SYSTEMS ENGINEERING RESEARCH CENTER

VIRGINIA TECH

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

Peter Beling (Va Tech), Tom McDermott (Stevens),
Tim Sherburne (Va Tech); Megan Clifford (Stevens)

WASHINGTON DC | VIRTUAL
ANNUAL SPONSOR RESEARCH REVIEW
NOV. 2-4 2021

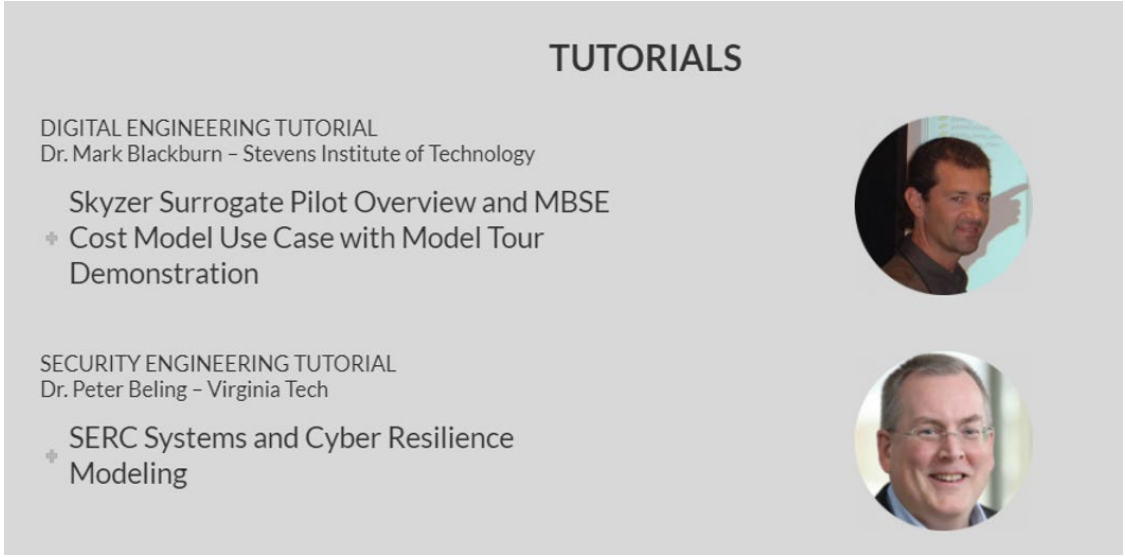
Agenda

- Motivation
- Cyber resilience
- Developmental test for cyber resilience
- FOREST
- Supporting methodologies
- Requirements, measures, and metrics
- Resources

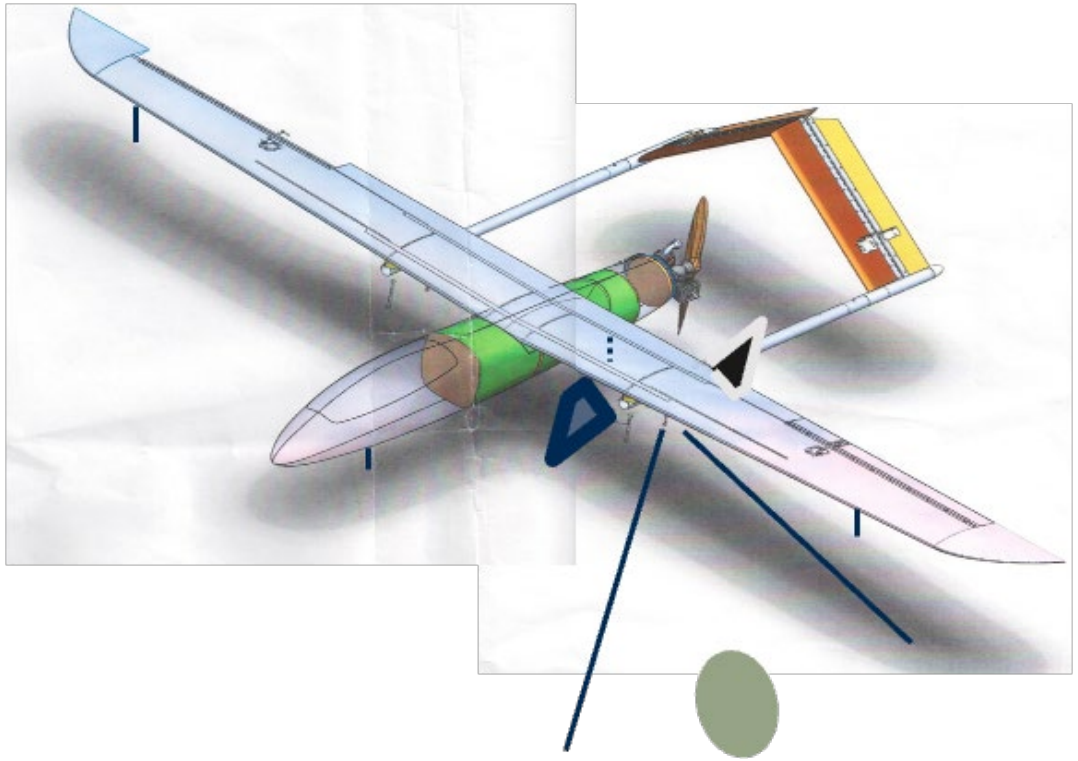
WRT-1033

Transitioning Mission Aware Concepts and Methods to Evaluate Cost Risk Decisions for Security Assurance Design

Mr. Tom McDermott, *Stevens*



Motivating Scenario



Assurance–Difficult!

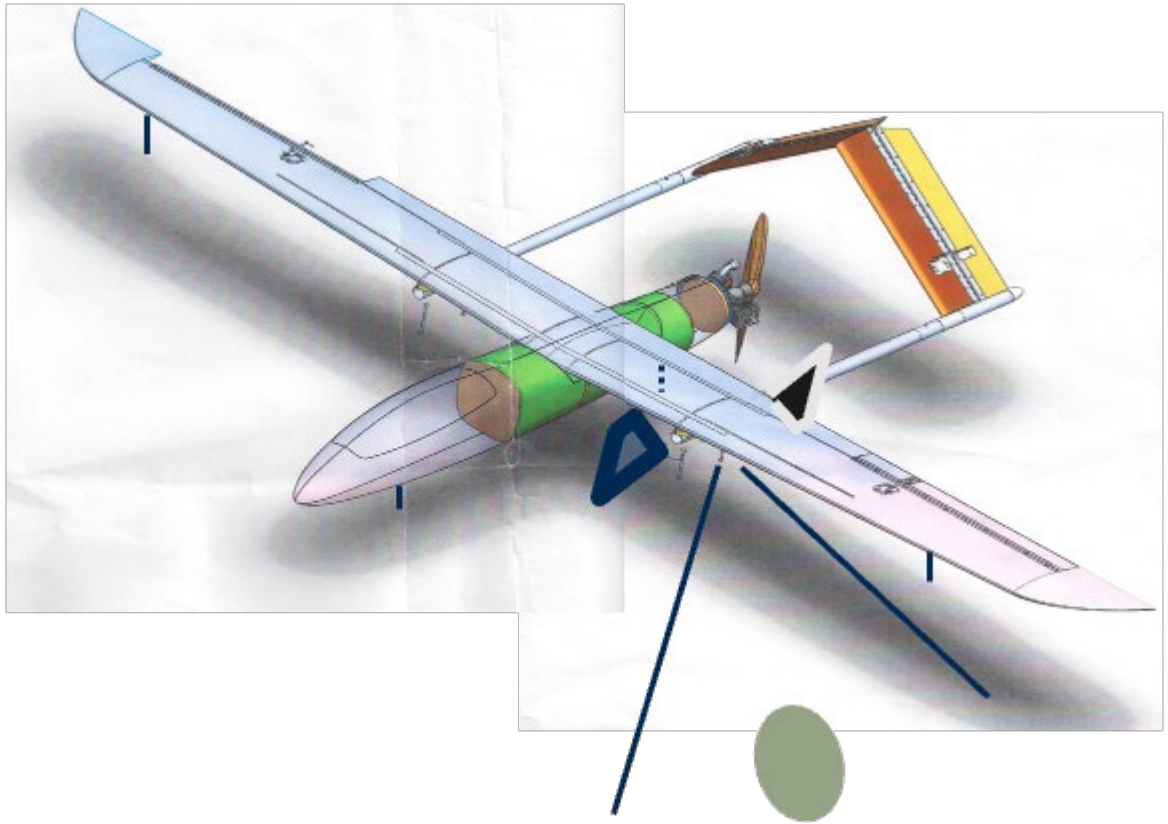
- Physical points of entry
- Off-the-shelf electronics
- Insider threat

Resilience

- Ensure acceptable mission outcome
- Condition on certainty of attack.
- “Point defense rather than perimeter defense.”

