SoSECIE Webinar

Welcome to the
2020 System of Systems Engineering Collaborators Information Exchange (SoSECIE)

National Defense Industrial Association

We will start at 11AM Eastern Time

Skype Meeting +1 (703) 983-2020, 46013573#

You can download today's presentation from the SoSECIE Website:

https://mitre.tahoe.appsembler.com/blog

To add/remove yourself from the email list or suggest a future topic or speaker, send an email to sosecie@mitre.org

NDIA System of Systems SE Committee

- **Mission**
  - To provide a forum where government, industry, and academia can share lessons learned, promote best practices, address issues, and advocate systems engineering for Systems of Systems (SoS)
  - To identify successful strategies for applying systems engineering principles to systems engineering of SoS
- **Operating Practices**
  - Face to face and virtual SoS Committee meetings are held in conjunction with NDIA SE Division meetings that occur in February, April, June, and August

NDIA SE Division SoS Committee Industry Chairs:
Mr. Rick Poel, Boeing
Ms. Jennie Horne, Raytheon
OSD Liaison:
Dr. Judith Dahmann, MITRE

Simple Rules of Engagement

- I have muted all participant lines for this introduction and the briefing.
- If you need to contact me during the briefing, send me an e-mail at sosecie@mitre.org.
- Download the presentation so you can follow along on your own
- We will hold all questions until the end:
  - I will start with questions submitted online via the CHAT window in Skype.
  - I will then take questions via telephone; State your name, organization, and question clearly.
- If a question requires more discussion, the speaker(s) contact info is in the brief.

Disclaimer

- MITRE and the NDIA makes no claims, promises or guarantees about the accuracy, completeness or adequacy of the contents of this presentation and expressly disclaims liability for errors and omissions in its contents.
- No warranty of any kind, implied, expressed or statutory, including but not limited to the warranties of non-infringement of third party rights, title, merchantability, fitness for a particular purpose and freedom from computer virus, is given with respect to the contents of this presentation or its hyperlinks to other Internet resources.
- Reference in any presentation to any specific commercial products, processes, or services, or the use of any trade, firm or corporation name is for the information and convenience of the participants and subscribers, and does not constitute endorsement, recommendation, or favoring of any individual company, agency, or organizational entity.

2020-2021 System of Systems Engineering Collaborators Information Exchange Webinars

Sponsored by MITRE and NDIA SE Division

June 16, 2020
Challenges for Systems of Systems / Mission Engineering in a Space Acquisition Environment
Lt Col Benjamin Bennett

June 30, 2020
Mission Engineering Playbook
Dr. Judith Dahmann

July 28, 2020
Addressing Mission Engineering from a Lead Systems Integration Perspective
Dr. Warren Vaneman

More coming soon!

“Can We Assure Resilience of Cyber-Physical Systems Using Model-Based Systems Engineering?”

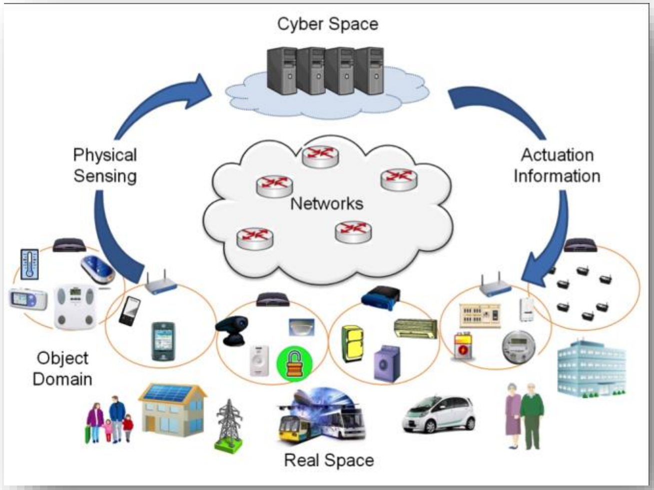
Tom McDermott, Peter Beling, Cody Fleming

June 2, 2020

This material is based upon work supported, in whole or in part, by the U.S. Department of Defense through the Systems Engineering Research Center (SERC) under Contract H98230-08-D-0171. The SERC is a federally funded University Affiliated Research Center (UARC) managed by Stevens Institute of Technology consisting of a collaborative network of over 20 universities. More information is available at www.SERCuarc.org

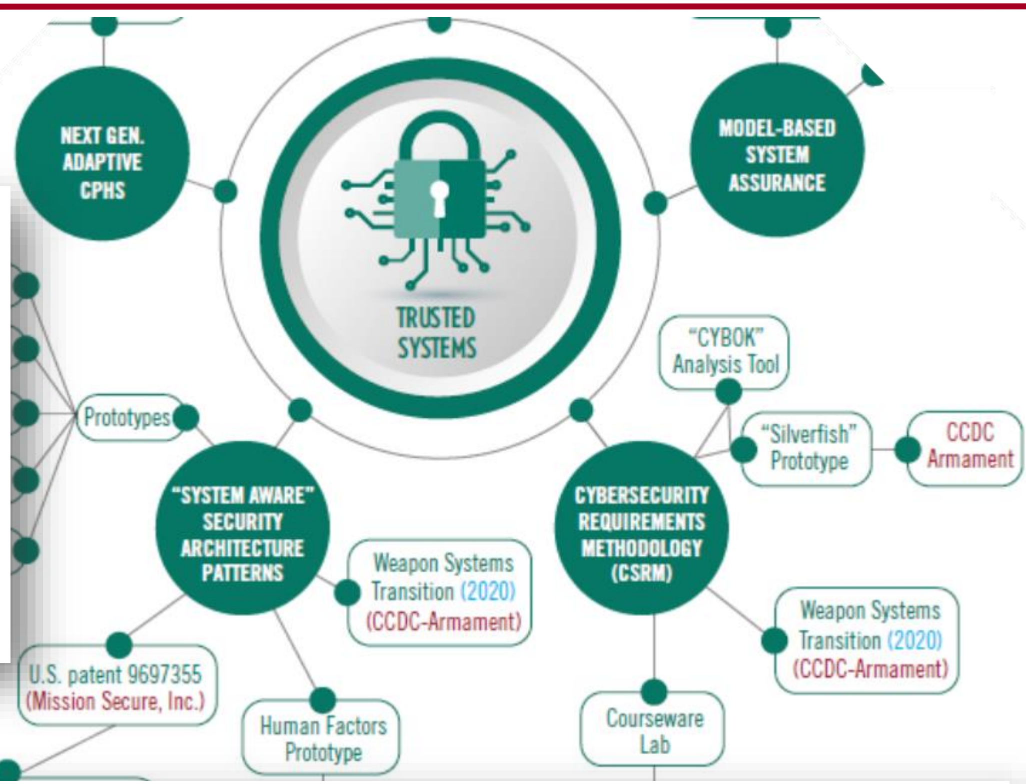
Background: Securing Physical Systems

- Standard cybersecurity approaches are infrastructural in nature
- There is little emphasis on protecting the applications within specific information systems: **Cyber-physical processes are apps**
- The cybersecurity community has limited experience in securing system application functions, especially physical system control functions
- And control system application designers, in general, do not have experience with designing for better cybersecurity, especially physical system designers

