CERIAS

The Center for Education and Research in Information Assurance and Security

Communications, information, and cybersecurity in Systems-of-Systems

Cesare Guariniello, Dr. Daniel DeLaurentis

School of Aeronautics and Astronautics, Purdue University

Overview

OBJECTIVE - Quantify impact of system interdependencies on the operability of System-of-Systems (SoS) under cyberattacks. Evaluate criticality of nodes and links, and robustness/resilience of SoS.

**Cyberattacks**

System-of-Systems

- Primary effects
- Secondary (internal) effects: disruption of services within the system under attack
- Tertiary (external) effects: cascading effects on the operability of other systems
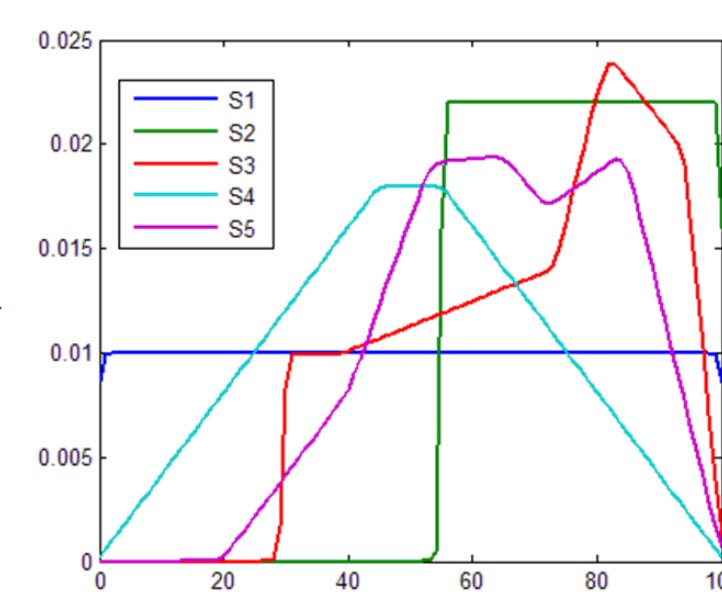
Operability in System-of-Systems

