SAND2022-8731C

32nd Annual INCOSE international symposium
hybrid event
Detroit, MI, USA
June 25 - 30, 2022

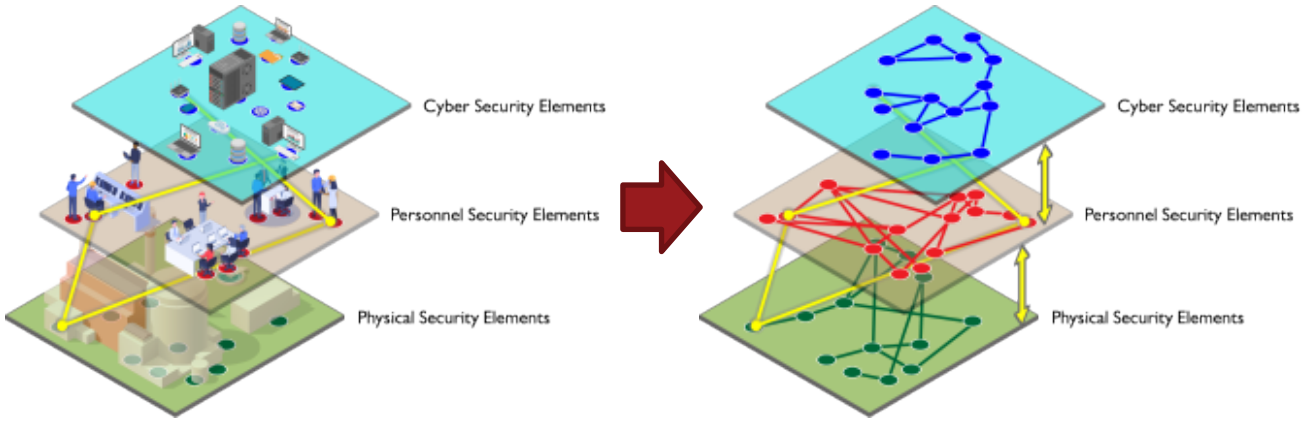
Multilayer Network Models for Coordinating Orchestration of Systems Security Engineering

Adam D. Williams, Gabriel C. Birch, Susan A. Caskey, Elizabeth S. Fleming, Thushara Gunda, Jamie Wingo, & Thomas Adams
Sandia National Laboratories

www.incose.org/symp2022

Outline

- Introduction
- Security Orchestration in FuSE
- Multilayer Networks → Security Orchestration
- Demonstration → Lone Pine Nuclear Power Plant
- Insights & Implications