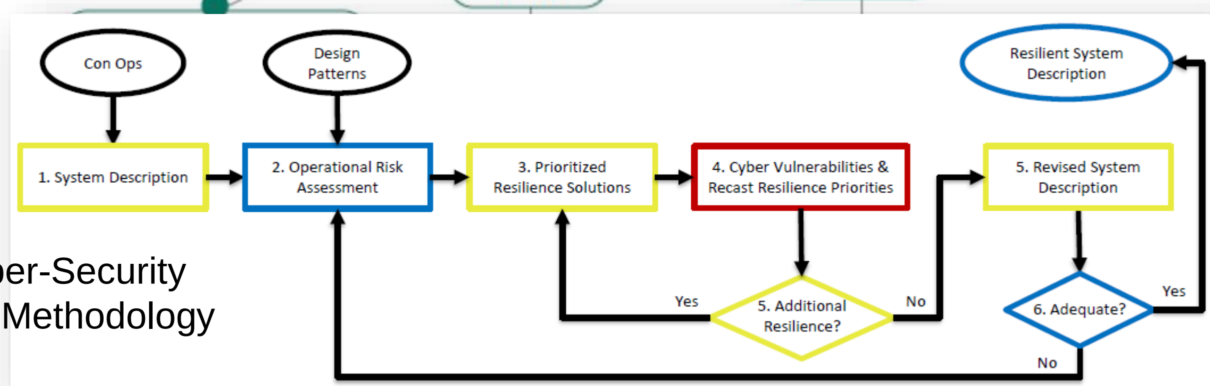


SERC Transition Activities, Trusted Systems

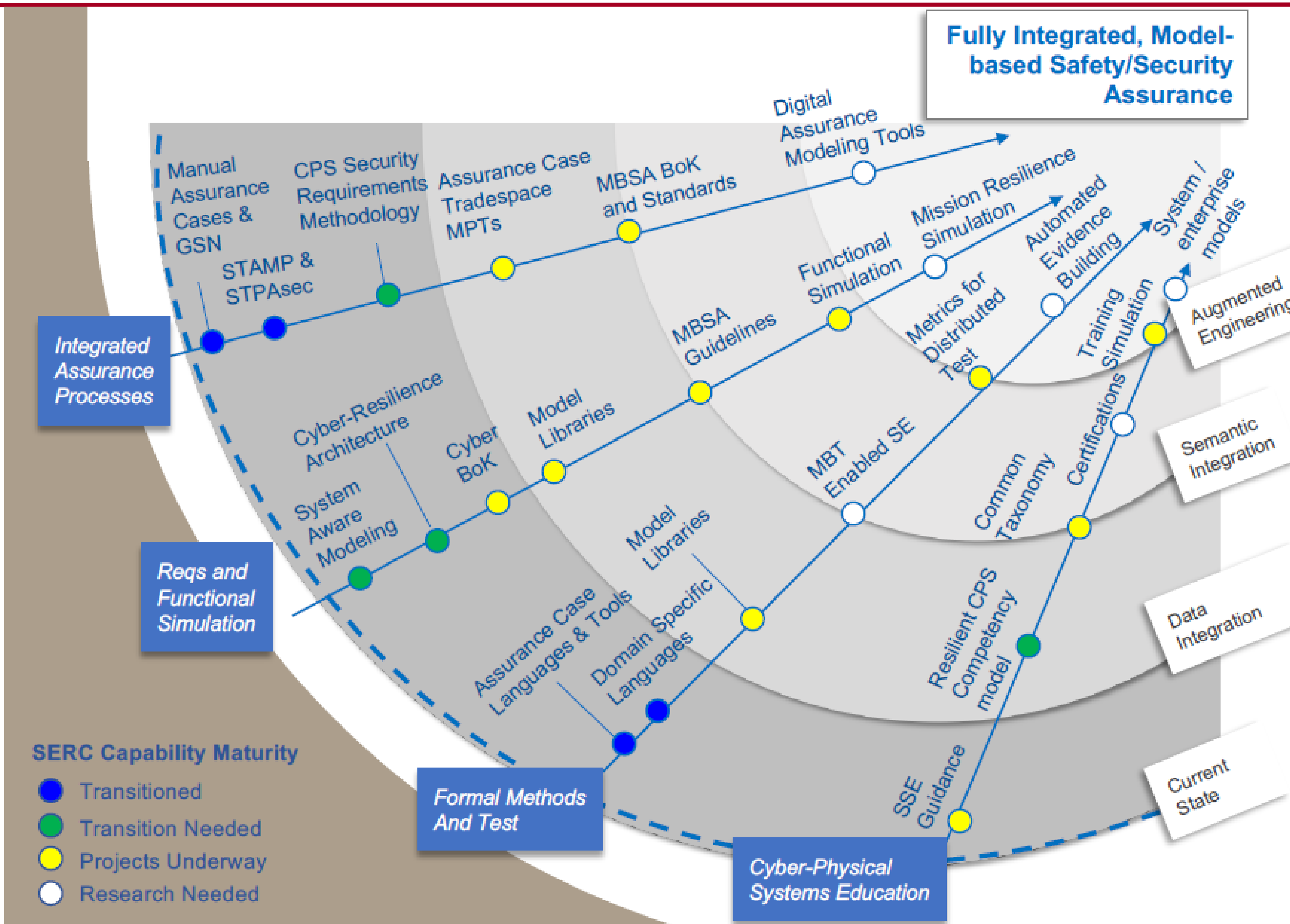
Prototype Evaluation



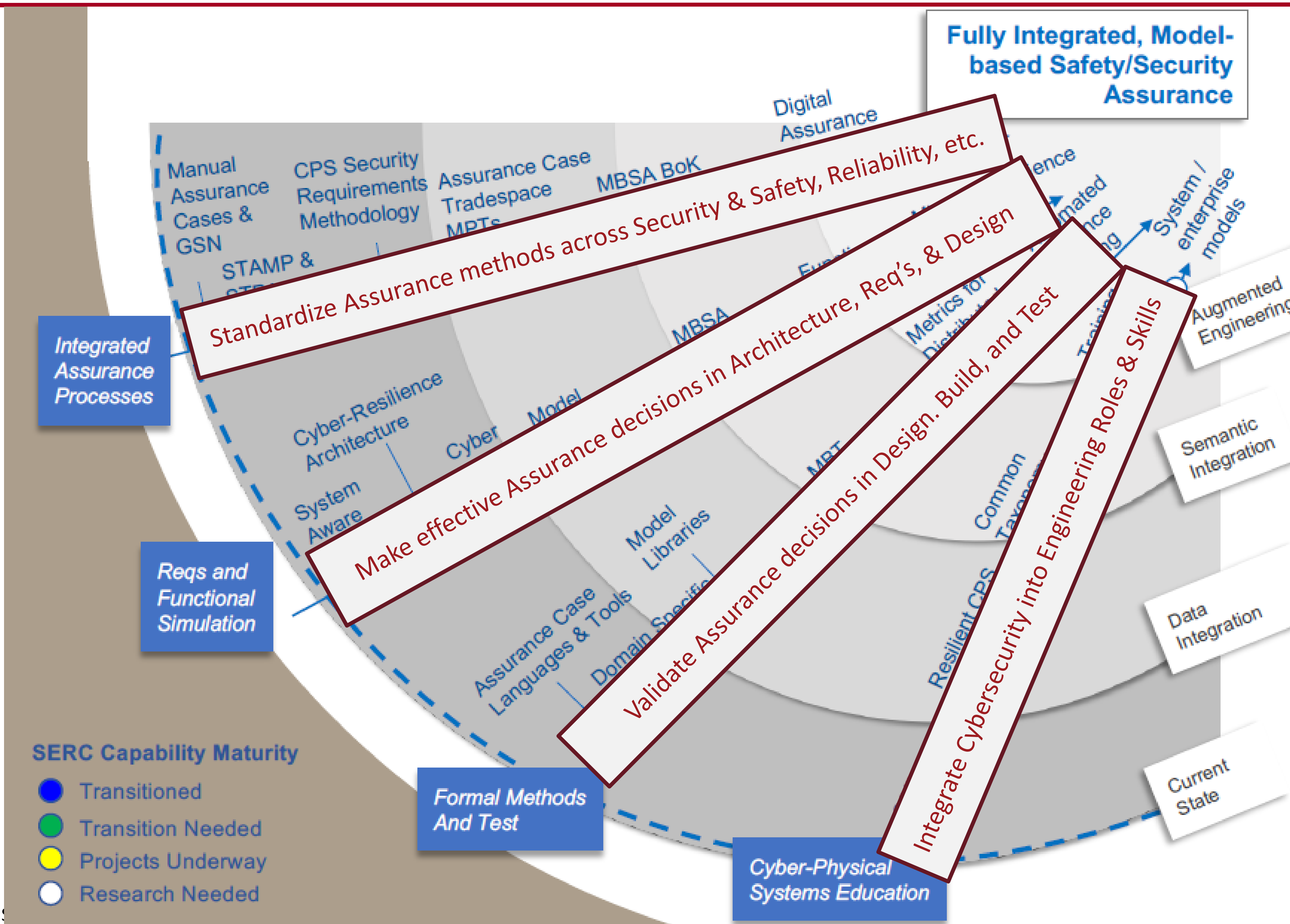
Standard Cyber-Security Requirement Methodology (CSRM)



SERC Model-Based System Assurance Roadmap

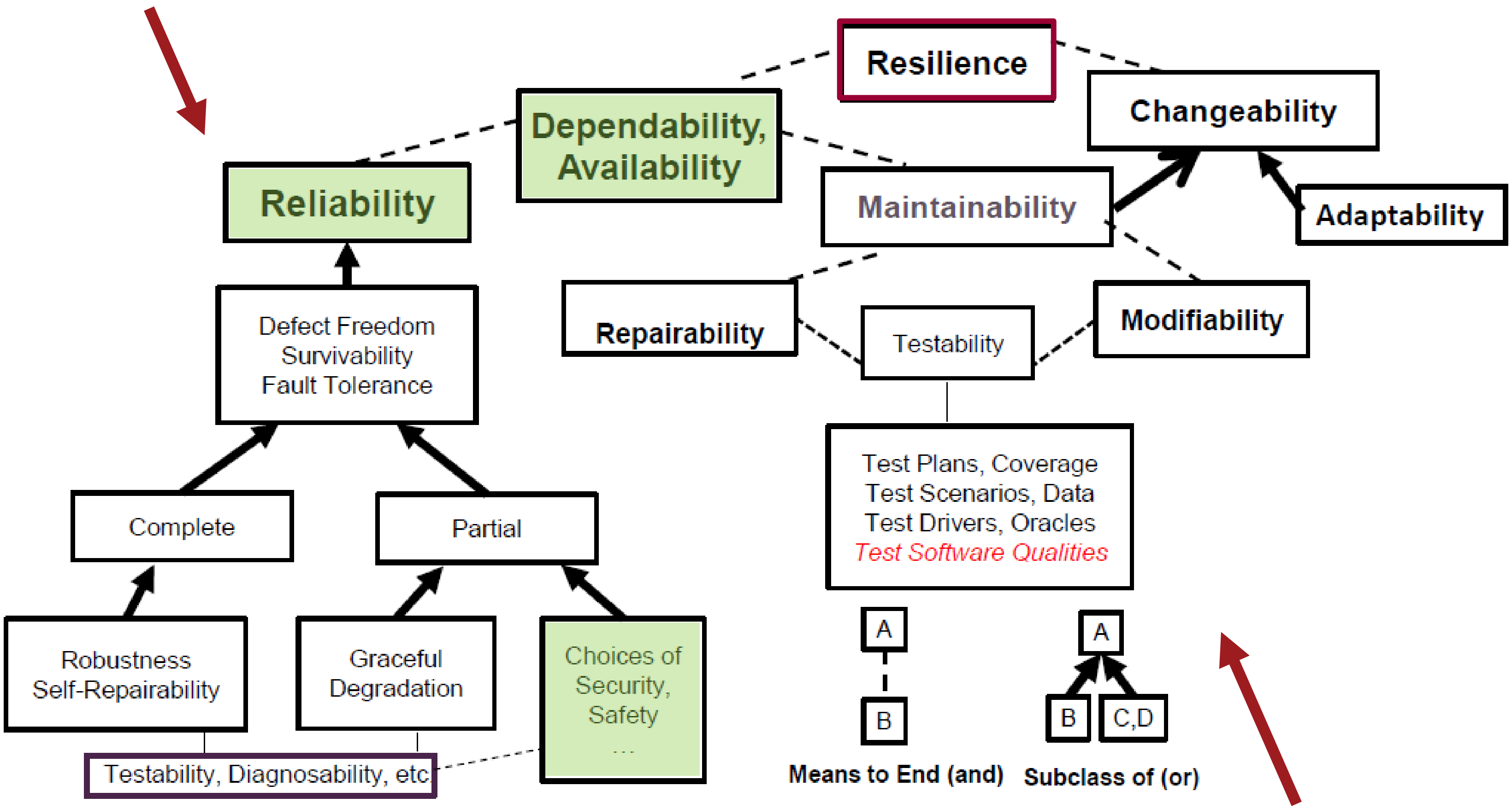


SERC Model-Based System Assurance Roadmap



Dependability, Changeability, and Resilience

- Importance of modeling System in Context

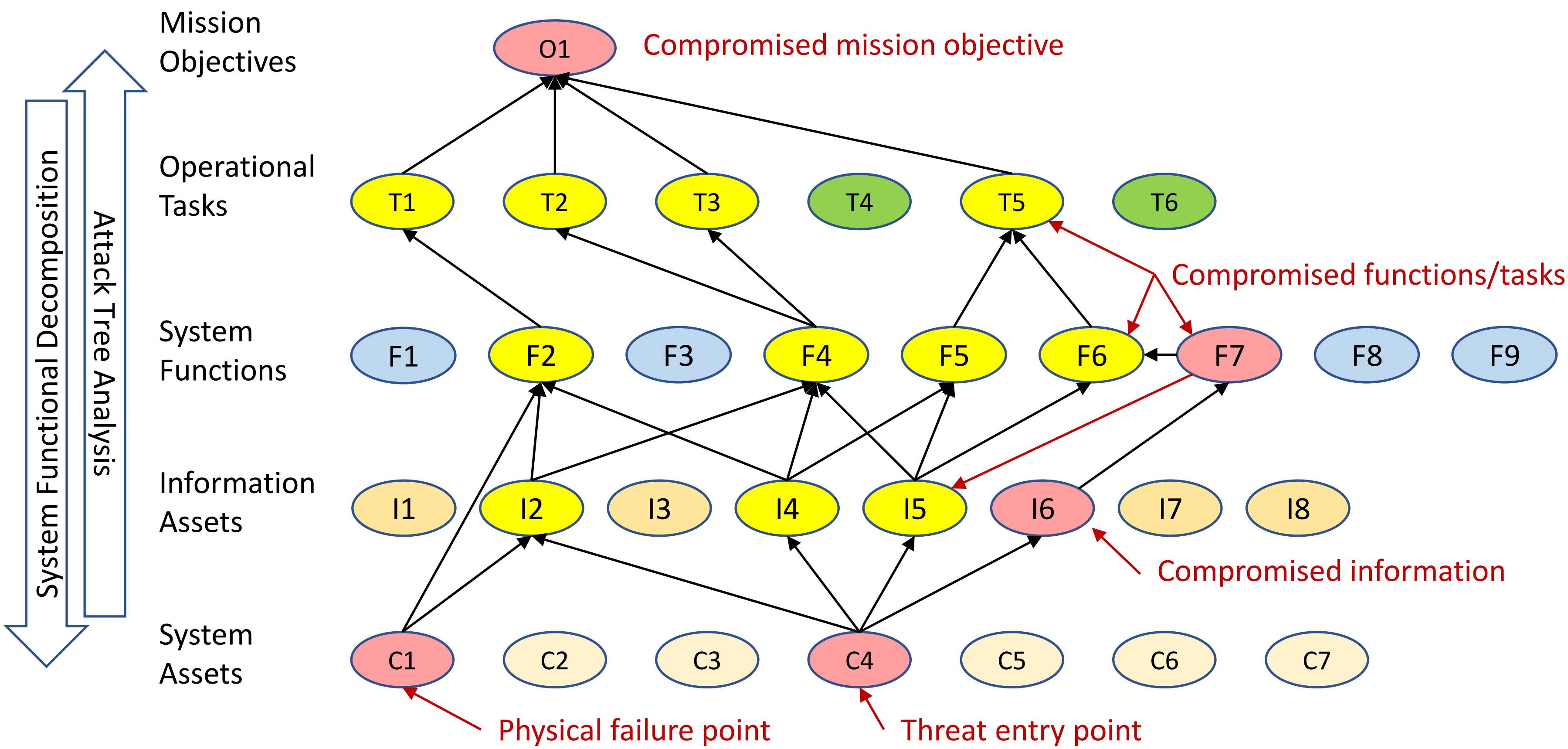


- Importance of System Validation

Barry Boehm, et al, SERC-2019-TR-012-System Qualities, Ontology, Tradespace, and Affordability (SQOTA) Phases 1-7

