INCOSE

International Council on Systems Engineering
A better world through a systems approach

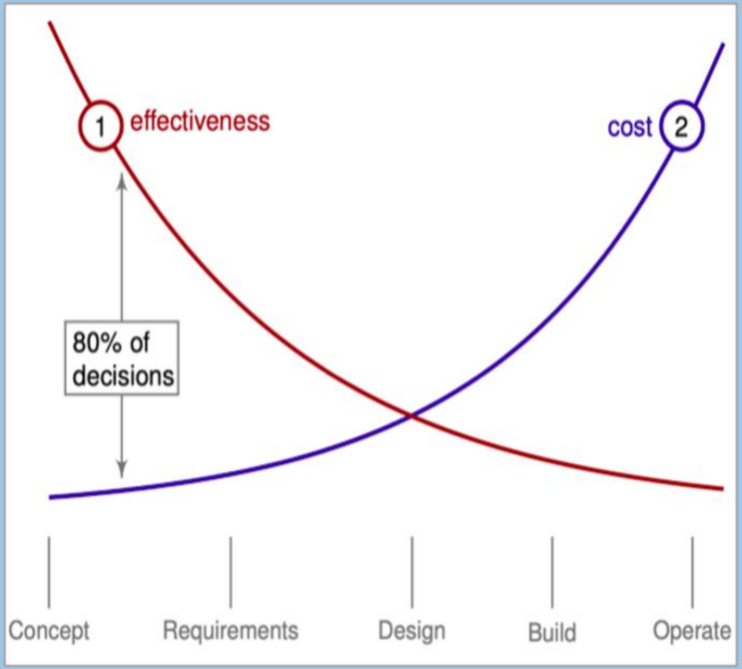
Secure Cyber Resilient Engineering: Cyber Vulnerabilities, Threat Detection, and the Adversity Chain

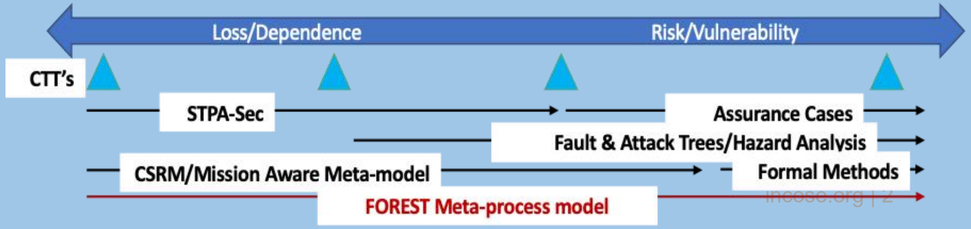
Tom McDermott, Stevens Institute of Technology
Peter Beling, University of Virginia
Megan M Clifford, Stevens Institute of Technology

INCOSE International Symposium 2025 | Ottawa, Canada

Secure Cyber Resilient Engineering

- 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/vulnerability management and assurance
- Continuous evaluation of assurance-related quality attributes





STPA-Sec

Assurance Cases

Fault & Attack Trees/Hazard Analysis

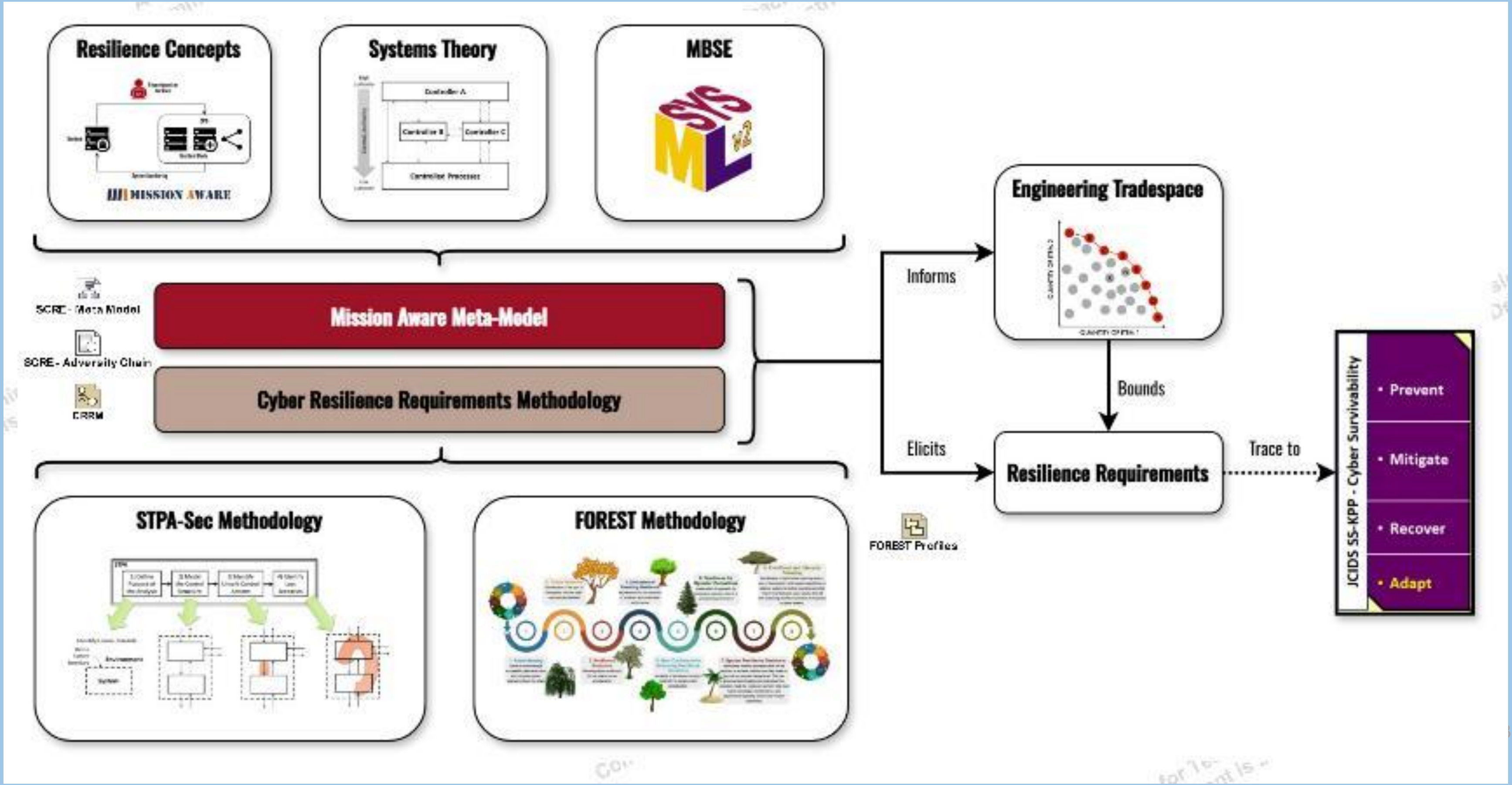
CSRM/Mission Aware Meta-model

Formal Methods

FOREST Meta-process model

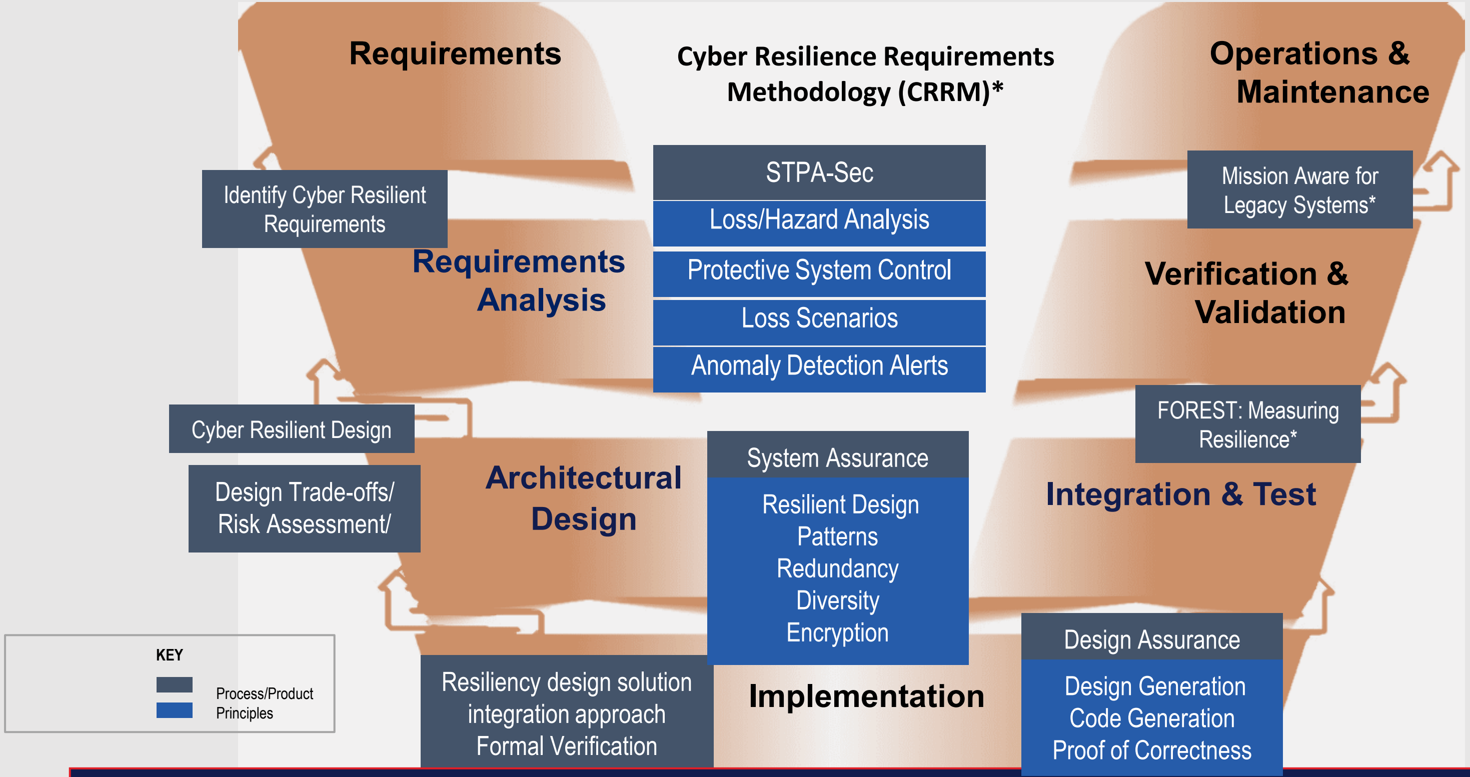
Cleared for open publication June 26,2025

Foundational Capabilities



Cleared for open publication June 26,2025

SCRE SE Methodologies (Processes & Principles)



Requirements

Cyber Resilience Requirements Methodology (CRRM)*

Operations & Maintenance

Identify Cyber Resilient Requirements

Requirements Analysis

STPA-Sec
- Loss/Hazard Analysis
- Protective System Control
- Loss Scenarios
- Anomaly Detection Alerts

Mission Aware for Legacy Systems*

Verification & Validation

Cyber Resilient Design

Design Trade-offs/ Risk Assessment/

Architectural Design

System Assurance
- Resilient Design Patterns
- Redundancy
- Diversity
- Encryption