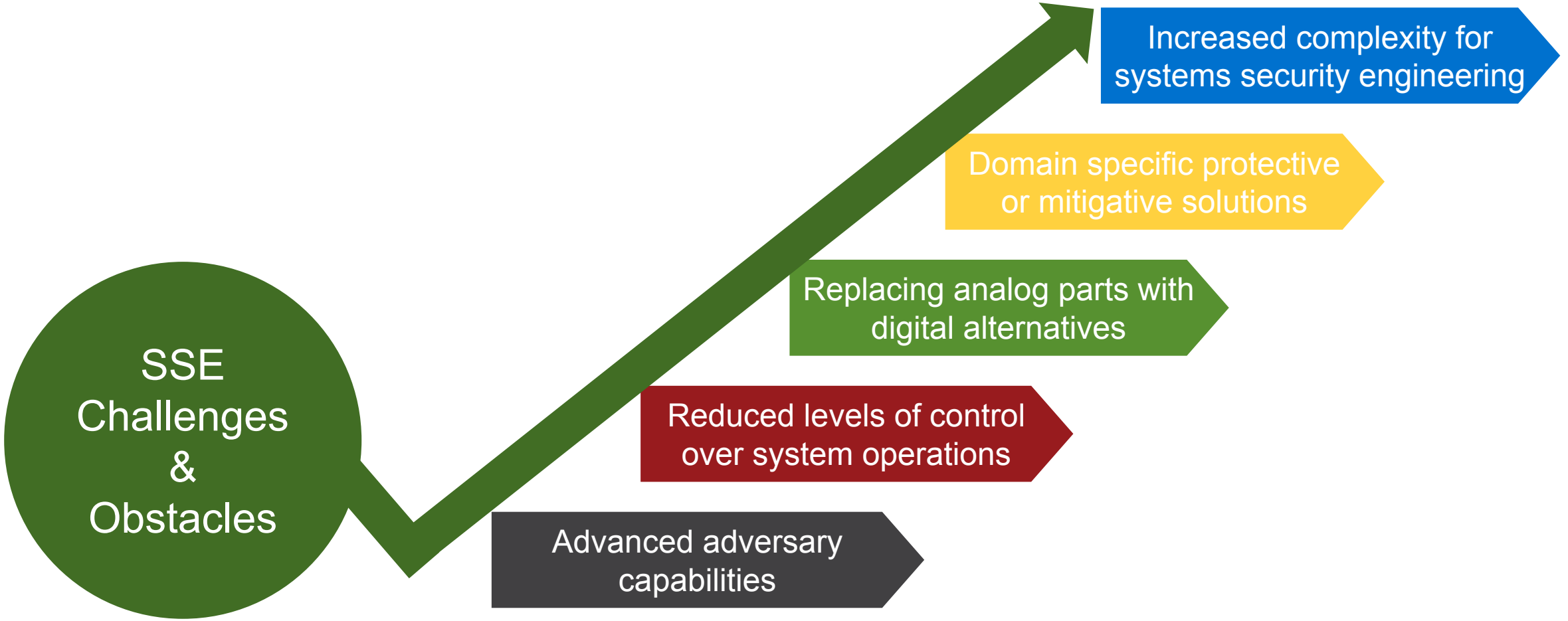


Introduction

Part of the challenge [in systems security engineering] is the lack of a system science discipline within which to ***integrate a system security science***...Security is predominantly a heuristic practice where we encase that which works in some attempt at engineering for repeatability and consistency...[yet] ***developing the science of system security and security engineering is preferable*** over doing more of the same harder (heuristics).

(Willet 2020, 5)