Motivating Scenario

1. Identify nightmare scenario
   - GPS compromise
2. Behavior-based detection mechanism
   - Compare outputs of two GPS units
3. Switch operating mode
   - Inertial navigation

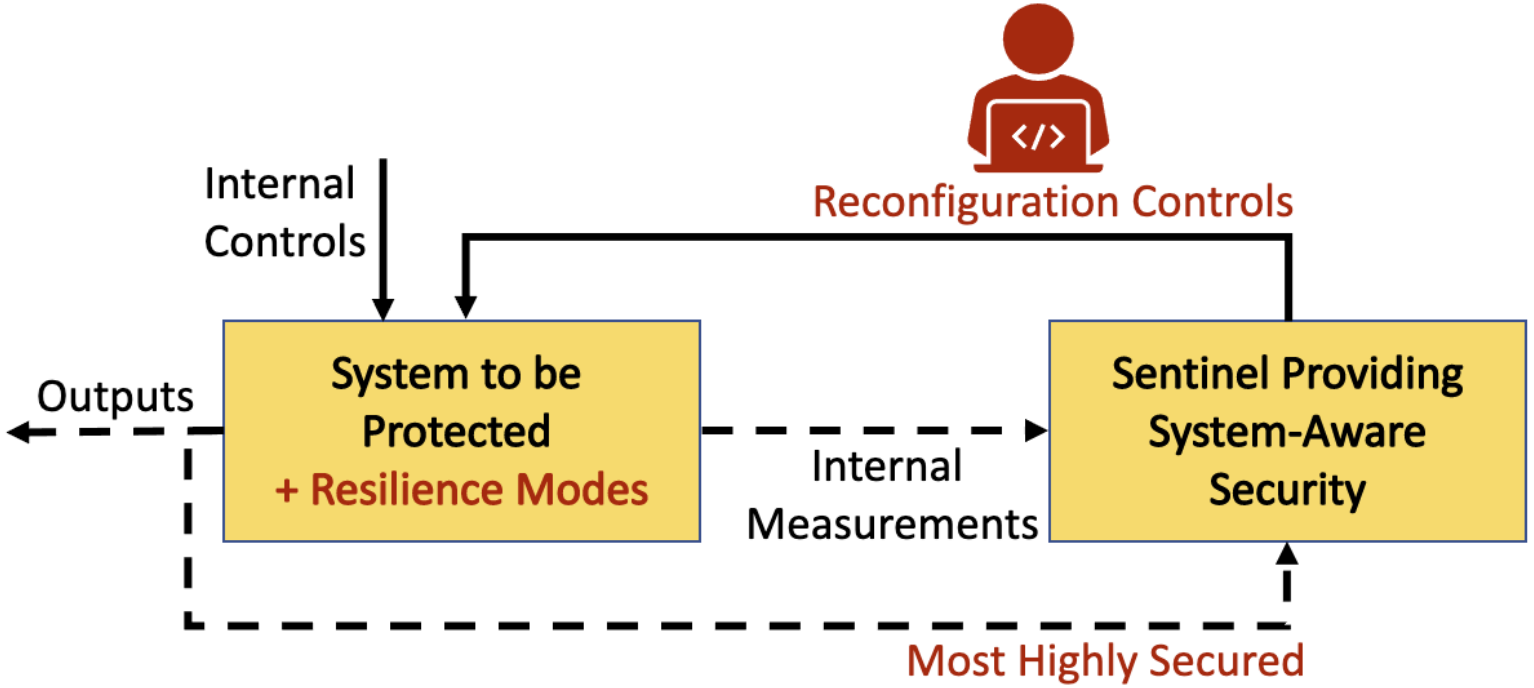


Additional Benefits:

- Reverse asymmetry; erode attacker confidence
- Minimize changes to the system while maximizing uncertainty for the attacker

Sentinel-based Cyber Resilience Concept

- A Resilience Mode is a distinct and separate method of operation of a component, device, or system based upon a diverse redundancy or other design pattern.
- A Sentinel is a pattern responsible for monitoring and reconfiguration of a system using available Resilience Modes. The Sentinel functions are expected to be far more secure than the system being addressed for resilience.

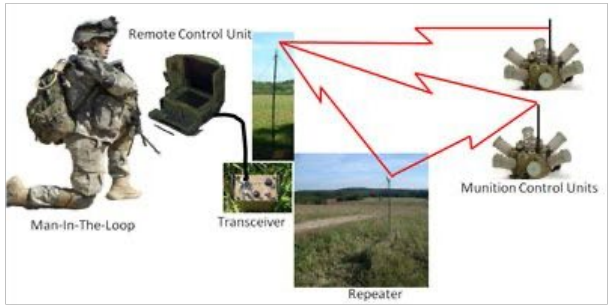


Prior Work

Ship Control
(Northrop Grumman)

3D Printers
(NIST)

Human Factors Experiments
(Air Force)



Networked Munitions
(Army)

Cars
(VA State Police)

Industrial Control Sytems
(Mission Secure Inc)

10

Cyber Resilience vs. Cyber Assurance

- **Cyber Assurance** is the justified confidence that a system functions as intended and is free of exploitable vulnerabilities, either intentionally or unintentionally designed or inserted as part of the system at any time during the life cycle.
  - System "functions as intended" and "free of exploitable vulnerabilities" represent the system's highest-level properties.
  - Assurance is a static property of the system as built.
- **Cyber Resilience** is the capacity of a system to maintain state awareness and to proactively maintain a safe level of operational normalcy in response to anomalies including threats of a malicious and unexpected nature.
  - Agnostic to particulars of attacks; assume attacks will happen.
  - Resilience is a dynamic property of the system as designed into a set of behaviors.

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.

MITRE: Cyber Resilience Techniques and Approaches

FIGURE 1: CYBER RESILIENCY TECHNIQUES AND IMPLEMENTATION APPROACHES

NIST 800.160 vol2

Some Cyber Resilience Challenges for Weapons Systems

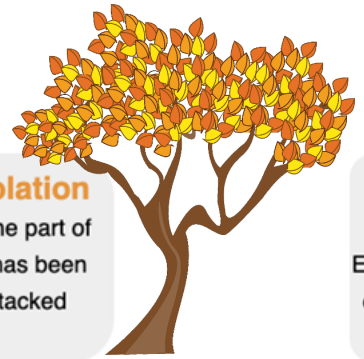
- Defining requirements for cyber resilience
  - Is it enough to say “the system shall have resilience with respect to cyber attacks”?
  - How do we reason about the behavior of systems that have yet to be built?
- Developmental test
  - What are measures and metrics associated with cyber resilience?
  - What are the intersections with operational test?
- Testable requirements
  - How do we anticipate test at the requirements stage?

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

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

- Technology
- Humans/operators
- Decision orientation

FOREST and the Testable Resilience Efficacy Elements (TREEs)



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

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

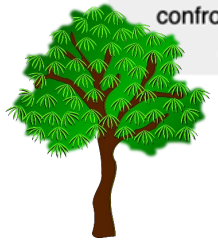
6. Readiness for Operator Evaluations
explanation of approach for addressing operator roles and anticipated performance

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.

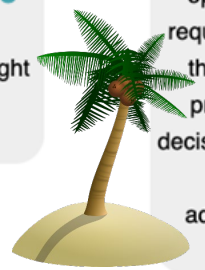
1 2 3 4 5 6 7 8

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

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



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



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.