Need Good Structural/Functional Models

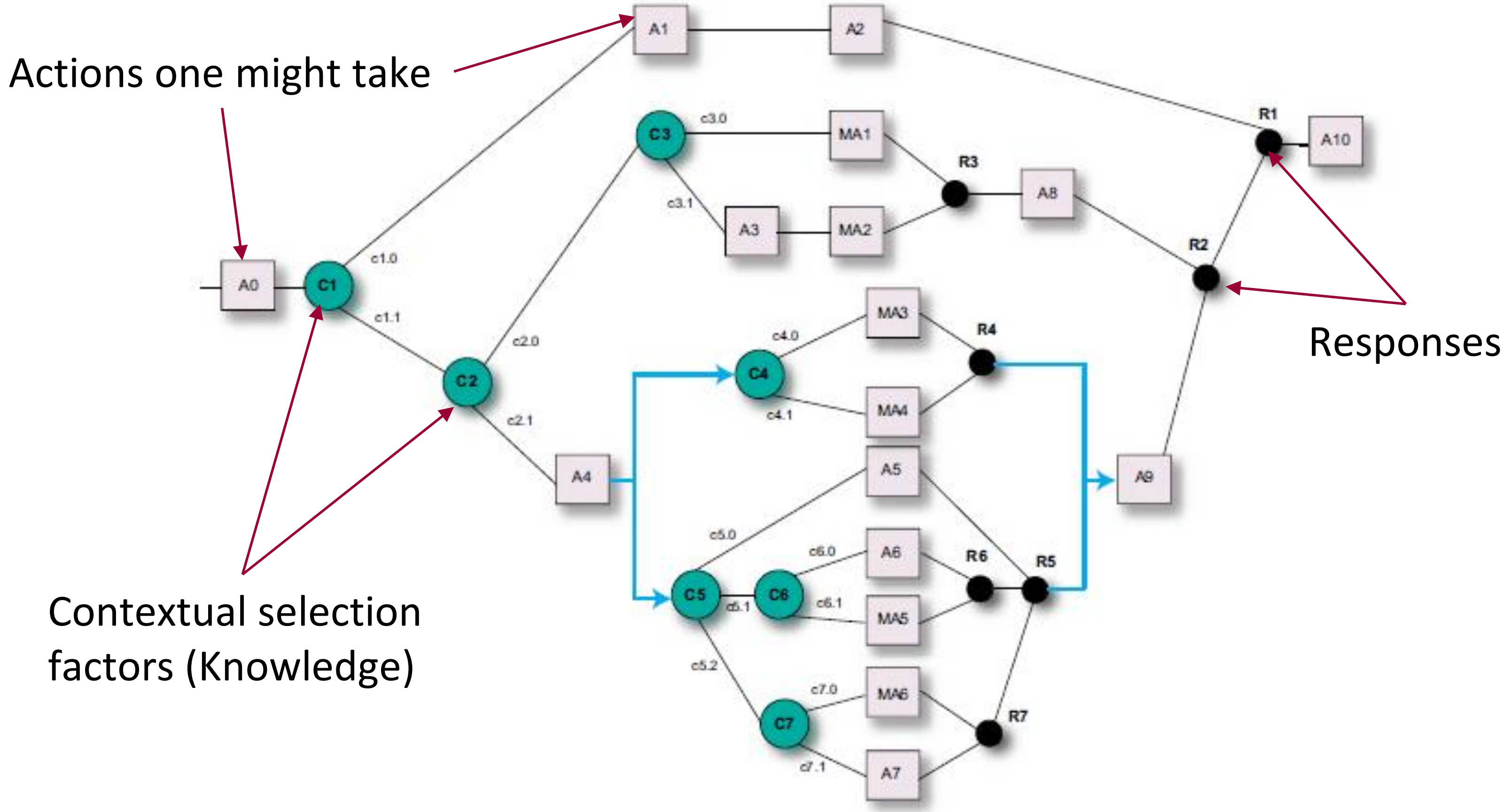
- What to protect and why? Which combination of design patterns to employ in which mission subsystems?



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

Need System Models and Graph Analytical Tools

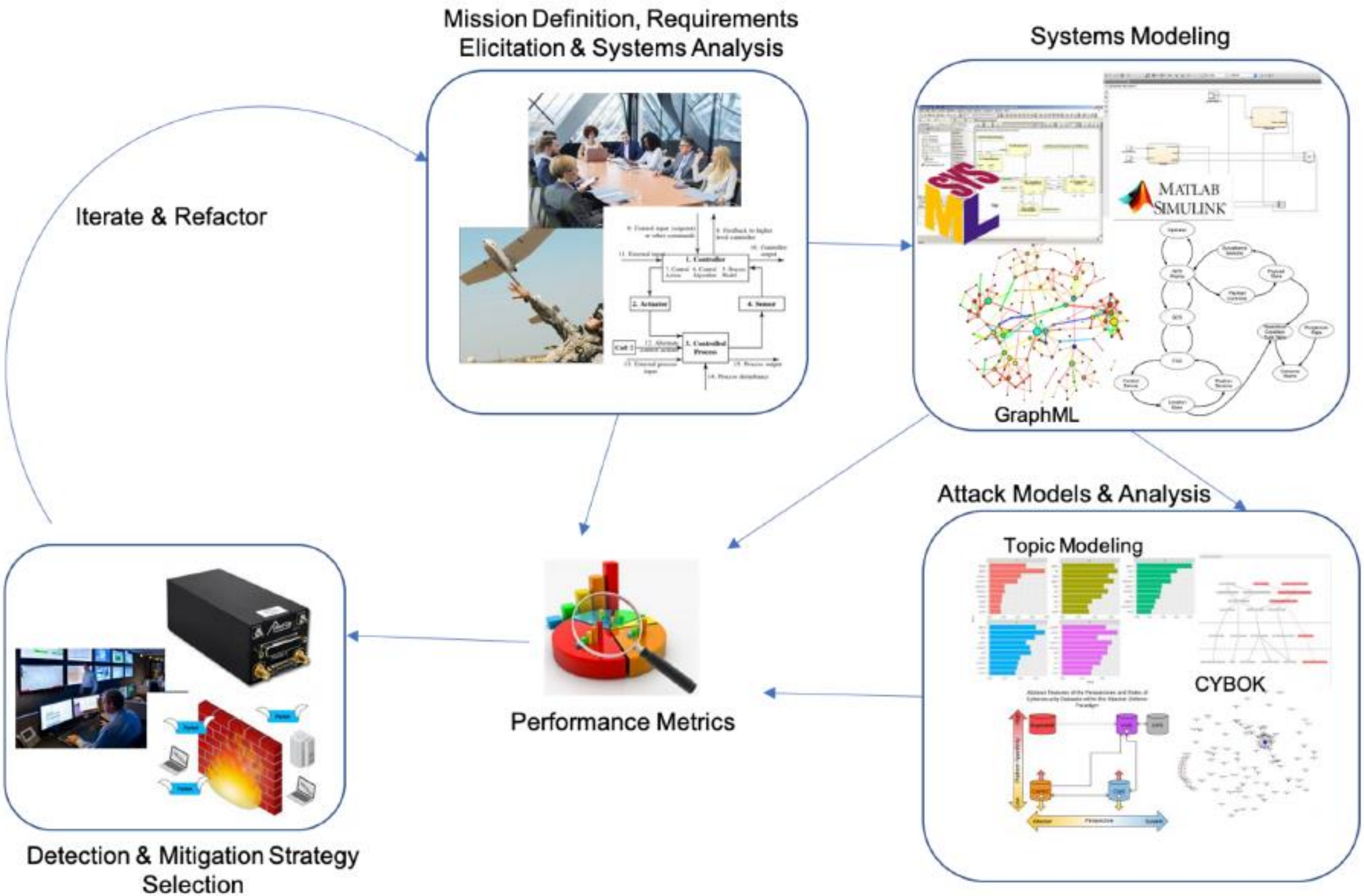
G. Kouadri Mostéfaoui, P. Brézillon / Electronic Notes in Theoretical Computer Science 146 (2006) 85–100



- Well-defined System Structural and Functional Models
- Well-defined Threat Functional Models
- Scalable Graph Structures for System Analysis

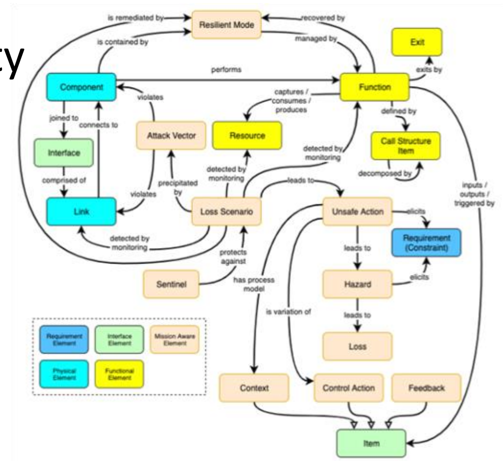
} Patterns

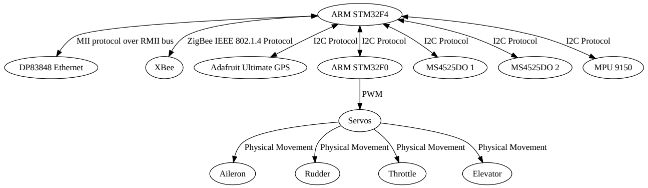
Mission Aware: Rigorous Functional Security Analysis and Modeling Process (UVA)



