SYSTEMS ENGINEERING RESEARCH CENTER

WWW.SERCUARC.ORG

Secure Cyber Resilient Engineering: Methods and Tools

November 12, 2024

Peter Beling & Tom McDermott

NATIONAL SECURITY INSTITUTE
VIRGINIA TECH

STEVENS INSTITUTE of TECHNOLOGY

RESEARCH TEAM

Virginia Tech
- Peter Beling
- Tim Sherburne
- Kelli Esser
- Nicole Hutchison
- Mary Nerayo
- Geoff Kerr

Stevens Institute of Technology
- Tom McDermott
- Megan Clifford

Related Prior SERC Projects
- WRT-1087: Center for Offshore Wind Energy
- WRT-1072: Mission Resilience Pilot
- WRT-1043: DAU Digital Engineering Simulation (SCRE methodology & courses)
- 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

Secure Cyber Resilient Engineering (SCRE)

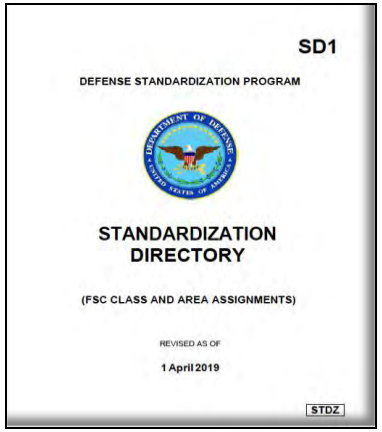
Cyber Resiliency Engineering

CNSSI 4009: "*The ability of systems to resist, absorb, and recover from or adapt to an adverse occurrence during operations that may cause harm, destruction, or loss of ability to perform mission-related functions.*"

NIST 800-160 v2 states: "*Cyber resiliency engineering intends to architect, design, develop, implement, maintain, and sustain the trustworthiness of systems with the capability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises that use or are enabled by cyber resources.*"

INCOSE: "*The ability of an engineered system to provide required capability when facing adversity. This includes the ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources.*"

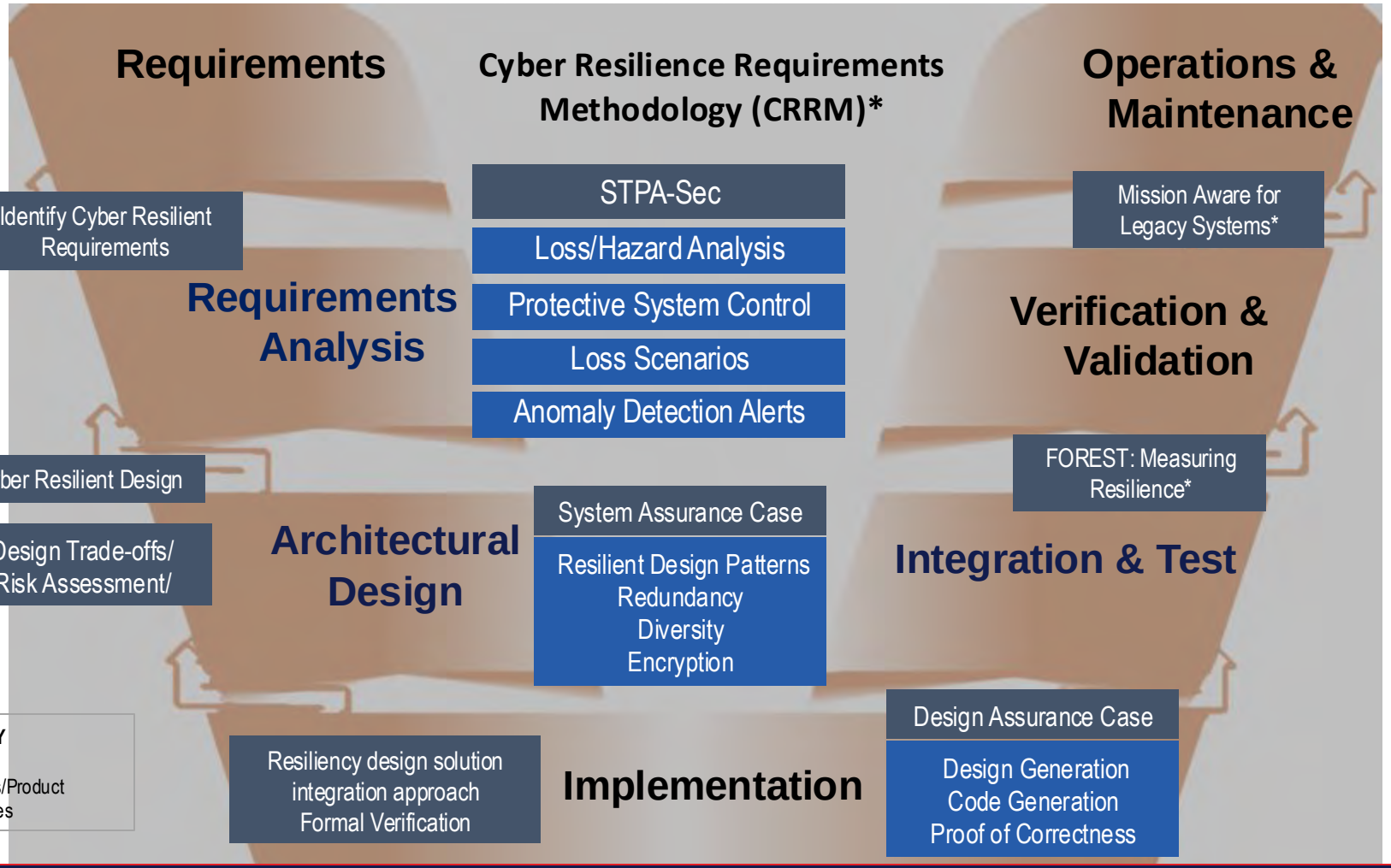
DI 5000.83 assigns responsibilities to USD(R&E) to: "*Establish and maintain S&T and program protection policy, guidance, education and training to manage technical risk, including: … Engineering secure cyber resilient systems.*"



SCRE Standardization Area

- Covers the ***integration of life cycle security and protection considerations*** in the requirements, design, test, demonstration, operations, maintenance, sustainment, and disposal of military systems that operate in physical and cyberspace operational domains
- Specifically encompasses the standards, specifications, methods, practices, techniques, and data requirements ***for the security aspects of systems engineering*** activities executed and artifacts produced, with explicit consideration of malicious and non-malicious adversity

