SYSTEMS ENGINEERING RESEARCH CENTER

Georgia Tech Research Institute

Systemic Security and the Role of Hierarchical Design in Cyber-Physical Systems

Sponsor: DASD(SE)

By

Dr. Valerie Sitterle and Mr. Tom McDermott

Georgia Tech Research Institute

9th Annual SERC Sponsor Research Review

November 8, 2017

FHI 360 CONFERENCE CENTER

1825 Connecticut Avenue NW, 8th Floor

Washington, DC 20009

www.sercuarc.org

Systems and Future Needs

Systems are increasingly …

Comprised of heterogeneous elements

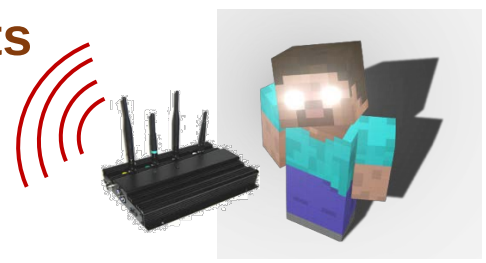
Cyber-ized

That are interdependent and independent

Logical and spatial in scale

New capabilities

New threats



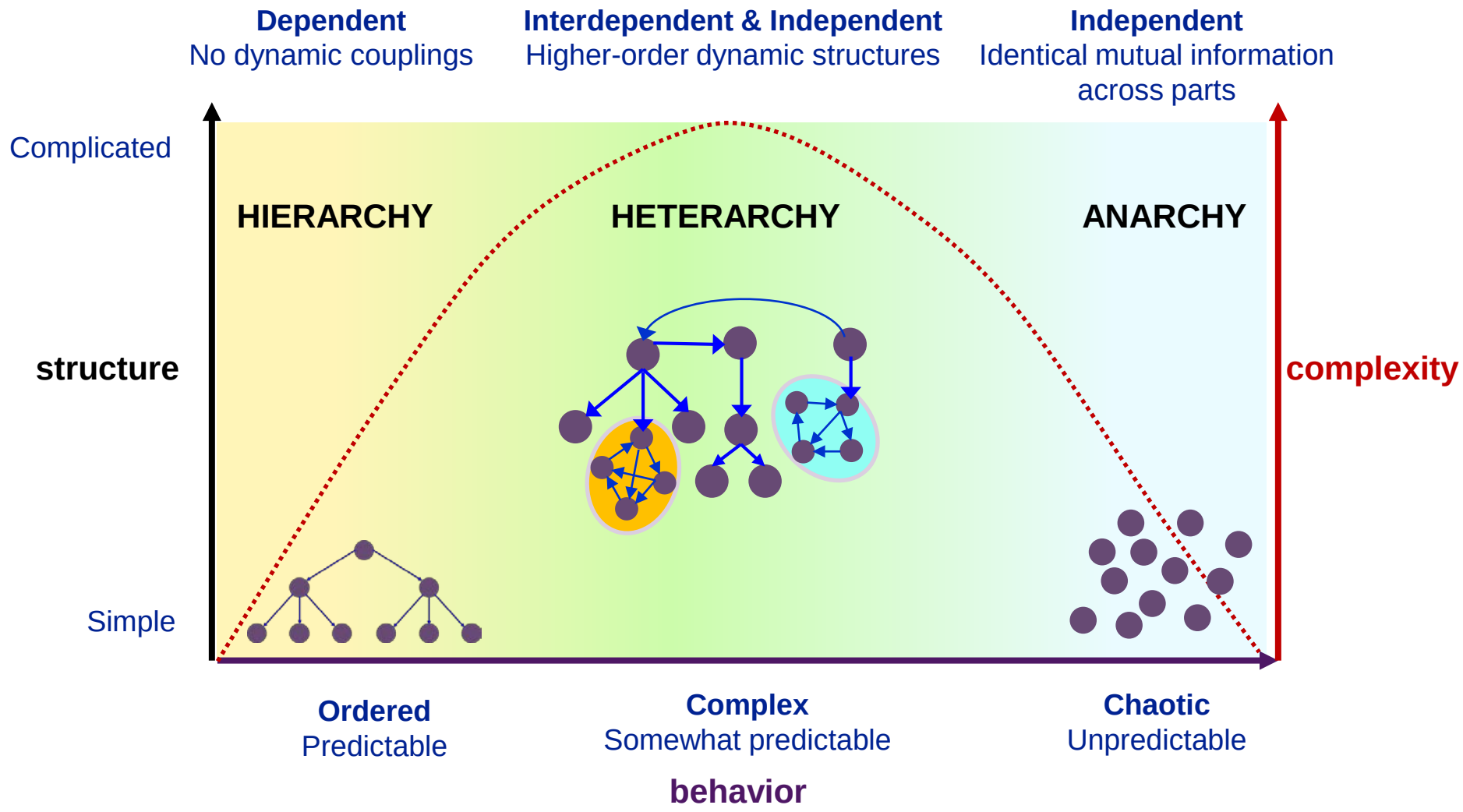
Context

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?

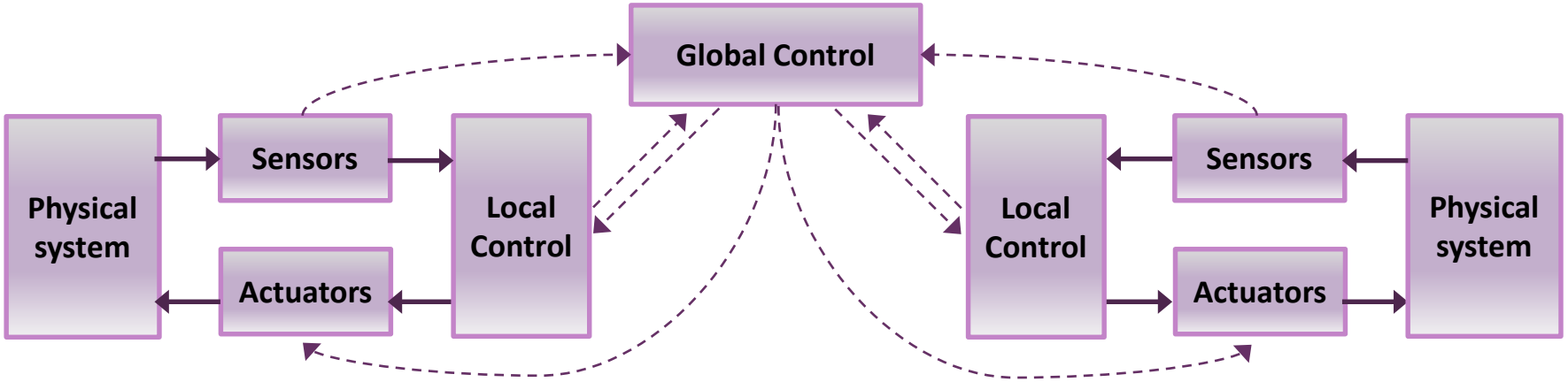
Cyber-Physical systems are a good model.

Order and Form



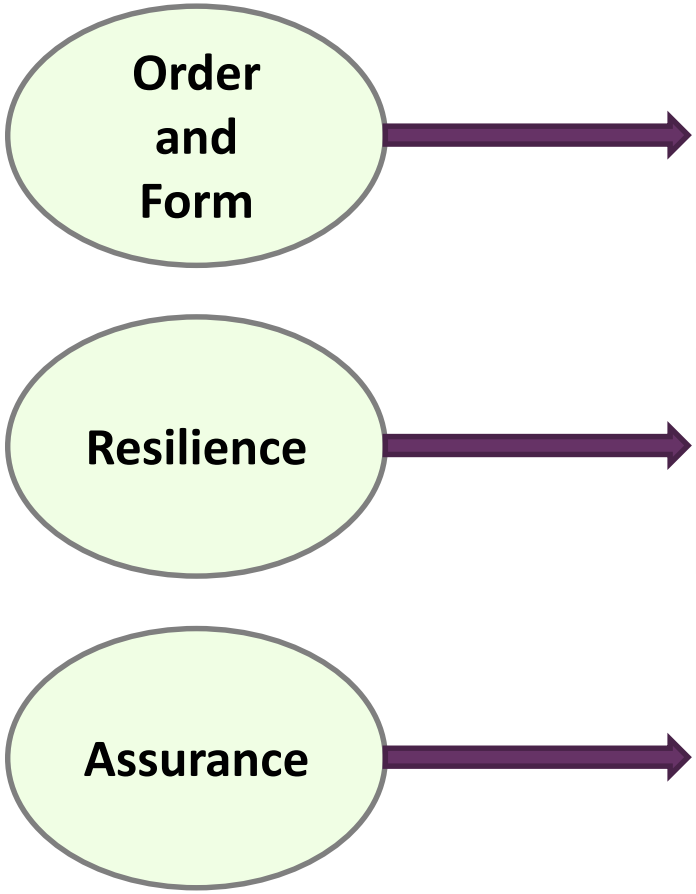
Structure and function are intrinsically linked.

