SYSTEMS ENGINEERING RESEARCH CENTER

Georgia Tech Research Institute

Security at Design Time: Addressing Resilience in Mission Critical Cyber-Physical Systems

Mr. Tom McDermott
Dr. Valerie Sitterle
Georgia Tech Research Institute

NDIA 20th Annual Systems Engineering Conference
26 October 2017

Springfield, Virginia

Model-Based System Assurance

- A workshop focused on identifying and prioritizing appropriate research questions related to next generation system assurance, i.e. Model-Based System Assurance (MBSA)
  - relevancy from a practitioners' perspective,
  - and uniqueness and rigor from a research and academic perspective

Weapon System Cyber Resiliency Critical to Mission Assurance

- We define the Cyber Resiliency of Military systems to be:
  - The ability of weapon systems *to maintain mission effective capability* under adversary offensive cyber operations
  - To *manage the risk* of adversary cyber intelligence exploitation
- Weapon systems differ from general administrative and business IT systems in ways that matter for implementing Cyber Resiliency

Cyber Campaign Plan FOCUS

Weapon Systems

Software/Hardware Design

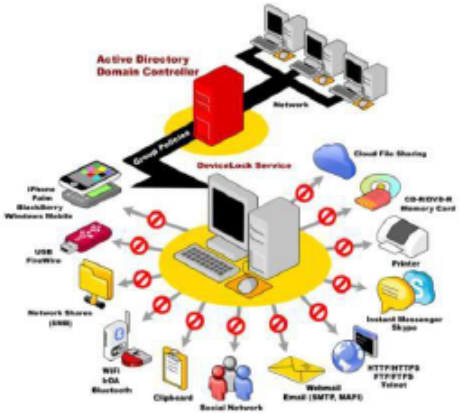
Government control — COTS

Architectures

Diverse — Common

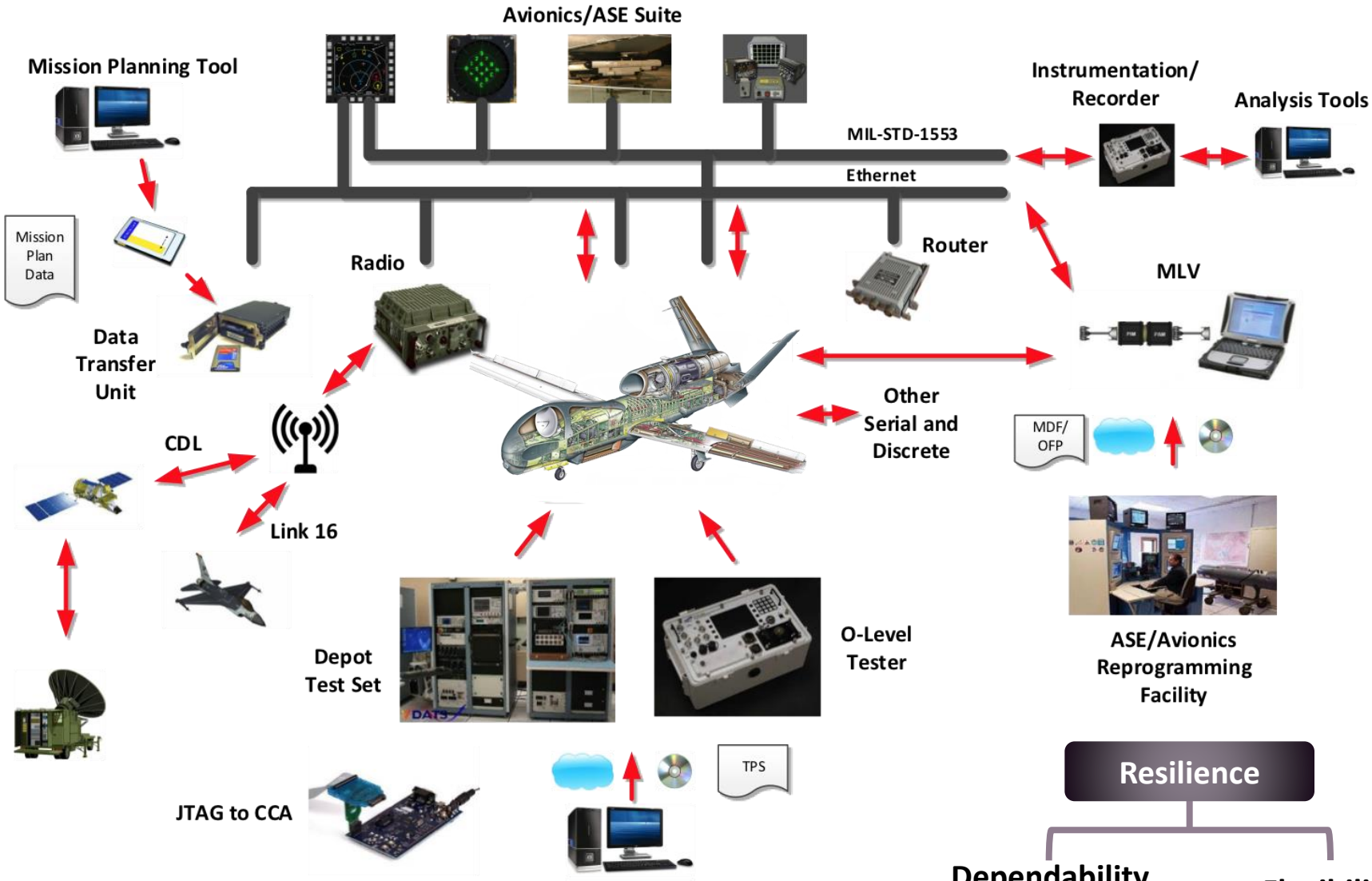
Interfaces

Customized — Standardized



IT Systems

Is My System Cyber-Resilient?



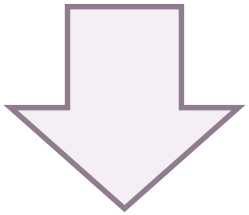
Resilience

- **Dependability and Security**
- **Flexibility**

Security at Design Time

1. To evaluate security for a system with cyber elements, we must holistically evaluate the system, the threat(s), and the protection (i.e., the security design pattern(s)) as a single ecosystem.

2. Resilience is best understood as a non-functional property that emerges from the dynamics across interdependent elements in an ecosystem. A single system perspective or a strictly topological perspective will be insufficient.



Executable, contextual, and analyzable representation of
"Did our 'designing-in' for Resilience
indeed preserve mission-critical functionality in the face of the threat(s)?"