Introduction



Introduction

Socio-cyber-physical paradigm

Move beyond domain-specific solutions
to focus on engineering for *interactions*

Security coordination

Including between protective solutions
& with *non*-protective (sub)systems

Multi-domain approaches

Dynamic decisions & operations
for relevant & adaptable system defense

Multilayer network models

Demonstrated approach that helps
capture interactions & coordination

From reactive → proactive

Aligning security functions with
real-world complexities & interactions

Introduction

Socio-cyber-physical paradigm

Move beyond domain-specific solutions
to focus on engineering for *interactions*

Security coordination

Including between protective solutions
& with *non*-protective (sub)systems

Multi-domain approaches

Dynamic decisions & operations
for relevant & adaptable system defense

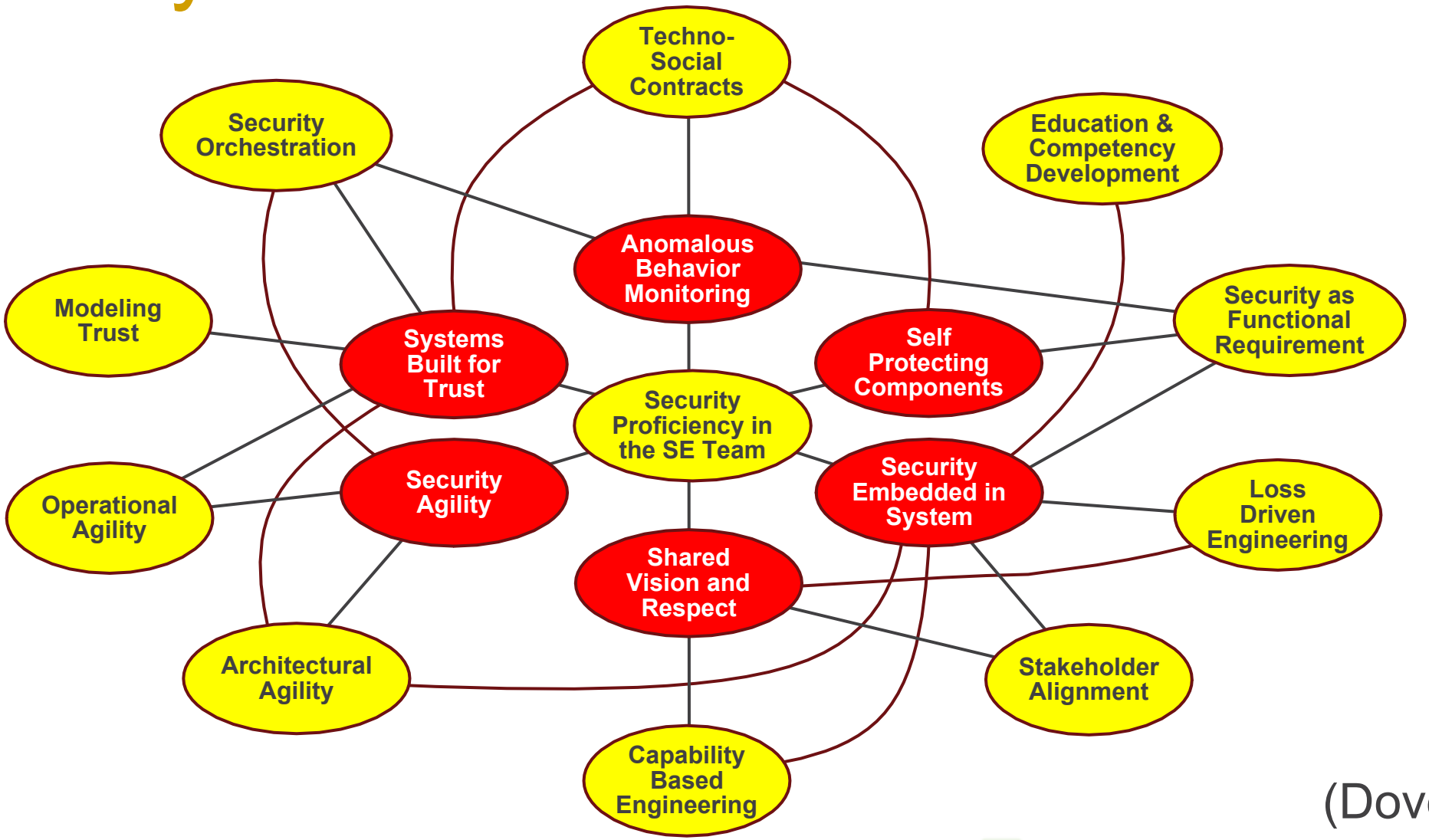
Multilayer network models

Demonstrated approach that helps
capture interactions & coordination

From reactive → proactive

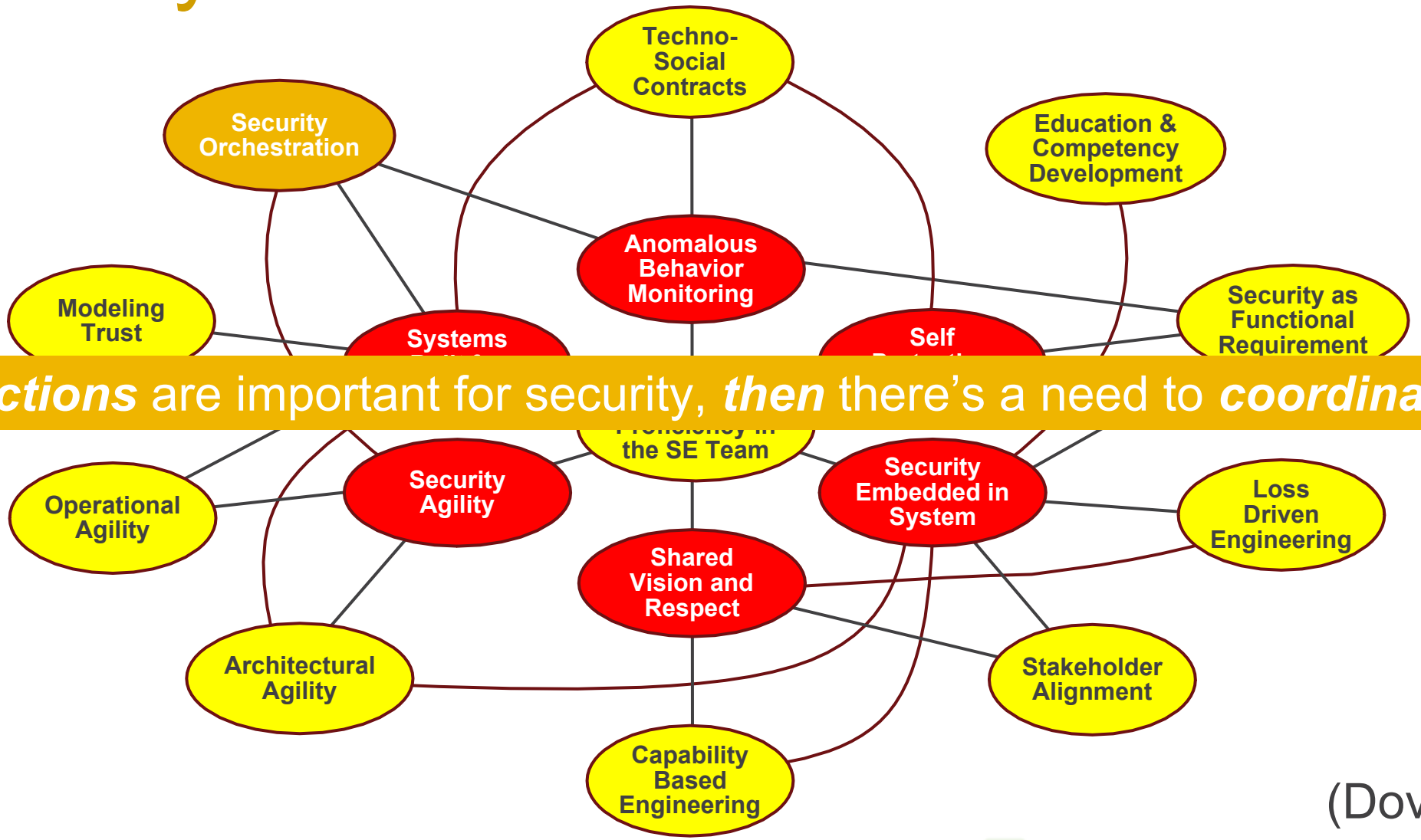
Aligning security functions with
real-world complexities & interactions

Security Orchestration: FuSE



(Dove, et. al 2021)

Security Orchestration: FuSE



If interactions are important for security, ***then*** there's a need to ***coordinate them***!