Decision Support for Design for Cyber Resilience

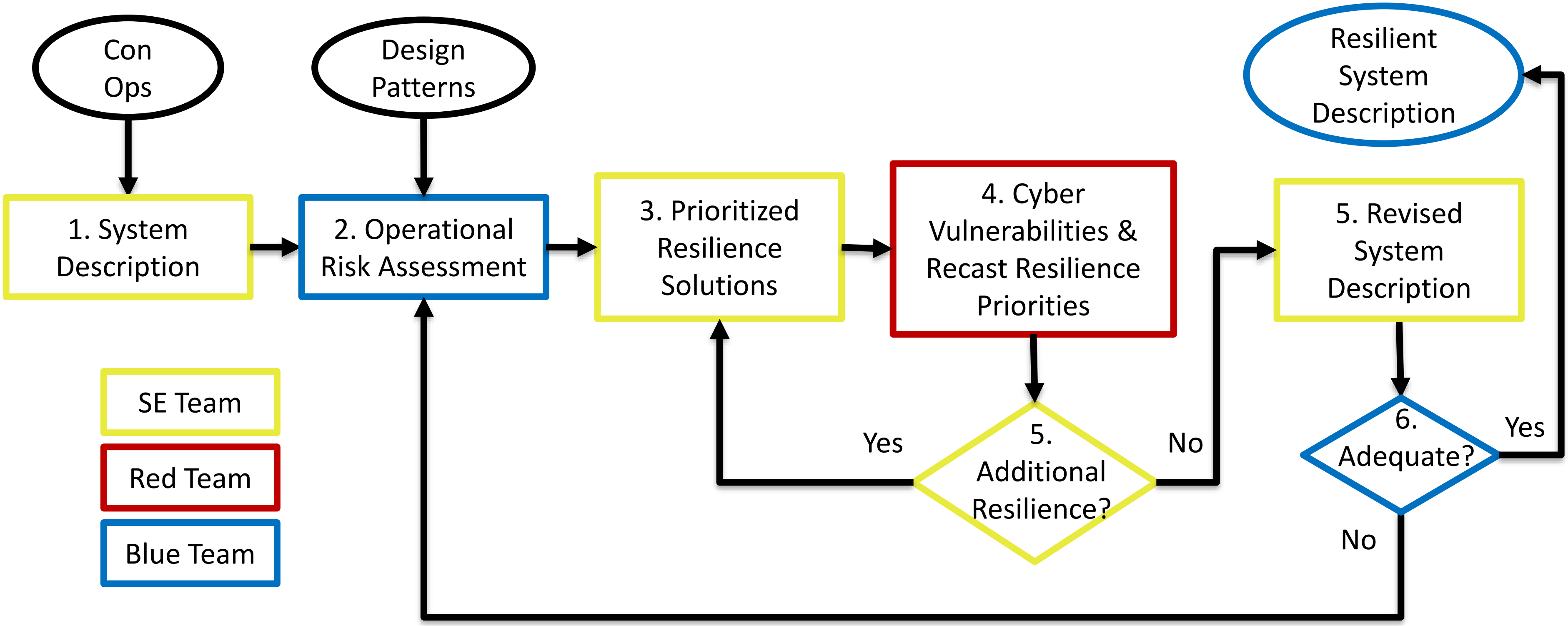
- What to protect and why? Which combination of design patterns to employ in which mission subsystems?
- Who to involve? What information to provide for decision support?
  - —Blue Team: the system/mission owners
    - ○ Provide structured elicitation process from safety community
    - ○ Receive priorities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





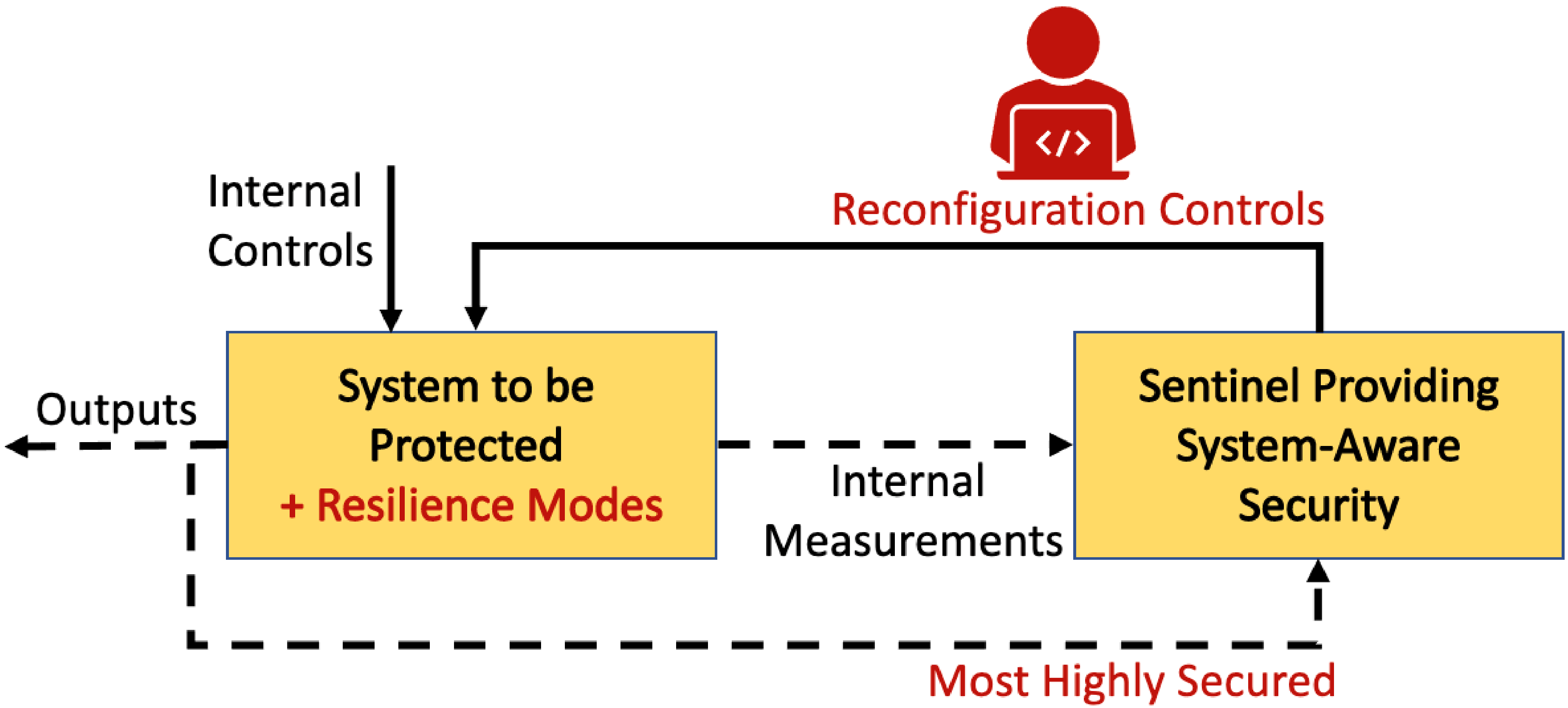
Cyber Security Requirements Methodology (CSRM)

- What to protect and why? Which combination of design patterns to employ in which mission subsystems?
- Standard Blue Team (Mission), Yellow Team (SE), Red Team (Threat) methodology for evaluating resilience with models



Mission Aware Concept (UVA)

- 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 another pattern responsible for monitoring and reconfiguration of a system using available Resilience Modes. The Sentinel subsystem is expected to be far more secure than the system being addressed for resilience.



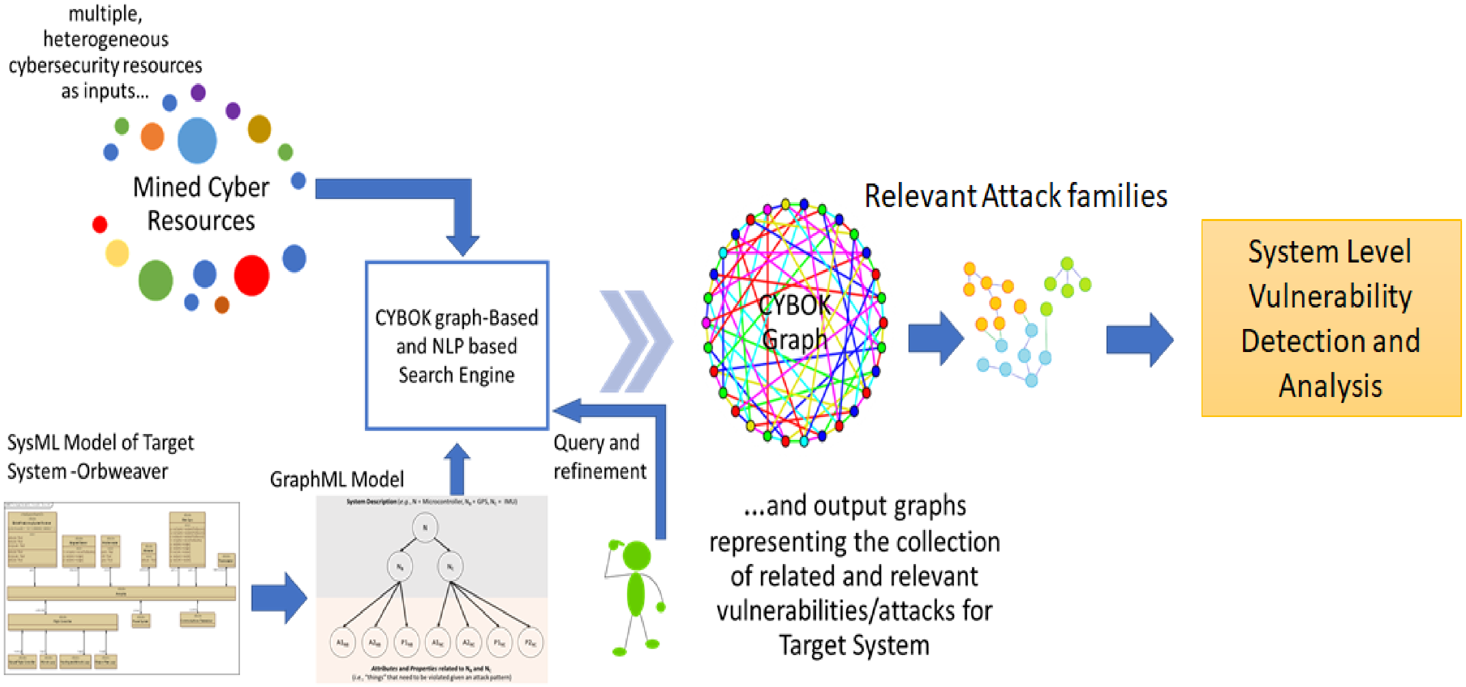
Resilience Modes and Detection Patterns (UVA, Siemens, SIT)