Order and Form



Structure and function are intrinsically linked.

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.

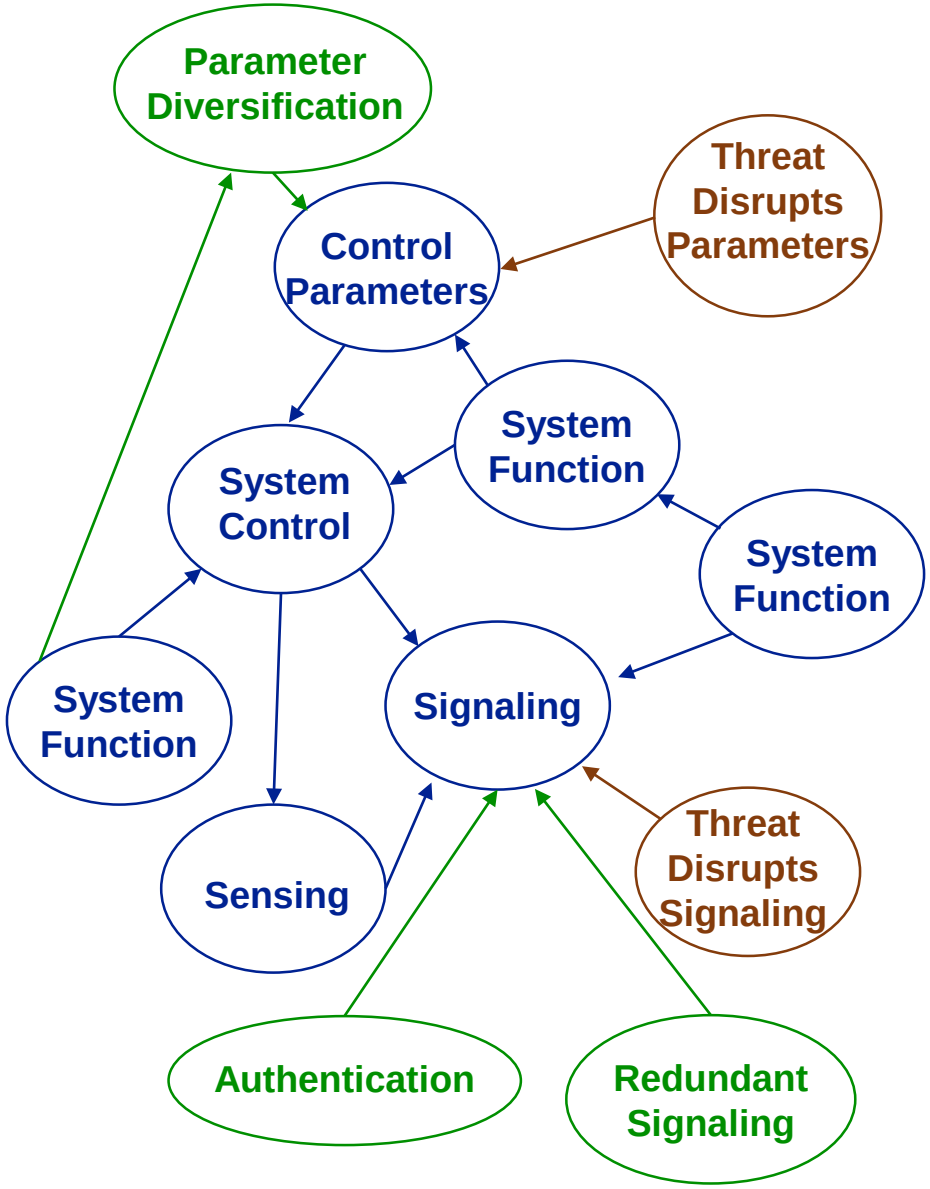
Is a measure of functional preservation by a control structure.