FOREST: Measuring Resilience*

Integration & Test

Resiliency design solution integration approach
Formal Verification

Implementation

Design Assurance
- Design Generation
- Code Generation
- Proof of Correctness

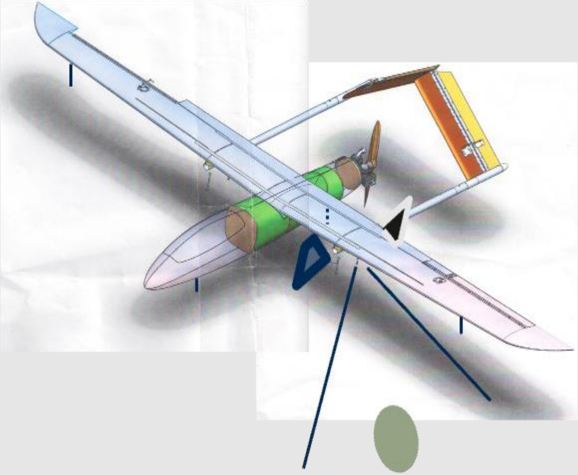
KEY

▬	Process/Product
▬	Principles

Integrating SCRE Principles and Processes into the Systems Engineering Process

Cleared for open publication June 26,2025

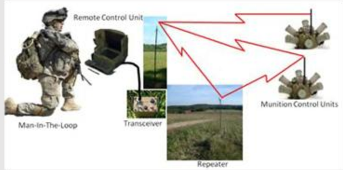
Previous Applications of SCRE


Surviellance Drone
(Army)

Ship Control
(Northrop Grumman)

3D Printers
(NIST)

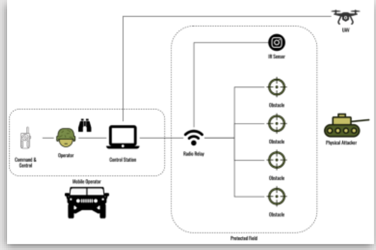
Human Factors Experiments
(Air Force)



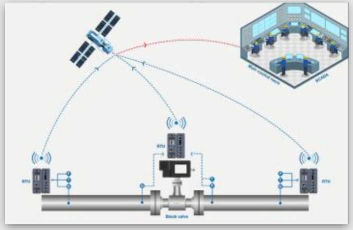
Networked Munitions
(Army)

Cars
(VA State Police)

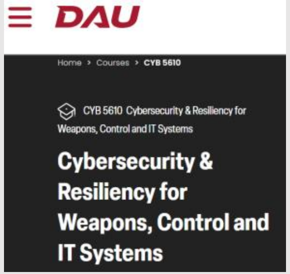
Industrial Control Sytems
(Mission Secure Inc)



Silverfish (Army)



Pipeline (ASD/RE)


DAU

Home > Courses > CYB 5610

CYB 5610 Cybersecurity & Resiliency for Weapons, Control and IT Systems

Cybersecurity & Resiliency for Weapons, Control and IT Systems

FLRAA (DTEA,
Army)

Dominion Energy
Powering Your Every Day
Coastal Virginia Offshore Wind
Coastal Virginia Offshore Wind
(CVOW) project is paving the way to a clean energy future in Virginia.
Wind Farms (R&E,
NNSA)

Cleared for open publication June 26,2025

Toward a Solution

Achieving Cyber Resilience

To achieve resilience, use the same ***System Engineering*** processes as when considering ***Safety***, ***Reliability*** and ***Survivability***

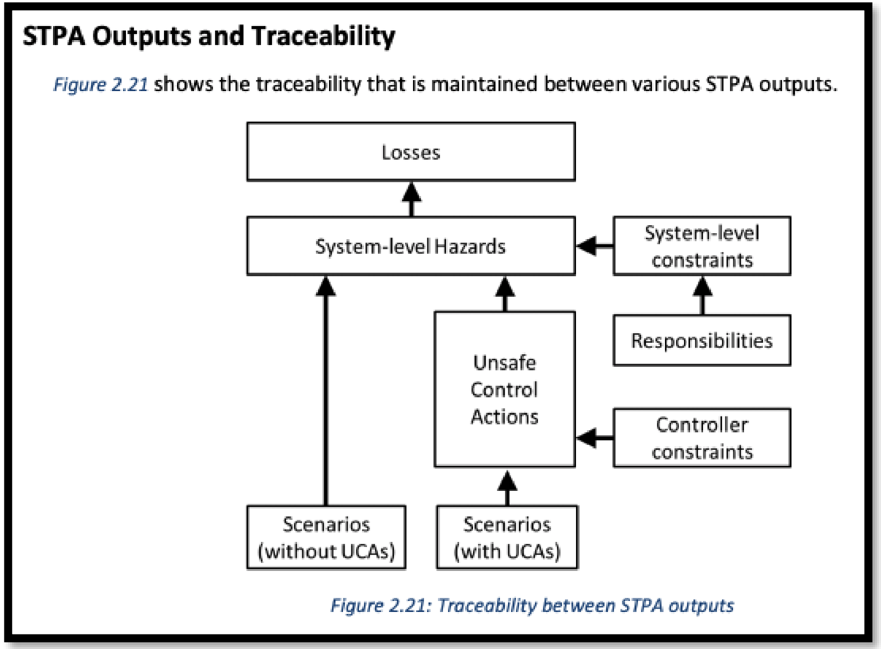
- Design in resilience
  - Engineered resilience responses
- Develop <u>measurable</u> cyber requirements alongside ***Performance***, ***Safety*** and other "-ility" requirements
  - Typical cyber requirements are security controls that do not relate directly to mission capability or defender response
- Use common ***Mitigate*** and ***Recover*** capabilities, <u>regardless of cause</u>, where possible
  - Loss-driven perspective

Cleared for open publication June 26,2025

Based on System Theoretic Process Assessment

STPA is an iterative, methodical hazard analysis technique to identify causes of hazardous conditions intended to improve or promote system safety. Systems-Theoretic Accident Model and Processes (STAMP) is the core modeling framework.

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



STPA Outputs and Traceability

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

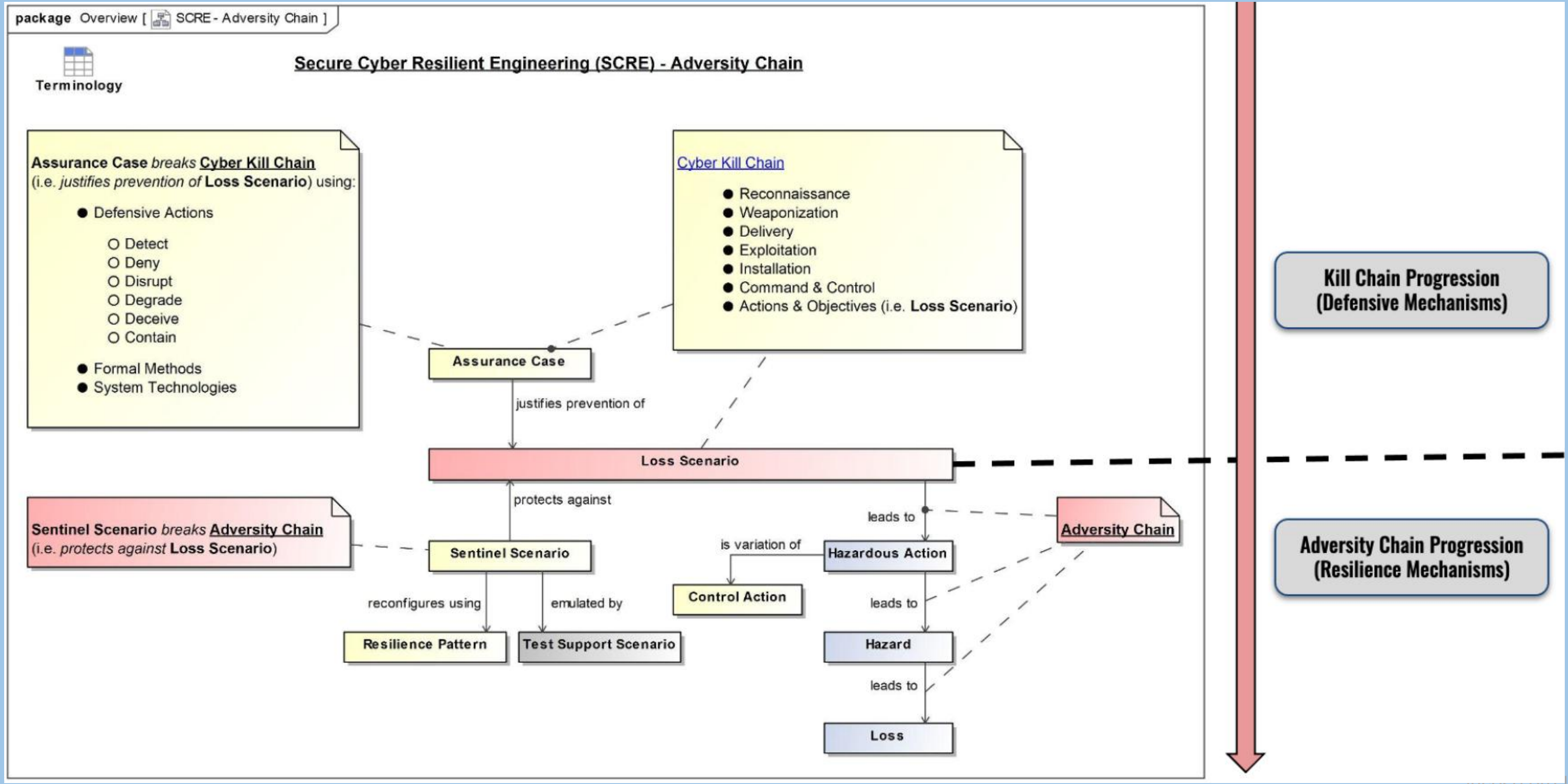
Figure 2.21: Traceability between STPA outputs

- 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.

Cleared for open publication June 26,2025

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

Use Models to Represent Adversity Chain and Assurance Cases



package Overview [SCRE - Adversity Chain]

Secure Cyber Resilient Engineering (SCRE) - Adversity Chain

Assurance Case *breaks* **Cyber Kill Chain**
(i.e. *justifies prevention of* **Loss Scenario**) using:

- Defensive Actions
  - ○ Detect
  - ○ Deny
  - ○ Disrupt
  - ○ Degrade
  - ○ Deceive
  - ○ Contain
- Formal Methods
- System Technologies

Cyber Kill Chain

- Reconnaissance
- Weaponization
- Delivery
- Exploitation
- Installation
- Command & Control
- Actions & Objectives (i.e. **Loss Scenario**)