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

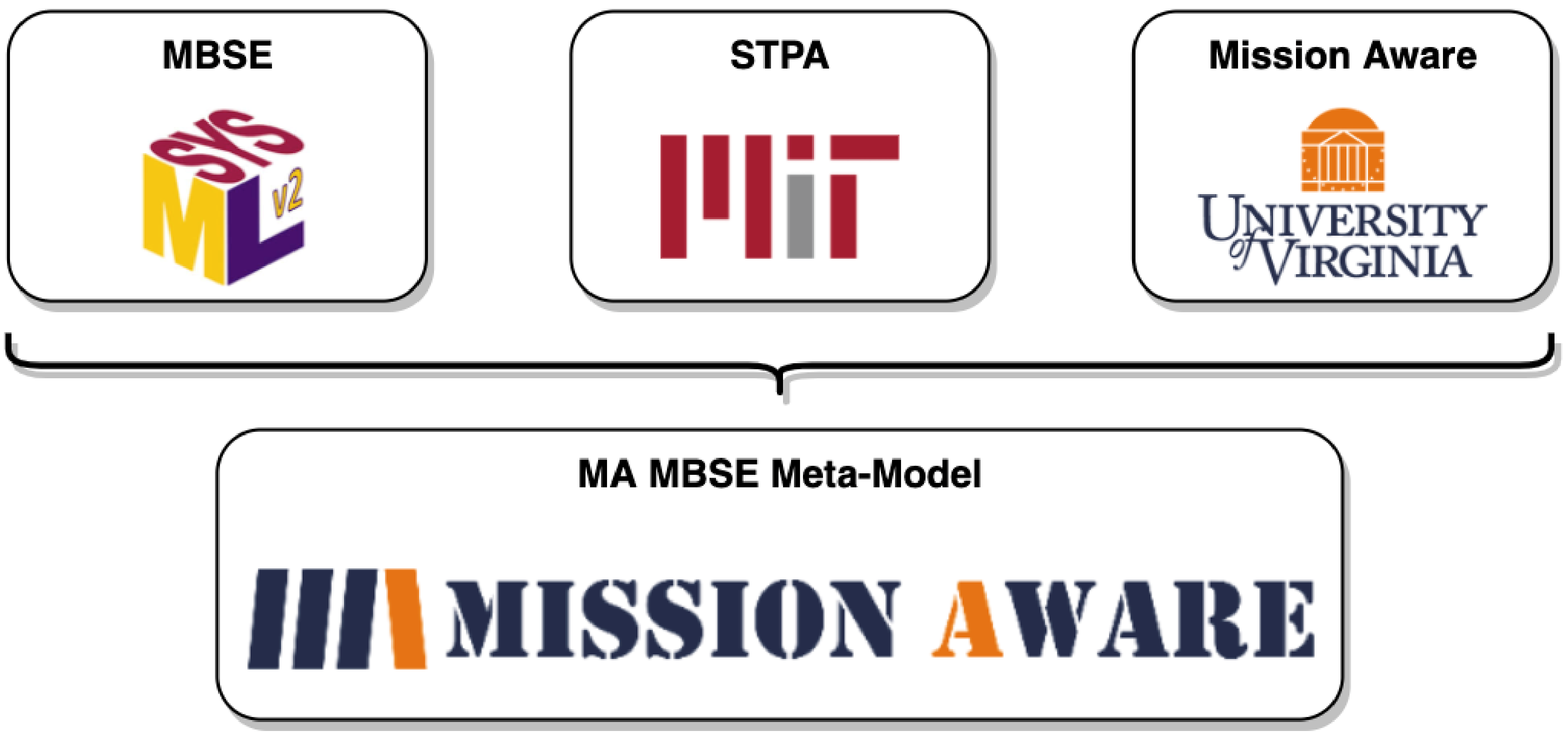
CYBOK: Cyber Body of Knowledge (VCU)

- CYBOK is a multi-view search engine on how to "relate" cyber threat information in a systems model context. It views the diverse set of cyber repositories (CAPEC, CWE, CVE, CPE, etc.) as greater than the sum of their individual parts.

- Uncovering the synergistic relations in these diverse set of repositories and casting the information into "system" model perspective is the innovative aspect of CYBOK.



The Mission Aware Metamodel (UVa)



System Theoretic Process Assessment (MIT)

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.

STPA Outputs and Traceability

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

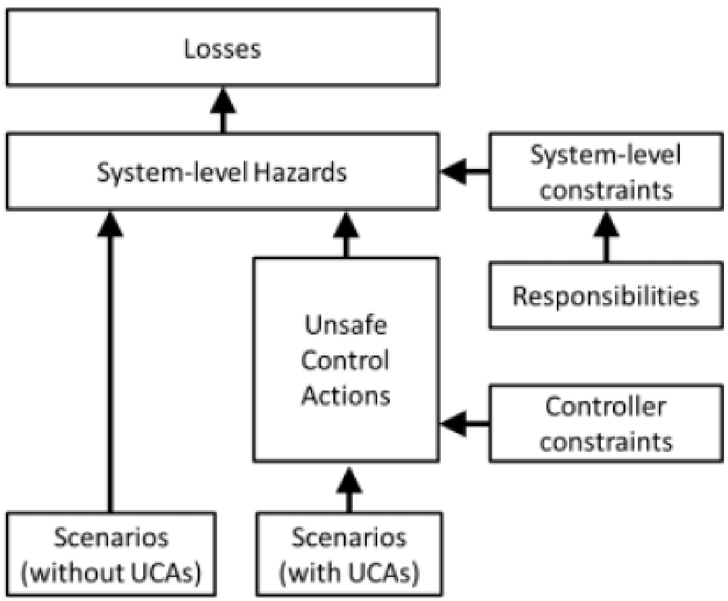


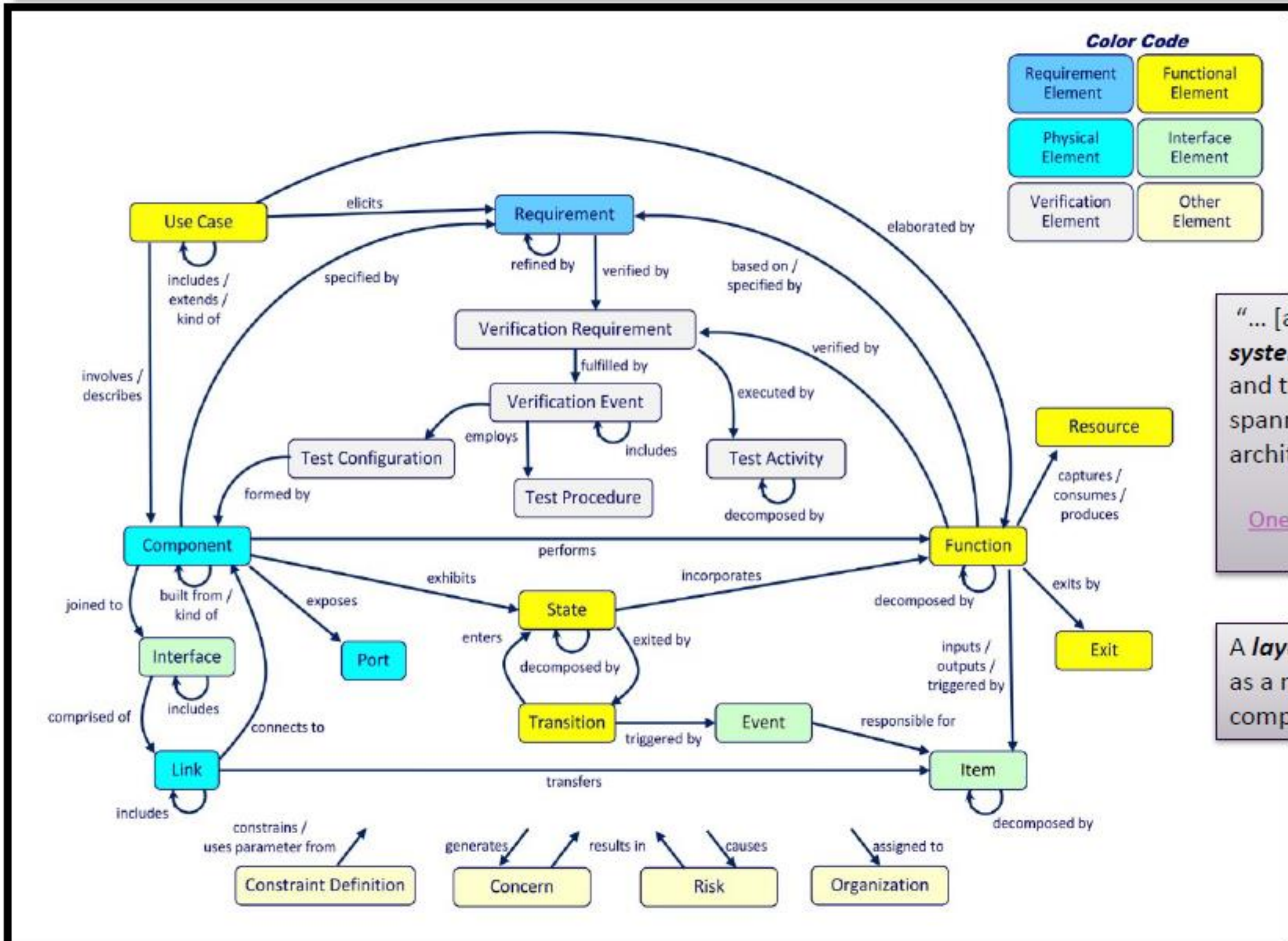
Figure 2.21: Traceability between STPA outputs

- 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 Handbook – Leveson & Thomas - 2018

Extending an SE Meta-Model to Assurance

Key requirement defined by Object Management Group (OMG) for SysML v2 is "*a meta-model of core SE concepts with precise semantics*." Vitech Corporation MBSE meta-model largely aligns with SysML v2 goals.

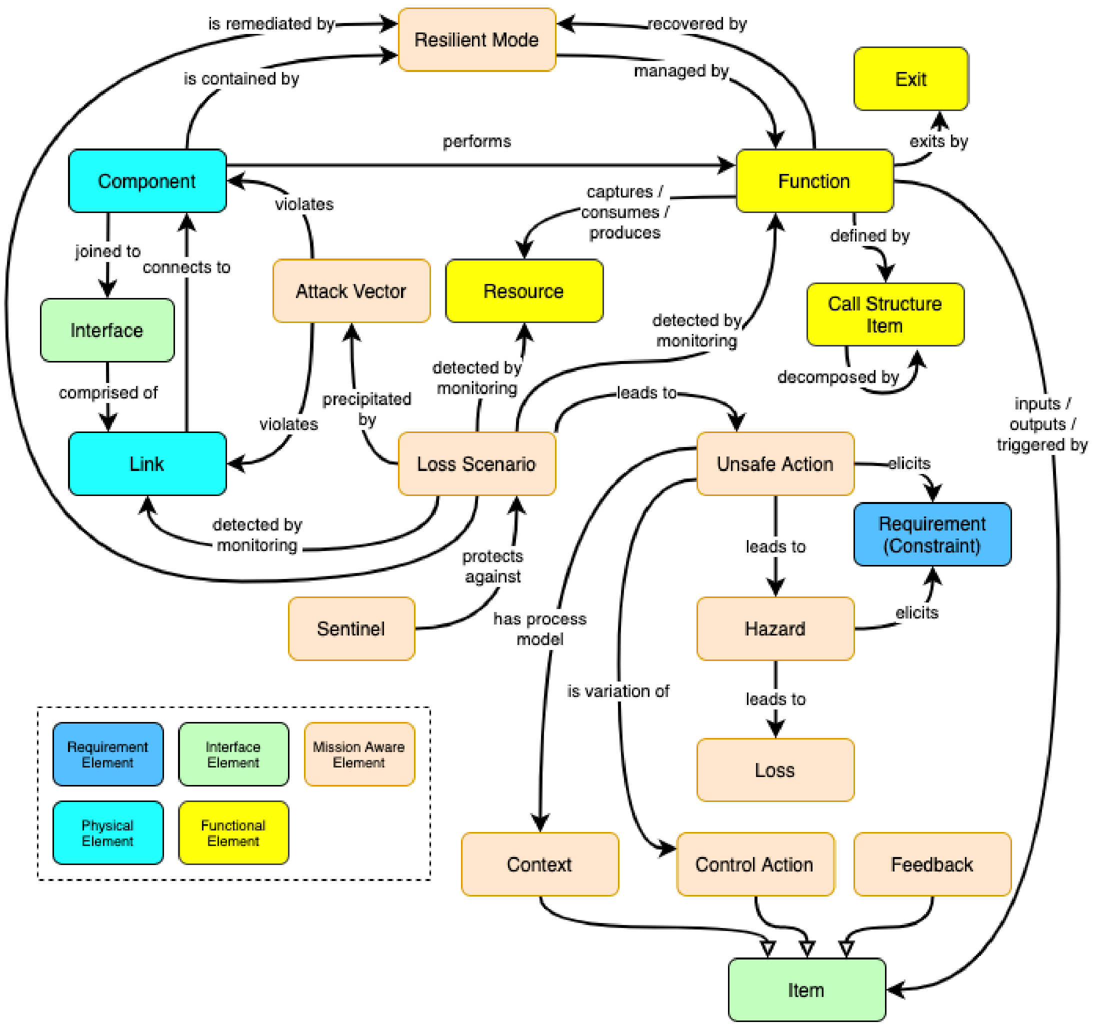


"... [a] representation of critical ***systems engineering concepts*** and their ***interrelationships*** spanning requirements, behavior, architecture, and test."