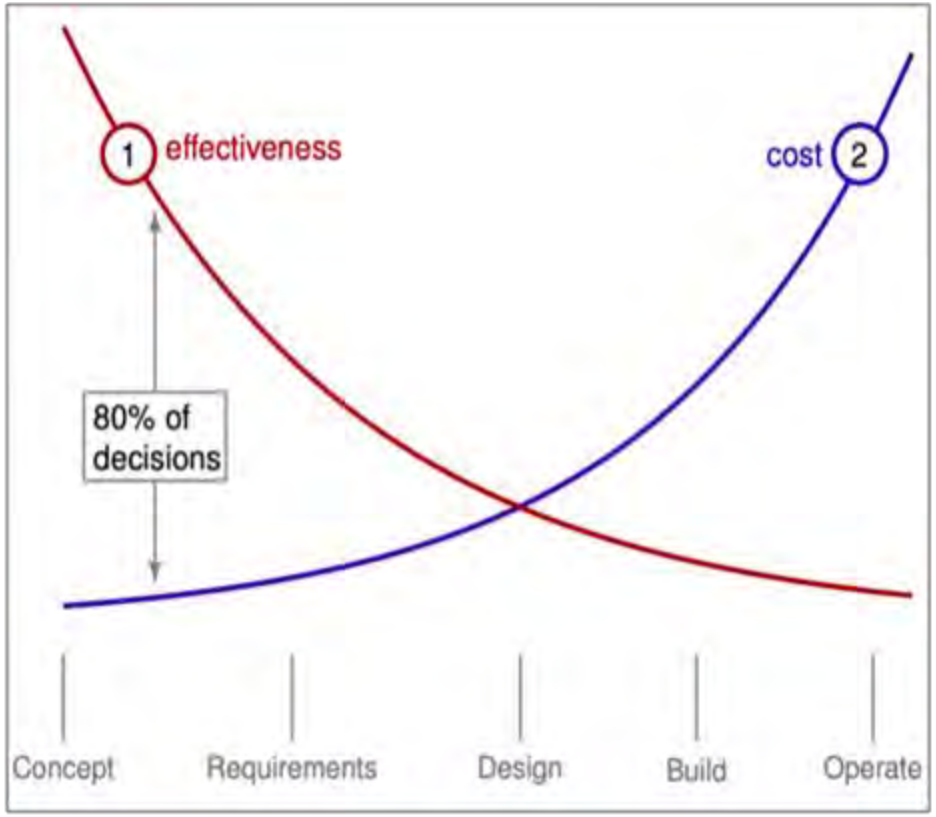
SCRE Methodologies (Processes & Principles)

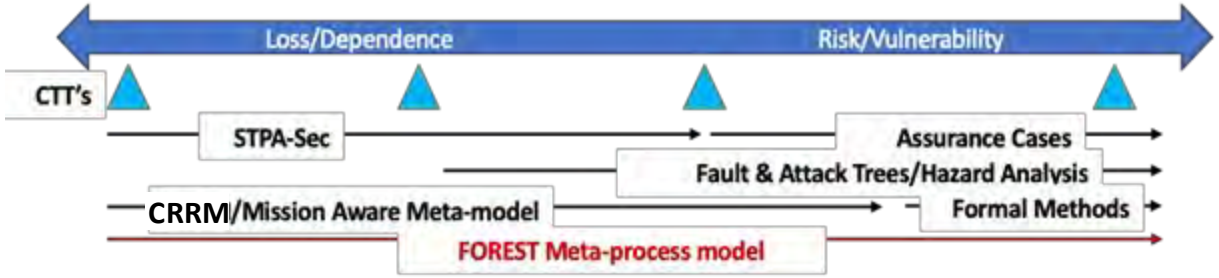


Integrating SCRE Principles and Processes into the Systems Engineering Process

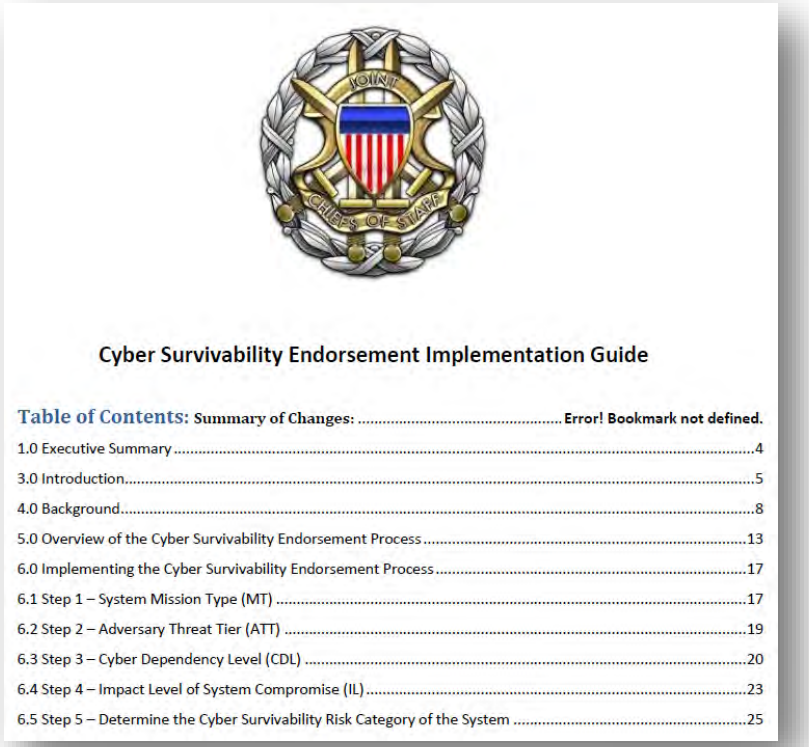
RESILIENCE & ASSURANCE METHODOLOGIES – FULL SYSTEM LIFE CYCLE