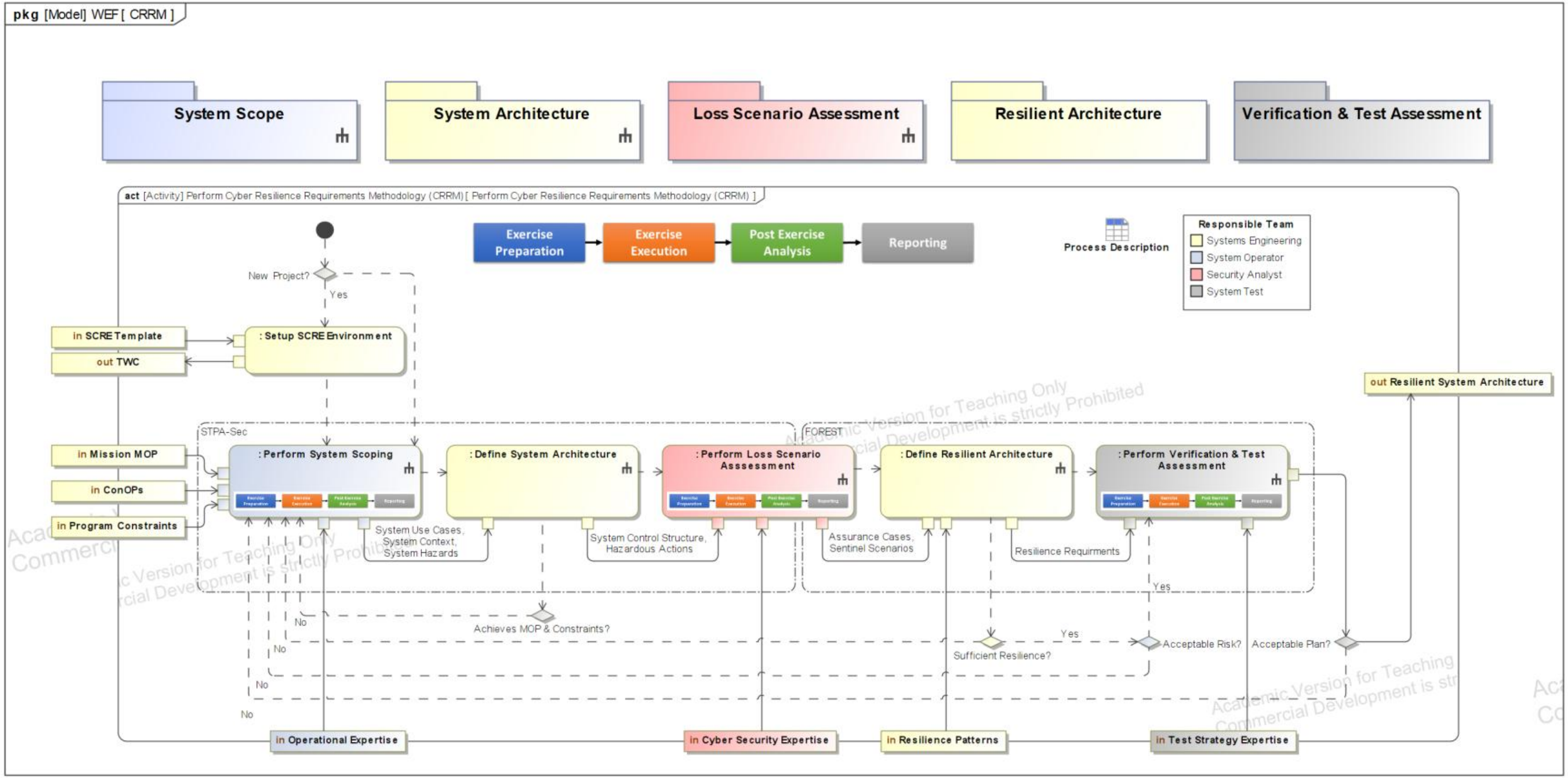
Sentinel Scenario *breaks* **Adversity Chain**
(i.e. *protects against* **Loss Scenario**)

Kill Chain Progression
(Defensive Mechanisms)

Adversity Chain Progression
(Resilience Mechanisms)

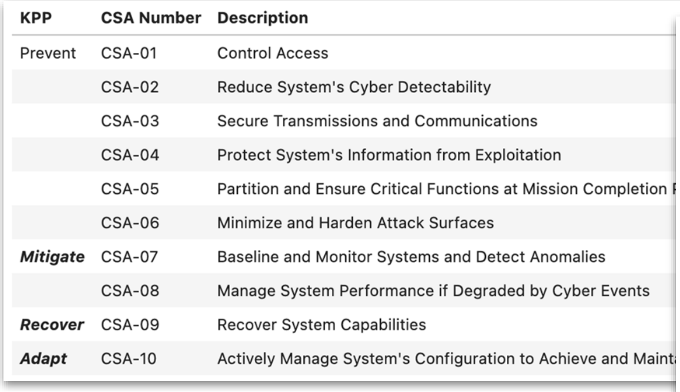
Cleared for open publication June 26,2025

Cyber Resilience Requirements Methodology

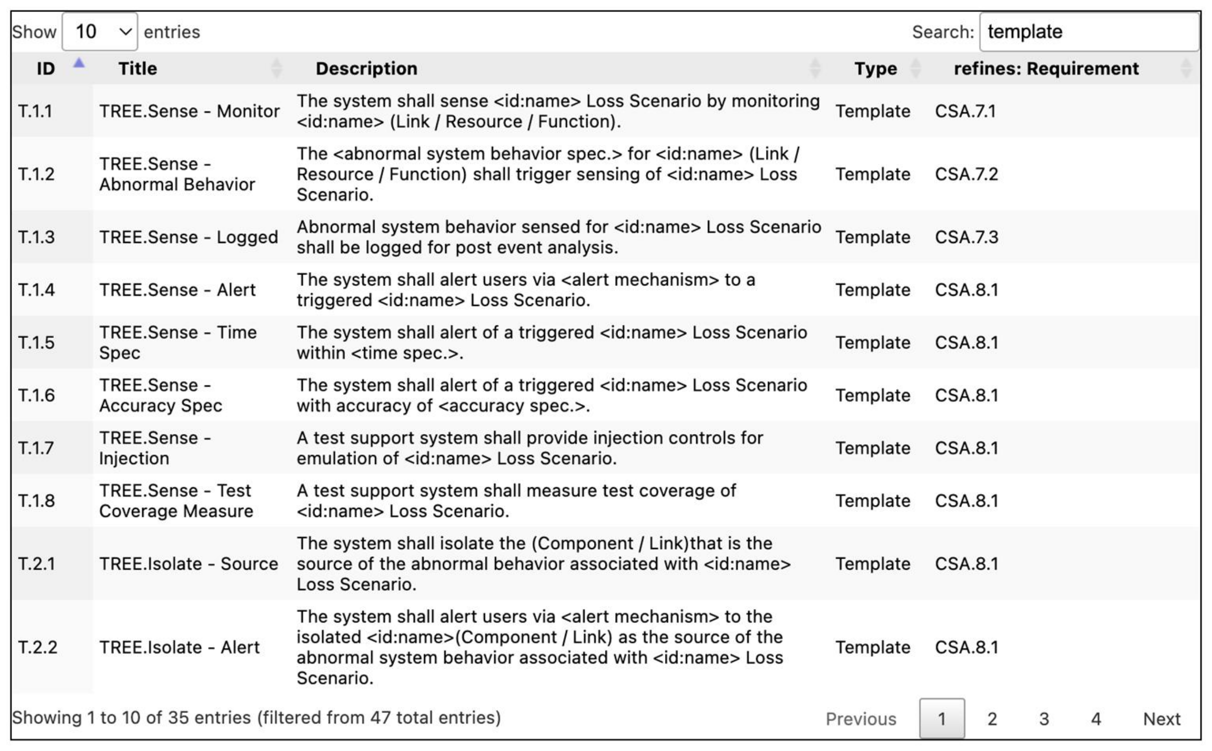


Cleared for open publication June 26,2025

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
	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



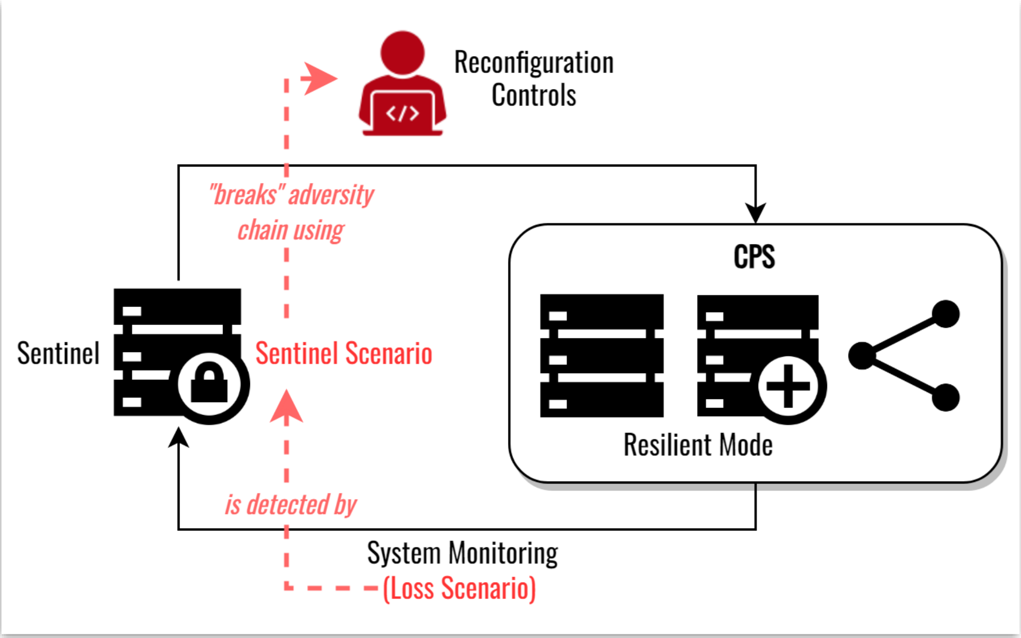
ID	Title	Description	Type	refines: Requirement
T.1.1	TREE.Sense - Monitor	The system shall sense <id:name> Loss Scenario by monitoring <id:name> (Link / Resource / Function).	Template	CSA.7.1
T.1.2	TREE.Sense - Abnormal Behavior	The <abnormal system behavior spec.> for <id:name> (Link / Resource / Function)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

Cleared for open publication June 26,2025

Resilience Mechanism – Breaking the Adversity Chain

Observe the System rather than the Adversary

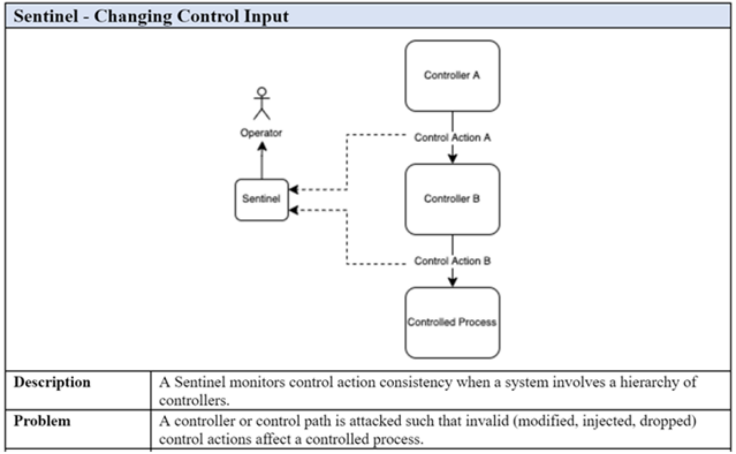


Can specify and test:

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

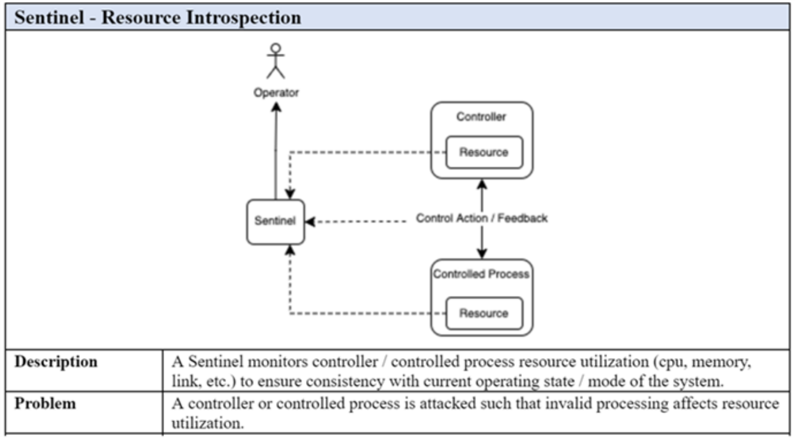
Cleared for open publication June 26,2025

