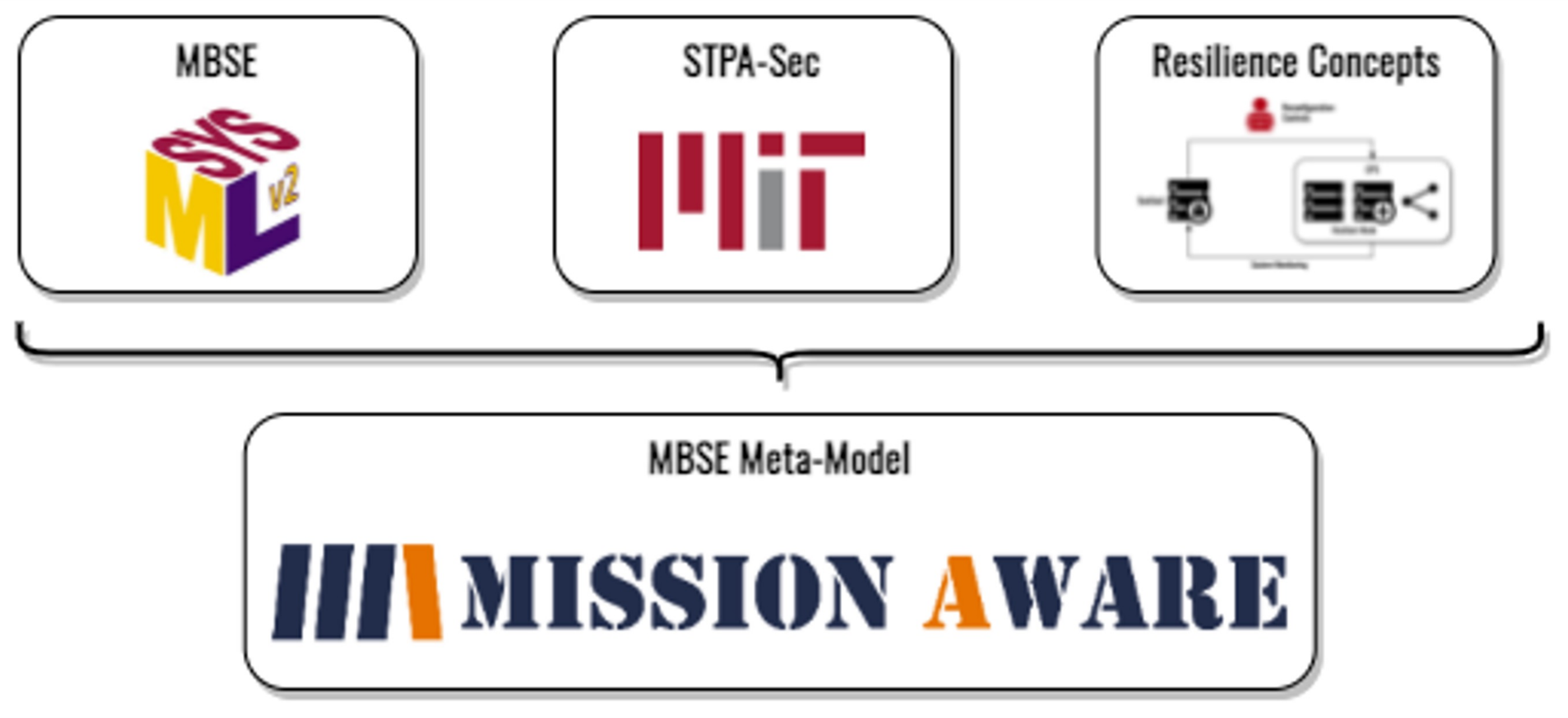
Distribution A - Cleared for Public Release by the Defense Office of Prepublication and Security Review, Case 23-S-0384, 10 November 2022

# Silverfish Case Study



Distribution A - Cleared for Public Release by the Defense Office of Prepublication and Security Review, Case 23-S-0384, 10 November 2022

# MA MBSE Meta-Model Building Blocks



MBSE

STPA-Sec

Resilience Concepts

MBSE Meta-Model

Distribution A - Cleared for Public Release by the Defense Office of Prepublication and Security Review, Case 23-S-0384, 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 sim
  - 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-0384, 10 November 2022

# Q & A

NATIONAL SECURITY INSTITUTE
VIRGINIA TECH

Distribution A - Cleared for Public Release by the Defense Office of Prepublication and Security Review, Case 23-S-0384, 10 November 2022

SYSTEMS ENGINEERING RESEARCH CENTER

# THANK YOU

| Stay connected with us online.