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

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

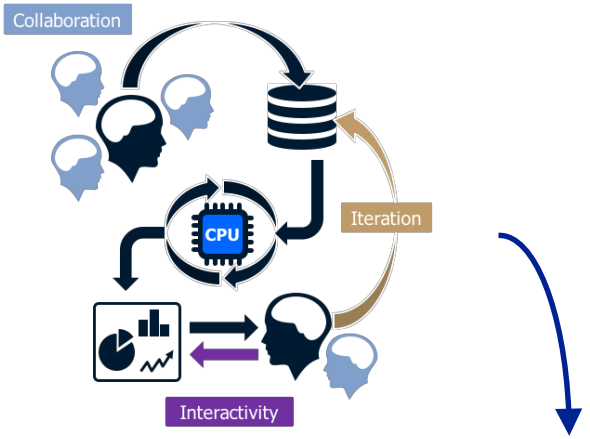


Resilience comes at a Cost

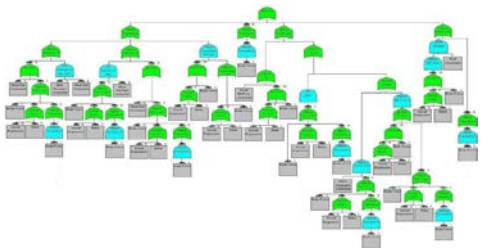
Reduce your space –

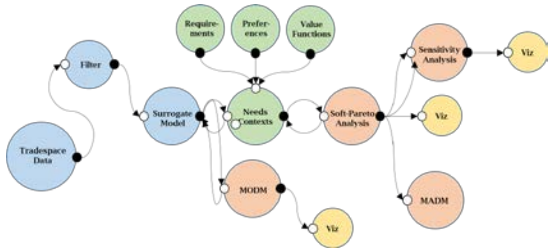
SME-guided analysis of system functions, attack vulnerabilities, and protection methods.

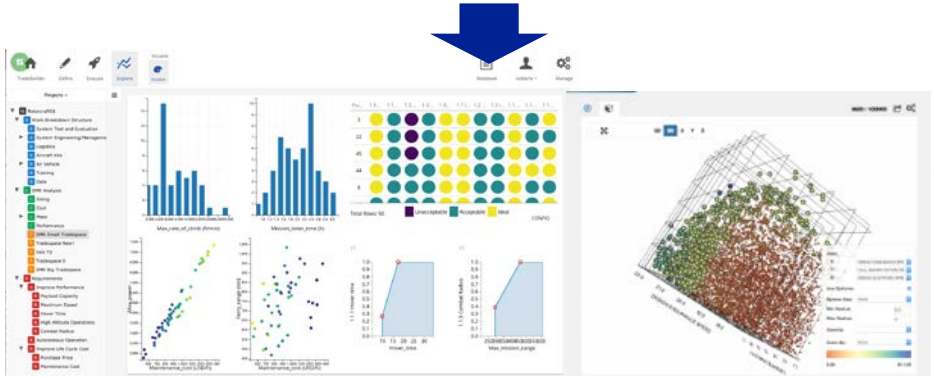
Protection methods serve as defense design patterns.