T&E Considerations per 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 Resilient options per Loss Scenario

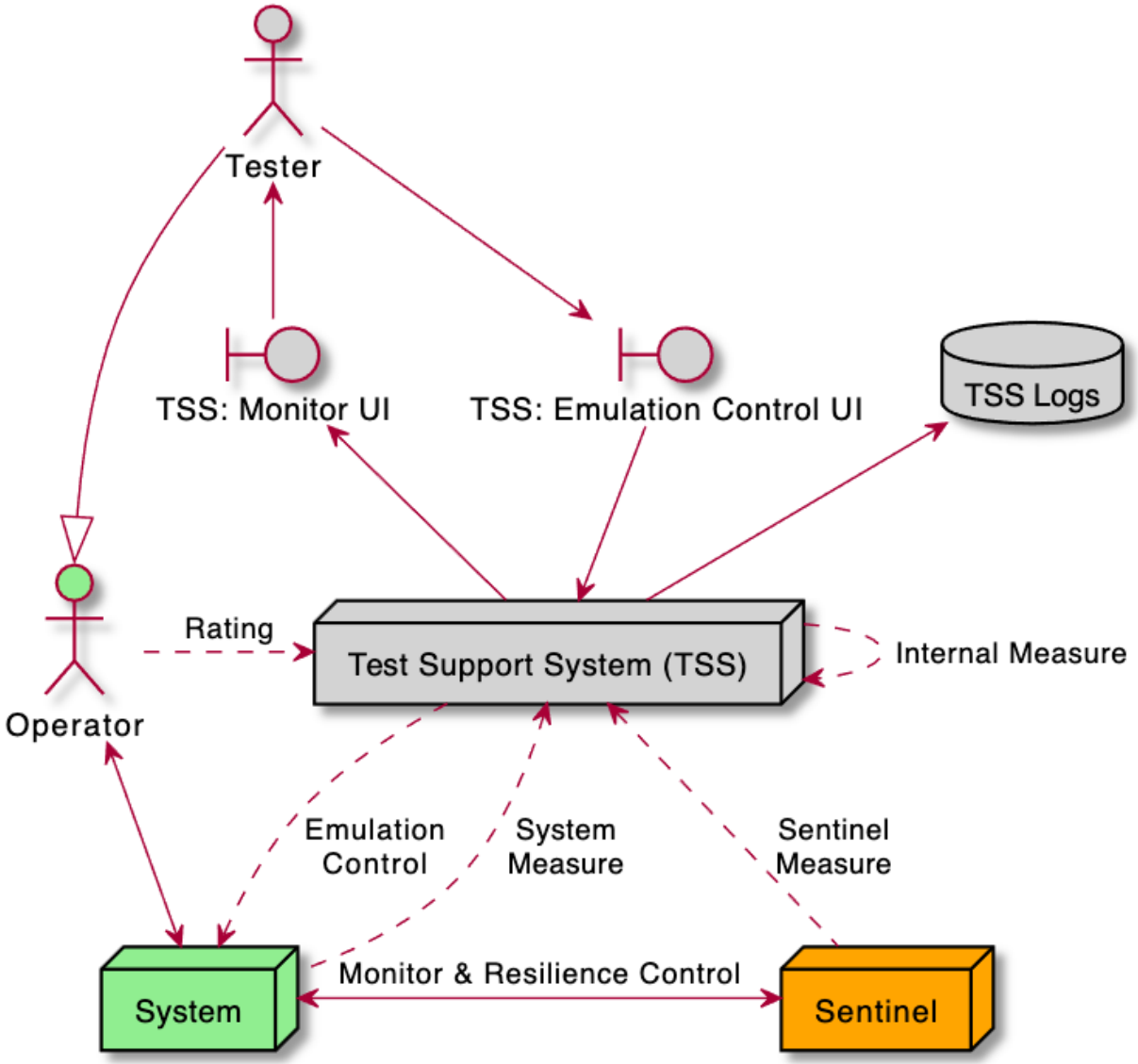
T4: Evaluation
- Technical Availability of Resilient Modes
- Operator judgement of Usability and Failure Transparency for Resilient Modes

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

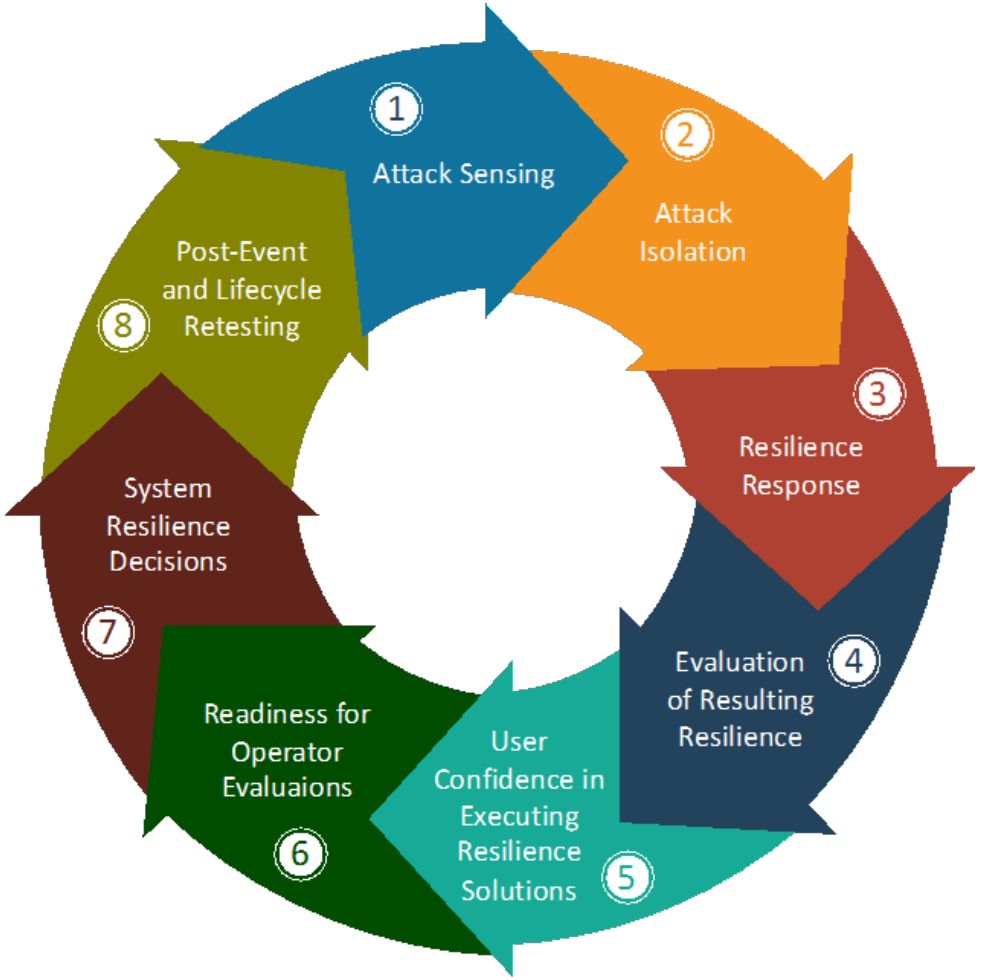
T7: Execution
- TSS to enable Emulation of Loss Scenarios with Execution of associated Resilient Modes
  - Test Coverage of Resilient Modes
  - System Stability with Resilient Modes