Functional Dependency Network Analysis (FDNA): Method to analyze and quantify interdependencies and cascading effects of disruptions on operability through networks of systems.
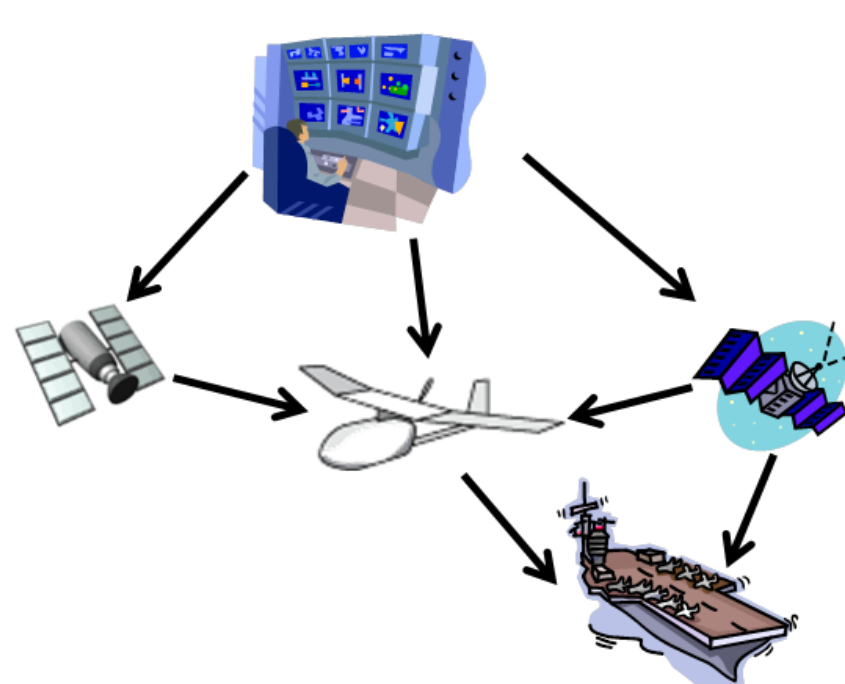
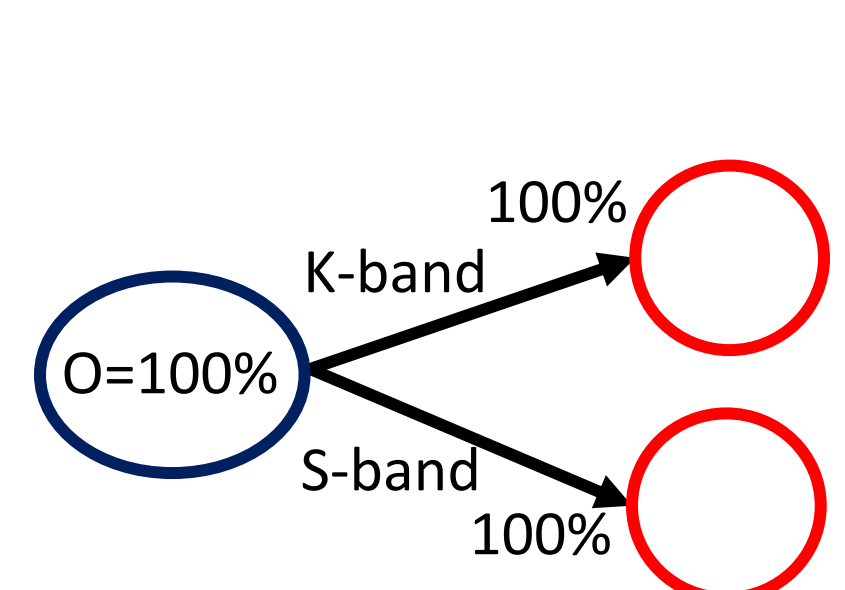Functional Dependency in a System-of-Systems