Systems and Future Needs

Systems are increasingly …

Comprised of heterogeneous elements

Cyber-ized

That are interdependent and independent

Logical and spatial in scale

New capabilities

New threats

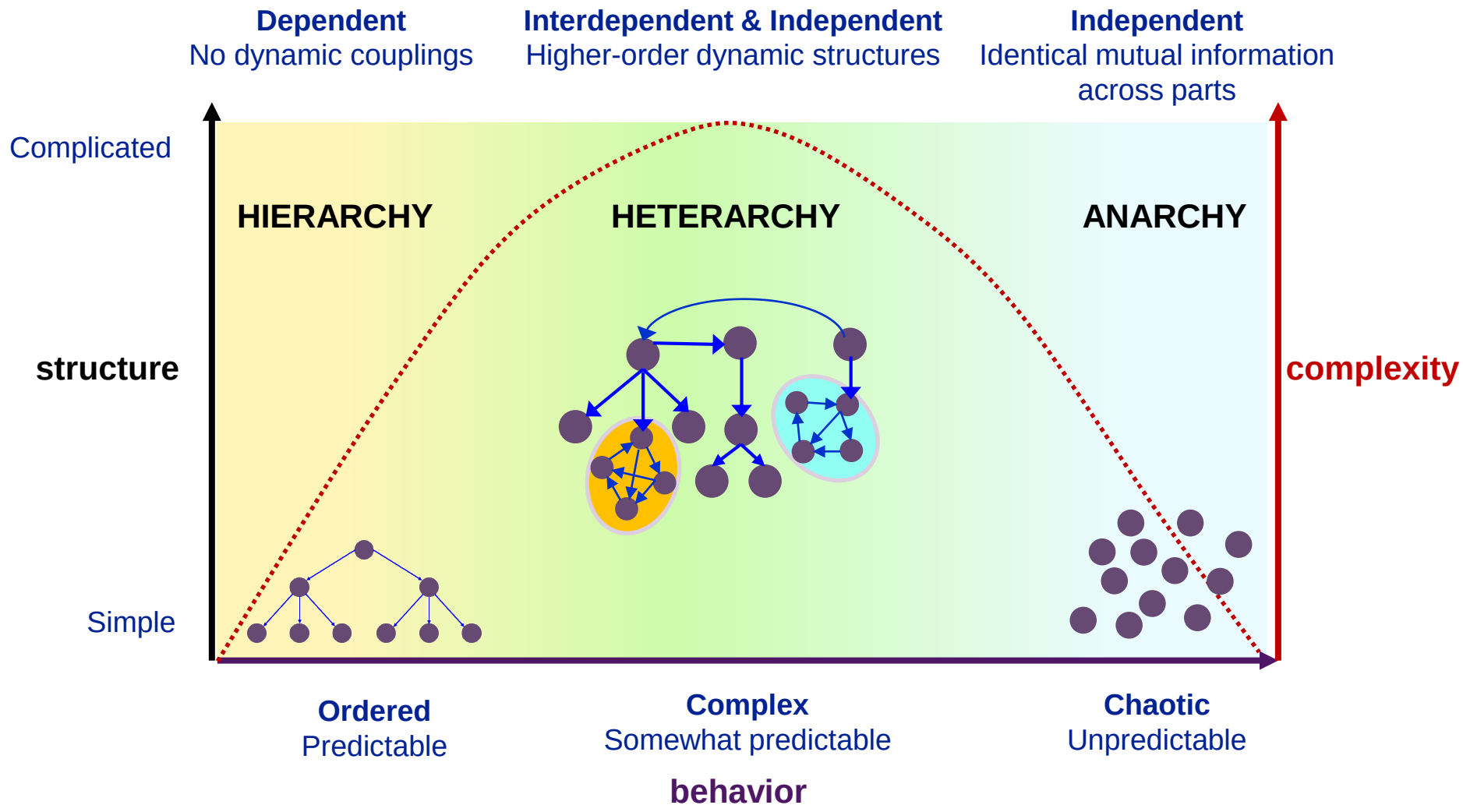
Context

Traditional Systems Engineering (SE) lacks external context inclusion in design selection M&S.

How can we 'design-in' Resilience at an earlier stages in the SE process?

Cyber-Physical systems are a good model.

Order and Form



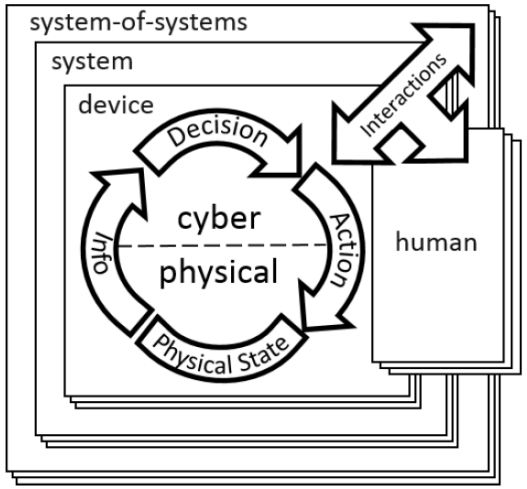
Structure and function are intrinsically linked.

System-Theoretic Accident Model and Processes (STAMP)

Nancy-Leveson_STAMP-Intro-2017.pdf

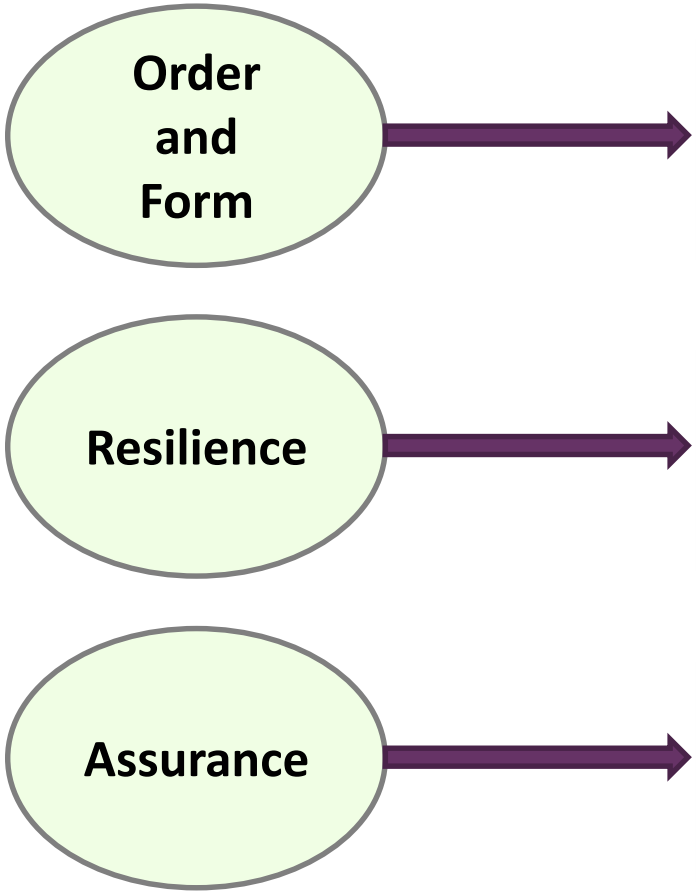
- ***Reductionist View***
  - Divide system into components
  - Assume system faults & failures are caused by component faults & failures
  - Identify chains of directly related physical or logical component failures that can lead to a loss (fault trees, event trees, attack trees,…)
  - Evaluate vulnerability or reliability of components separately and later combine analysis results into a system vulnerability or reliability value

- ***System Theoretic View***
  - Safety and security are emergent properties of the structure, function, and behaviors of a complex system
  - Safety and security are assured by controlling emergent properties (e.g., enforcing constraints) from individual components and interactions
  - View safety and security as a control structure



- ***Goal: Design an effective control structure that eliminates or reduces adverse events***

Where Does This Leave Us?