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



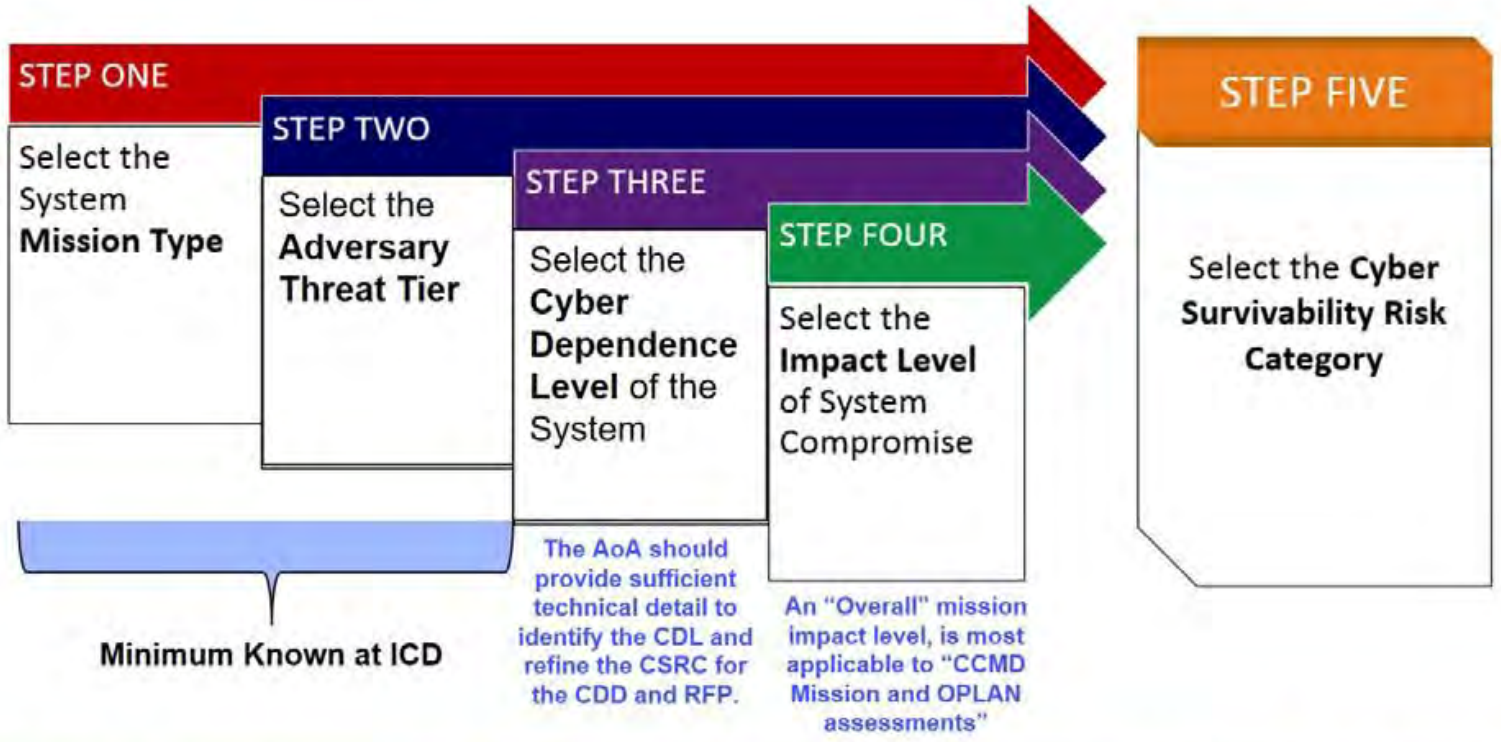


THE CYBER SURVIVABILITY ENDORSEMENT (CSE) PROCESS



Cyber Survivability Endorsement Implementation Guide

Table of Contents: Summary of Changes: ..... Error! Bookmark not defined.



The CSE 5 step risk managed approach takes into account several variables … the resulting CSRC provides consistency between levels of CS requirements, development, testing and O&M

CYBER DEPENDENCY LEVEL

- Systems Modeling informs CDL levels for candidate systems

Level	Degree of Connectivity (Operational Requirements for Internal and External Information Exchange)	Technical Exposure
CDL 4	**Extreme** - Systems are entirely dependent on cyber connectivity and functionality, and may not function at all without full high bandwidth network support (both wired and wireless). Ex. Continuous comm over minimally protected networks or complex SW/HW, with no human to take control in Unmanned and Robotic/Autonomous Systems.	Broad
CDL 3	**High** - Systems are dependent on cyber connectivity and functionality, but are able to function to a limited extent with intermittent or low bandwidth network support (both wired and wireless).	Limited
CDL 2	**Moderate** - Systems are somewhat dependent on cyber connectivity and functionality, and can operate effectively with intermittent or low bandwidth network support (both wired and wireless).	Restricted
CDL 1	**Low** - Systems have little dependence on cyber connectivity and functionality, and can operate effectively with little or no network support.	Narrow

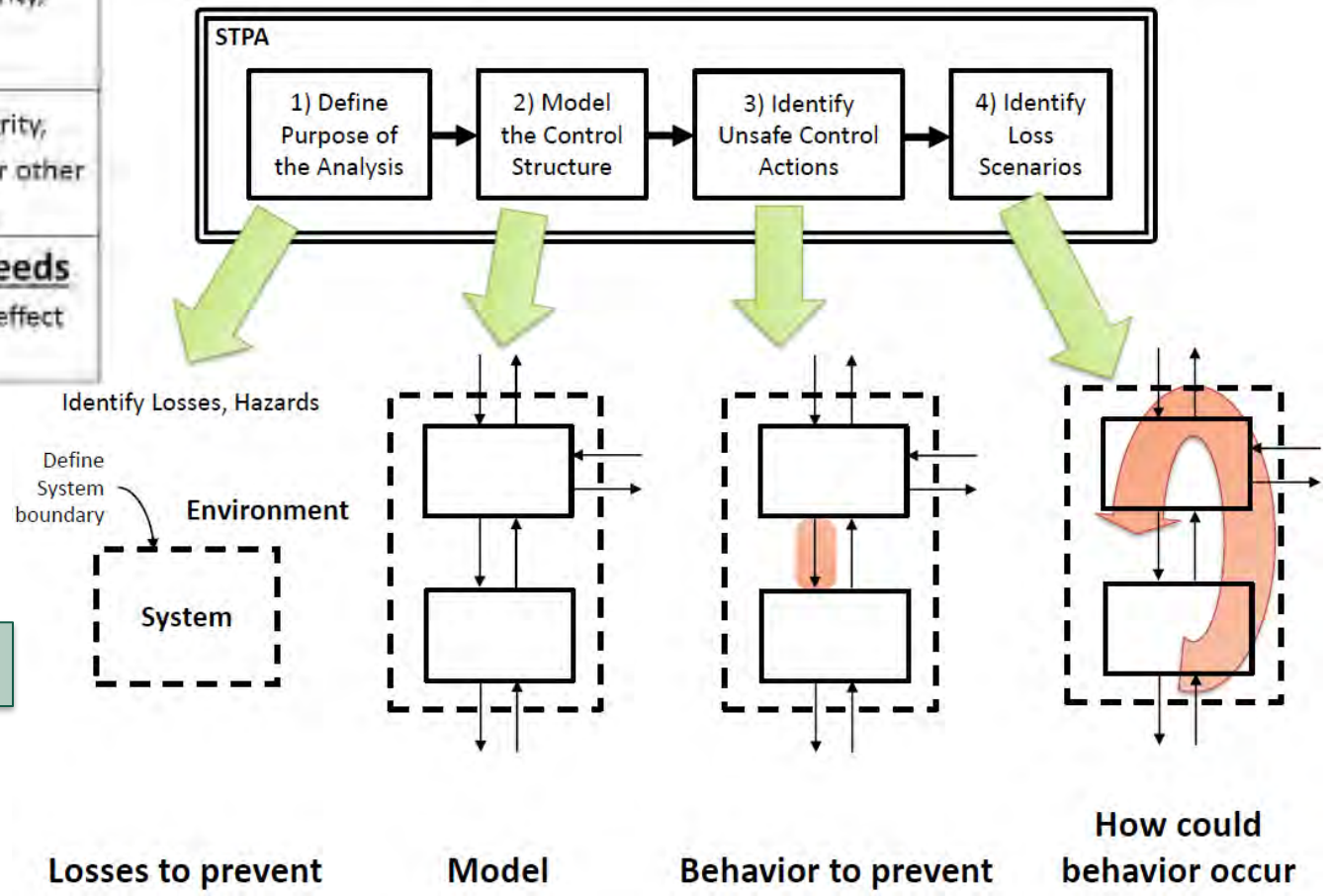
- The Dependency Level selection can be aided by a mission & system architecture model developed as part of the AoA
- Requires not just a subsystems view
  - which networks the system connects to
- but also a functional view
  - what capabilities require the networks
  - how they use the information to perform these capabilities
  - what happens if this connectivity is lost
- Result is a critical functions list