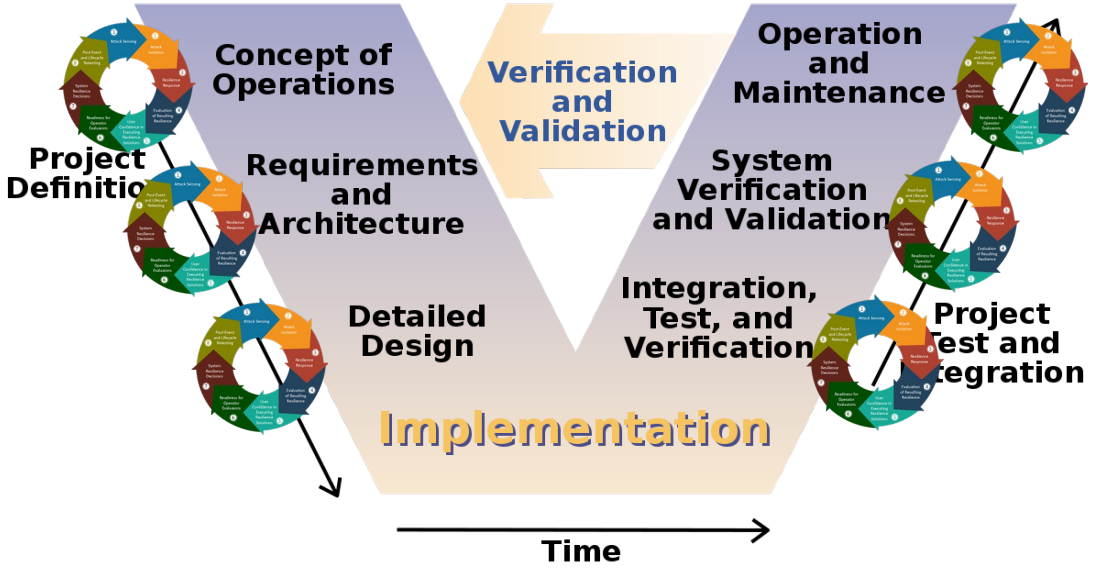
Cyber Resilience Test - Reference Architecture



- Many standard tests can be done through manipulation of the external environment
- Resilience tests require manipulation of the system's internal states

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

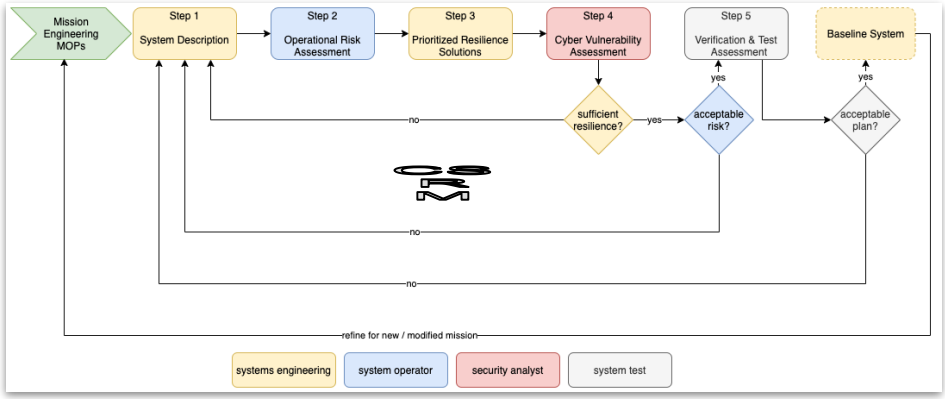


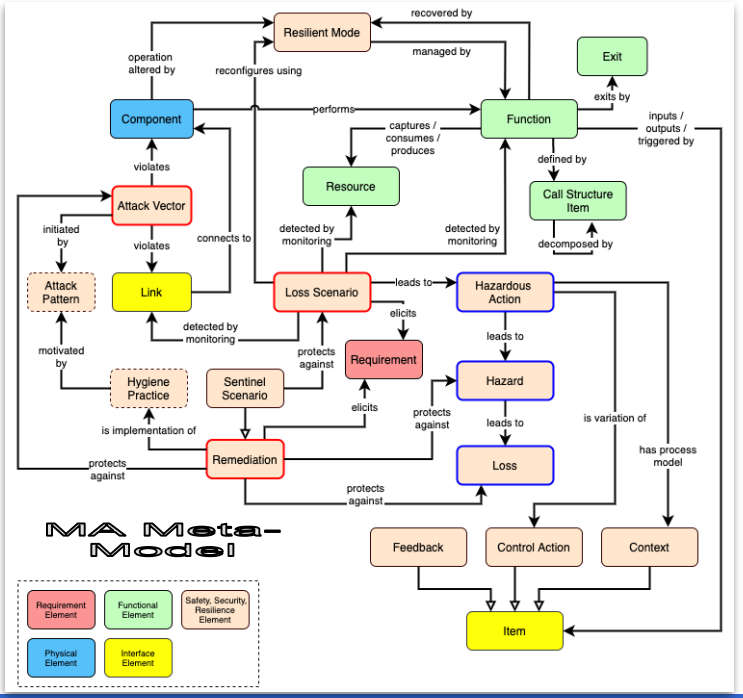


Continuous evaluation of assurance-related quality attributes

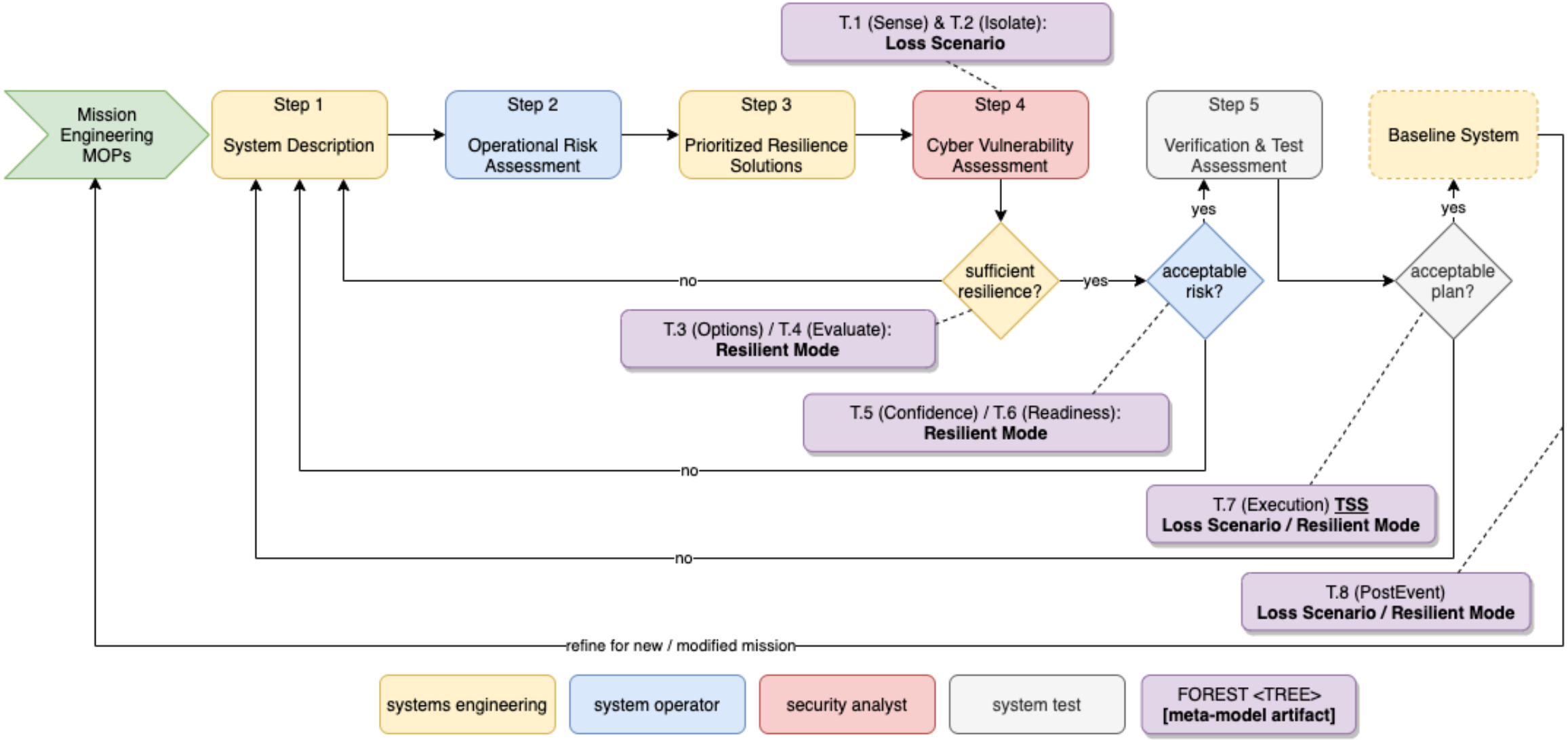
Developing Functional Understanding of System under Adversity