(Dove, et. al 2021)

Security Orchestration

Category	Architectural Premises for the Future of Systems Security Engineering
Foundational	• *integrate system security & cybersecurity engineering (mutually influential) ** • *context matters → context-aware systems with flexible human interfaces**
Strategic Framing	• security is an infinite game of continual adaptation to retain/regain the advantage • international coalitions for governance & adjudication to influence standards • avoid one-size-fits-all & create options with varying principles & risk tolerance • cybersecurity is (likely) the primary national security risk for many countries • *successful security & cybersecurity depend on successful national coordination** • hedge digital failures with analog alternatives → reduce risk in a digital world • *system value determines levels of resistance & resilience in the design** • avoid Gordian knots of liability by framing structure & accountability in design
Tactical Framing	• security is a functional requirement for engineered systems • the science of system security & security engineering is preferable to heuristics • *all technology is not equal & equality today's relationships may change** • adaptability ("to fix") & expendability ("to fry") are key to complex systems • compositional security, where readily available modules are less prone to error • *encoding axiomatic principles to facilitate non-deterministic systems action** • *automated logic in compositional security to resolve views across contexts*** • *design principles include varying (in)dependence in systems security*** • adaptively identify & encode early indicators as part of system design • context driven dependencies & constraints force prioritizing security principles
	*Premises determined to influence the context for security orchestration **Premises specifically identified by Willett (2020) for "security orchestration"

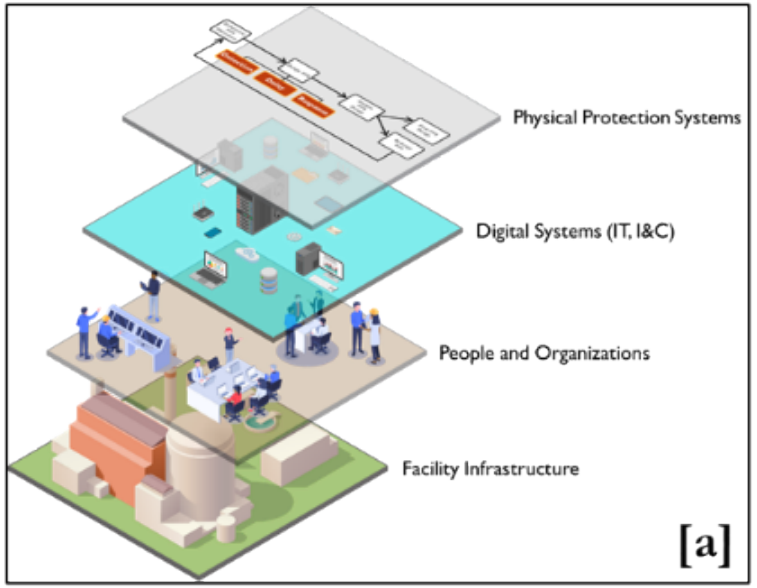
Security Orchestration: Definition

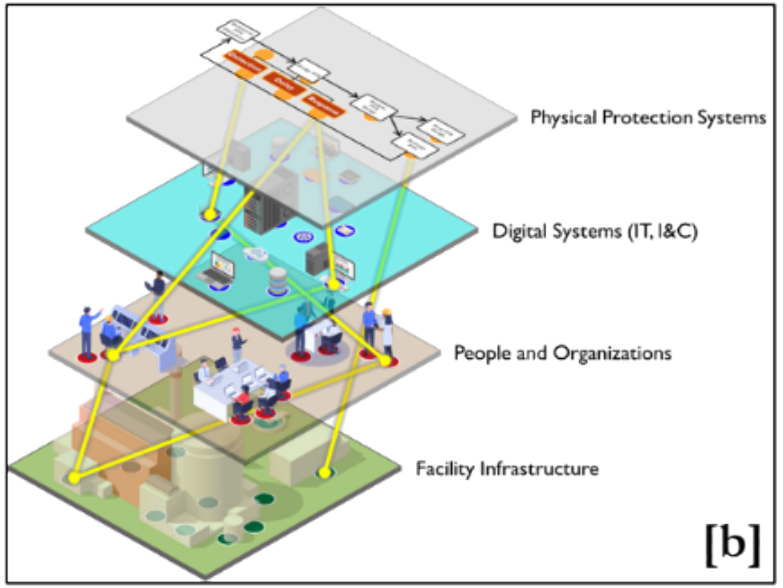
Category	Architectural Premises for the Future of Systems Security Engineering
Foundational	• *integrate system security & cybersecurity engineering (mutually influential) **
	& encode early indicators as part of system design
	driven dependencies & constraints force prioritizing security principles
	*Premises determined to influence the context for security orchestration **Premises specifically identified by Willett (2020) for "security orchestration"

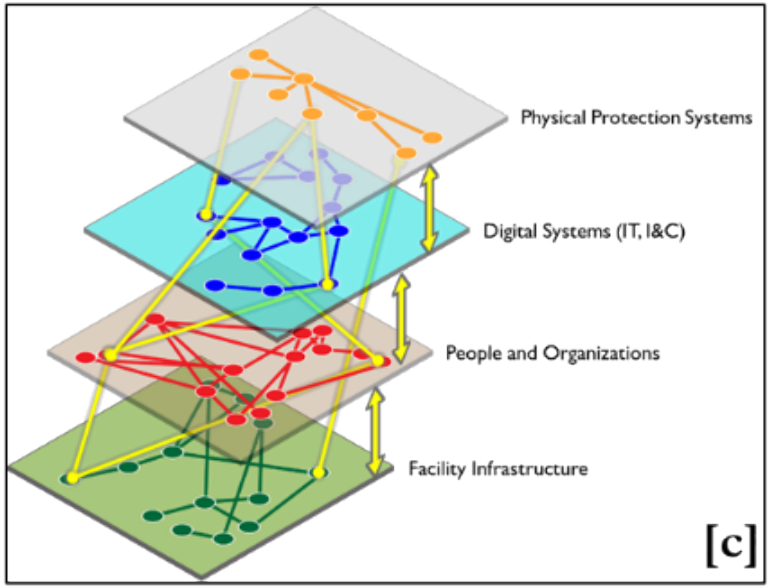
Security orchestration → "…***connecting disparate security*** technologies through standardized and automatable workflows ***that enables security*** teams to effectively carry out ***incident response*** and security ***operations***."