Impact Level (IL) of System Loss/Compromise
IL 4: Catastrophic Adverse Effect – A compromise of system confidentiality, integrity, and availability would lead to complete mission failure with few, if any, mission objectives accomplished and likely friendly force losses.
IL 3: Serious Adverse Effect – A compromise of system confidentiality, integrity, and availability would seriously degrade mission performance leaving some mission objectives unaccomplished and endangering friendly forces.
IL 2: Limited Adverse Effect – A compromise of system confidentiality, integrity, and availability would partially degrade mission performance, requiring more time or other resources to accomplish mission objectives and possibly endangering friendly forces.
IL 1: Risks Acceptable for Meeting Military and Organization Needs – A compromise of system confidentiality, integrity, and availability would have little effect on mission accomplishment and would not likely endanger friendly forces.

Informed by Loss Assessment

The Impact Level selection can be aided by a mission loss assessment using STPA-Sec

- Cyber Resilience Requirements Methodology/Systems Theoretic Process Assessment



CSE PROCESS DETERMINES CYBER SURVIVABILITY ATTRIBUTES

SS KPP Pillars (Mandatory)	Cyber Survivability Attributes (CSAs) (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

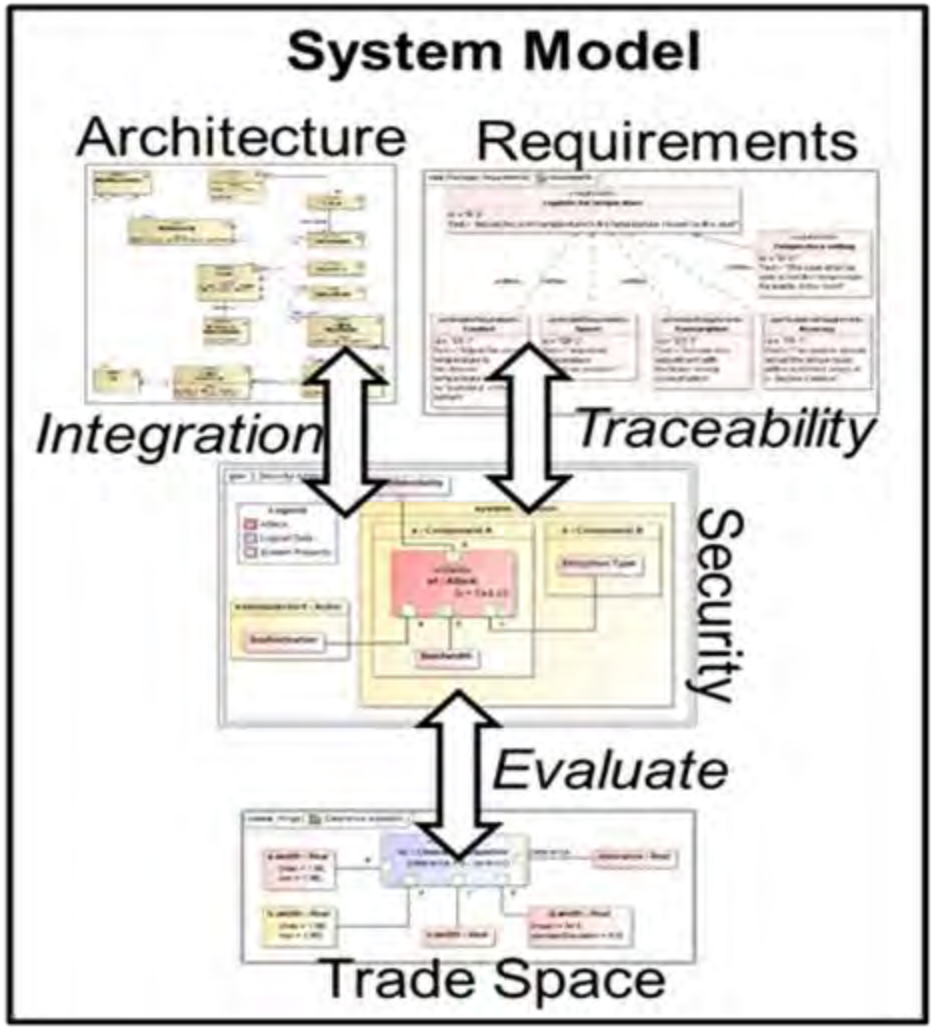
EXPERIENCE WITH DIRECT USE OF CSA IN A PROGRAM

- FLRAA – Native Digital Program
- Government Furnished Information (GFI) input to contractors
  - Pilot Program - GFI was Cameo MBSE
- Allocated Baseline from Contractors
  - Indications of how GFI was used
- Recommendations
  - Provide contractors with detailed process
    - CRRM with Meta-Model Artifacts (SCRE)
  - Operational Use Case Realization (Activity Diagrams)

FLRAA (DTEA, Army)

SYSTEMS ENGINEERING RESEARCH CENTER

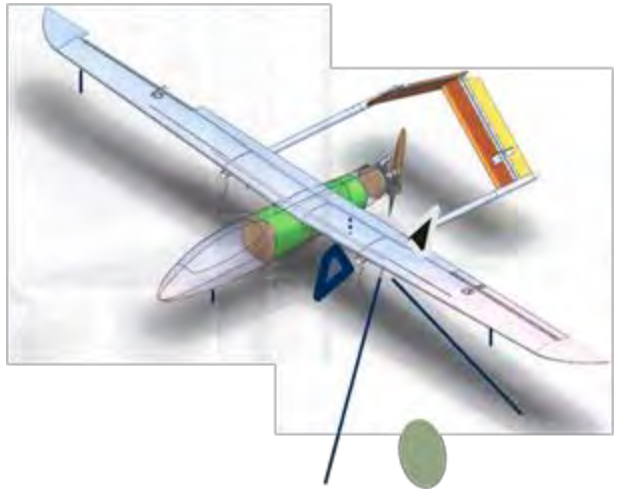
RESILIENCE REQUIRES ENGINEERING



- CSAs are high level requirements
  - —Engineers need lower-level measurable requirements to demonstrate progress during development
- Engineers must define performance specifications that articulate CSAs as requirements for performance in cyberspace
  - —No cookie cutter controls here!
  - —Need to flow down, map, and deconflict requirements (including both technology and program protection) from the cyber survivability KPP down to functional and technical/ performance requirements
- Contractor must be required to decompose performance specs down to lower levels and government must support scope with mission and threat context
  - —Define traceable technical performance measures (TPMS)
  - —DoD uses Mission-Based Cyber Risk Assessments (MBCRAs)