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

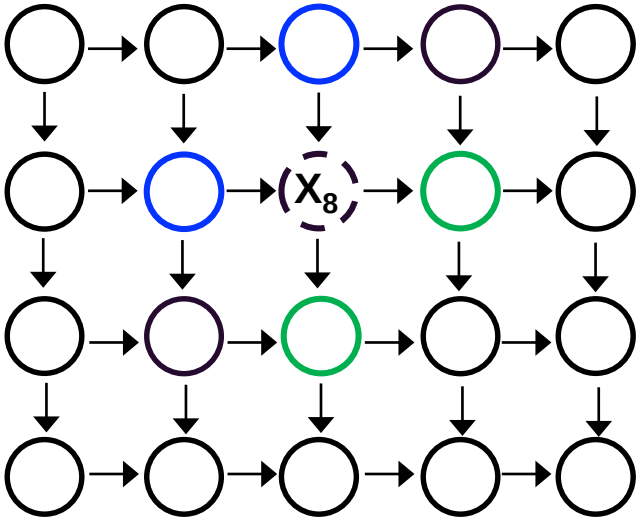


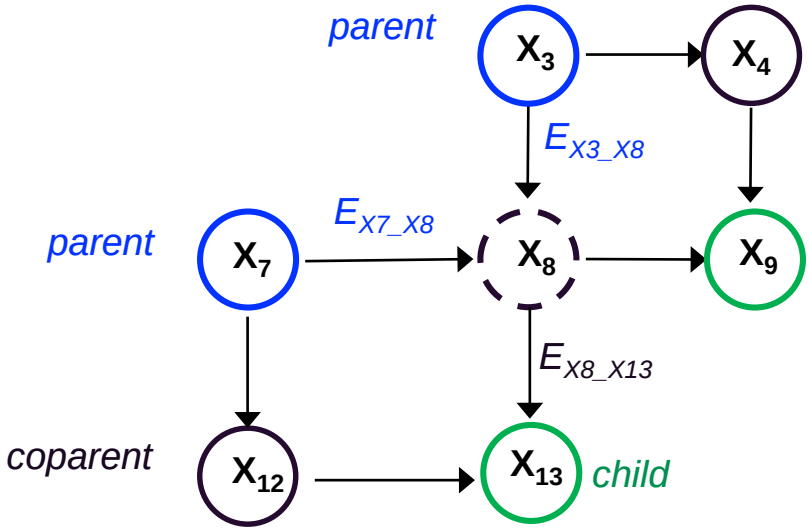




- Prioritize threats and security implementations via decision tool.
- Perform trades on effectiveness, ease, and "cost" parameters.
- Narrow down threat and security implementation spaces.

Execute
– Develop Relational State Rules





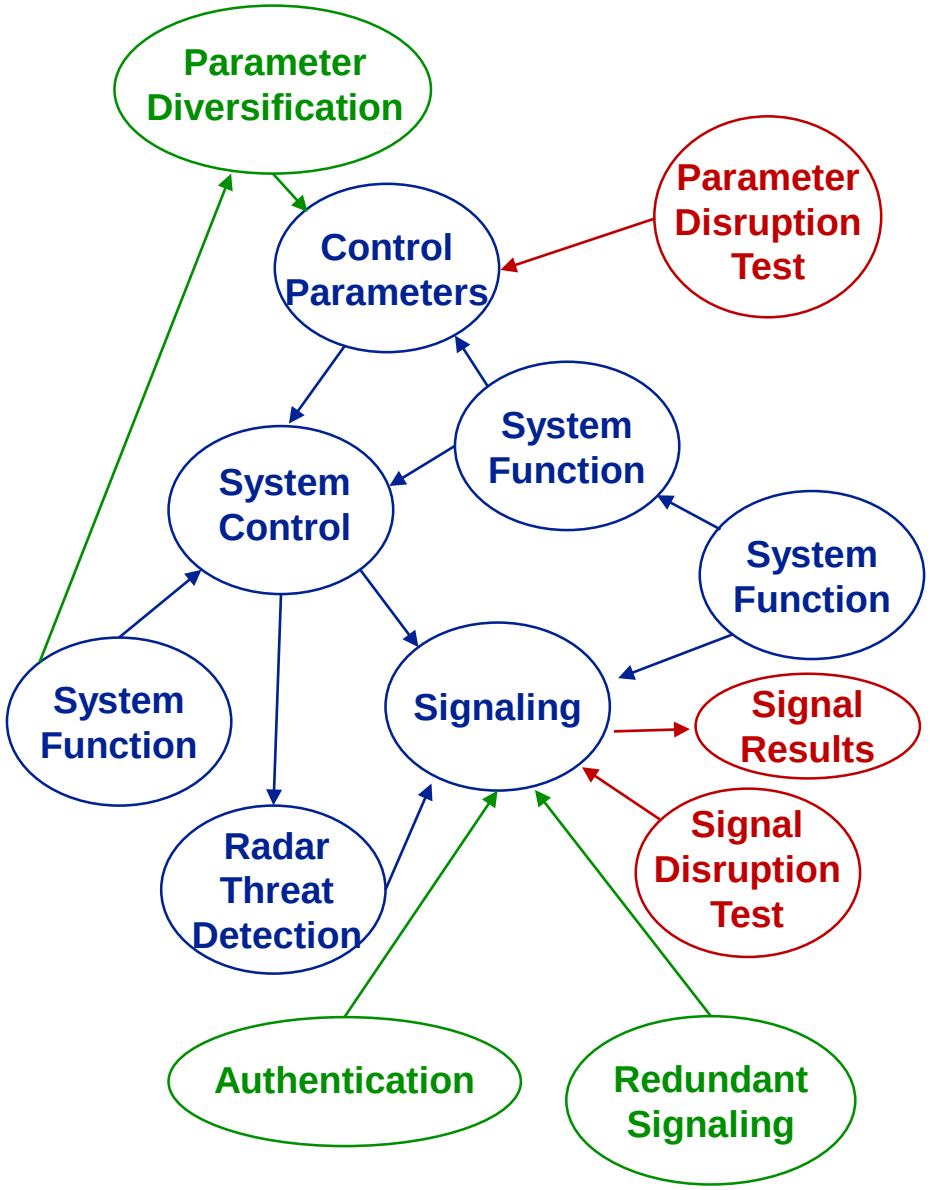
$$\text{State of Functional Capability or Asset } X_8(t_i) = f\left\{\begin{array}{l}\text{node\_self\_class } (X_8),\\ \text{node\_parent\_class } (X_3, X_7),\\ \text{node\_child\_class } (X_9, X_{13})\end{array}, \begin{array}{l}E_{X3\_X8}(t_i, X_3(t_i)),\\ E_{X7\_X8}(t_i, X_7(t_i))\end{array}\right\}$$