(Iyer 2019)

Security Orchestration: Multilayer Networks



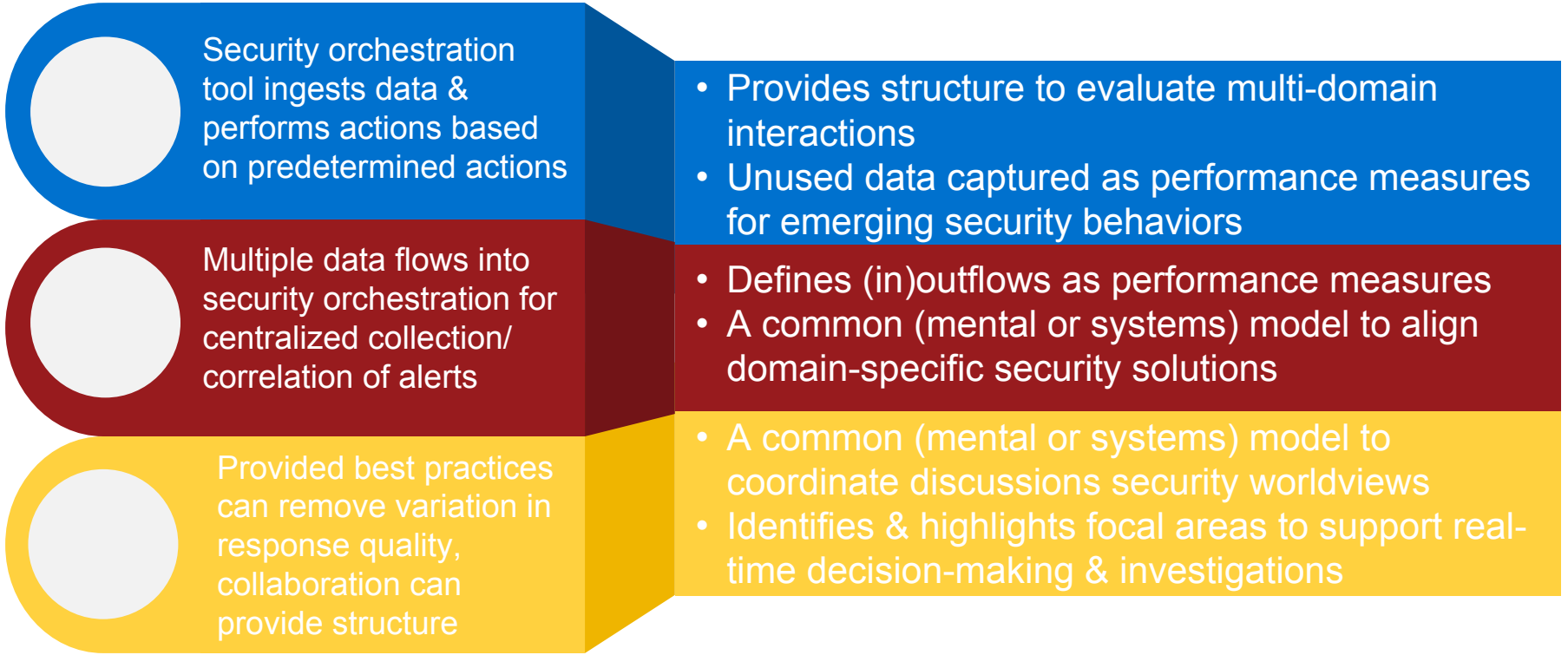




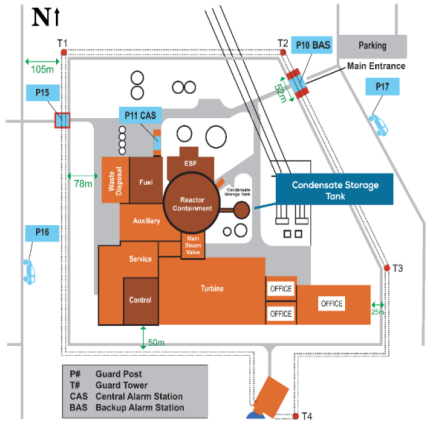
Security Orchestration: Multilayer Networks