SYSTEMS ENGINEERING RESEARCH CENTER

Applications of SCRE

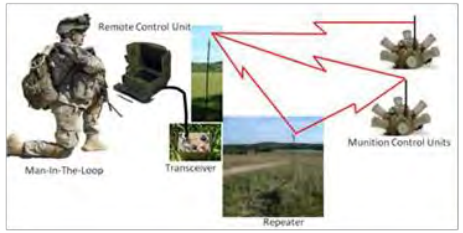


Surviellance Drone
(Army)

Ship Control
(Northrop Grumman)

3D Printers
(NIST)

Human Factors Experiments
(Air Force)

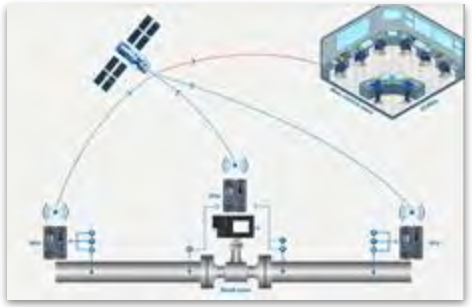


Networked Munitions
(Army)

Cars
(VA State Police)

Industrial Control Sytems
(Mission Secure Inc)

Silverfish (Army)



Pipeline (ASD/RE)

FLRAA (DTEA, Army)

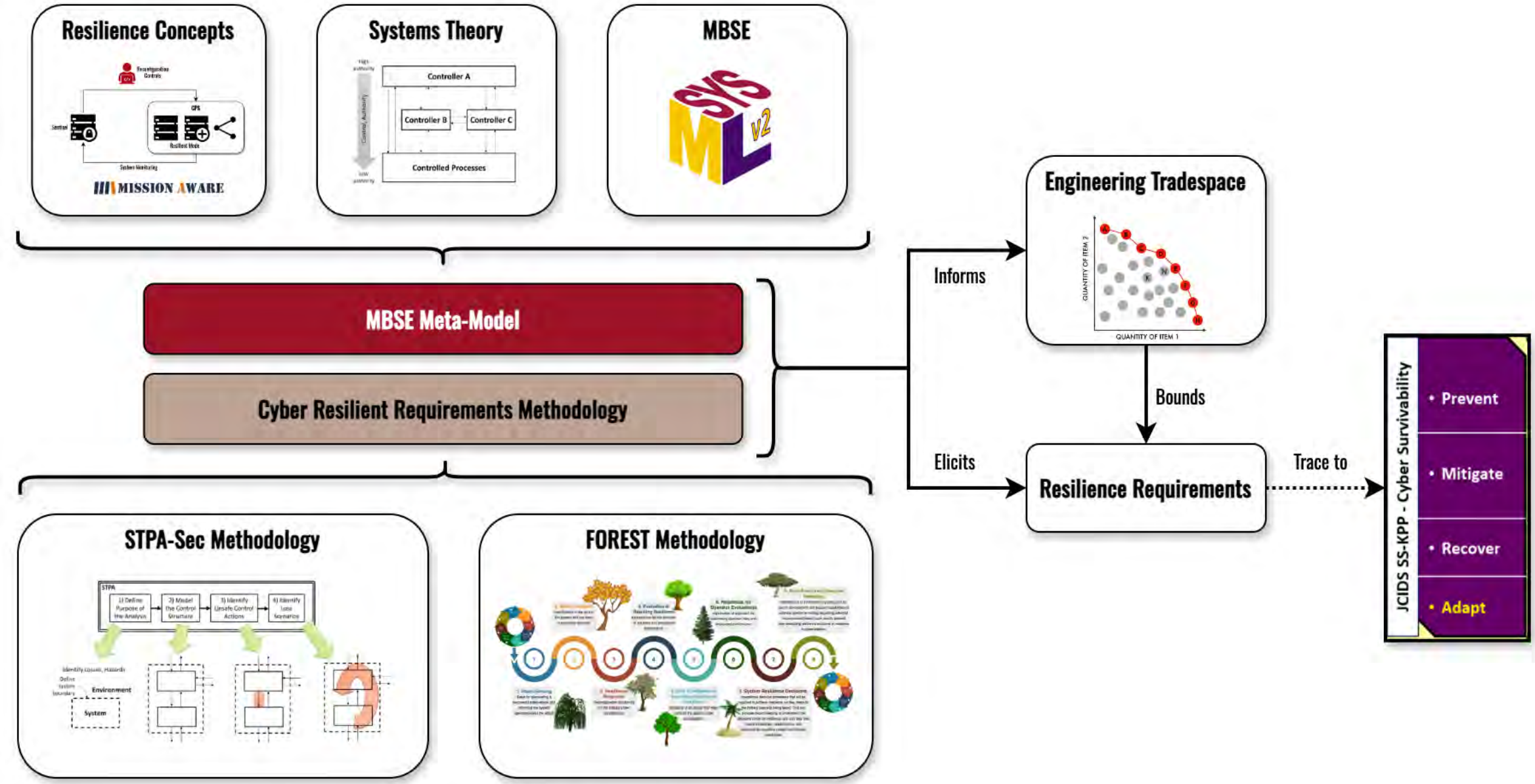
Wind Farms (R&E, NNSA)