- What to protect and why? Which combination of design patterns to employ in which mission subsystems?
- Who to involve? What information to provide for decision support?
  - Blue Team: the system/mission owners
    - Input: structured elicitation process from safety community
    - Output: priorities for system functions
  - Gold Team: the systems engineers
    - Input: scoping from Blue Team
    - Output: systems models (e.g. SysML)
  - Red Team: the in-house adversaries
    - Input: systems models and ML tools to cross reference with known attacks
    - Output: vulnerability assessment

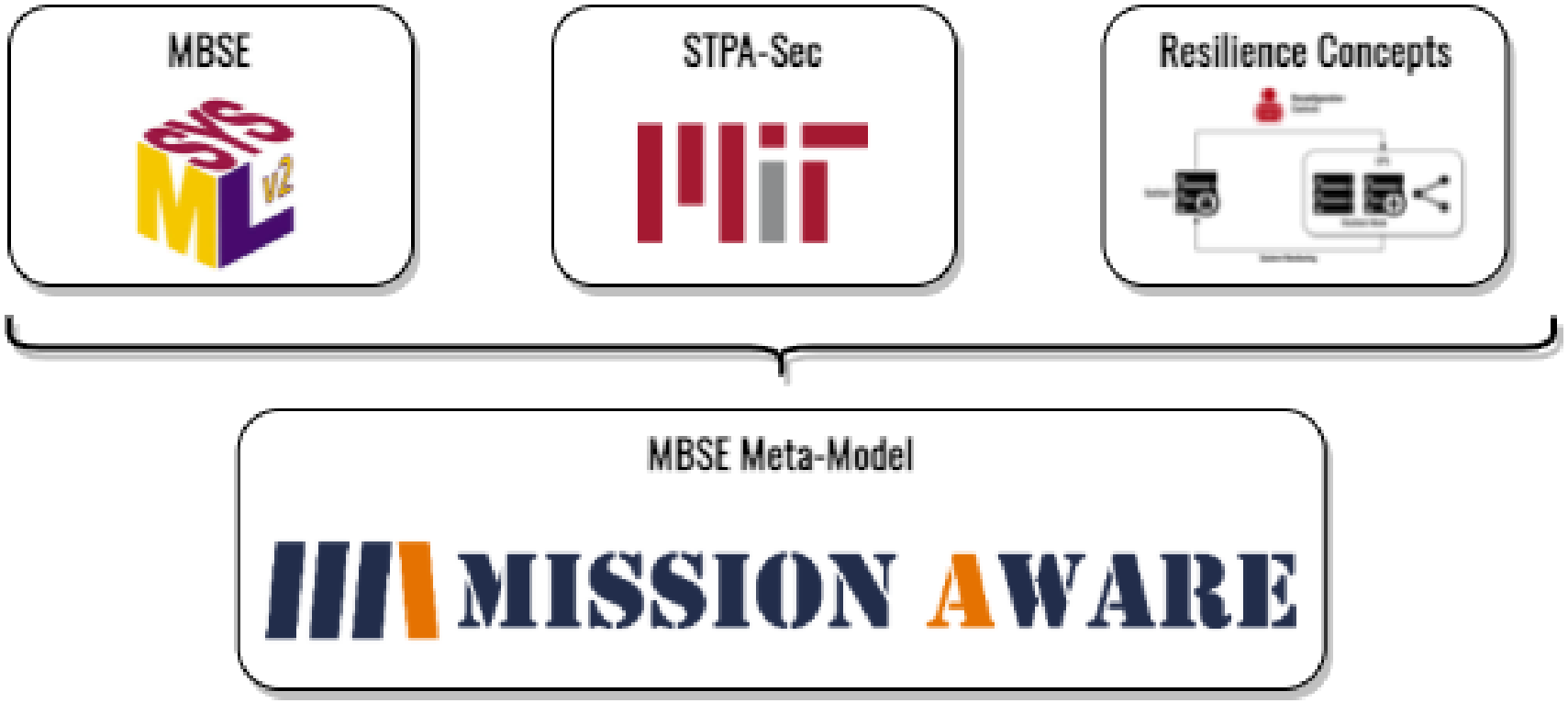




Cyber Security Requirements Methodology (CSRM)



MA MBSE Meta-Model Building Blocks



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.

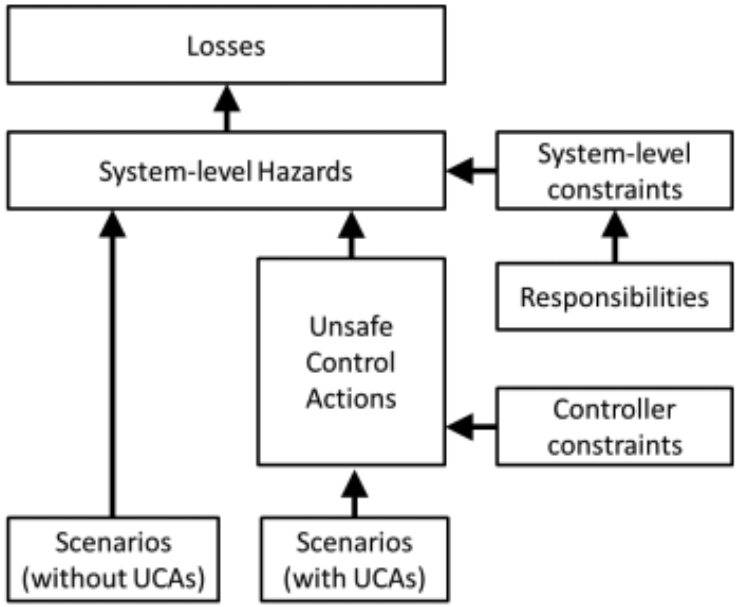


Figure 2.21: Traceability between STPA outputs

- 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.
- An ***Unsafe Control Action*** (UCA) 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 unsafe control and to hazards.

STPA-Sec Overview

- Addresses adversarial causal factors (spoofed, tampered, etc.)
- Incorporates mission view/mission engineering

Young, http://psas.scripts.mit.edu/home/wp-content/uploads/2014/03/Young_STAMP_2014_As-delivered.pdf