$$\text{State of Edge}_{X8\_X13}(t_i) = g\left\{\begin{array}{l}\text{node\_self\_class } (X_8),\\ \text{node\_coparent\_class } (X_{12}),\\ \text{node\_child\_class } (X_{13})\end{array}, \begin{array}{l}\text{State of Functional}\\ \text{Capability or}\\ \text{Asset } X_8(t_i)\end{array}\right\}$$

Where to End?

– Test an executable functional ecosystem model

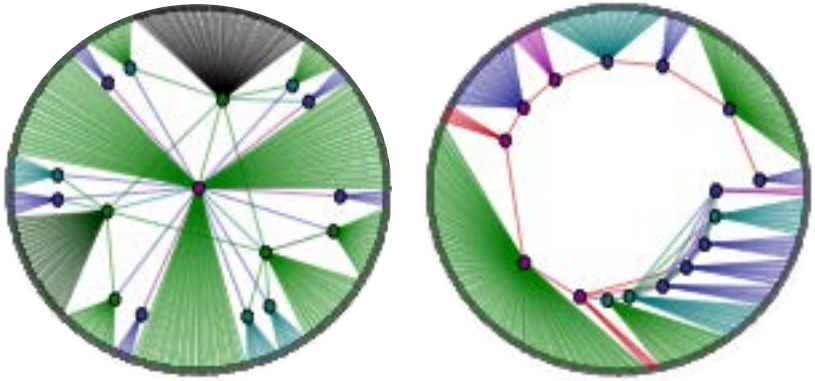
- **Extract system functional information**
- **Extract relationships between threat vectors and functional assets**
- **Extract a semantic mapping of Blue design patterns**
- **Create assurance test framework and patterns to:**
  - Evaluate system response to threat
  - Maintain explicit knowledge of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



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.