TOWARD A SOLUTION

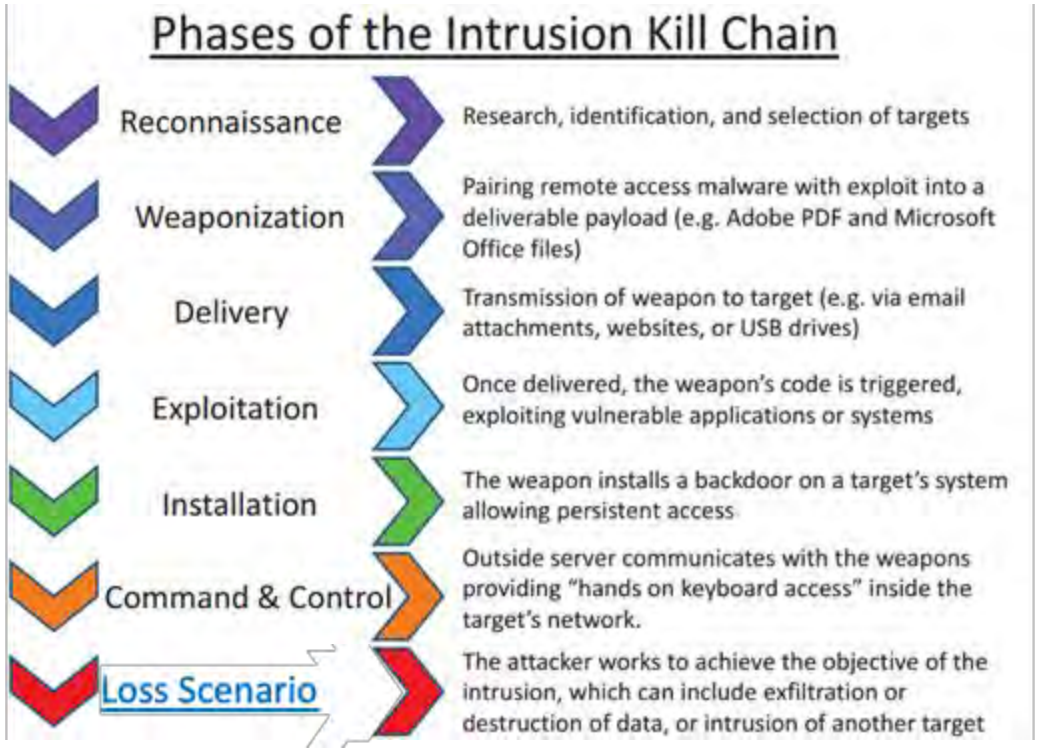
To achieve resilience, use the same ***System Engineering*** processes as when considering ***Safety***, ***Reliability*** and ***Survivability***

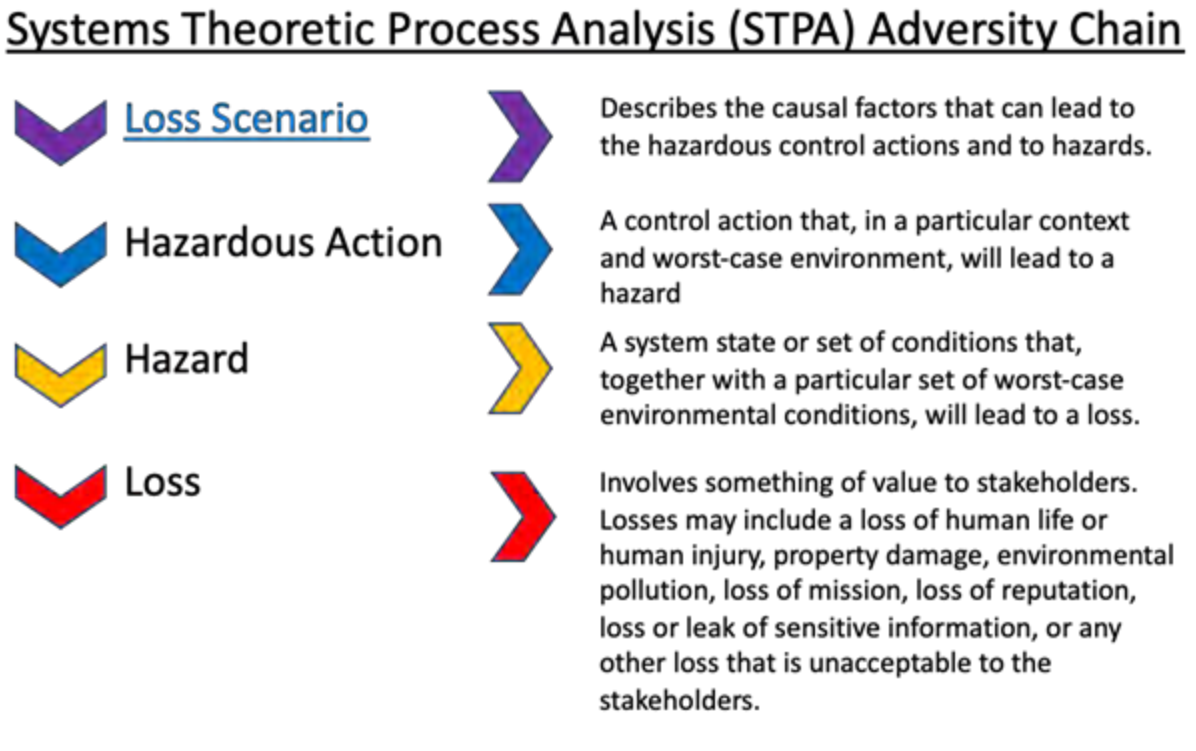
- Design in resilience
  - Engineered resilience responses
- Develop measurable cyber requirements alongside ***Performance***, ***Safety*** and other "-ility" requirements
  - Typical cyber requirements are security controls that do not relate directly to mission capability or defender response
- Use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

OVERVIEW OF SERC CONTRIBUTIONS TO SCRE



RISK=LIKELIHOOD X CONSEQUENCE





- Break Cyber Kill Chain using Assurance Cases
- Model the Adversary TTP
- Threat and Vulnerability Driven
- Difficult to Test even in Operational Setting

- Break STPA Adversity Chain using Resilience Mechanisms
- Model our own System
- Hierarchical Control Model Independent of Component Choice
- Well Matched to Technology Test

16

SYSTEM-THEORETIC PROCESS ASSESSMENT (STPA) OVERVIEW

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.