STPA Outputs and Traceability

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

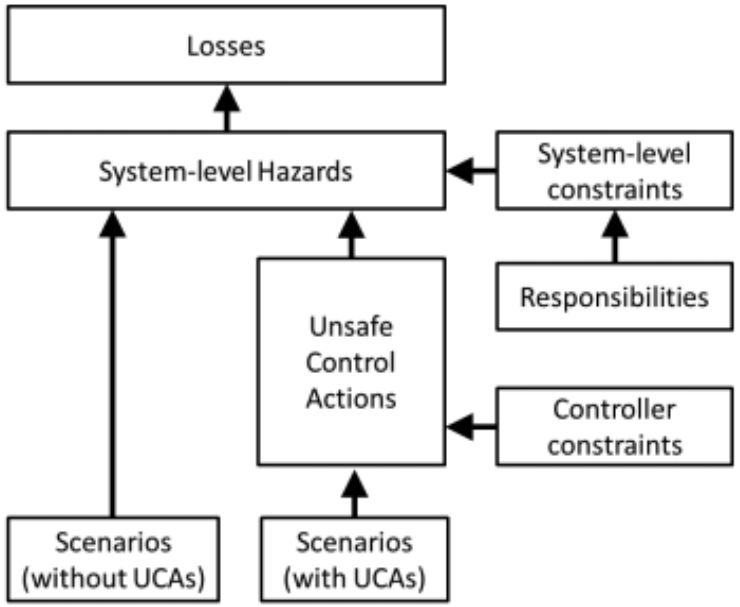
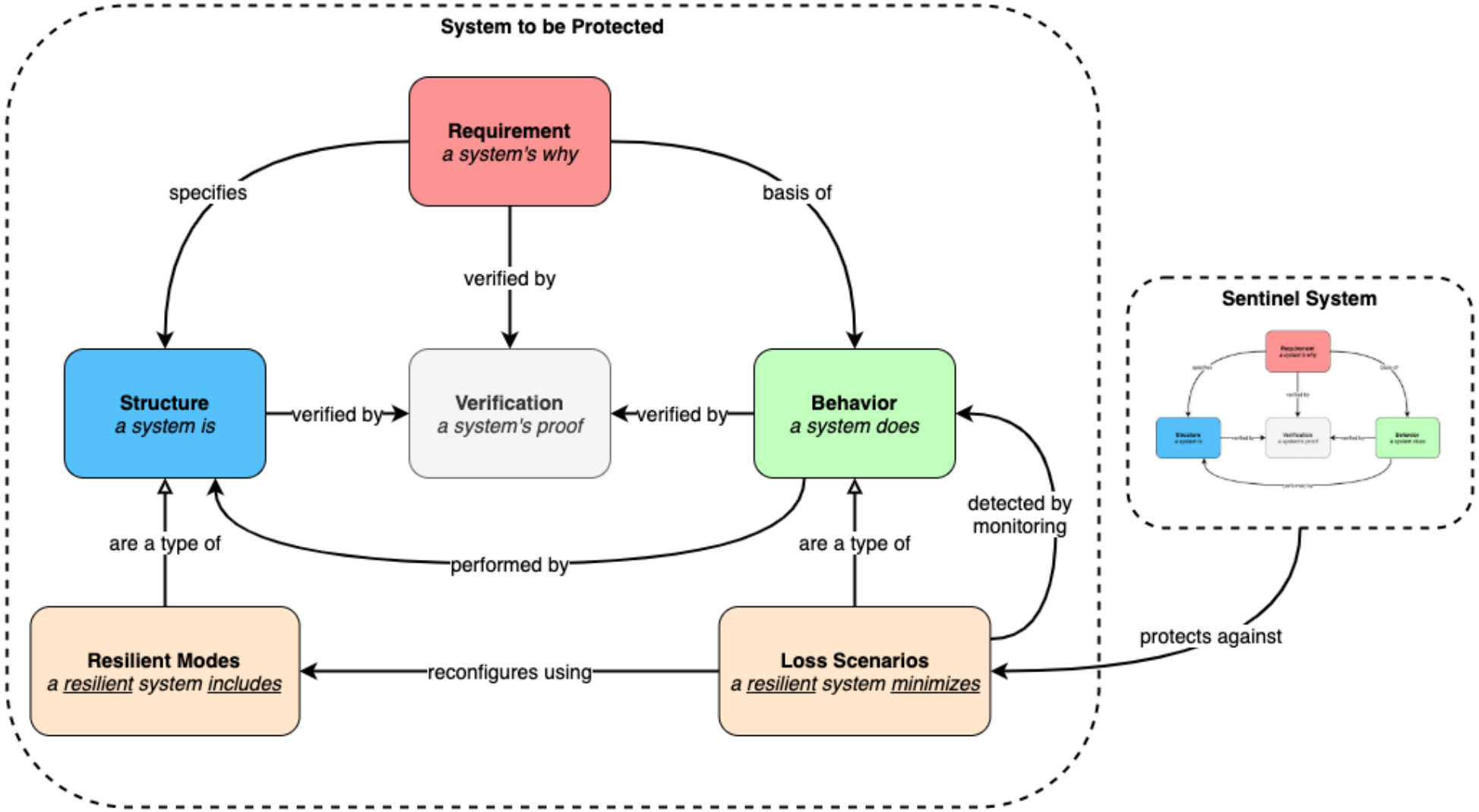


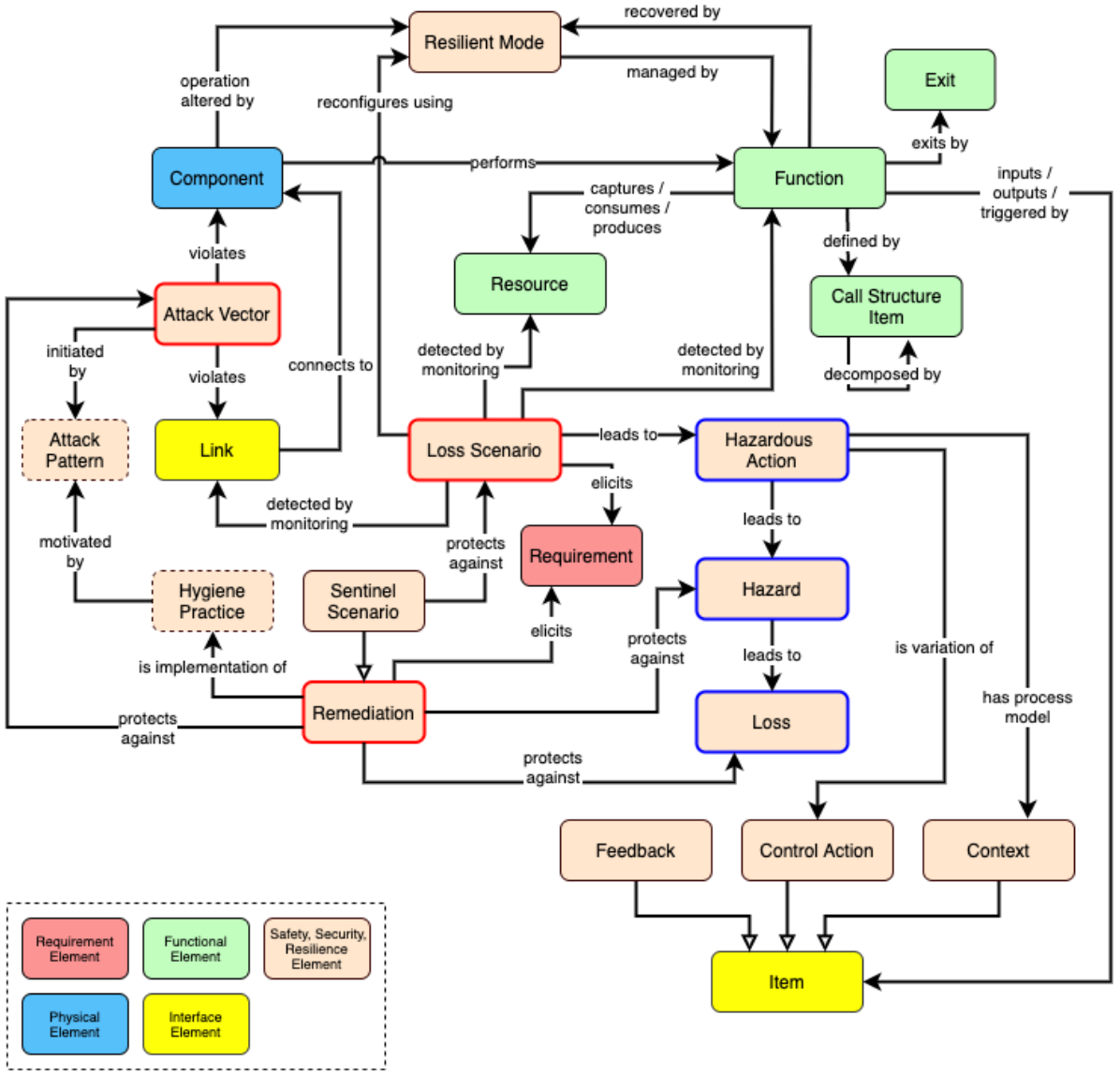
Figure 2.21: Traceability between STPA outputs

- 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.
- An ***Unsafe Control Action*** (UCA) 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 unsafe control and to hazards.