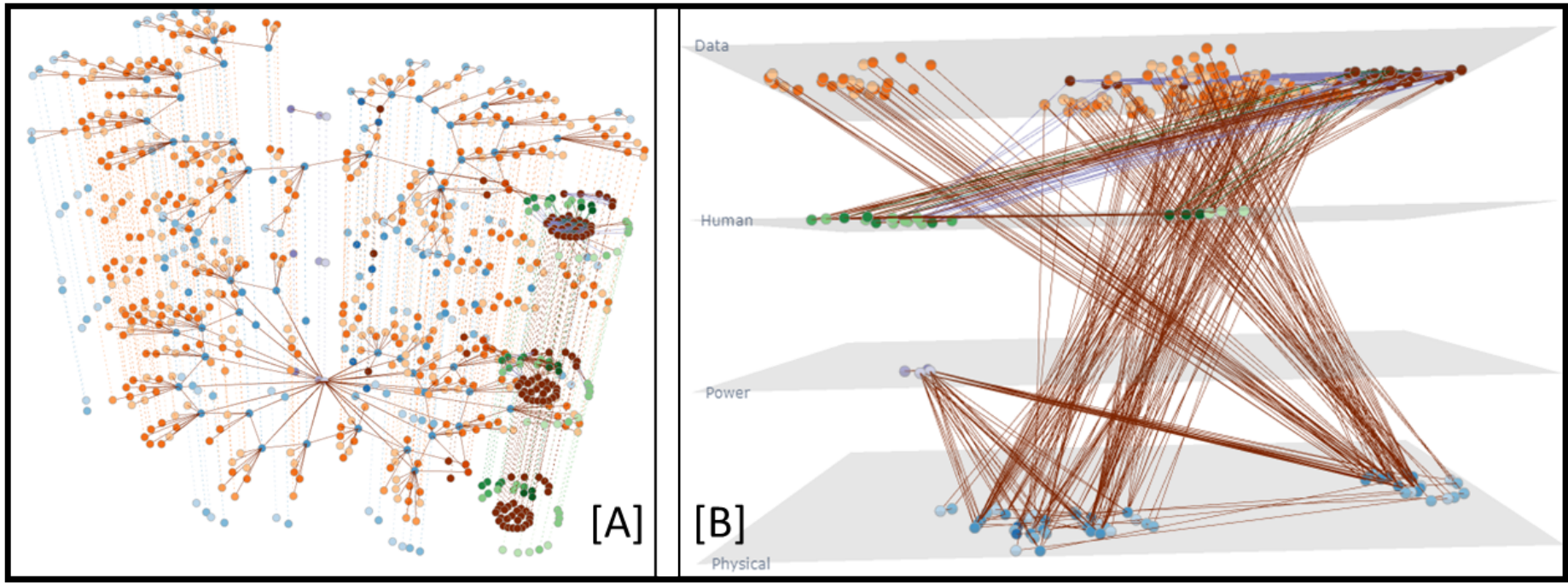
Multilayer Network models can help fill gaps identified by (Iyer, 2019)