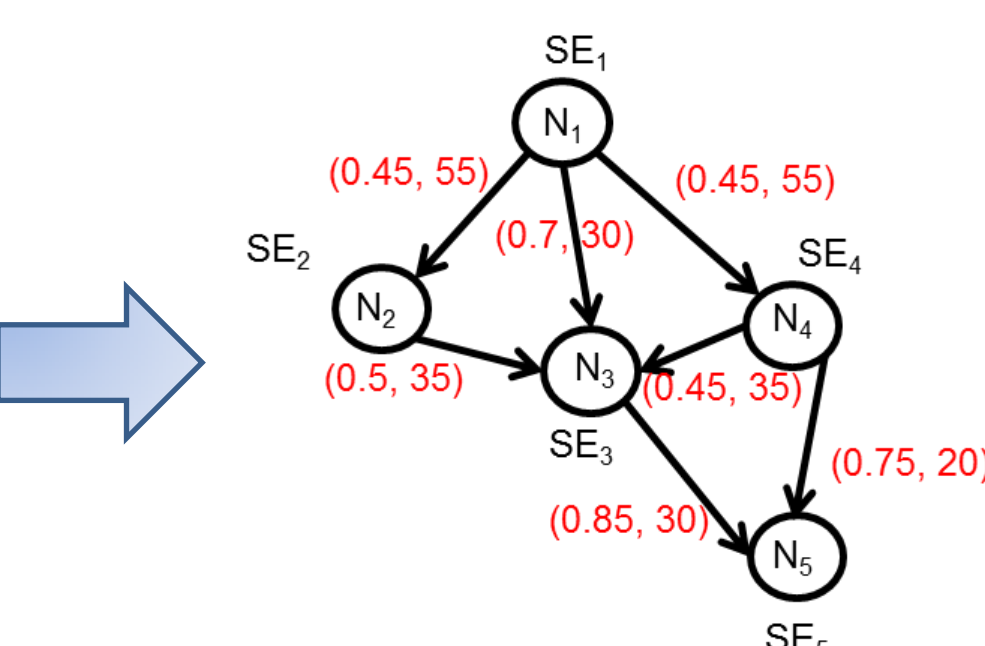
FDNA representation: operability depends on internal status (Self-Effectiveness SE), and Strength and Criticality of Dependency
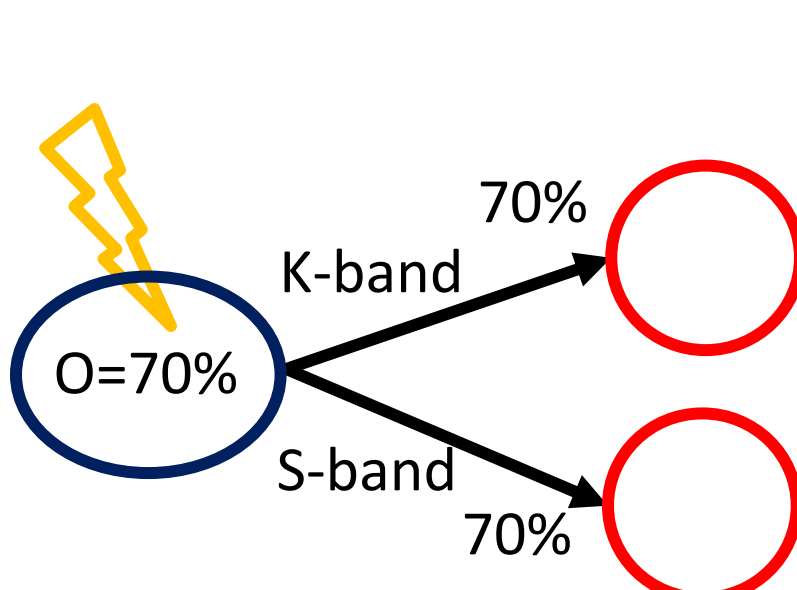
Effects of attack on 2 systems