Sentinel Patterns



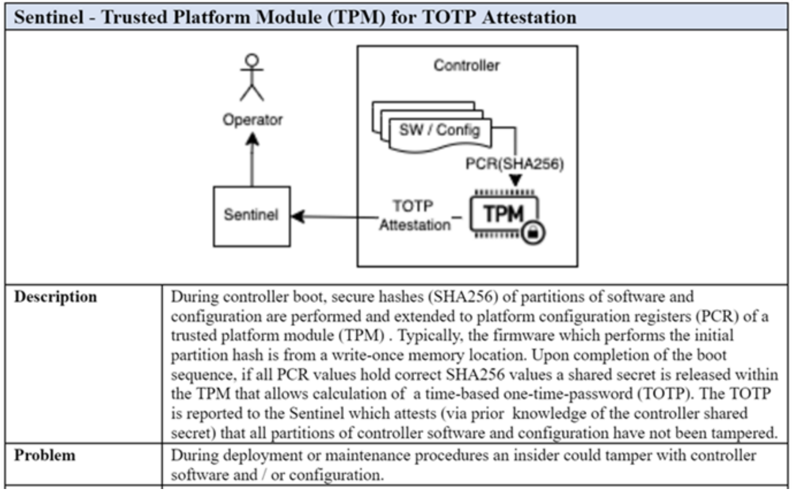
Sentinel - Changing Control Input

Description	A Sentinel monitors control action consistency when a system involves a hierarchy of controllers.
Problem	A controller or control path is attacked such that invalid (modified, injected, dropped) control actions affect a controlled process.



Sentinel - Resource Introspection

Description	A Sentinel monitors controller / controlled process resource utilization (cpu, memory, link, etc.) to ensure consistency with current operating state / mode of the system.
Problem	A controller or controlled process is attacked such that invalid processing affects resource utilization.

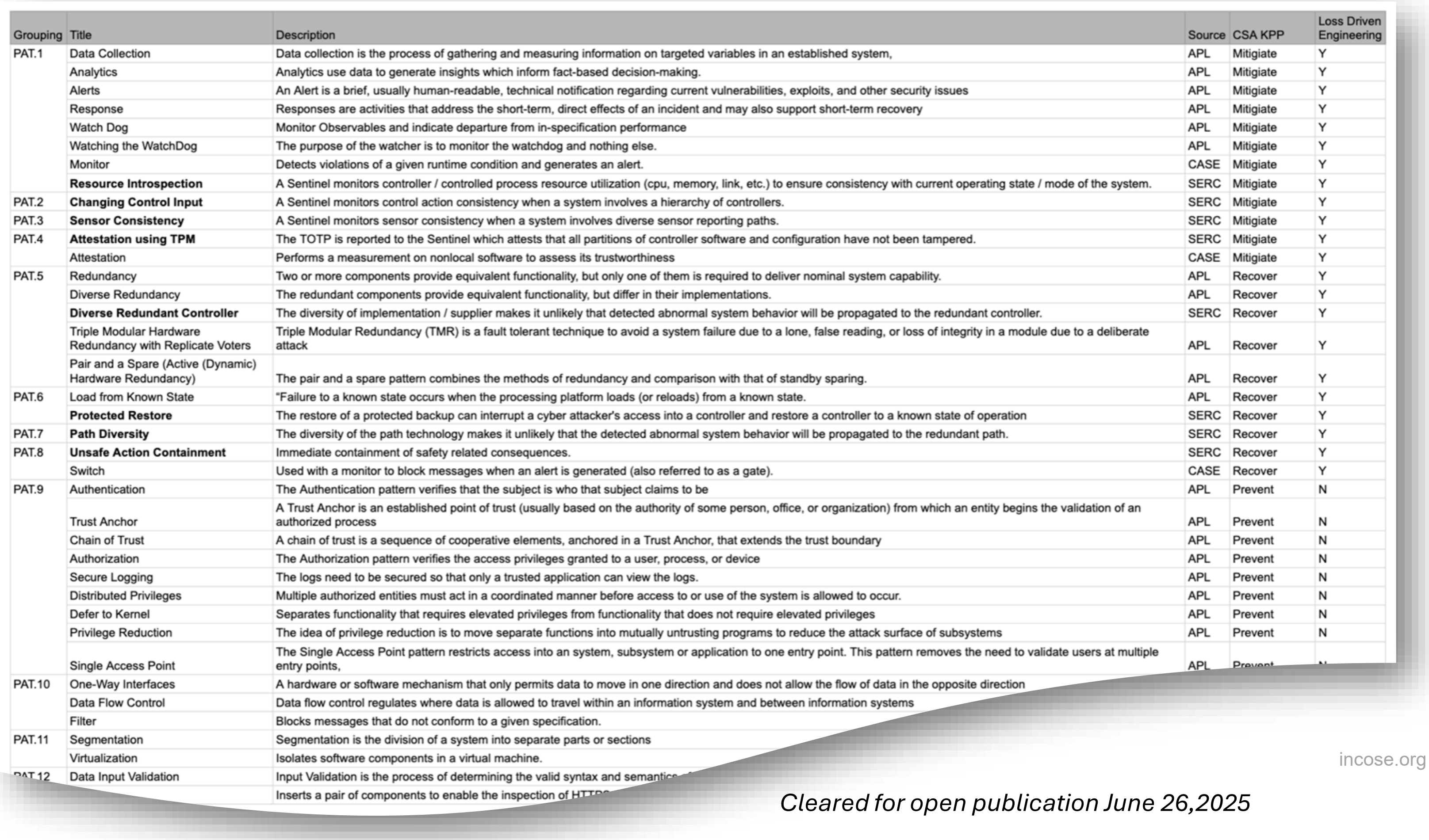


Sentinel - Trusted Platform Module (TPM) for TOTP Attestation

Description	During controller boot, secure hashes (SHA256) of partitions of software and configuration are performed and extended to platform configuration registers (PCR) of a trusted platform module (TPM) . Typically, the firmware which performs the initial partition hash is from a write-once memory location. Upon completion of the boot sequence, if all PCR values hold correct SHA256 values a shared secret is released within the TPM that allows calculation of a time-based one-time-password (TOTP). The TOTP is reported to the Sentinel which attests (via prior knowledge of the controller shared secret) that all partitions of controller software and configuration have not been tampered.
Problem	During deployment or maintenance procedures an insider could tamper with controller software and / or configuration.