Defense systems of the future will tend toward 'Ordered Complexity'.

Behavior not fully revealed via decomposition.

Is contextual and emergent.

A System-only view is insufficient to understand and evaluate Resilience.

Cannot be explicitly determined up front.

Is a measure of functional preservation by a control structure.

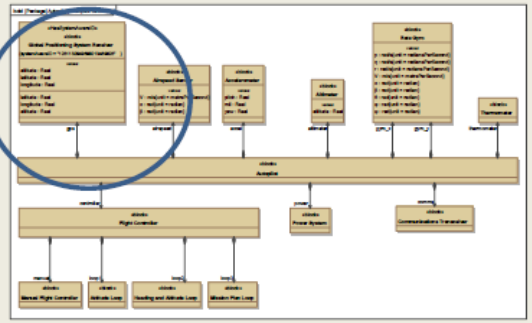
Designing-in Resilience therefore requires both bringing in the context and elucidating structure-function relationships to behavior.

SERC System-Aware Cyber-Security

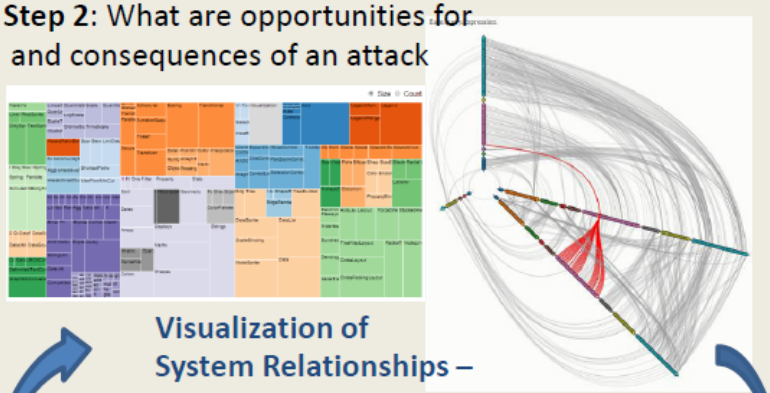
System Aware Cyber Security Framework: V2.0

Step 1: Identify Critical Assets

SysML models of UAV
(High fidelity Model Semantics)



Step 2: What are opportunities for and consequences of an attack

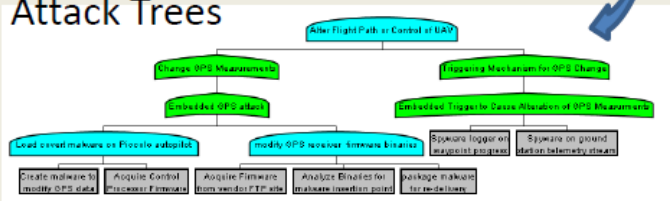


Visualization of System Relationships – Better Coverage of Attack Surfaces

Explicit information exchange- Information from SysML models helps create Attack Trees closer to reality

Step 3: What is exploitable and by whom

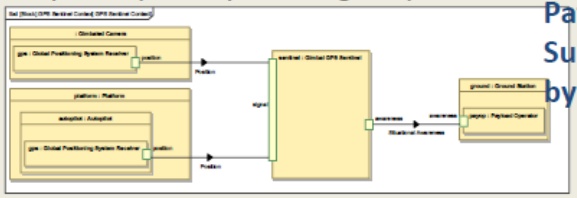
Attack Trees



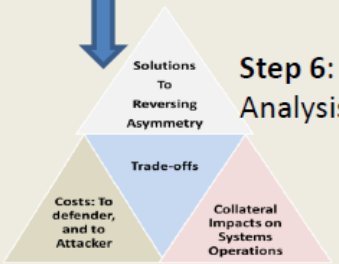
Output:
- Ease of Attack
- Capabilistic Propensity
- Relative Risk

Step 4 and 5: Select/Evaluate Best Design Patterns to effect Adversary's capability to exploit Target System