Secondary and tertiary effects of attacks

O=100%, K-band 100%, S-band 100%

Relevant system has full operability. Dependent systems receive all the required input

O=70%, K-band 70%, S-band 70%

Relevant system has reduced operability due to attacks (secondary effects). Dependent systems are affected the reduced operability (tertiary effects)

O=100%, K-band 50%, S-band 100%
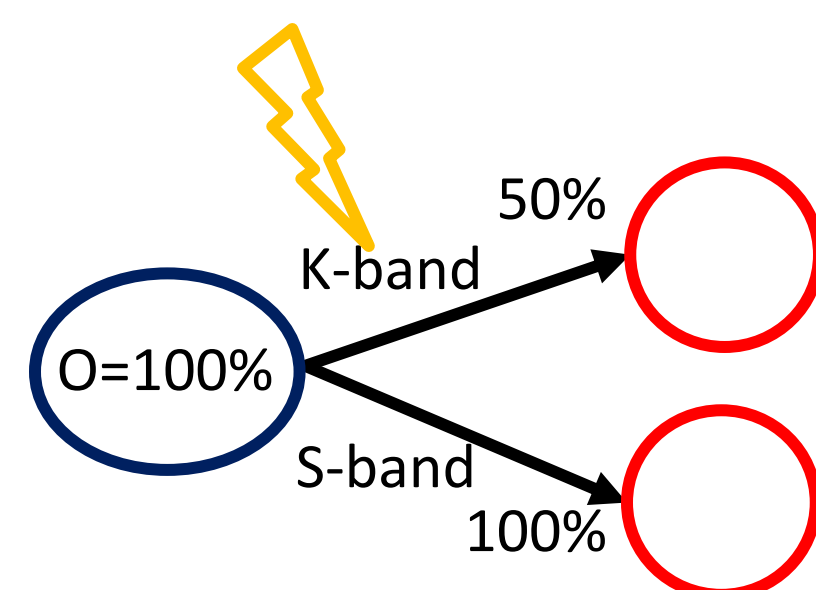