1. A lot of data but little follow-up
2. Tools that don't talk to each other
3. People that don't talk to each other



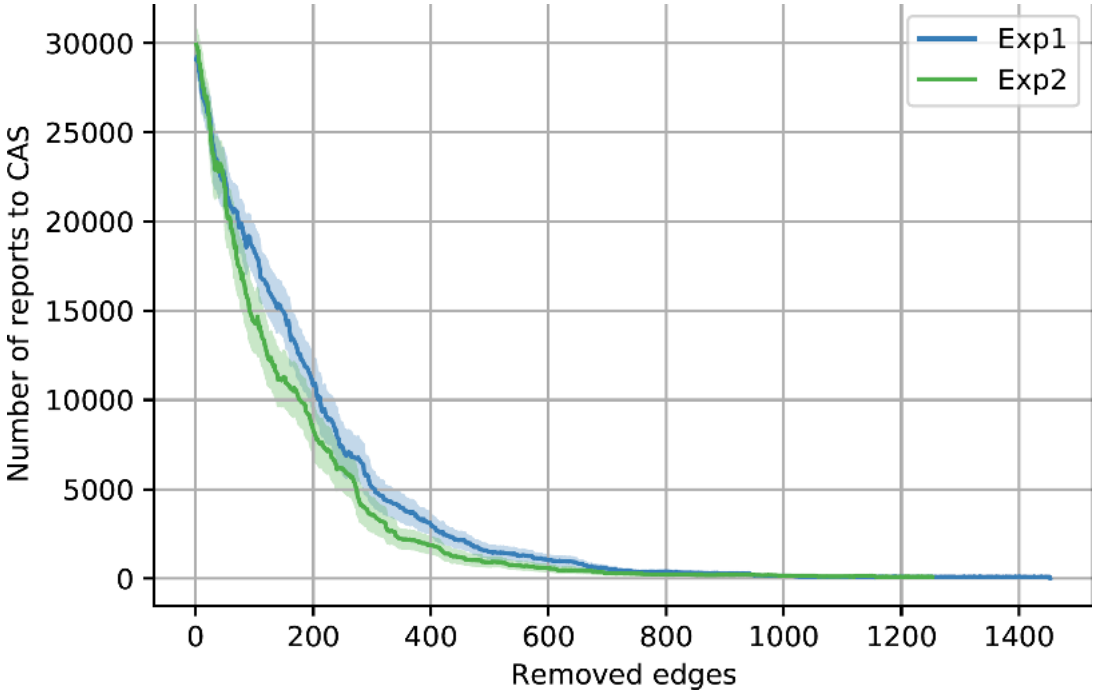
Security Orchestration: Demonstration





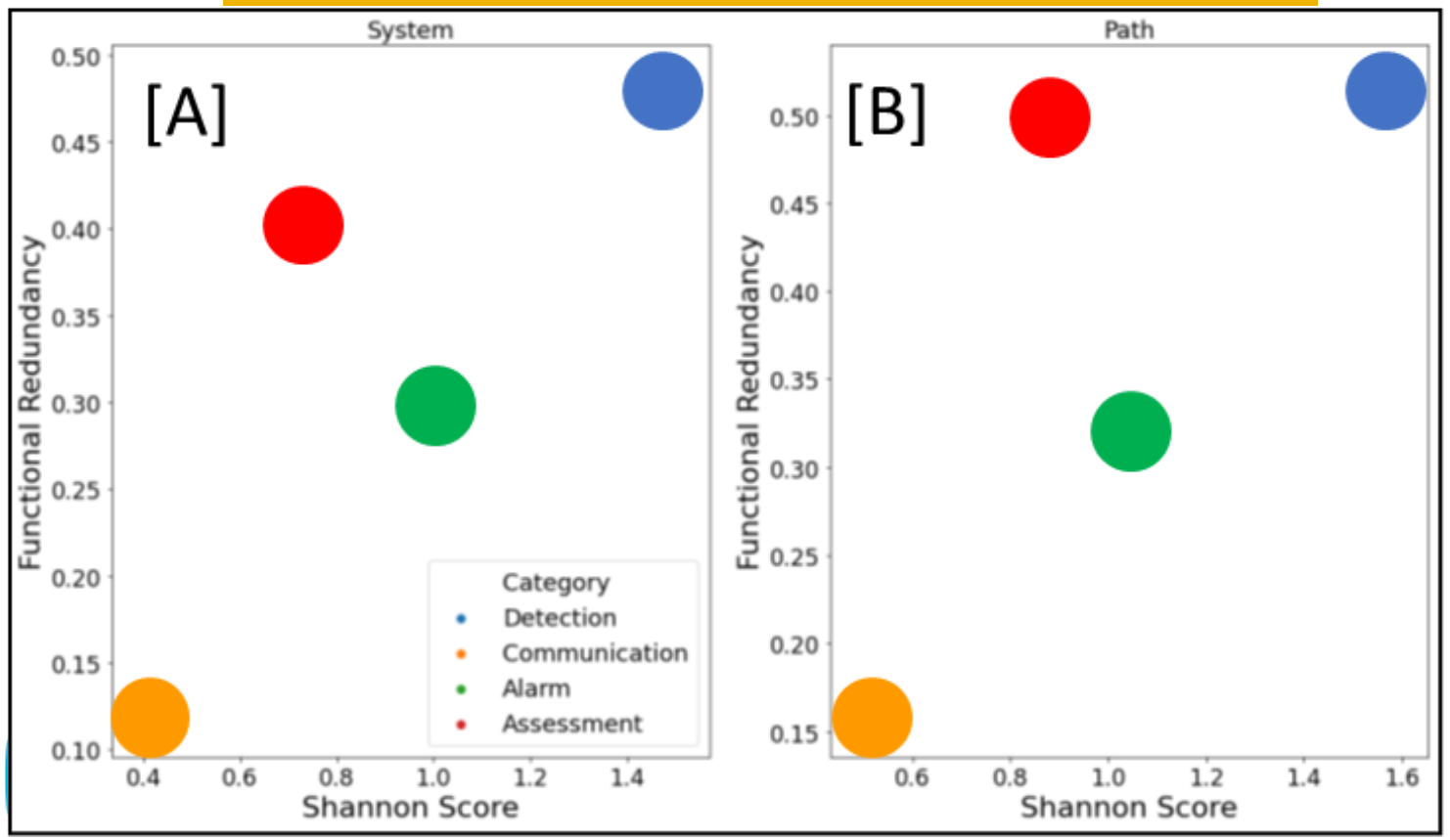
Security Orchestration: Demonstration

	Experimental Condition	Conclusions & Insights
Green	• Random node removal • *No communications rerouting* in the security system	• Complete communications failure follows power law behavior • Baseline for pushing curve up & right
Blue	• Random node removal • *Small communications rerouting* capability in the security system	• Complete communications failure follows power law behavior • Rerouting capabilities delays complete communications failure



Security Orchestration: Demonstration

Diversity → a desired SSE outcome to be orchestrated within the system



- Measures of diversity:
  - Shannon Index
  - Functional redundancy

- For the LPNPP:
  - *Shannon Index (SI)*: ratio of passive infrared sensors among the total number of different detection sensors
  - *Functional redundancy (FR)*: detection can be achieved by technical sensors, digital pattern tracing, or human observation

- SI vs FR plots for LPNPP
  - High FR, low SI → high variance in detection, but limited variance for assessment
  - Design goal: improve variance in assessment (higher & to the right)