Cleared for open publication June 26,2025

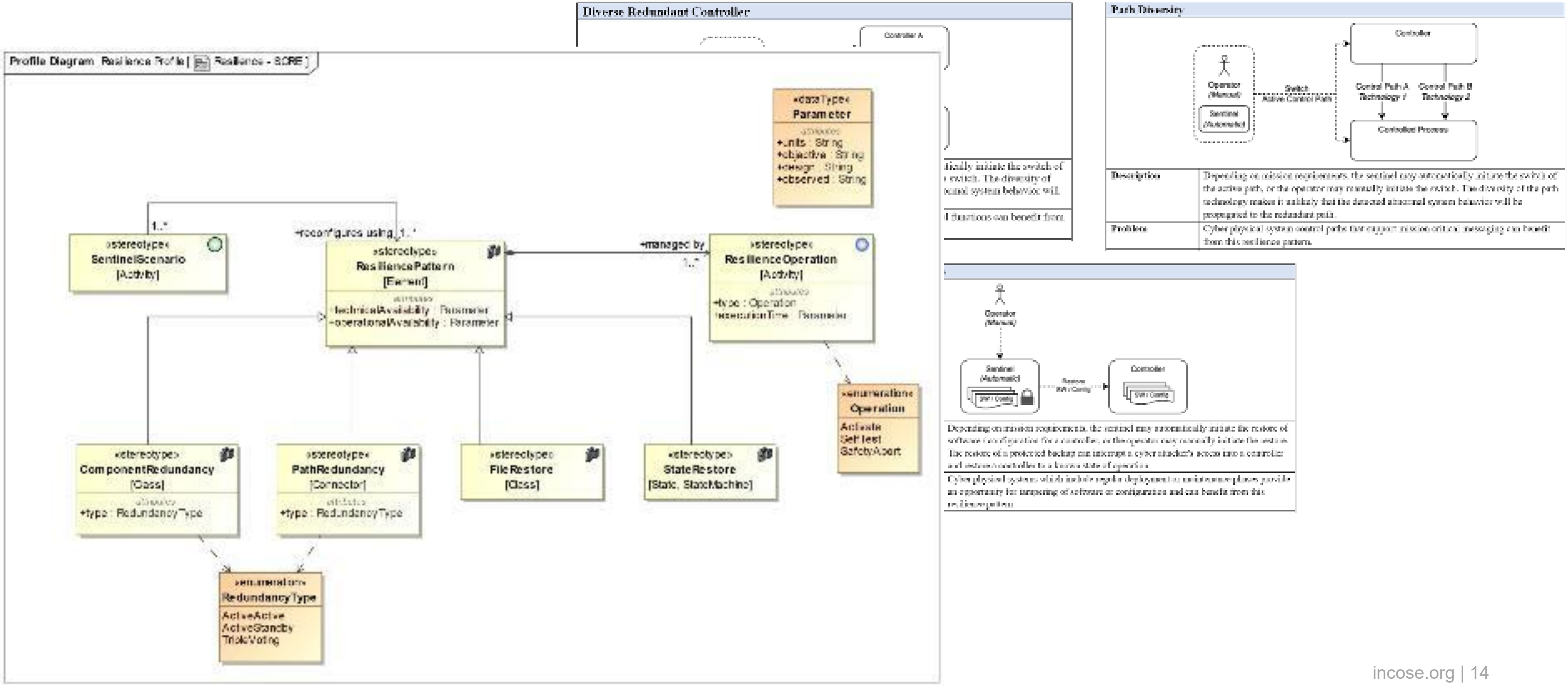
Resilience Pattern Catalog



Grouping	Title	Description	Source	CSA KPP	Loss Driven Engineering
PAT.1	Data Collection	Data collection is the process of gathering and measuring information on targeted variables in an established system,	APL	Mitigiate	Y
	Analytics	Analytics use data to generate insights which inform fact-based decision-making.	APL	Mitigiate	Y
	Alerts	An Alert is a brief, usually human-readable, technical notification regarding current vulnerabilities, exploits, and other security issues	APL	Mitigiate	Y
	Response	Responses are activities that address the short-term, direct effects of an incident and may also support short-term recovery	APL	Mitigiate	Y
	Watch Dog	Monitor Observables and indicate departure from in-specification performance	APL	Mitigiate	Y
	Watching the WatchDog	The purpose of the watcher is to monitor the watchdog and nothing else.	APL	Mitigiate	Y
	Monitor	Detects violations of a given runtime condition and generates an alert.	CASE	Mitigiate	Y
	Resource Introspection	A Sentinel monitors controller / controlled process resource utilization (cpu, memory, link, etc.) to ensure consistency with current operating state / mode of the system.	SERC	Mitigiate	Y
PAT.2	**Changing Control Input**	A Sentinel monitors control action consistency when a system involves a hierarchy of controllers.	SERC	Mitigiate	Y
PAT.3	**Sensor Consistency**	A Sentinel monitors sensor consistency when a system involves diverse sensor reporting paths.	SERC	Mitigiate	Y
PAT.4	**Attestation using TPM**	The TOTP is reported to the Sentinel which attests that all partitions of controller software and configuration have not been tampered.	SERC	Mitigiate	Y
	Attestation	Performs a measurement on nonlocal software to assess its trustworthiness	CASE	Mitigiate	Y
PAT.5	Redundancy	Two or more components provide equivalent functionality, but only one of them is required to deliver nominal system capability.	APL	Recover	Y
	Diverse Redundancy	The redundant components provide equivalent functionality, but differ in their implementations.	APL	Recover	Y
	Diverse Redundant Controller	The diversity of implementation / supplier makes it unlikely that detected abnormal system behavior will be propagated to the redundant controller.	SERC	Recover	Y
	Triple Modular Hardware Redundancy with Replicate Voters	Triple Modular Redundancy (TMR) is a fault tolerant technique to avoid a system failure due to a lone, false reading, or loss of integrity in a module due to a deliberate attack	APL	Recover	Y
	Pair and a Spare (Active (Dynamic) Hardware Redundancy)	The pair and a spare pattern combines the methods of redundancy and comparison with that of standby sparing.	APL	Recover	Y
PAT.6	Load from Known State	"Failure to a known state occurs when the processing platform loads (or reloads) from a known state.	APL	Recover	Y
	Protected Restore	The restore of a protected backup can interrupt a cyber attacker's access into a controller and restore a controller to a known state of operation	SERC	Recover	Y
PAT.7	**Path Diversity**	The diversity of the path technology makes it unlikely that the detected abnormal system behavior will be propagated to the redundant path.	SERC	Recover	Y
PAT.8	**Unsafe Action Containment**	Immediate containment of safety related consequences.	SERC	Recover	Y
	Switch	Used with a monitor to block messages when an alert is generated (also referred to as a gate).	CASE	Recover	Y
PAT.9	Authentication	The Authentication pattern verifies that the subject is who that subject claims to be	APL	Prevent	N
	Trust Anchor	A Trust Anchor is an established point of trust (usually based on the authority of some person, office, or organization) from which an entity begins the validation of an authorized process	APL	Prevent	N
	Chain of Trust	A chain of trust is a sequence of cooperative elements, anchored in a Trust Anchor, that extends the trust boundary	APL	Prevent	N
	Authorization	The Authorization pattern verifies the access privileges granted to a user, process, or device	APL	Prevent	N
	Secure Logging	The logs need to be secured so that only a trusted application can view the logs.	APL	Prevent	N
	Distributed Privileges	Multiple authorized entities must act in a coordinated manner before access to or use of the system is allowed to occur.	APL	Prevent	N
	Defer to Kernel	Separates functionality that requires elevated privileges from functionality that does not require elevated privileges	APL	Prevent	N
	Privilege Reduction	The idea of privilege reduction is to move separate functions into mutually untrusting programs to reduce the attack surface of subsystems	APL	Prevent	N
	Single Access Point	The Single Access Point pattern restricts access into an system, subsystem or application to one entry point. This pattern removes the need to validate users at multiple entry points,	APL	Prevent	N
PAT.10	One-Way Interfaces	A hardware or software mechanism that only permits data to move in one direction and does not allow the flow of data in the opposite direction			
	Data Flow Control	Data flow control regulates where data is allowed to travel within an information system and between information systems			
	Filter	Blocks messages that do not conform to a given specification.			
PAT.11	Segmentation	Segmentation is the division of a system into separate parts or sections			
	Virtualization	Isolates software components in a virtual machine.			
PAT.12	Data Input Validation	Input Validation is the process of determining the valid syntax and semantics			
		Inserts a pair of components to enable the inspection of HTTPS			

Cleared for open publication June 26,2025

Resilience Profile within SCRE Model (SysML v1)


Profile Diagram Resilience Profile [Resilience - SCRE]
«dataType» Parameter
attributes
+units : String
+objective : String
+design : String
+observed : String
1..*
+reconfigures using 1..*
+managed by
1..*
«stereotype» SentinelScenario [Activity]
«stereotype» ResiliencePattern [Element]
attributes
+technicalAvailability : Parameter
+operationalAvailability : Parameter
«stereotype» ResilienceOperation [Activity]
attributes
+type : Operation
+executionTime : Parameter
«enumeration» Operation
Activate
Self Test
SafetyAbort
«stereotype» ComponentRedundancy [Class]
attributes
+type : RedundancyType
«stereotype» PathRedundancy [Connector]
attributes
+type : RedundancyType
«stereotype» FileRestore [Class]
«stereotype» StateRestore [State, StateMachine]
«enumeration» RedundancyType
ActiveActive
ActiveStandby
TripleVoting
Diverse Redundant Controller
Controller A
Path Diversity
Controller
Operator (Manual)
Switch Active Control Path
Sentinel (Automated)
Control Path A Technology 1
Control Path B Technology 2
Controlled Process
Operator (Manual)
Sentinel (Automatic)
SW / Config
Restore SW / Config
Controller
SW / Config

tically initiate the switch of
e switch. The diversity of
ormal system behavior will

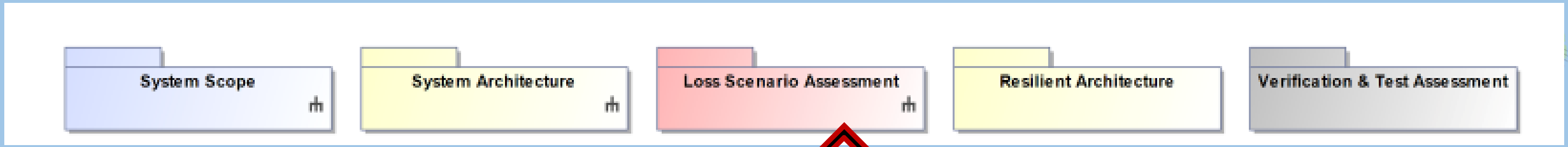
l functions can benefit from

Description	Depending on mission requirements, the sentinel may automatically initiate the switch of the active path, or the operator may manually initiate the switch. The diversity of the path technology makes it unlikely that the detected abnormal system behavior will be propagated to the redundant path.
Problem	Cyber physical system control paths that support mission critical messaging can benefit from this resilience pattern.

Depending on mission requirements, the sentinel may automatically initiate the restore of software / configuration for a controller, or the operator may manually initiate the restore. The restore of a protected backup can interrupt a cyber attacker's access into a controller and restore a controller to a known state of operation.

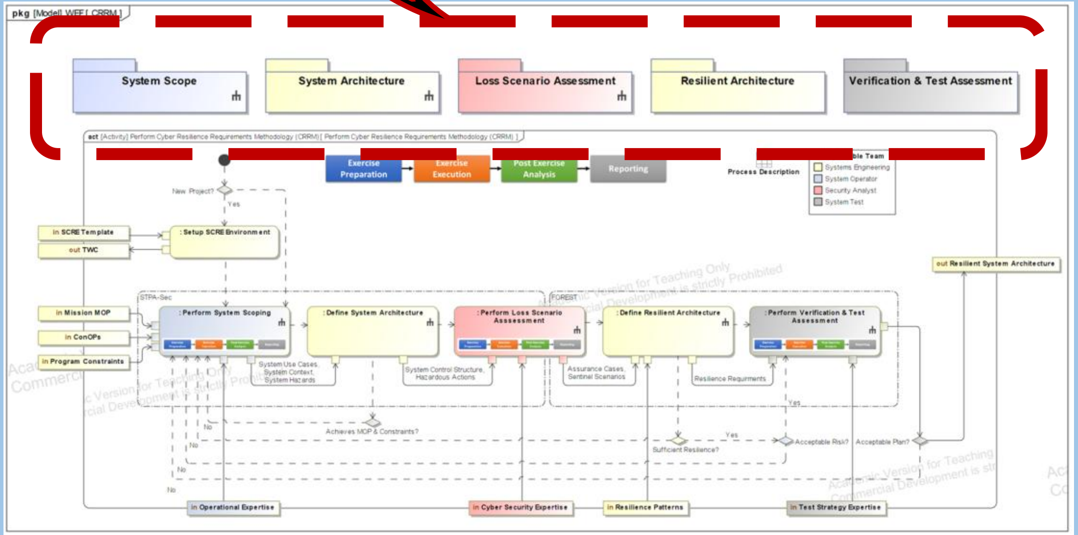
Cyber physical systems which include regular deployment or maintenance phases provide an opportunity for tampering of software or configuration and can benefit from this resilience pattern.

Cleared for open publication June 26,2025



Offshore Wind Farms: Modeling system transitions from a loss scenario to mitigate cascading failures

SCRE's simulation methods for balancing resilience trade-offs and its applications. The SERC team performed Resilience-Driven, Loss-Based Cyber Table Tops to derive loss scenarios.



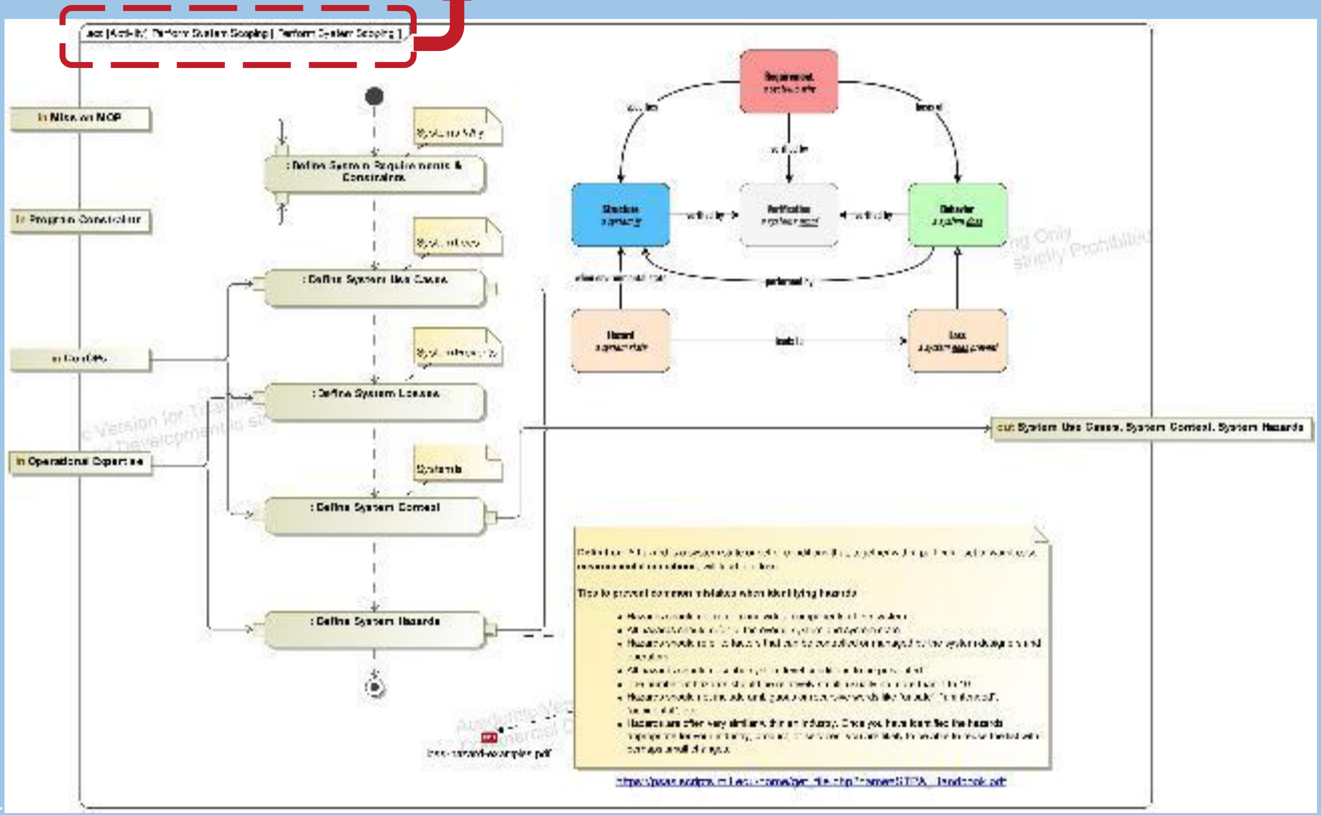
Cleared for open publication June 26,2025