Mission Aware Meta-Model: Top-Level



Mission Aware Meta-Model: Detail View

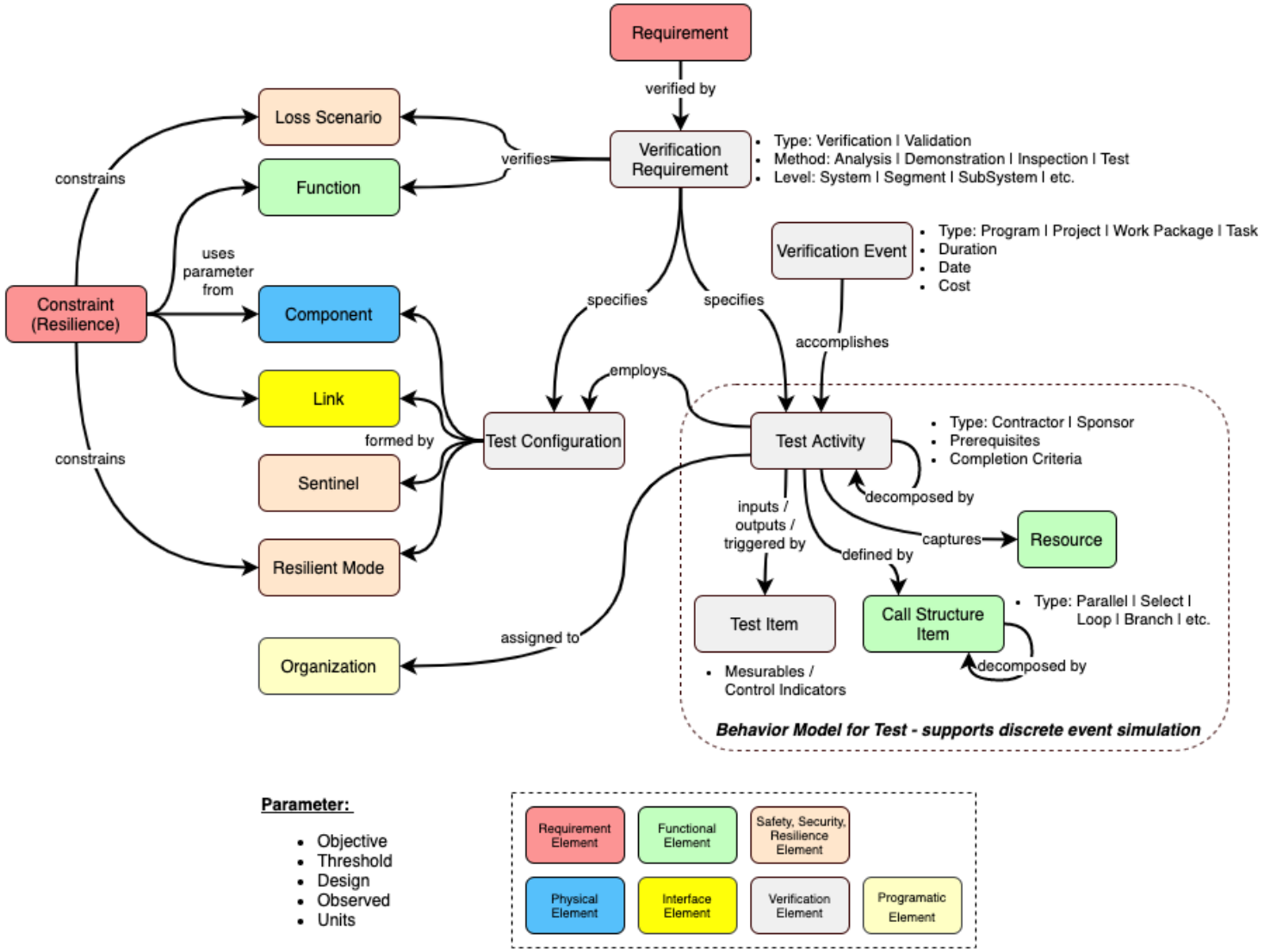


MISSION AWARE

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

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

TREE-based Quality Attributes

(✔ System Measure ✔ Operator Rating ☑ Development Consideration)

Quality Attribute	T.1: Sense	T.2: Isolate	T.3: Options	T.4: Evaluate	T.5: Confidence	T.6: Readiness	T.7: Execution	T.8: PostEvent
accuracy	✔	✔						
adaptability						✔		
affordability								☑
availability				✔		✔		
composability			✔					☑
extensibility								☑
failure transparency				✔				
learnability					✔			
predictability					✔			
recoverability				✔				
repeatability					✔			
safety			✔					
stability							✔	
survivability						✔		
testability	✔						✔	☑
timeliness	✔	✔		✔	✔	✔	✔	☑
usability				✔				

Quality Attribute Types:

- *Quantitative* System Measures
- *Qualitative* Operator Ratings

CSA Top-Level Requirements

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 Performance Levels
	CSA-06	Minimize and Harden Attack Surfaces
Mitigate	CSA-07	Baseline and Monitor Systems and Detect Anomalies
	CSA-08	Manage System Performance if Degrated by Cyber Events
Recover	CSA-09	Recover System Capabilities
Adapt	CSA-10	Actively Manage System's Configuration to Achieve and Maintain an Operationally Relevant Cyber Survivability Risk Posture (CSRP)

CSA	Req Number	Description
CSA-07	CSA.07.1	The system shall monitor operational parameters, boundaries, and configuration controls.
	CSA.07.2	The system shall analyze performance through a baseline comparison to detect anomalies and attacks.
	CSA.07.3	The system shall generate and store logs.
CSA-08	CSA.08.1	The system shall alert users of detected anomalies and attacks.
	CSA.08.2	The system shall provide capabilities to shed non-mission-critical functions, systems/sub-systems, and interfaces.
	CSA.08.3	The system shall maintain mission-critical functions in a cyber contested operational environment during/after observed anomaly(ies).
	CSA.08.4	The system shall maintain safety-critical functions in a cyber contested operational environment during/after observed anomaly(ies).
	CSA.08.5	The system shall fail secure when mission-critical functions are no longer operational in a contested environment.
	CSA.08.6	The system shall maintain flight-critical functions in a cyber contested operational environment during/after observed anomaly(ies).
CSA-09	CSA.09.1	The system shall provide the capability to recover to a known state in near real time.
CSA-10	CSA.10.1	The system shall have the capability to update scans to ensure appropriate, applicable requirements are captured (e.g. STIGS, SRG, etc.) for: (a) hardware (b) software (c) firmware
	CSA-10.2	Actively manage System's Configurations to achieve and maintain an Operationally Relevent Cyber Survivability Risk Posture (CSRP).

*MITRE, Relationships Between Cyber Resiliency Constructs and Cyber Survivability Attributes (CSA), 2019

Loss Scenario Elicited Requirements (TREE.1 & TREE.2)

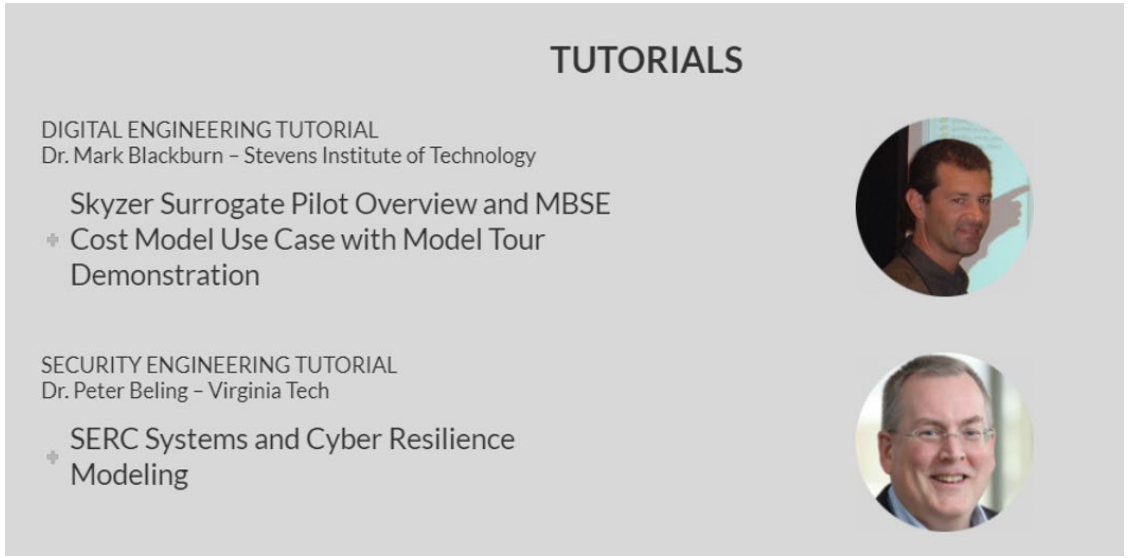
TREE	Req Number	Description	Type	Trace
T.1:Sense	T.1.01.<id>	The system shall **sense** <id:name> *Loss Scenario* by monitoring <id:name> *(Link / Resource / Function)*.	Functional	CSA.07.1
	T.1.02.<id>	The *<abnormal system behavior spec.>* for <id:name> *(Link / Resource / Function)* shall trigger **sensing** of <id:name> *Loss Scenario*.	Functional	CSA.07.2
	T.1.03.<id>	Abnormal system behavior **sensed** for <id:name> *Loss Scenario* shall be logged for post event analysis.	Functional	CSA.07.3
	T.1.04.<id>	The system shall **alert** users via <alert mechanism> to a triggered <id:name> *Loss Scenario*.	Functional	CSA.08.1
	T.1.05.<id>	The system shall **alert** of a triggered <id:name> *Loss Scenario* within <time spec.>.	Performance	CSA.08.1
	T.1.06.<id>	The system shall **alert** of a triggered <id:name> *Loss Scenario* with accuracy of <accuracy spec.>.	Performance	CSA.08.1
T.2:Isolate	T.2.01.<id>	The system shall **isolate** the *(Component / Link)* that is the source of the abnormal behavior associated with <id:name> *Loss Scenario*	Functional	CSA.08.1
	T.2.02.<id>	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*.	Functional	CSA.08.1
	T.2.03.<id>	The system shall **alert** of isolated <id:name> *(Component / Link)* within <time spec>.	Performance	CSA.08.1
	T.2.04.<id>	The system shall **alert** of isolated <id:name> *(Component / Link)* with accuracy of <accuracy spec>.	Performance	CSA.08.1