One Model, Many Interests, Many Views - Vitech 2018

A ***layered / hierarchical*** model as a mechanism to manage complexity.

Extended MA-MBSE Meta-Model (UVa)

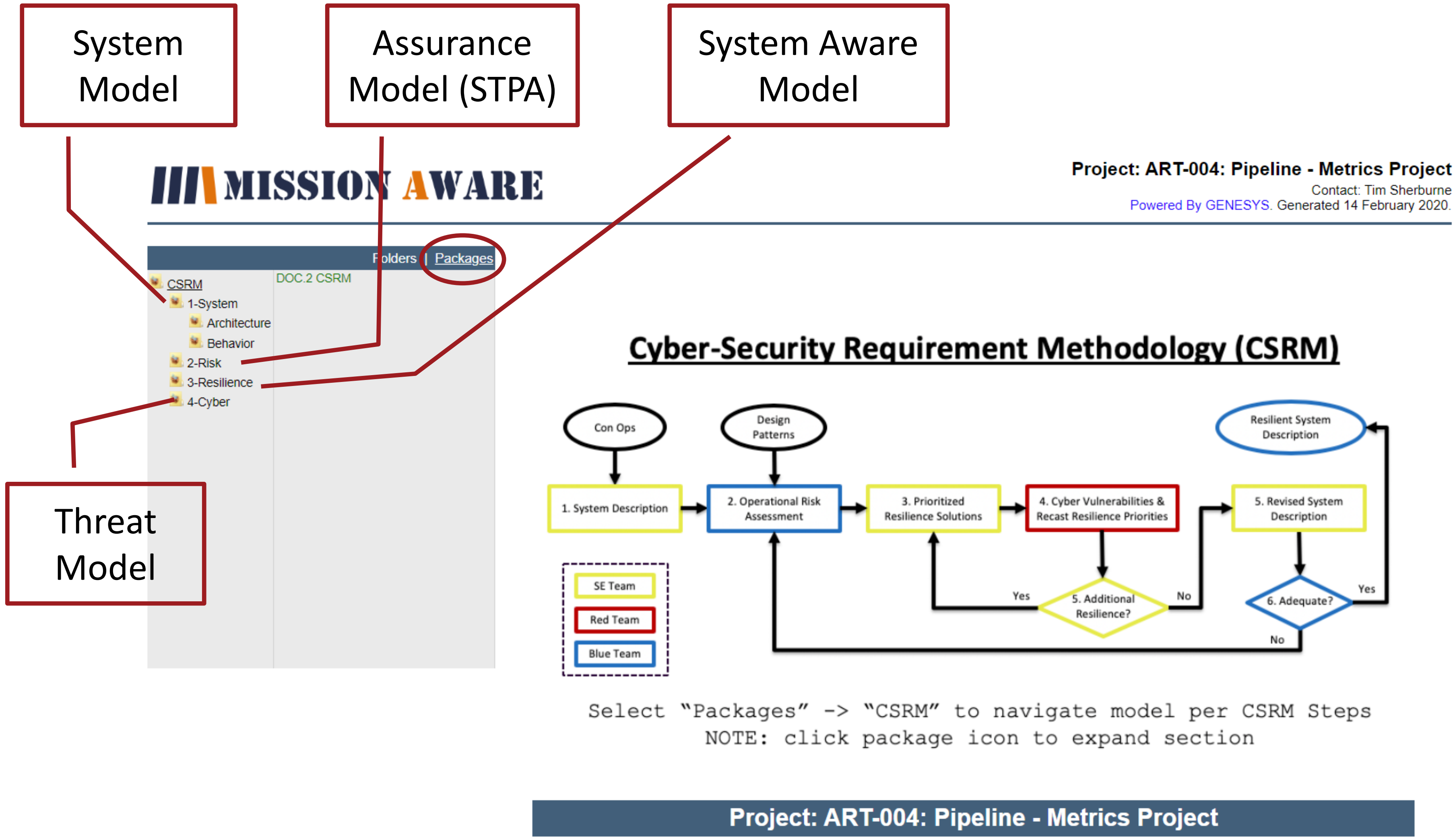


MISSION AWARE

<u>CSRM Steps:</u>

1. System Description
   - Component, Link
   - Function, Exit, Resource, Call Structure, Control Action, Feedback, Context
2. Risk Analysis
   - Loss, Hazard, Unsafe Action
3. Resilience Solutions
   - Resilient Mode
4. Cyber Vulnerability Assessment
   - Loss Scenario, Attack Vector
5. Iterate Resilience Solutions (Metrics)
6. Iterate Vulnerability Assessment

Modeling the System across the Meta-Model

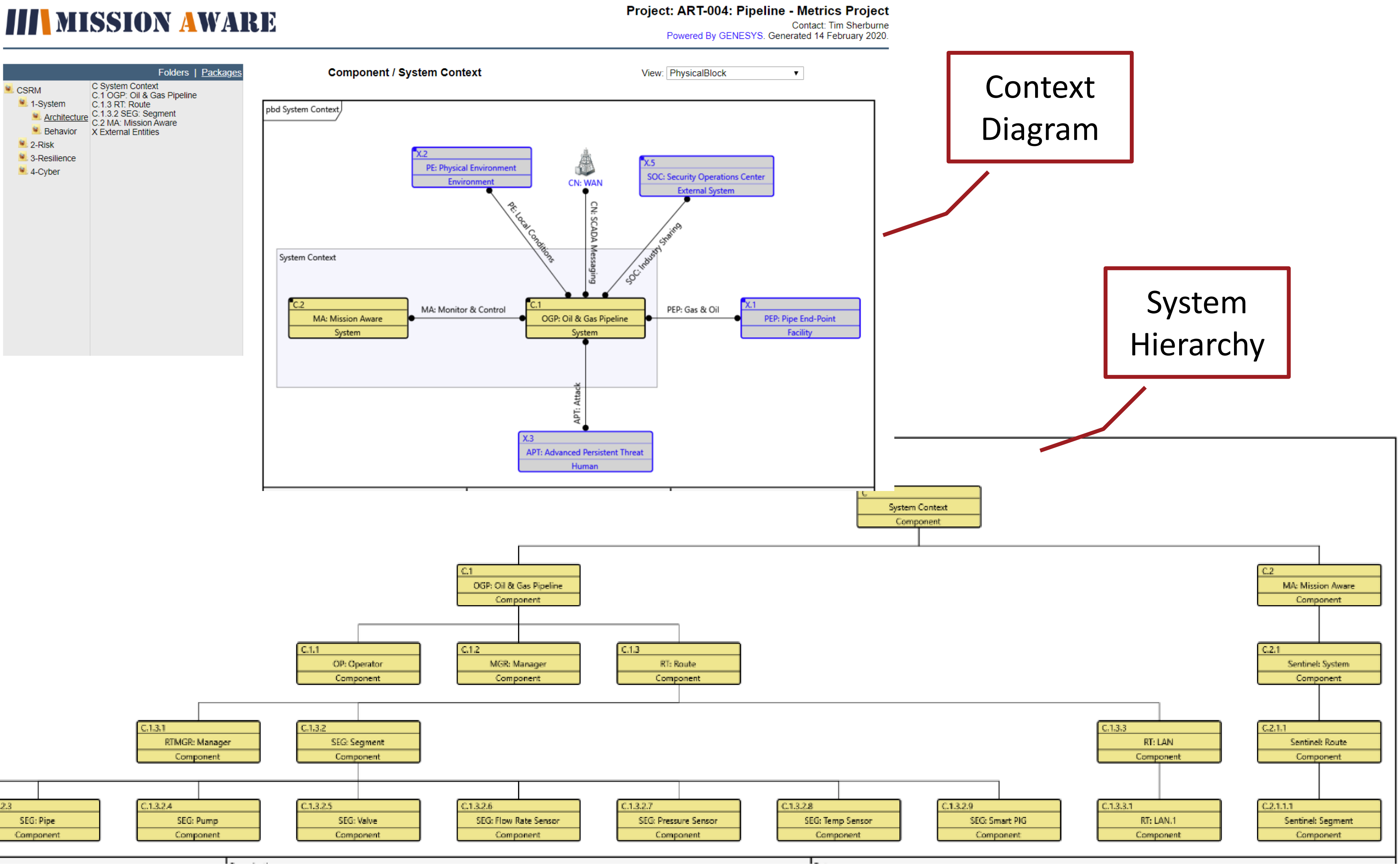


Application to a Complex System-of-Systems

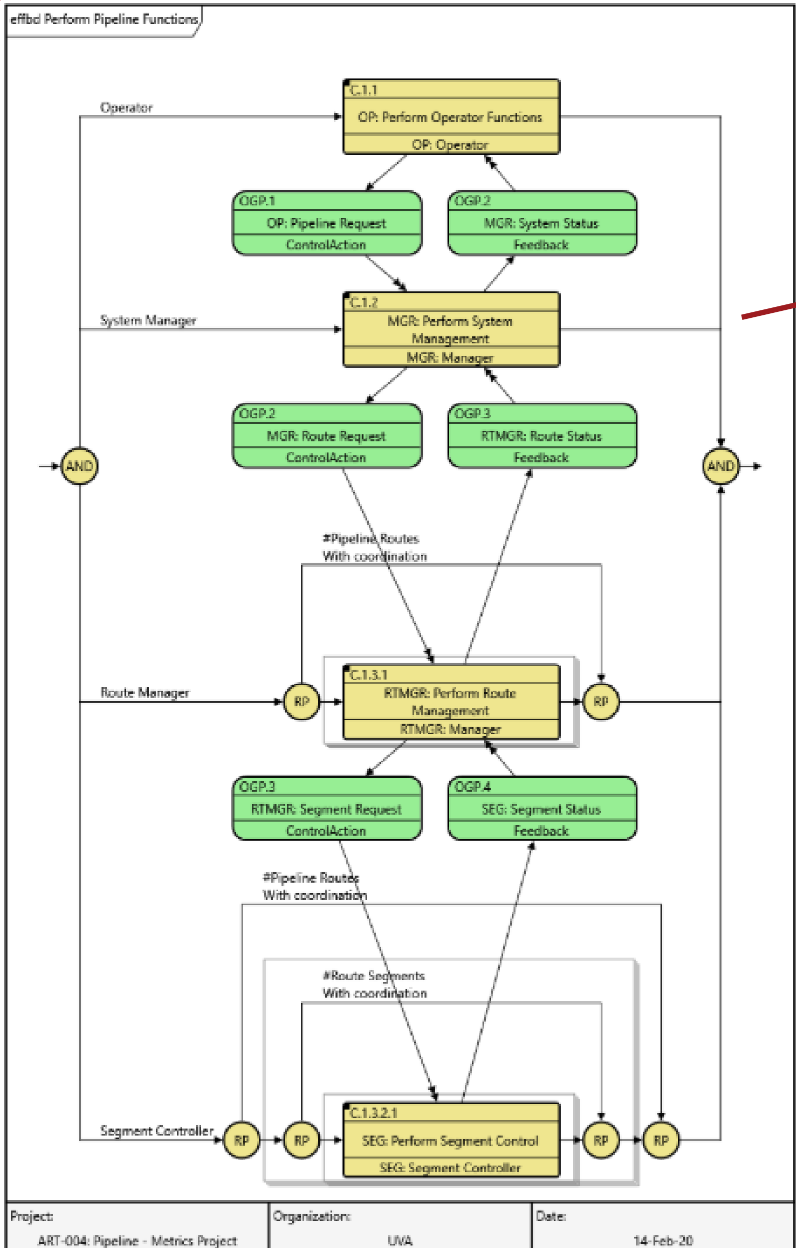
Scenario (Developed by students in Ga Tech Sam Nunn School of International Affairs, Scenario Building class):