Evaluation of Design Patterns Now Supported by Functional Models



Step 6: Cost Benefit Analysis



Decision making now aided with Easy to use Data Analysis/Visualization Tools

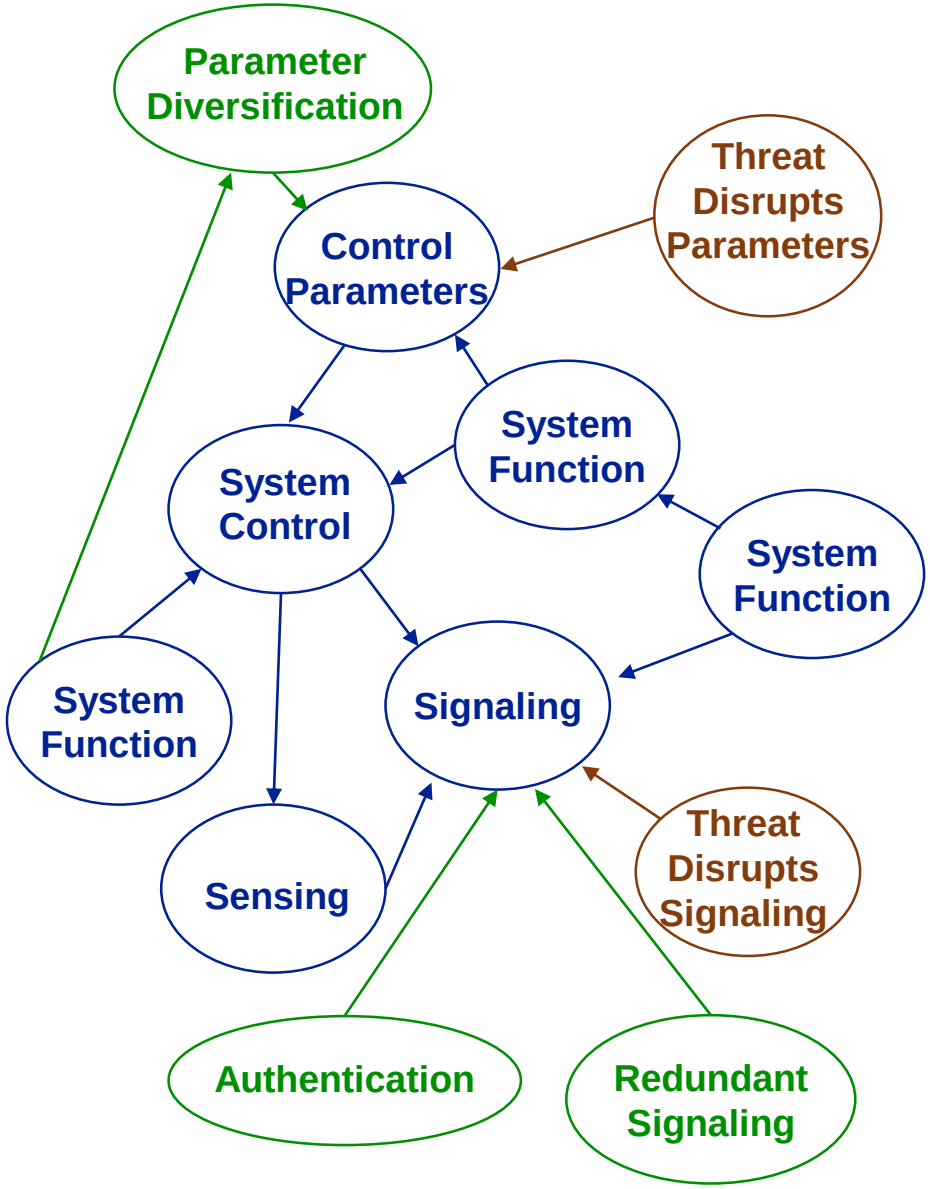
Resources for Attack

Attack Descriptions

Agent Profiles

Where to Start?
– Think executable functional model of the ecosystem

- **Extract system functional information**
  - Directed Acyclic Graph
- **Extract relationships between threat vectors and functional assets**
  - Attack vectors captured in an attack tree
  - Semantic mapping of attack vector descriptors to targeted assets
- **Extract a semantic mapping of Blue design patterns to:**
  - Their functional capabilities
  - Assets they require to achieve capabilities
  - Critical functions/assets they will protect
  - Specific threat capabilities and/or threat assets they are designed to detect or counter through direct connective action