Perform System Scoping

"A system to do {What = Purpose} by means of {How = Method} in order to contribute to {Why = Goals}"

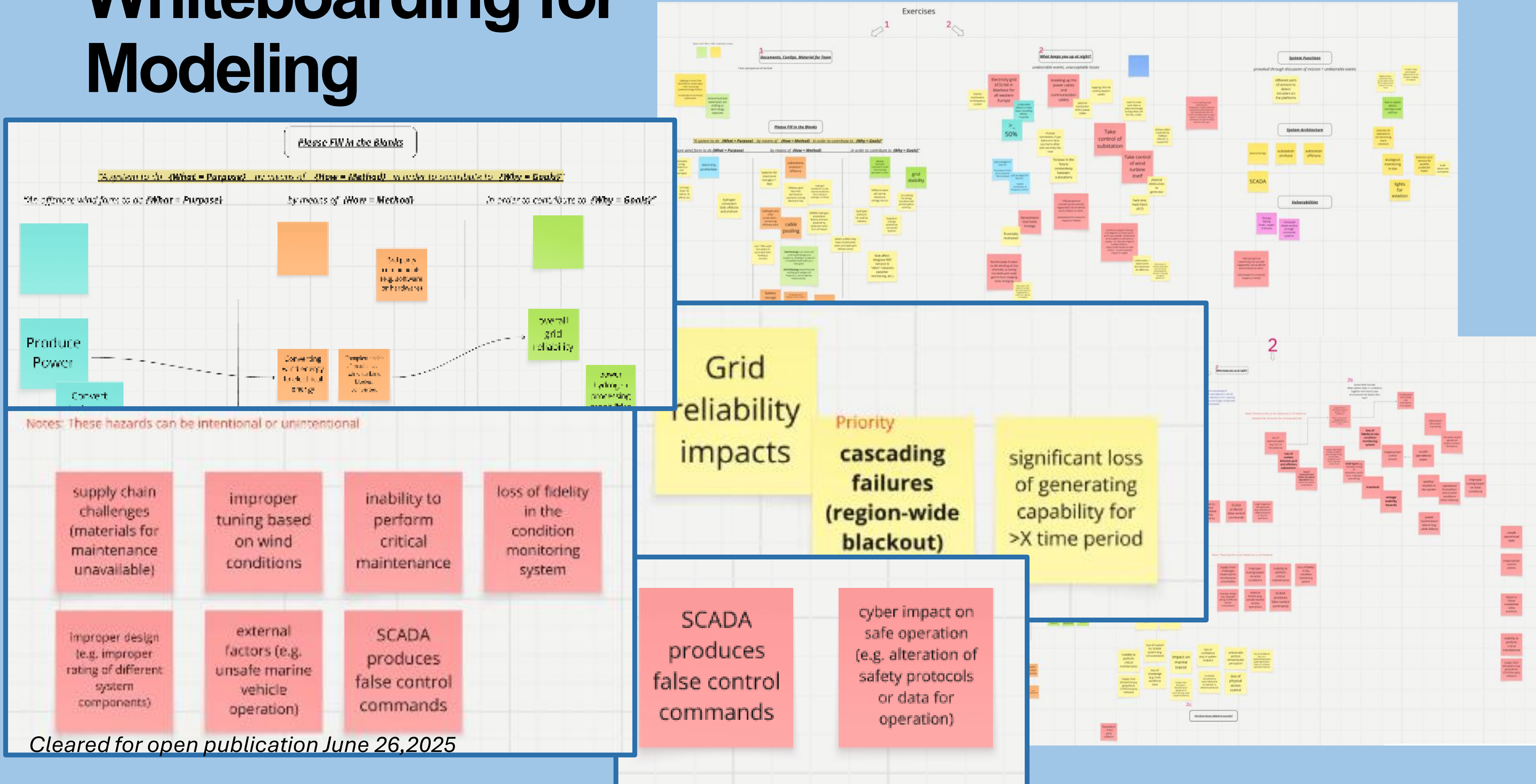
What keeps you up at night? Undesirable events, unacceptable losses

act [Activity] Perform System Scoping [Perform System Scoping]


act [Activity] Perform System Scoping [Perform System Scoping]
in Mission NOP
in Program Constraints
in ConOPs
in Operational Expertise
: Define System Requirements & Constraints
: Define System Use Cases
: Define System Losses
: Define System Context
: Define System Hazards
System
Requirement
Structure
Verification
Behavior
Hazard
Loss
verified by
performed by
leads to
out System Use Cases, System Context, System Hazards
Tips to prevent common mistakes when identifying hazards

Cleared for open publication June 26,2025

Whiteboarding for Modeling



Please Fill in the Blanks

"A system to do {What = Purpose} by means of {How = Method} in order to contribute to {Why = Goals}"

"An offshore wind farm to do {What = Purpose} by means of {How = Method} in order to contribute to {Why = Goals}"

Notes: These hazards can be intentional or unintentional

- supply chain challenges (materials for maintenance unavailable)
- improper tuning based on wind conditions
- inability to perform critical maintenance
- loss of fidelity in the condition monitoring system
- improper design (e.g. improper rating of different system components)
- external factors (e.g. unsafe marine vehicle operation)
- SCADA produces false control commands

Grid reliability impacts

Priority cascading failures (region-wide blackout)

significant loss of generating capability for >X time period

SCADA produces false control commands

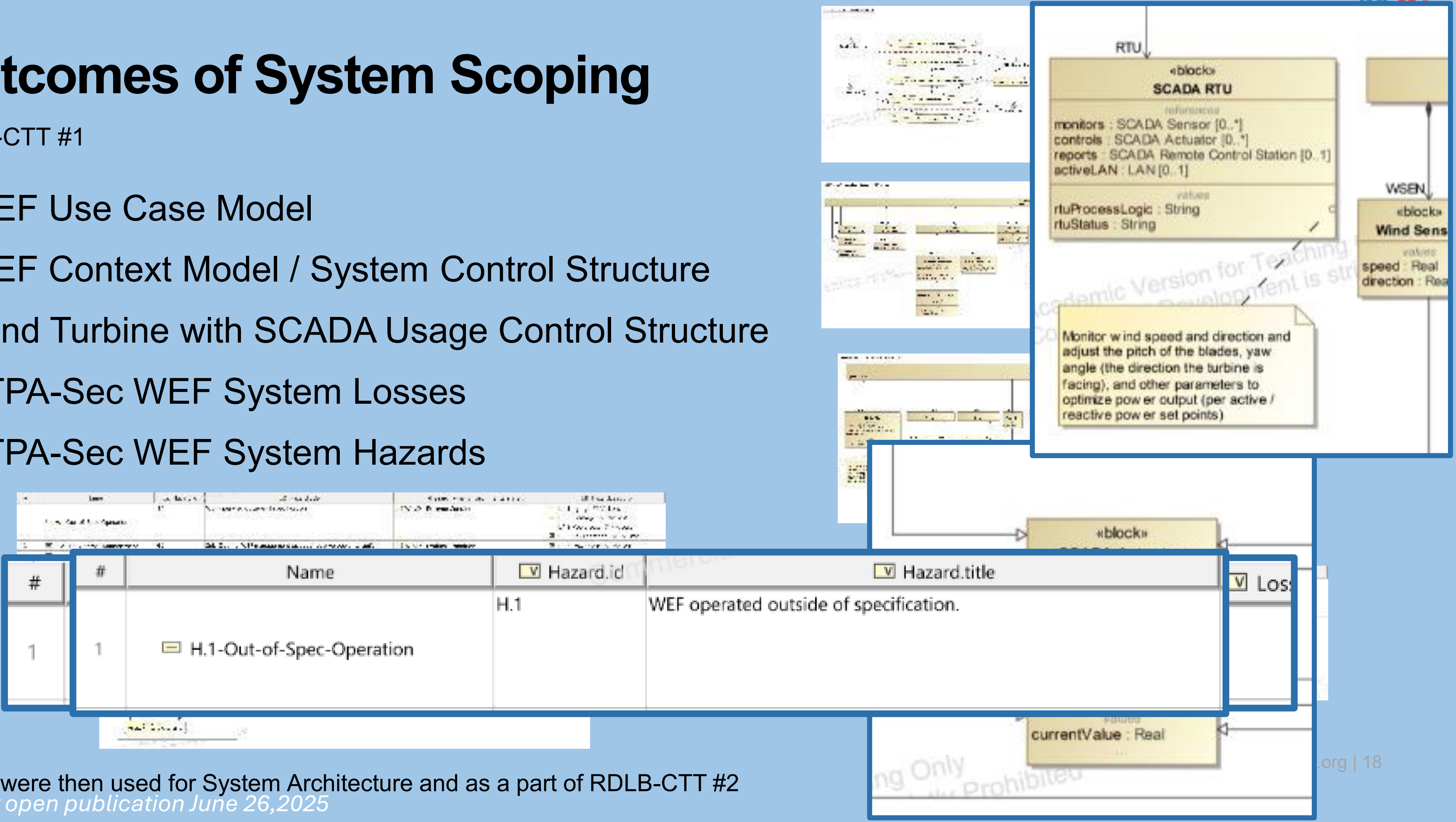
cyber impact on safe operation (e.g. alteration of safety protocols or data for operation)

Cleared for open publication June 26,2025

Outcomes of System Scoping

RDLB-CTT #1

- WEF Use Case Model
- WEF Context Model / System Control Structure
- Wind Turbine with SCADA Usage Control Structure
- STPA-Sec WEF System Losses
- STPA-Sec WEF System Hazards



RTU
«block»
SCADA RTU
references
monitors : SCADA Sensor [0..*]
controls : SCADA Actuator [0..*]
reports : SCADA Remote Control Station [0..1]
activeLAN : LAN [0..1]
values
rtuProcessLogic : String
rtuStatus : String
WSEN
«block»
Wind Sens
values
speed : Real
direction : Rea
Monitor wind speed and direction and adjust the pitch of the blades, yaw angle (the direction the turbine is facing), and other parameters to optimize power output (per active / reactive power set points)
«block»
values
currentValue : Real