Quality Attributes Measures and Metrics

- For each FOREST TREE, the test team evaluates relevant quality attributes
  - The team determines measures and metrics for each quality attribute (example in red below)
    - Quality Attribute: Accuracy
      - Description: Closeness of the measurements to a specific value
        - Measure: emulatedLossScenarioCount[id]
          - Units: count
            - Description: Number of times a specific [id] Loss Scenario is emulated in the System
              - Source: TSS
                - Metric: sensedRatio[id]
                - Calculation: sesedLossScenarioCount[id] / emulatedLossScenarioCount[id]
                - Aligned CSA: Most closely aligned with CSA 07

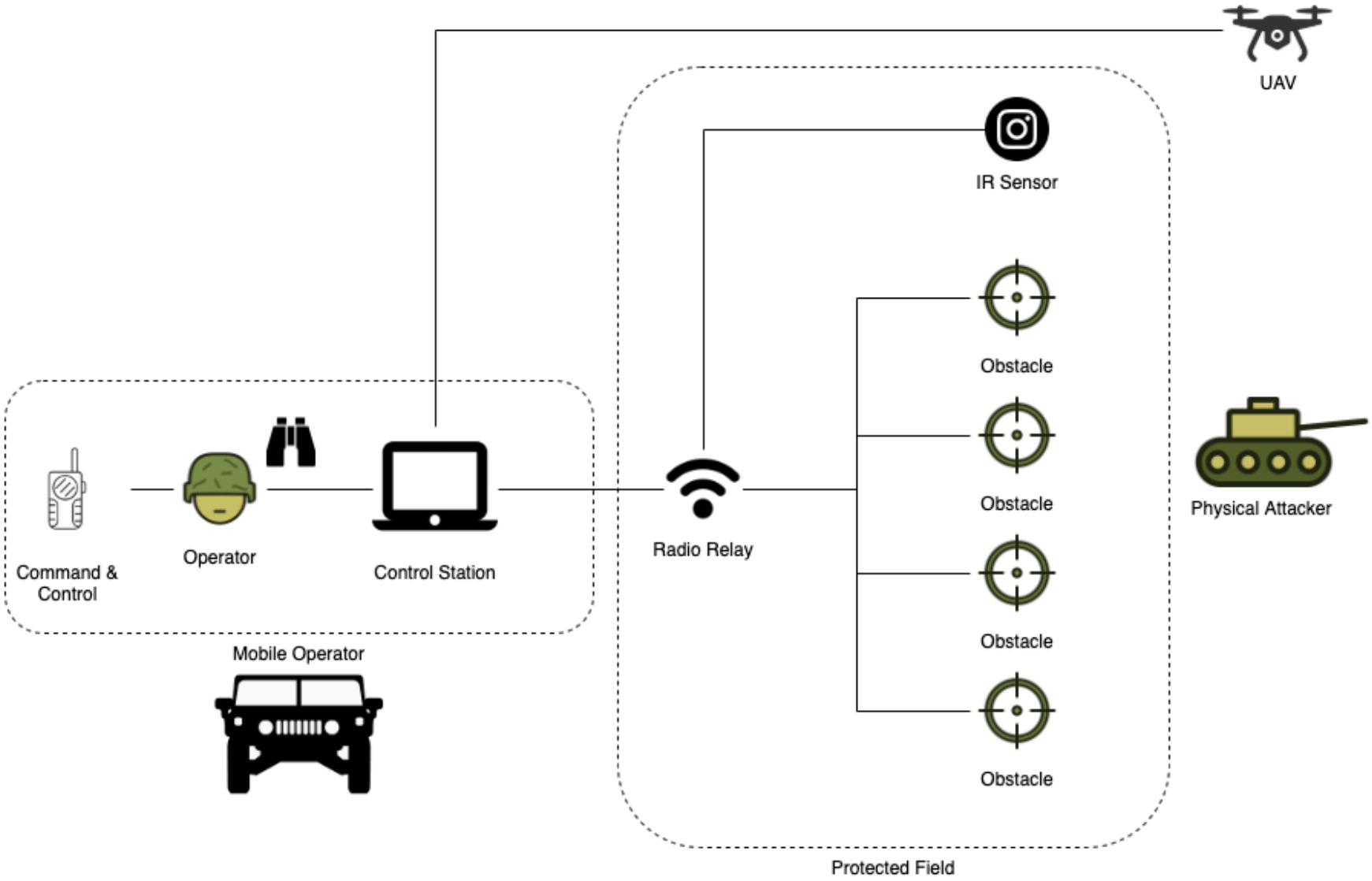
- The team focuses on the various CSAs and which category the attribute and its metrics best align.

Additional Resources



- Website:
  - https://mission-aware.net

Silverfish Case Study



Cyber Resiliency Course Details

- **Level 1 Cyber Resiliency Foundational Course (1 Day ILT)**
  - The course introduces the concept of Mission Resiliency and Survivability. It provides an approach to addressing Cyber Survivability KPPs (Prevent, Mitigate, Recover) and the Cyber Survivability Attributes (10)
  - Students will dive into the CSRM Methodology and loss based engineering (full process).
  - Students will map the CSAs to applicable security disciplines (ie. AT, CyEng, RMF, SW Assr, HW Assr)
  - Students will analyze applicable Cyber Attacks and Cyber defensive techniques
  - Course may leverage AF SSE Practitioners Course an guidebook, DAU Operational Resiliency Workshop, STPA SEC, MITRE Resiliency Framework, MITRE ATT&CK, MITRE DEFENSE, NIST Cyber Resiliency Techniques, and the MITRE OSD Principles for Trustworthiness, AJs Loss Based Engineering Approach, Cyber Incident Response.
  - Example Scenario of a Loss based system (Silverfish, UAV, Ship, Car, etc..)
- **Level 2 Cyber Resiliency Practitioner Course (2.5 Day ILT)**
  - The course provides training on Modeling Mission Resiliency in a SysML model.
  - STPA SEC, Mission Awareness, Modeling Trust, Model the Principles of Trustworthiness
  - Course may leverage AF Cyber Model, the UAV SERC Mission Aware Model
  - Students will work in a distributed Cameo or Vitech Genesis model of a real system to incorporate Cyber Resiliency techniques and TTPs.
  - Students will present a capstone model of a resilient system

www.DAU.edu

DAU

Questions?