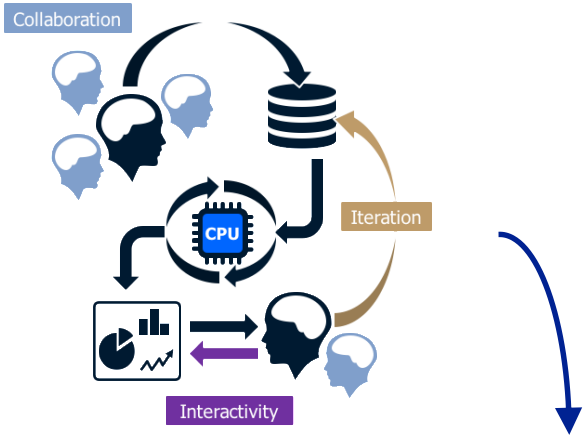


Resilience comes at a Cost

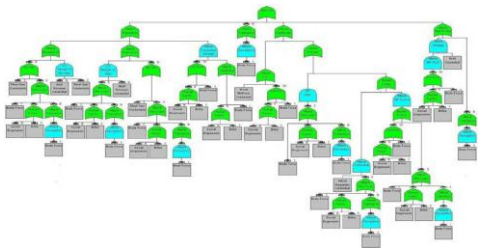
Reduce your space –

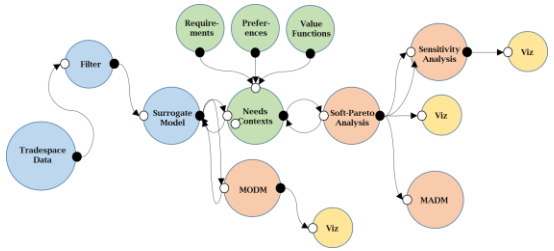
SME-guided analysis of system functions, attack vulnerabilities, and protection methods.

Protection methods serve as defense design patterns.



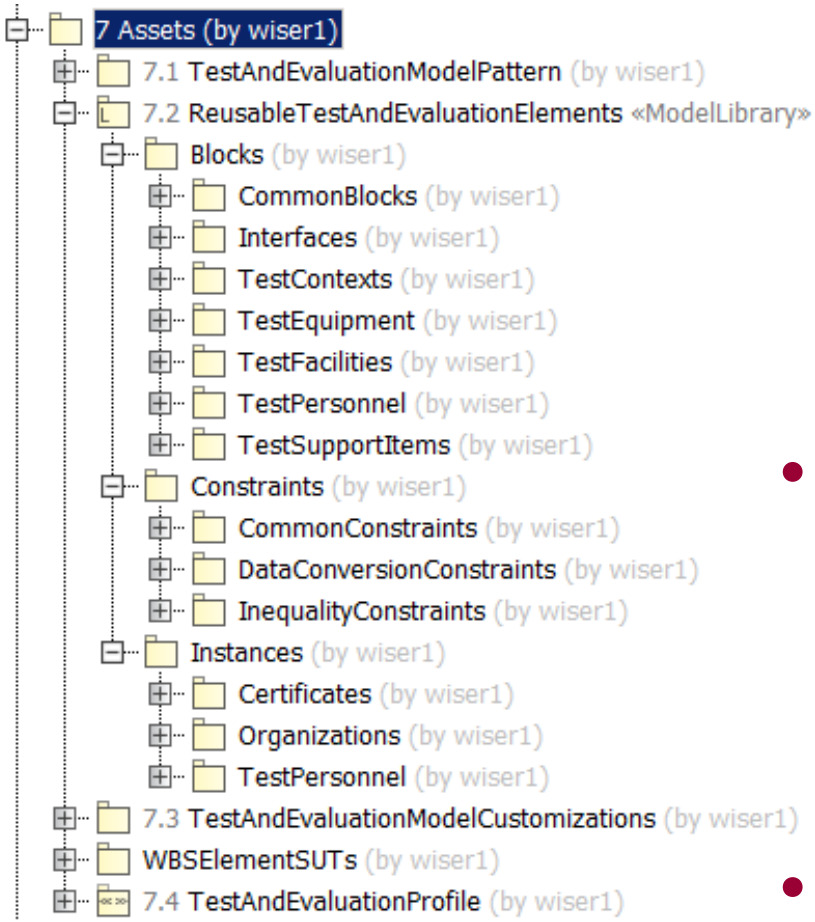
Create a "library" of security design patterns and associated threats.





- Prioritize threats and security implementations via decision tool.
- Perform trades on effectiveness, ease, and "cost" parameters.
- Narrow down threat and security implementation spaces.