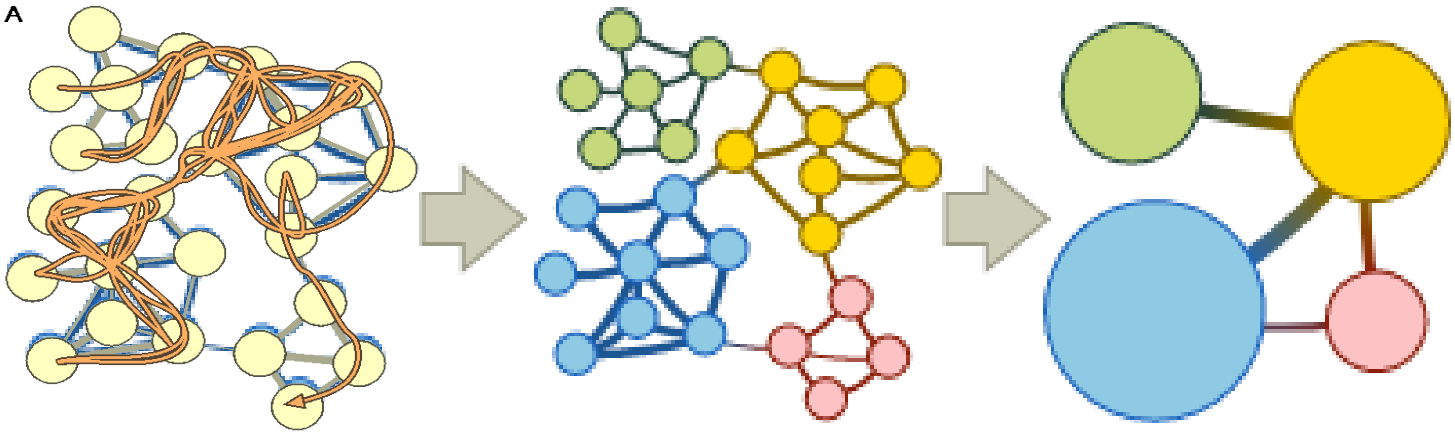


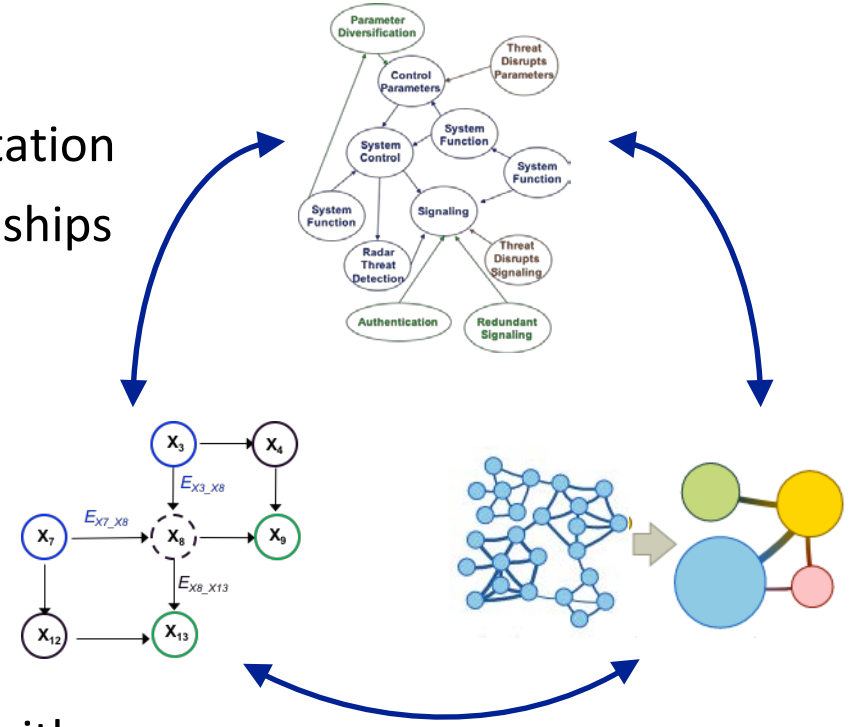
Image from Li (2005)

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

Elucidate Structure-Function relationships by discovery.

Research Challenges

- **What is different?**
  - —Deriving an ecosystem DiGraph
  - —Dynamically executing DiGraph representation
  - —Reveal hidden structure-function relationships via dynamic mapping



- **What are the main challenges?**
  - —Scalability
  - —Methodological rigor and consistency
  - —Repeatable methodology to provide SEs with otherwise hidden insights that result in more effective design decisions
  - —Extensibility of developed methods to a broad class of systems

Research Supports 2 Main premises

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)?"