Relevant system has full operability. Due to attacks on a communication band, one dependent system "sees" reduced operability (tertiary effects)
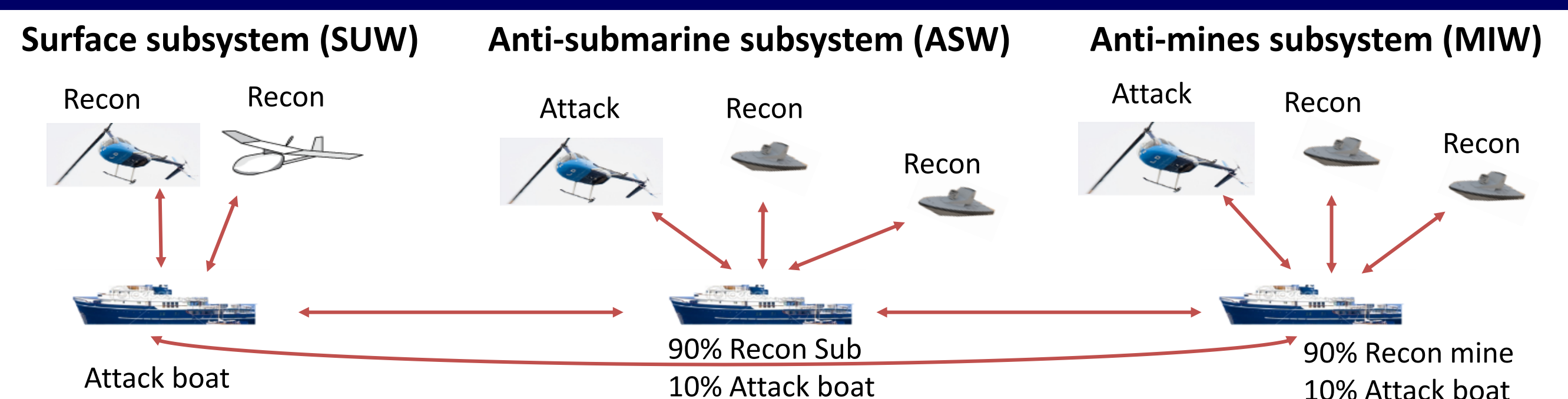
Critical nodes and links
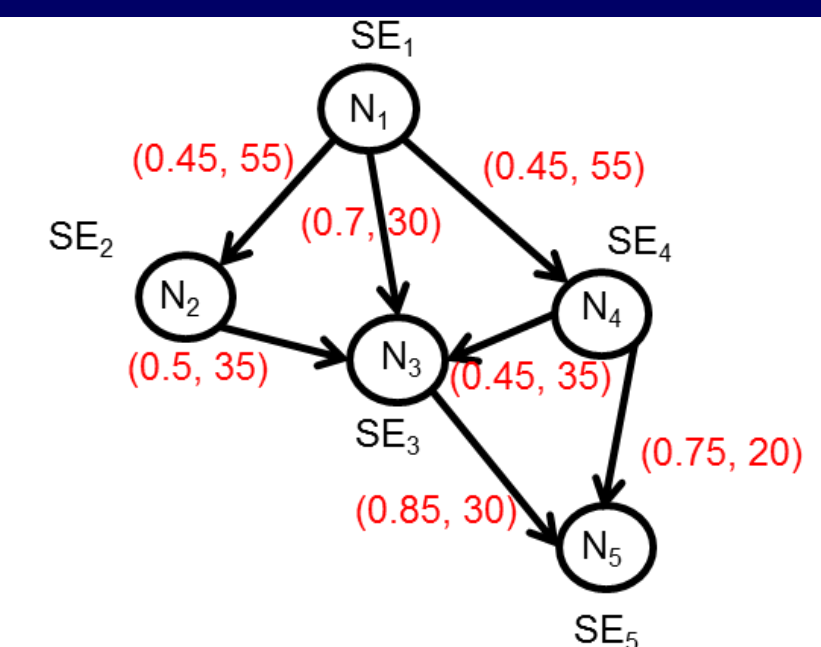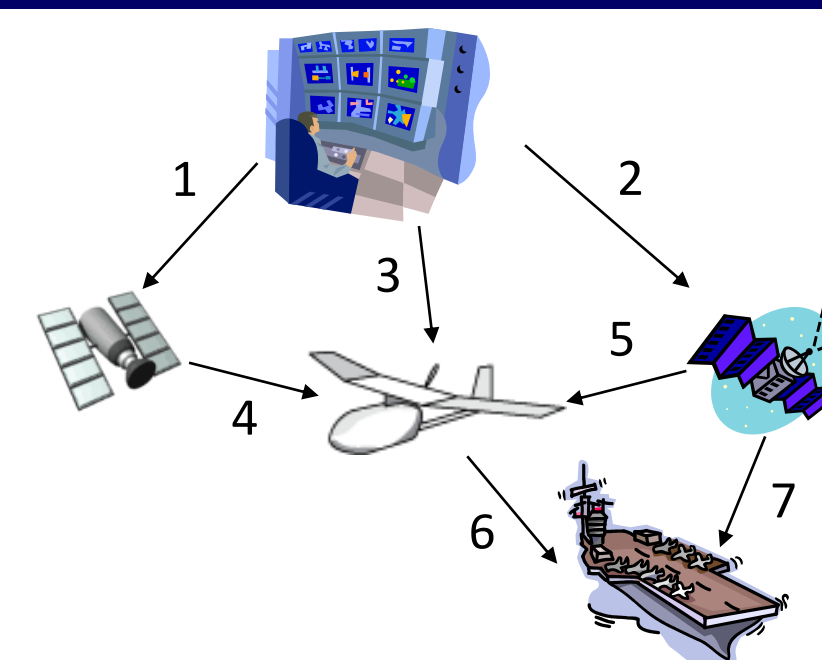
Disrupted node (25% operability)	Variation in the operability of the carrier
1	-31.68%
2	-2.92%
3	-14.34%
4	-21.25%
5	-15%