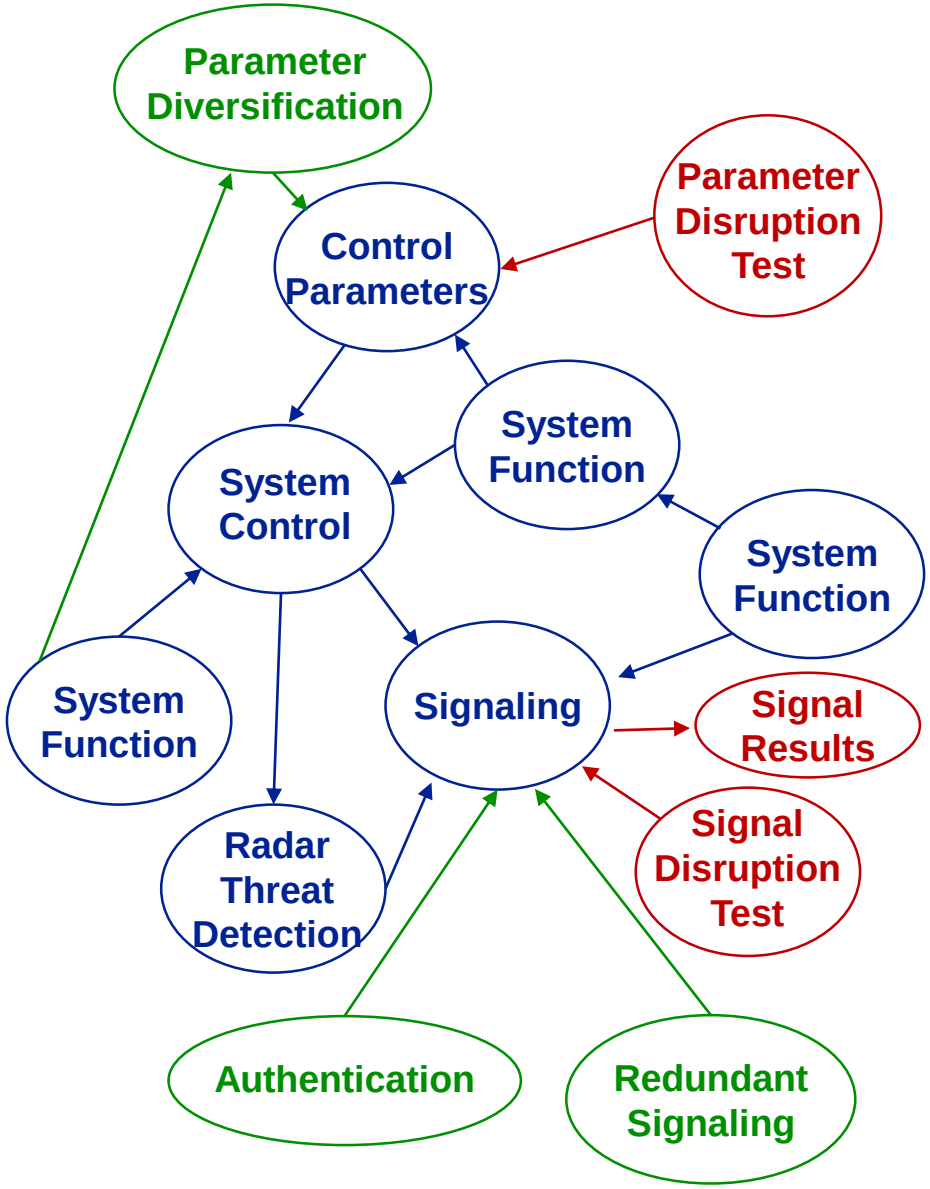
SysML for Test Framework



- Forces Test and SE teams to <u>get specific</u>
  - Captures test knowledge
  - Provides leadership with clear and comprehensive vision of how system will be integrated (and tested),
- It's integrated with the design model
  - The T&E strategy, implementation, and status are integrated with our design model (i.e. our 'source of truth').
- Consistency
  - Assists in the transition process as personnel turnover responsibilities

Where to End?
– Test an executable functional ecosystem model

- **Extract system functional information**
- **Extract relationships between threat vectors and functional assets**
- **Extract a semantic mapping of Blue design patterns**
- **Create assurance test framework and patterns to:**
  - Evaluate system response to threat
  - Maintain explicit knowledge of vulnerabilities and corrective patterns in design model
  - Build standard libraries of test strategies



Motivation for Research

Represent:

(a) impact of a threat, and

(b) impact of a protective implementation, and

(c) How it was evaluated, on

(d) the critical functional capabilities of a CPS.

… but challenges remain.

Structure-Function Relationships

- How do we reveal complex structure-function relationships that may not be visible via the functional decomposition model produced in early-stage design?

Identical number of nodes, links, and degree distribution.

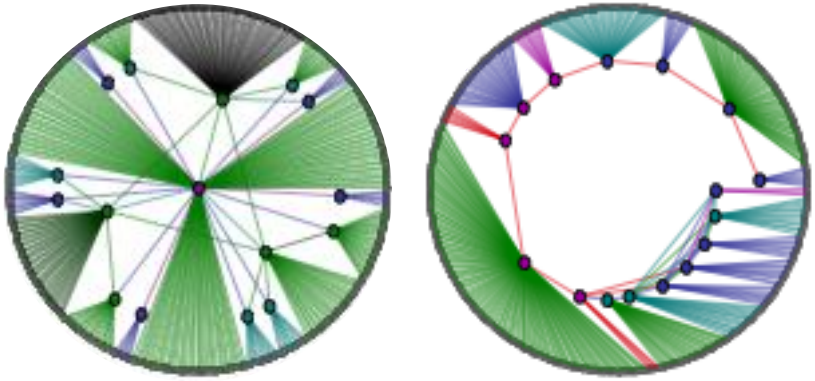


Image from Li (2005)