#	#	Name	Hazard.id	Hazard.title	Los
1	1	H.1-Out-of-Spec-Operation	H.1	WEF operated outside of specification.	

These were then used for System Architecture and as a part of RDLB-CTT #2

Cleared for open publication June 26,2025

Loss Scenario Assessment

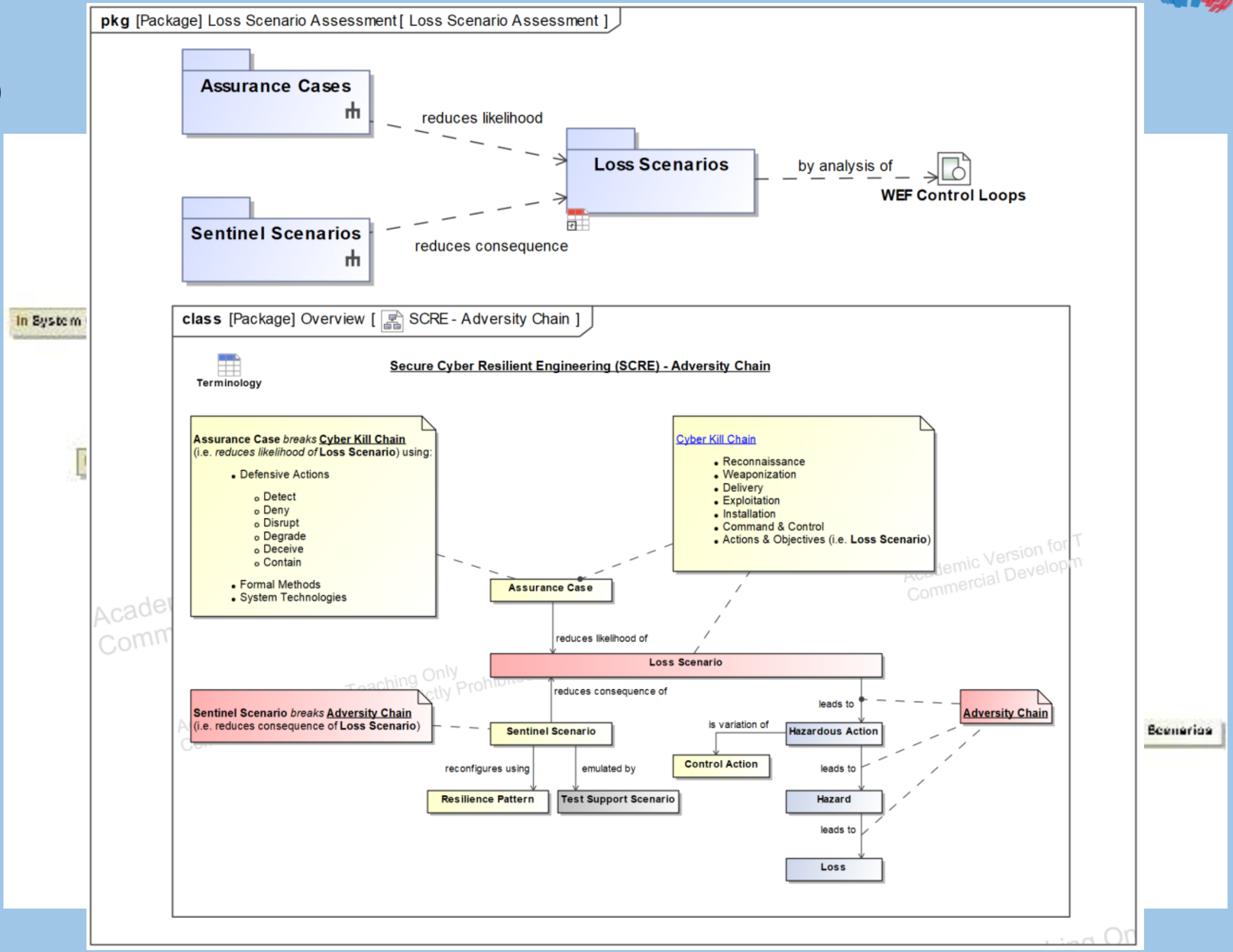
Hazardous Control Actions and Loss Scenarios

Evaluate the chosen Loss Scenario

Reduce likelihood via Assurance case

And/or

Reduce consequence via Sentinel Scenario (how to detect) / Resilient Mode (what is reconfigured)



pkg [Package] Loss Scenario Assessment [Loss Scenario Assessment]
Assurance Cases
Sentinel Scenarios
reduces likelihood
reduces consequence
Loss Scenarios
by analysis of
WEF Control Loops
class [Package] Overview [SCRE - Adversity Chain]
Secure Cyber Resilient Engineering (SCRE) - Adversity Chain
Terminology
In System
Scenarios

Assurance Case *breaks* **Cyber Kill Chain**
(i.e. *reduces likelihood of* **Loss Scenario**) using:

- Defensive Actions
  - Detect
  - Deny
  - Disrupt
  - Degrade
  - Deceive
  - Contain
- Formal Methods
- System Technologies

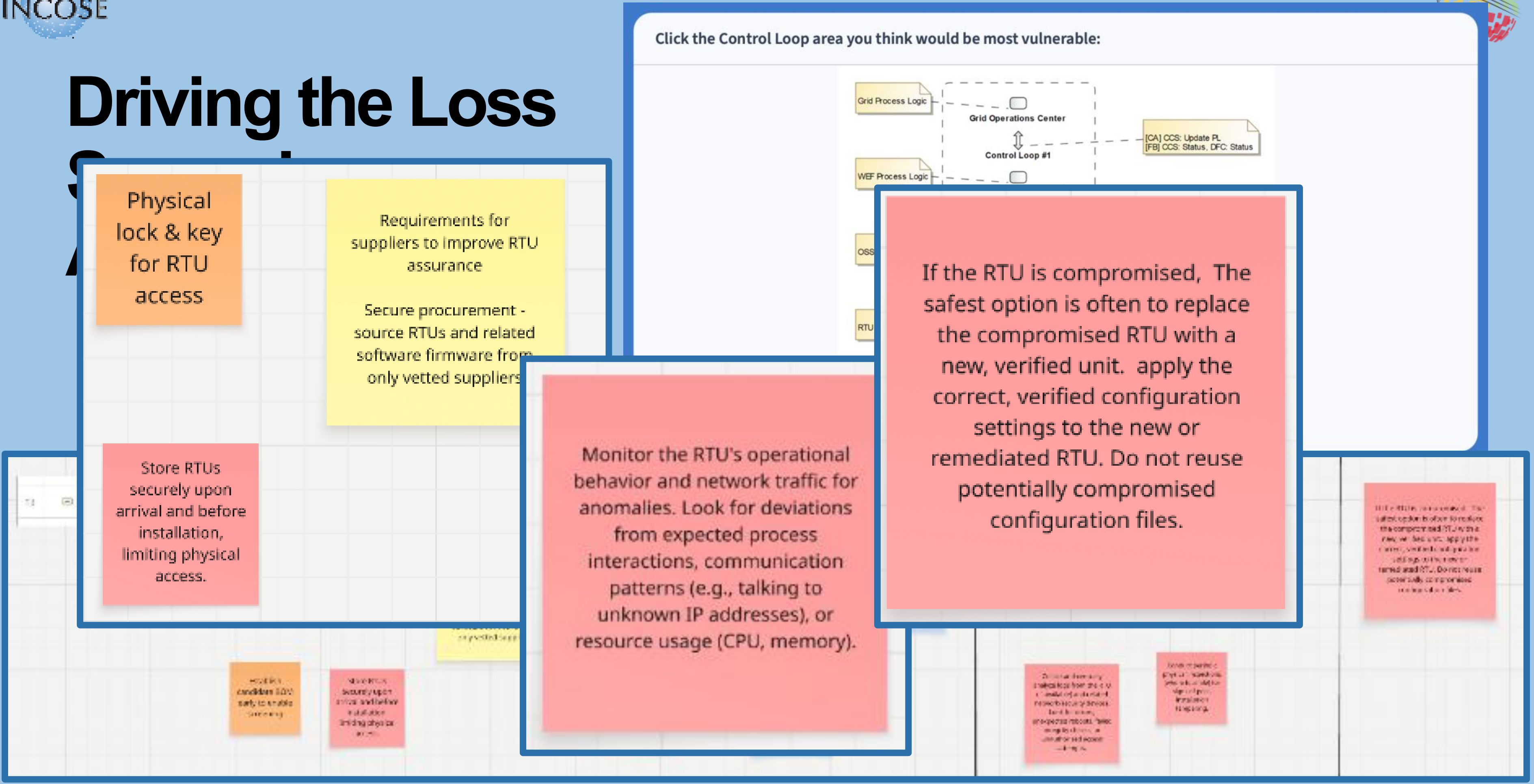
Cyber Kill Chain

- Reconnaissance
- Weaponization
- Delivery
- Exploitation
- Installation
- Command & Control
- Actions & Objectives (i.e. **Loss Scenario**)

Sentinel Scenario *breaks* **Adversity Chain**
(i.e. reduces consequence of **Loss Scenario**)

Cleared for open publication June 26,2025

Driving the Loss



Click the Control Loop area you think would be most vulnerable:

Physical lock & key for RTU access

Requirements for suppliers to improve RTU assurance

Secure procurement - source RTUs and related software firmware from only vetted suppliers

Store RTUs securely upon arrival and before installation, limiting physical access.

Monitor the RTU's operational behavior and network traffic for anomalies. Look for deviations from expected process interactions, communication patterns (e.g., talking to unknown IP addresses), or resource usage (CPU, memory).

If the RTU is compromised, The safest option is often to replace the compromised RTU with a new, verified unit. apply the correct, verified configuration settings to the new or remediated RTU. Do not reuse potentially compromised configuration files.

Outcomes from Loss Scenario Assessment

From RDLB-CTT #2

- Prioritized Control Loop with Example Mitigations
- Example Assurance Cases
- Example Sentinel Scenario
- **Updated WEF Model with Resilient Architecture**
- Updated Offshore Substation with Resilient Components
- Updated Wind Turbine Model with Resilient Components