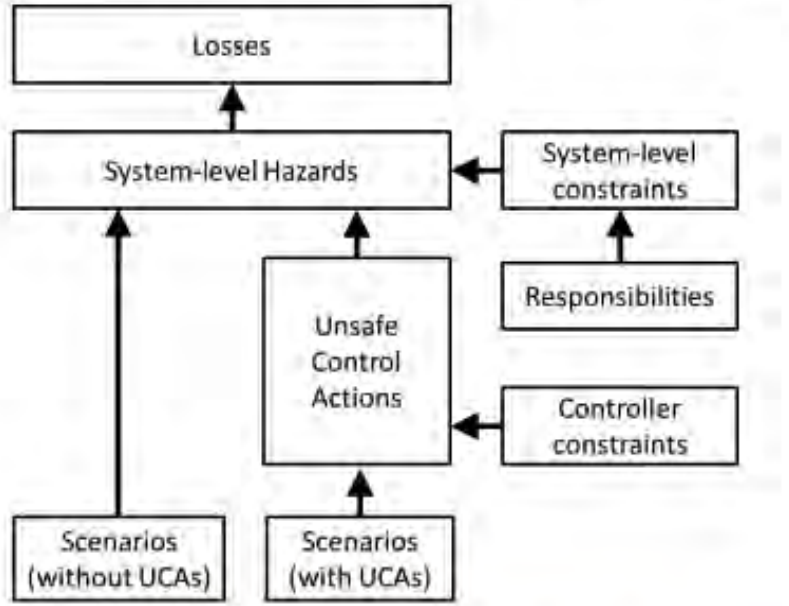
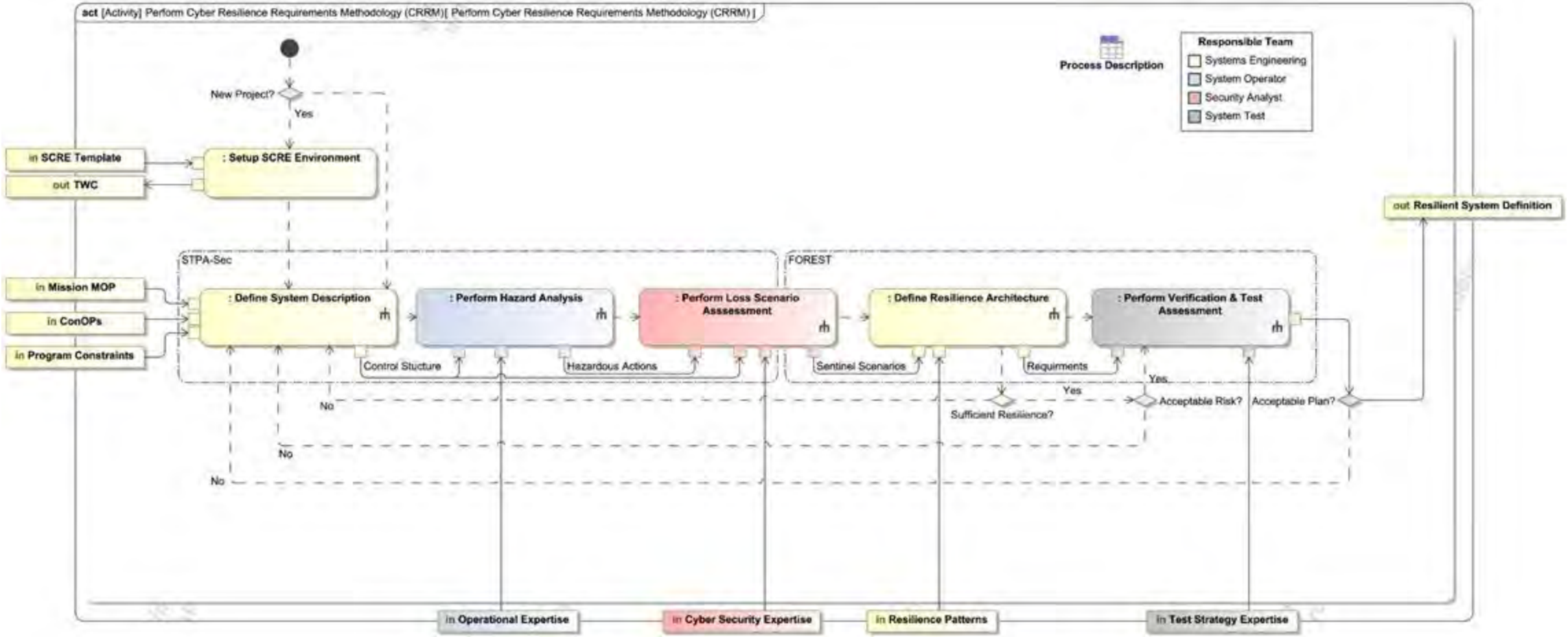


Figure 2.21: Traceability between STPA outputs

- 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.

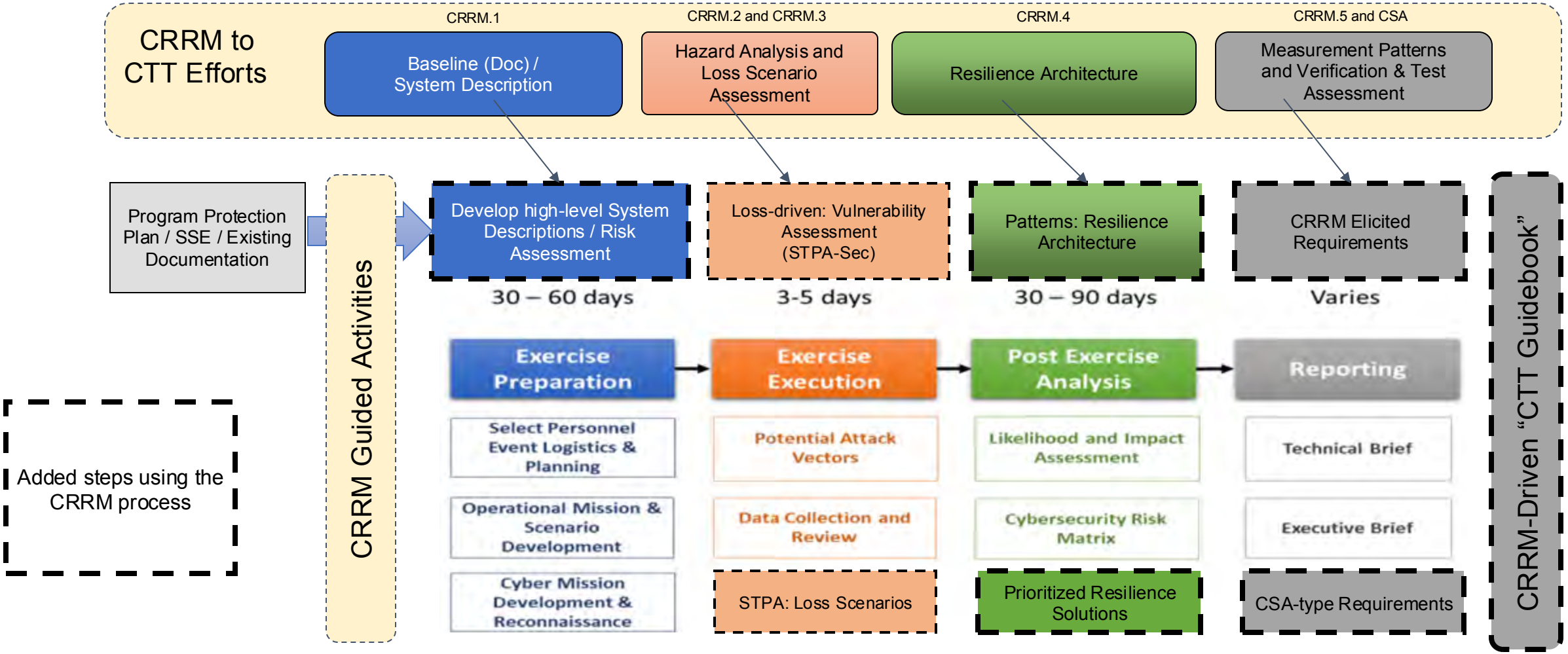
Leveson, Thomas https://psas.scripts.mit.edu/home/get_file.php?name=STPA_handbook.pdf

CRRM – CYBER RESILIENCE REQUIREMENTS METHODOLOGY



- CRRM is a means of identifying resilience requirements during the initial design phase of physical systems.
- The methodology involves five sequential steps, iteratively executed by one of four distinct teams representing stakeholders in the security engineering process.