Disrupted link (successor receives 25% operability)	Variation in the operability of the carrier
1	-2.39%
2	-19.13%
3	-14.81%
4	-17%
5	-17%
6	-45%
7	-55%

Naval Warfare Scenario SoS

Surface subsystem (SUW) — Recon, Recon, Attack boat

Anti-submarine subsystem (ASW) — Attack, Recon, Recon, 90% Recon Sub, 10% Attack boat

Anti-mines subsystem (MIW) — Attack, Recon, Recon, 90% Recon mine, 10% Attack boat

Three different architectures (A, B, and C), characterized by different time of deployment of the constituent systems, and different flexibility (systems can perform various tasks, replacing each other if needed, and serve as communication relays)

Robustness (capability to maintain high operability following disruption at time step 75)

Resilience (capability to recover operability, at least partially, following disruption at time step 75)
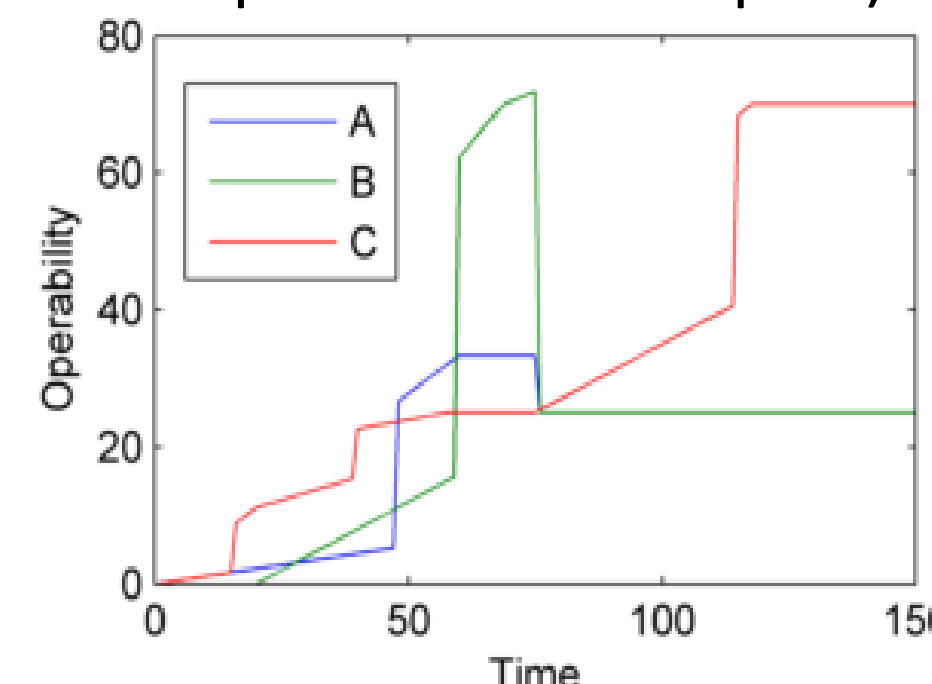
Operability: engage enemy mines. Disruption: loss of MIW helicopter link
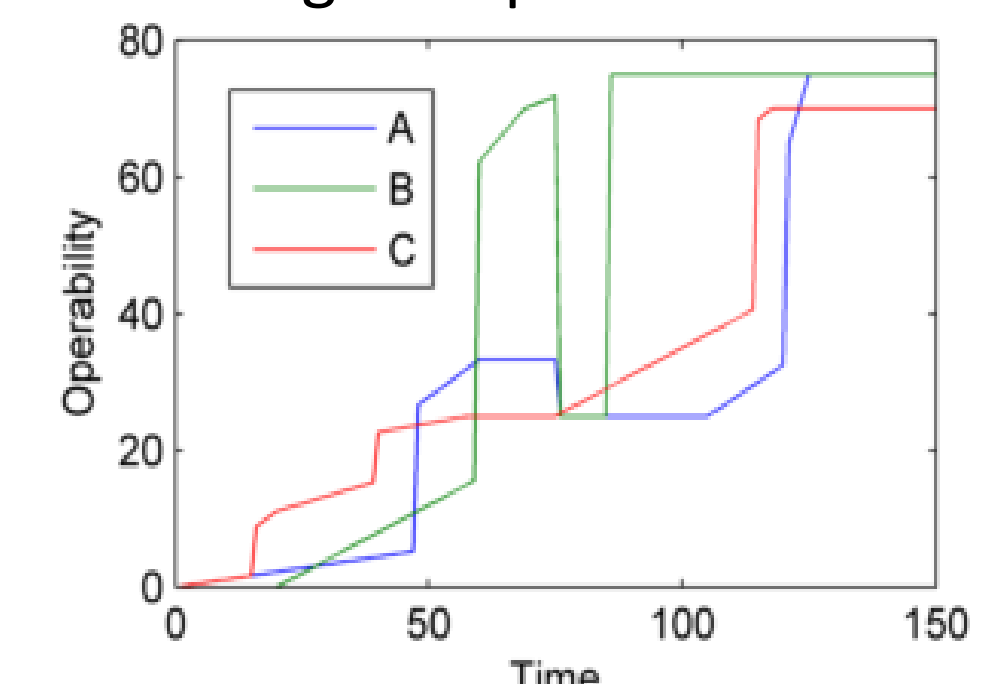
Future: synthesis of SoS architectures

OBJECTIVE – Combine FDNA with development schedule (another method, dealing with schedule, is being developed in this research). Use the resulting metrics and evaluation of features of the SoS to design and architect better SoS in terms of flexibility, robustness, resilience

Contact and references

PURDUE UNIVERSITY