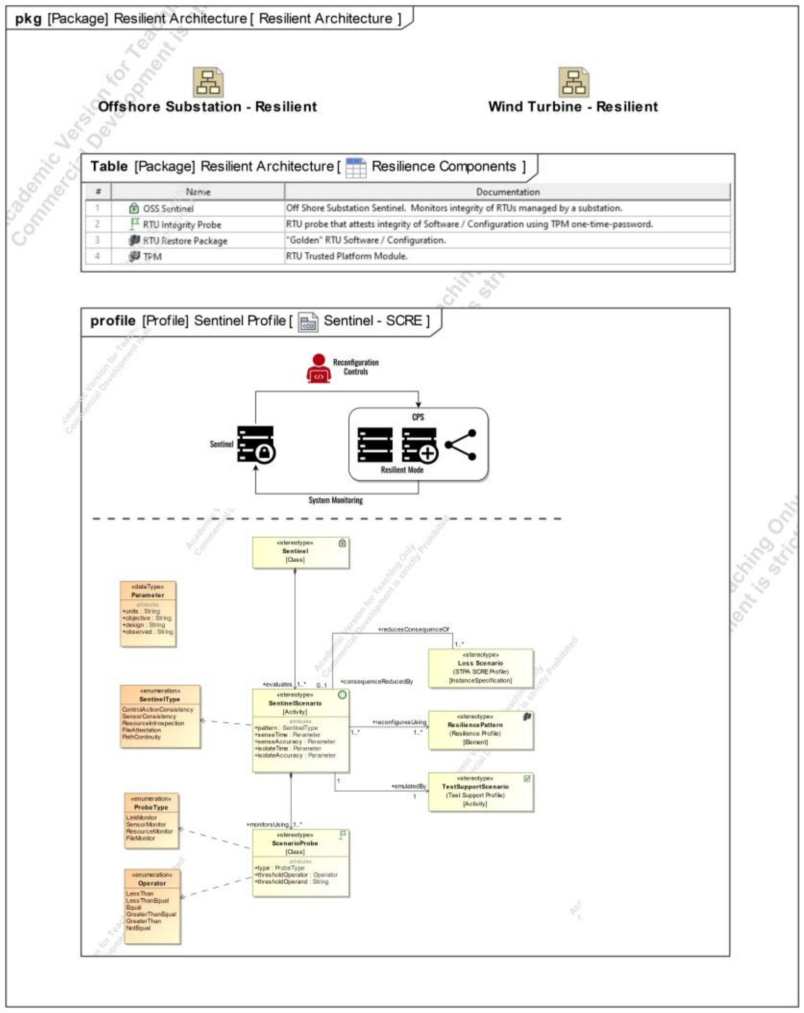
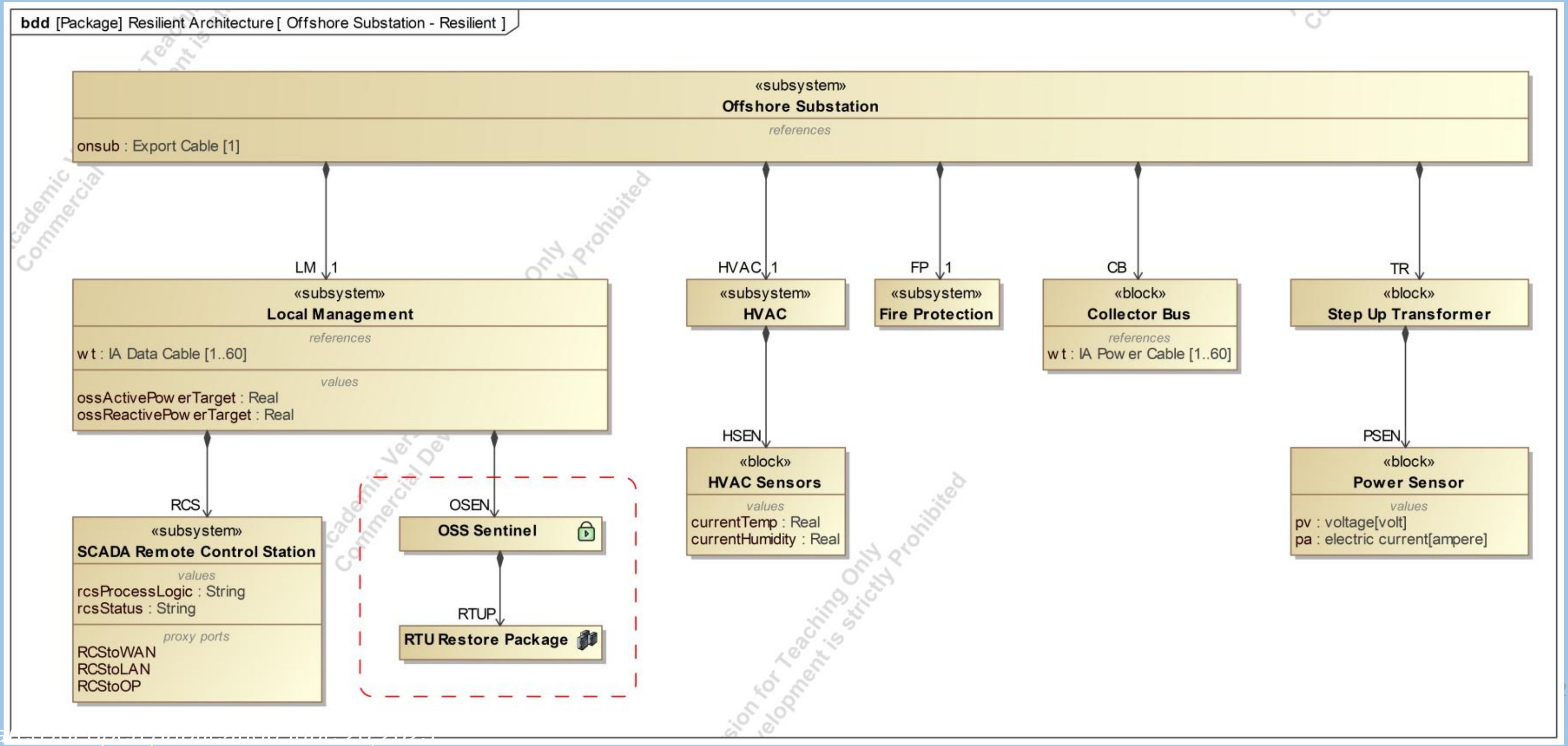

pkg [Package] Resilient Architecture [Resilient Architecture]
Offshore Substation - Resilient
Wind Turbine - Resilient

Table [Package] Resilient Architecture [Resilience Components]

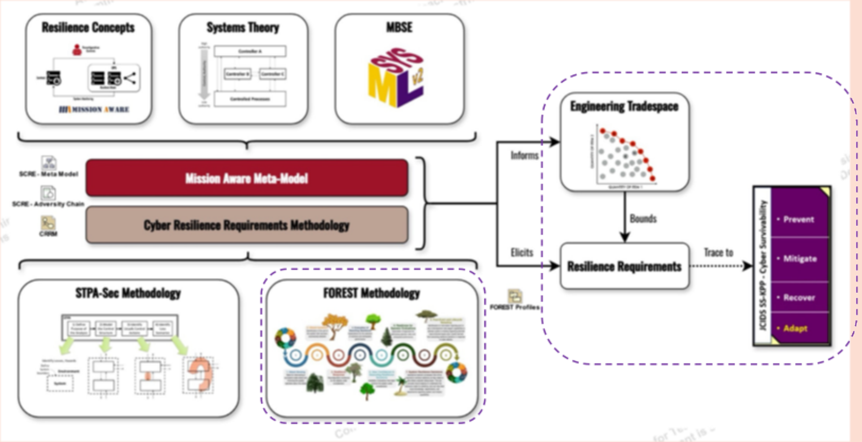
#	Name	Documentation
1	OSS Sentinel	Off Shore Substation Sentinel. Monitors integrity of RTUs managed by a substation.
2	RTU Integrity Probe	RTU probe that attests integrity of Software / Configuration using TPM one-time-password.
3	RTU Restore Package	"Golden" RTU Software / Configuration.
4	TPM	RTU Trusted Platform Module.

Cleared for open publication June 26,2025

Updated WEF Model with Resilient Architecture, cont.



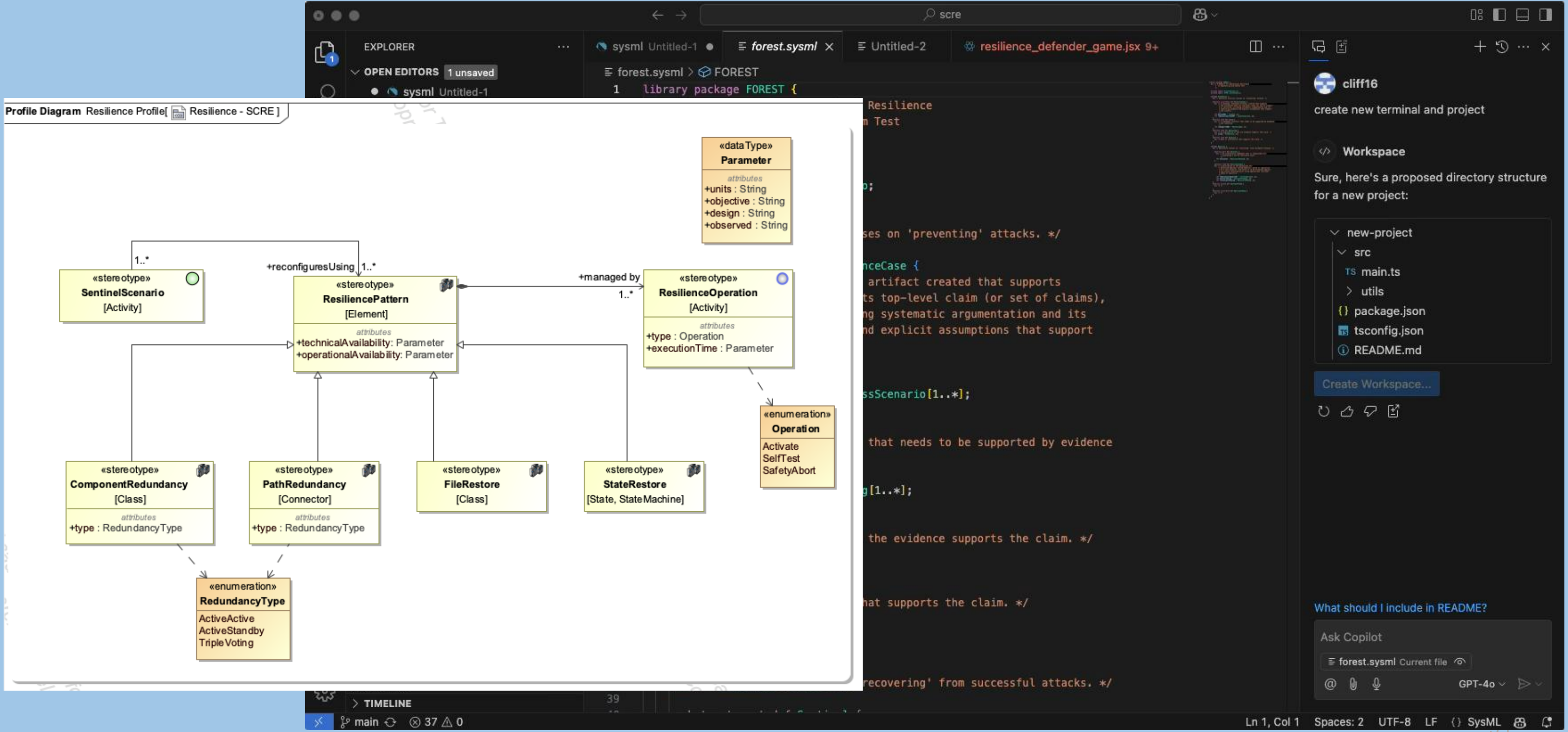
Verification and Test Assessment



- Provide the SCRE Requirement Traceability – linking Sentinel Scenarios and risk assessments from CTT #2 into structured, testable requirements.
- Illustrate the Integration into MBSE Artifacts – modeling SCREs within the Cameo environment to inform design and decision-making.
- Perform Verification Strategy Development – exploring test methods for both cyber assurance and resilience mechanisms.
- Perform Tradespace Exploration – identifying constraints, risks, and impacts of resilience measures on the overall system design.
- Review Planning Forward – preparing a roadmap for how SCREs and resilience goals would be verified throughout the lifecycle.

Cleared for open publication June 26,2025

FOREST into SysML v2



```
library package FOREST {
 Resilience
m Test
o;
ses on 'preventing' attacks. */
nceCase {
 artifact created that supports
ts top-level claim (or set of claims),
ng systematic argumentation and its
nd explicit assumptions that support
ssScenario[1..*];
 that needs to be supported by evidence
g[1..*];
 the evidence supports the claim. */
hat supports the claim. */
recovering' from successful attacks. */
```

cliff16

create new terminal and project

Workspace

Sure, here's a proposed directory structure for a new project:

```
new-project
  src
    main.ts
    utils
  package.json
  tsconfig.json
  README.md
```

Create Workspace...

What should I include in README?

Ask Copilot

forest.sysml Current file

GPT-4o

Cleared for open publication June 26,2025

Summary

- Rigorous SE process for designing cyber resilience into systems, as early as conceptualization
- Table-top driven evaluations based on STPA-Sec and loss-driven analysis
  - Focused on control flows
- Produces more detailed requirements than other approaches
- Specifically defines test and measurement criteria (FOREST)
- All aspects of the threat, analysis, and design captured in MBSE
- “Sentinel” functions validated to provide protection in real-world cases

35th Annual INCOSE international symposium

hybrid event

Ottawa, Canada
July 26 - 31, 2025

Tom McDermott: tmcdermo@stevens.edu