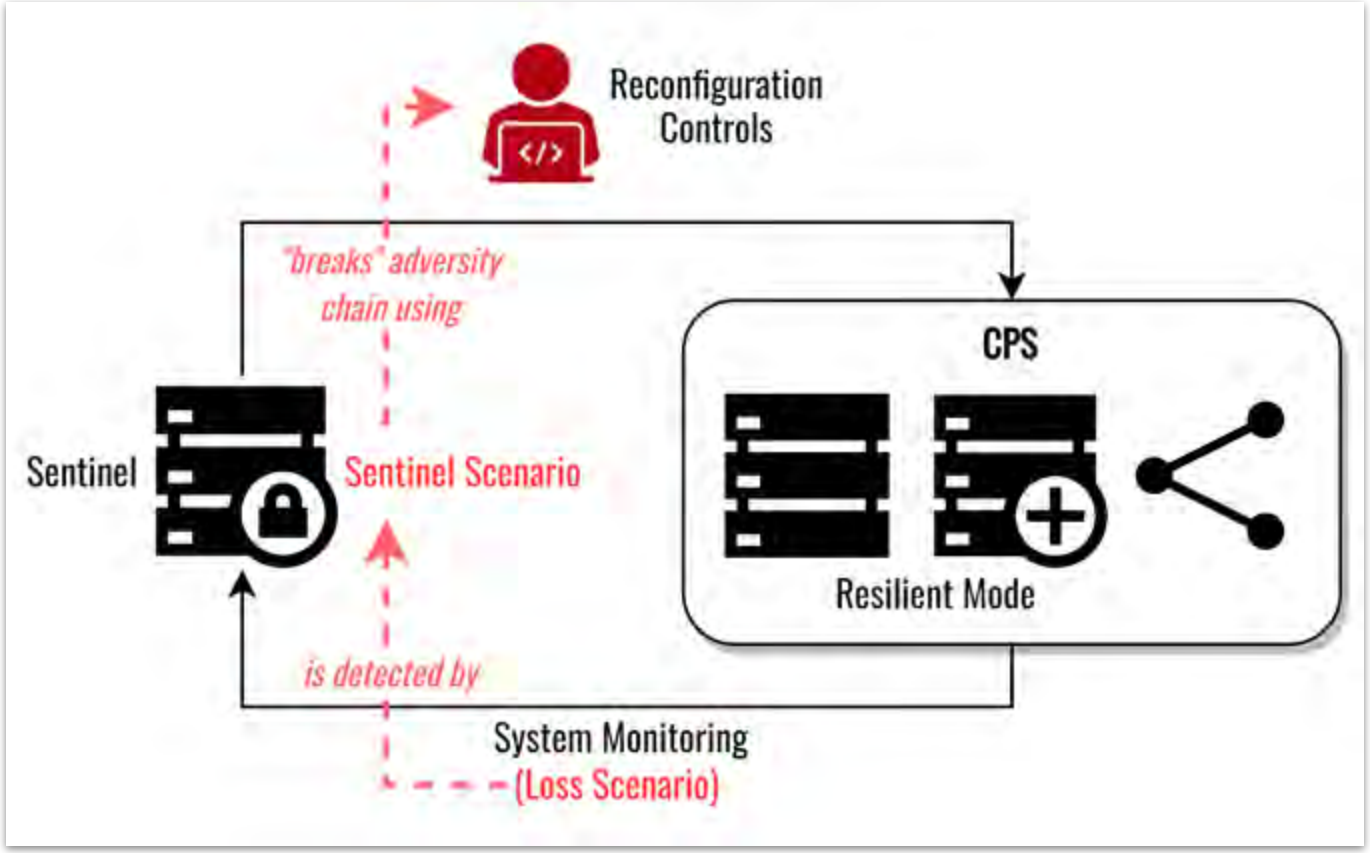
RESILIENCE-FOCUSED "CTT" PROCESS FLOW



CTT Process flow steps from Fig. 2, DAU Cyber Table-Top Guide

RESILIENCE MECHANISM – BREAKING ADVERSITY CHAIN

Observe the System rather than the Adversary

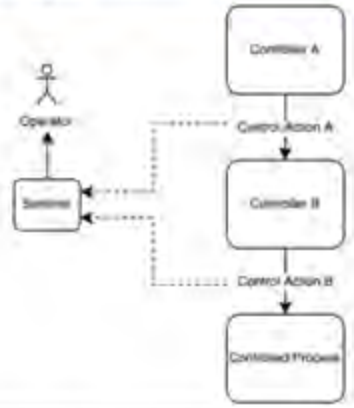


Can specify and test:

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

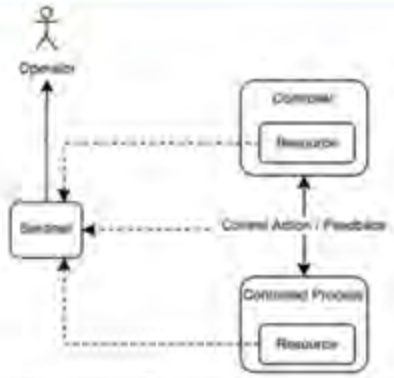
SENTINEL PATTERNS

Sentinel - Changing Control Input



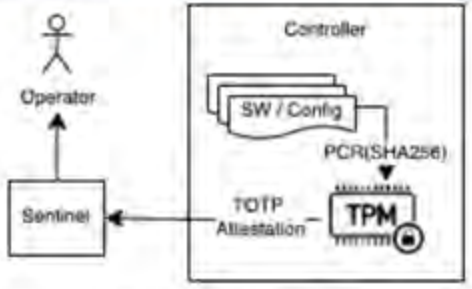
Description	A Sentinel monitors control action consistency when a system involves a hierarchy of controllers.
Problem	A controller or control path is attacked such that invalid (modified, injected, dropped) control actions affect a controlled process.

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.

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	APL	Prevent	N
	Data Flow Control	Data flow control regulates where data is allowed to travel within an information system and between information systems	APL	Prevent	N
	Filter	Blocks messages that do not conform to a given specification.	CASE	Prevent	N
PAT.11	Segmentation	Segmentation is the division of a system into separate parts or sections	APL	Prevent	N
	Virtualization	Isolates software components in a virtual machine.	CASE	Prevent	N
PAT.12	Data Input Validation	Input Validation is the process of determining the valid syntax and semantics of information system inputs	APL	Prevent	N
	Proxy	Inserts a pair of components to enable the inspection of HTTPS message payloads.	CASE	Prevent	N

OFFSHORE WIND ENERGY PROJECT

SCRE GENERIC MODELING: OVERVIEW