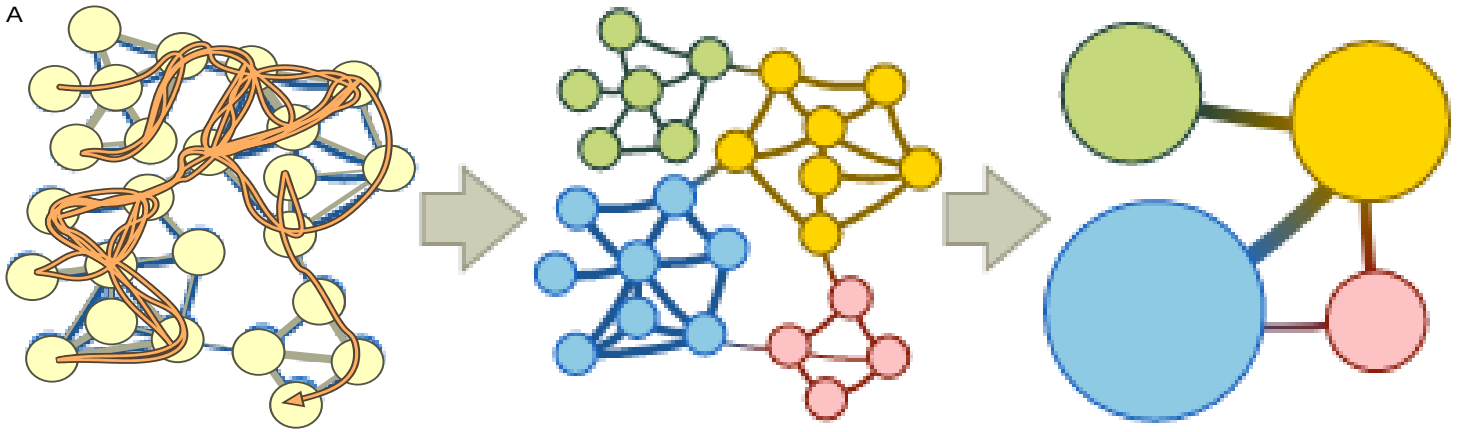
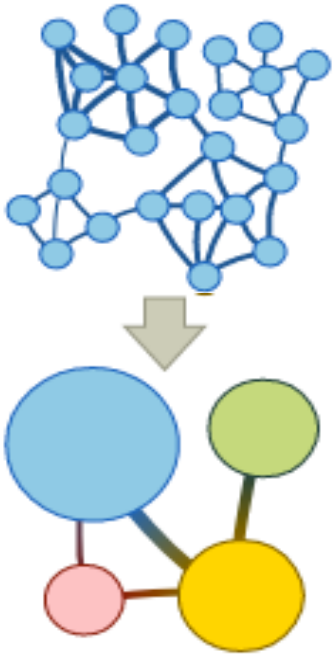


Image from Rosvall, http://www.tp.umu.se/~rosvall/

Elucidate Structure-Function relationships by discovery.

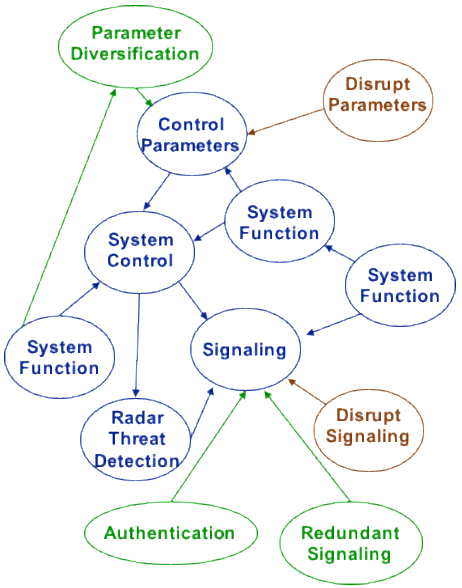
Synergy between Relationship Mapping and Model-Based System Design Processes

Embrace natural complexity of systems, revealing emergent behaviors, economies and diseconomies of scale, and consequences otherwise hidden



Research questions:

- Explain relationship between functional representations
- What does mapping reveal about fault or failure modes not discernible in the original topology?
- Do structural design changes preserve functionality of system?
- Can we use to determine impact of different approaches –
- Did our design decisions preserve functionality for our system?



Model-Based System Assurance

SYSTEMS ENGINEERING RESEARCH CENTER

A U.S. DEPARTMENT OF DEFENSE UNIVERSITY AFFILIATED RESEARCH CENTER

- Please see me to request an invite
- Tom.mcdermott@gtri.gatech.edu