- Posited cyber attack on Saudi Aramco Riyadh & Yanbu, Baiji (Iraq), and SPC refineries
- Fancy Bear (Russian hacker group) gains remote access to refinery controls, report false flow rates, pressure, temperature of trunk lines
- Russian refineries report "similar spills" as time goes on, and come out with malicious code "found" in their own refineries, solving the irritation plaguing the three countries
- Russia offers world-class cyber security services to all three countries - but also installs backdoor measures to take control in future
- Used to manipulate critical pipeline pumping stations to refineries, attacks degrade flow
- Causes yield of oil decreases by 6.2m barrels/ day (10% decrease in global oil availability)
- 50% price of oil increase for 30 days estimated at $31B market price impact
- **Significant profits in oil futures**

Oil/Gas Pipeline Model (demo)

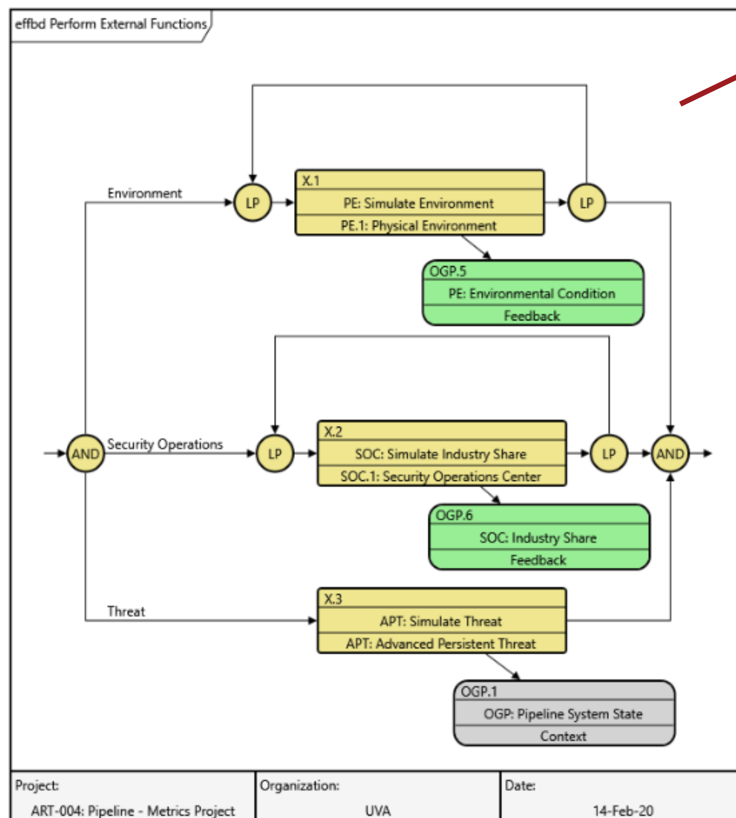


Oil/Gas Pipeline Model (demo)

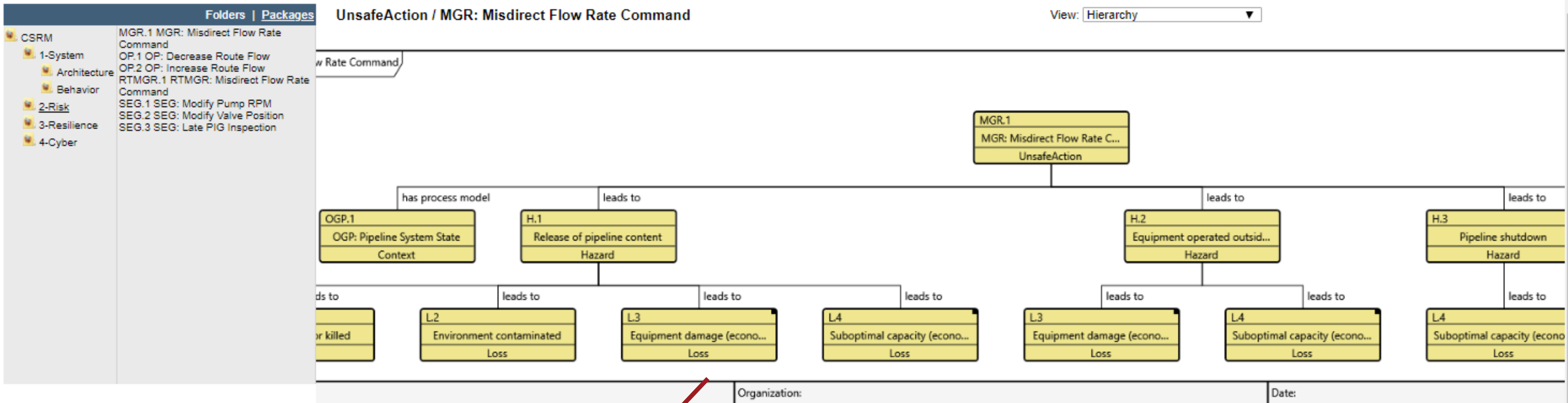


System Functional Flows

External Functional Flows

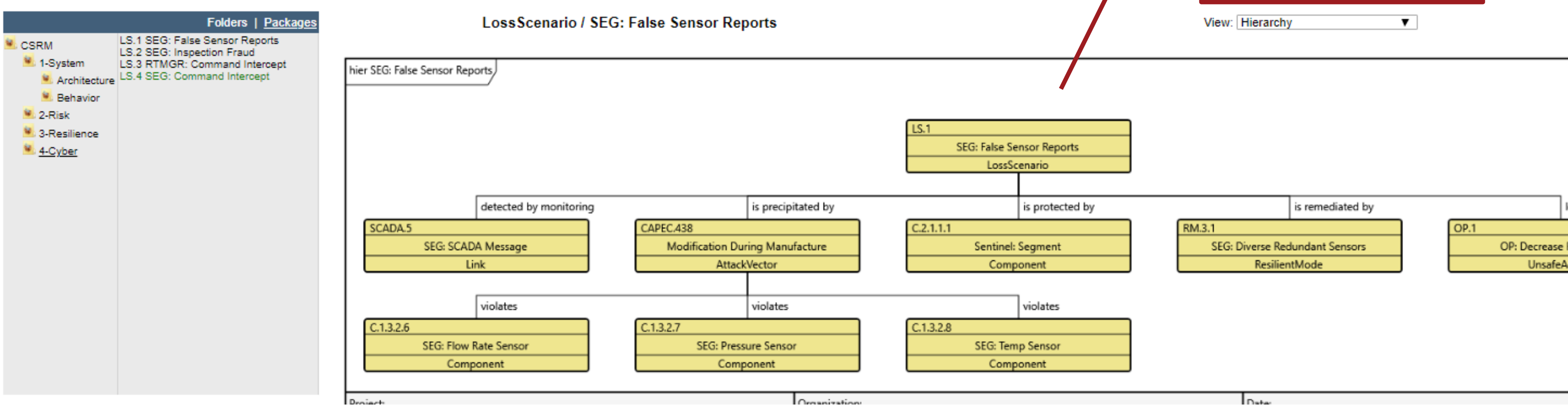


Oil/Gas Pipeline Model (demo)

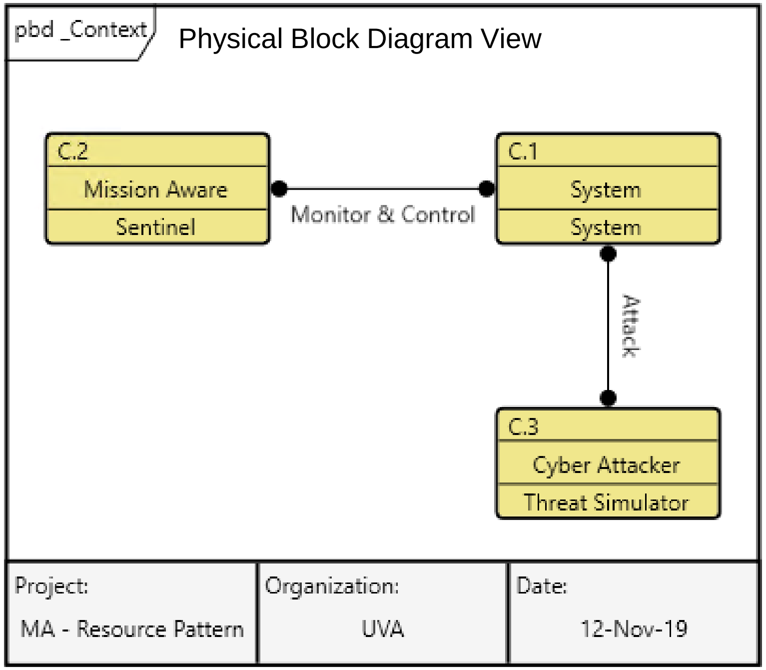


Risk Model (STPA)

Cyber Threat Model



Example: Architecture Model



Loss Scenario – Attack Pattern:

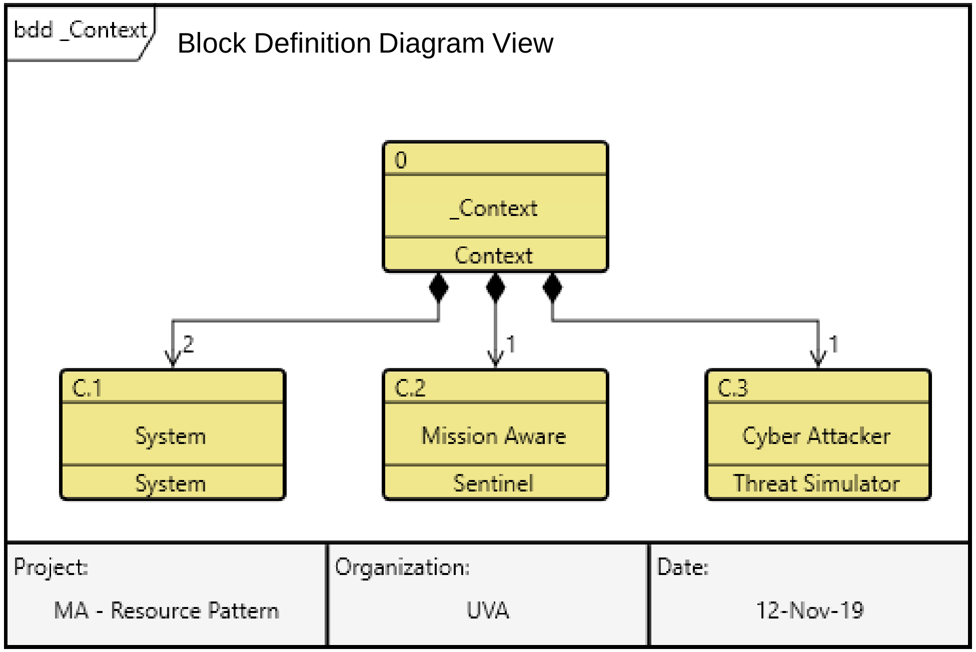
- CPU Overload
- CAPEC-443: Malicious Logic Inserted Into Product Software by Authorized Developer

Sentinel - Design Pattern:

- Resource Introspection - CPU Idle Time

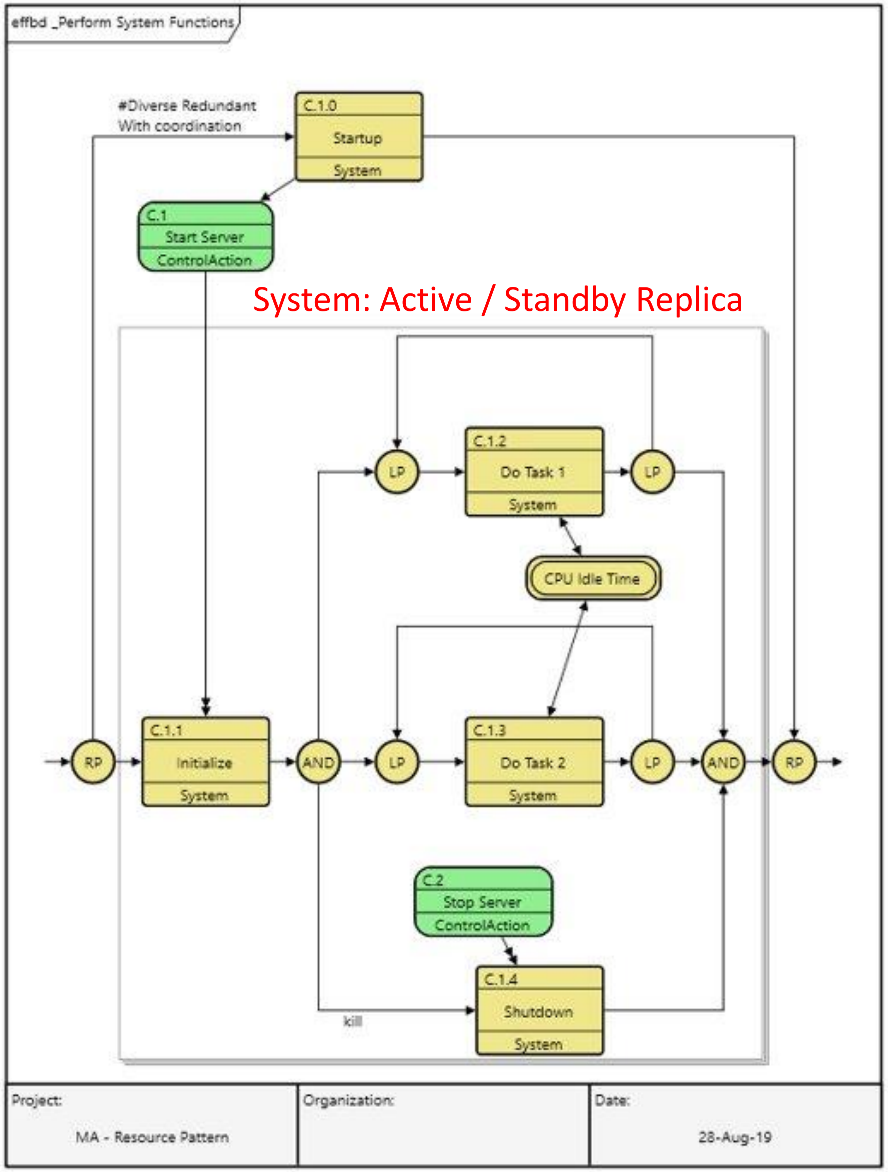
Resilient Mode:

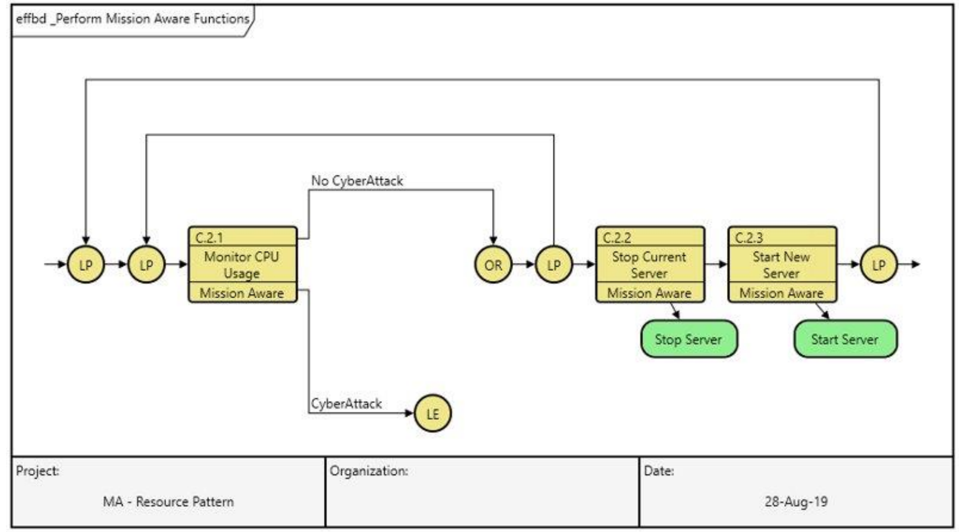
- Active / Standby

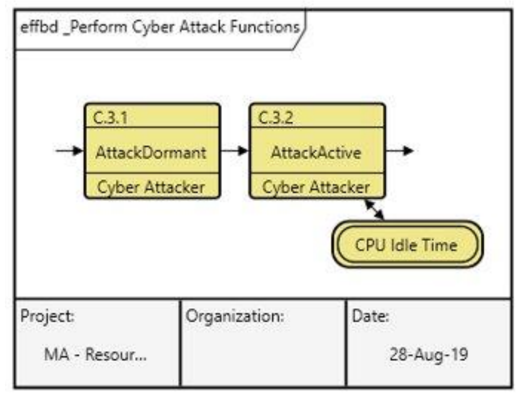


SYSTEMS ENGINEERING RESEARCH CENTER

Example: Behavior Model

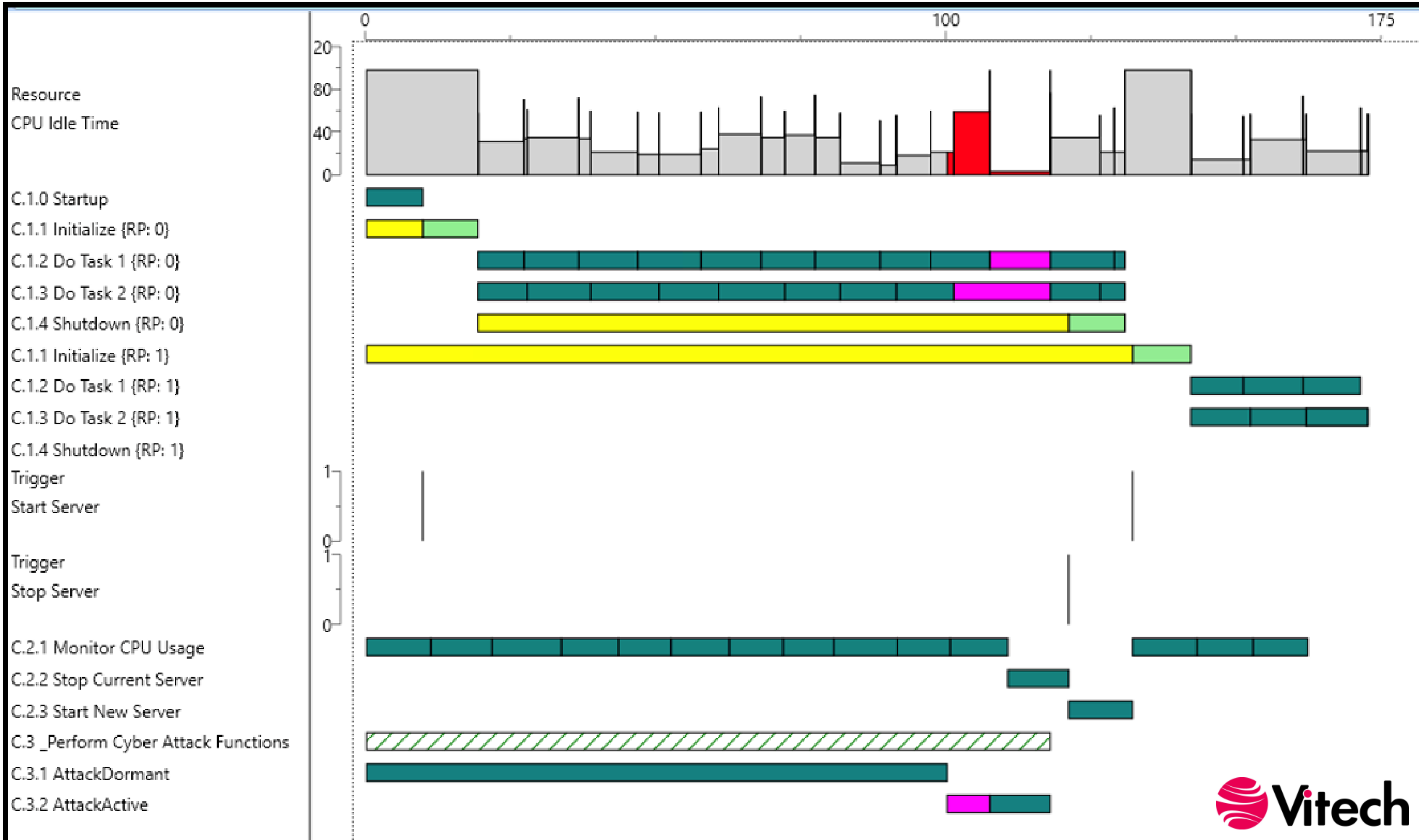






The Enhanced Functional Flow Block Diagram (EFFBD), like its SysML cousin the activity diagram, is a complete representation of behavior. EFFBDs unambiguously represent the *flow of control* through sequencing of functions as well an overlay of *data* and *resource* interactions.

Example: Simulation Transcript



SYSTEMS ENGINEERING RESEARCH CENTER

Sample Modeled Resilience Evaluation Metrics

Object	Metric	Values	Notes
Loss	missionImpact	High / Med / Low	Blue Team
Loss Scenario	attackLikelihood	High / Med / Low	Red Team
	detection Time	seconds	Time budget to detect loss. Impact tradeoff for Sentinel interfaces: • polling-based (system / link loading) • event-based, etc.
	isolateTime	seconds	Time budget to isolate loss via system /component tests.
Resilient Mode	complexity	High / Med / Low	Number of model "contained by" associations. Indication of cost.
	effectiveness	High / Med / Low	Impact on remediating High "likelihood" attacks associated with High "mission impact".
	operationalImpact	High / Med / Low	Degree of operator training need. Degree of mission interruption.
	restoreTime	seconds	Time budget to restore system function via resilient mode. Impact tradeoff for Resilient Modes: • Active/Active • Active/Standby (Hot / Warm / Cold)
	operatorDecisionTime	seconds	Time budget for operator decision time to enable resilient mode. 0 implies automated resilient mode.
Function -> RecoveredBy	recoveryRatio [per Loss Scenario] *Calculated:* Measured / Expected	< 1: Acceptable > 1: Not Acceptable	Recovery time includes: • Detection • Isolation • Restoration Including: • Technical: System Components • Operational: System-of-System Interactions • Operator: Expected Decision Times

Research Transition Activities

- We have a consistent methodology built on standard systems engineering methods, processes and tools
- Transition effort 1:
  - Use MA framework to develop metrics and associated test methodologies for developmental test and evaluation (DT&E) of cyber resilience in CPS.
  - Demonstration on hypothetical design-stage weapons system.
- Transition effort #2:
  - Integration of the MA Meta-Model with Mission Engineering activities
  - Integration of the MA Meta-Model with SW code generation and assurance analysis tools
  - Integration of the MA Meta-Model with dynamic simulation tools