Insights & Implications

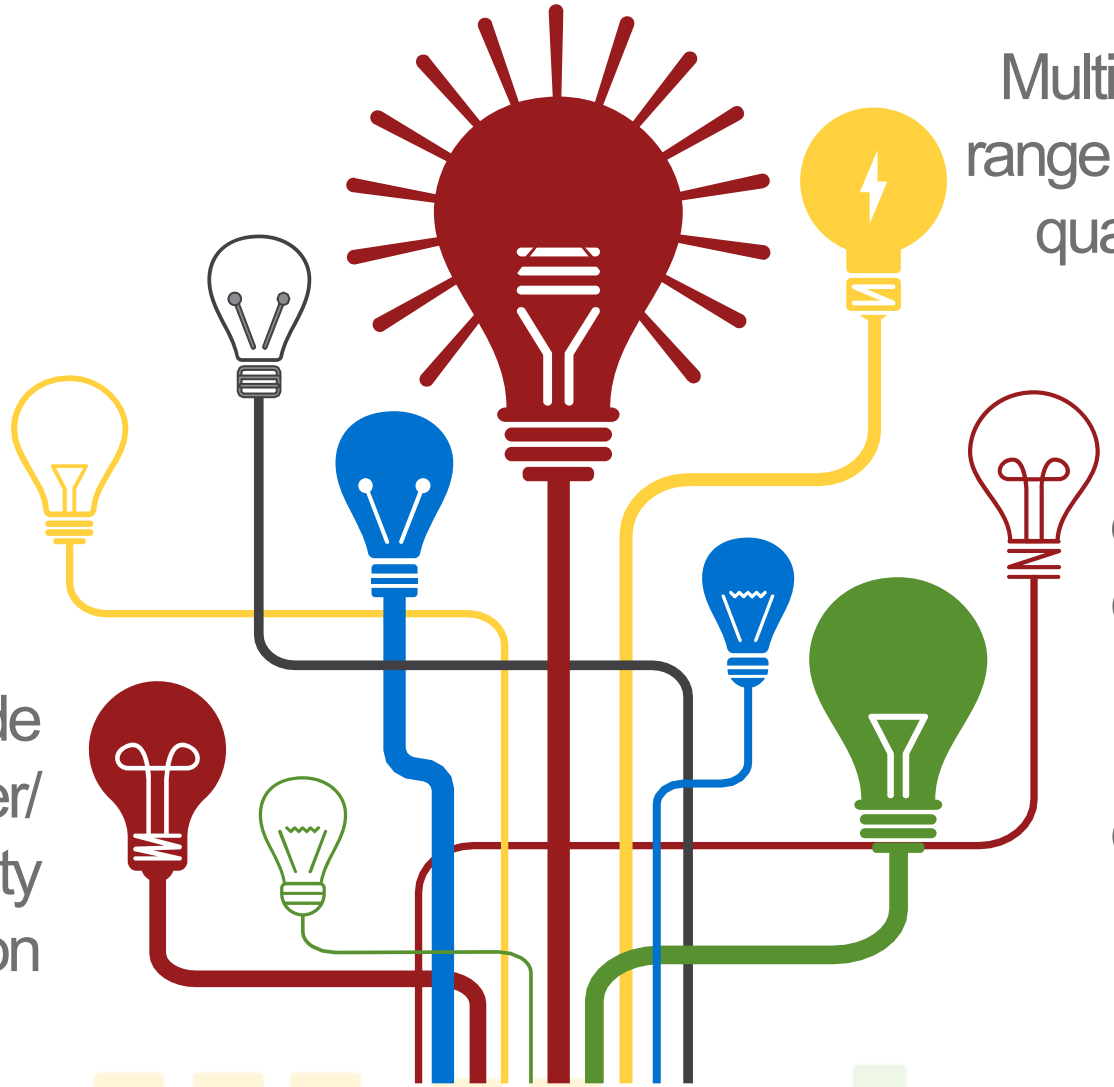
Category	Premises for Future Systems Security Engineering: Security Orchestration	Related Elements of Multilayer Network Models for Systems Security
Foundational	• integrate system security & cybersecurity engineering (mutually influential)	• Common (mental/systems) model & cross-domain (intra-layer) measures
	• context matters → context-aware systems with flexible human interfaces	• Dynamic & topological multilayer network performance measures
Strategic Framing	• successful security & cybersecurity depend on successful national coordination	• Common (mental or systems) model of security & cross-domain (e.g., intra-layer) performance measures
	• system value determines levels of resistance & resilience in the design	• Dynamic/topological multilayer metrics → emergent behaviors
Tactical Framing	• all technology is not equal & equality today's relationships may change	• Dynamic & topological multilayer network performance measures
	• encoding axiomatic principles to facilitate non-deterministic systems action	• Emergent behaviors via component selection & relationship definition
	• automated logic in compositional security to resolve views across contexts*	• Inter-/Intra-layer edge connections & related performance measures
	• design principles include varying (in)dependence in systems security*	• Cross-domain (e.g., intra-layer) performance measures

*Premises specifically identified by Willett (2020) for "security orchestration"

Insights & Implications

Multilayer networks → produce range of performance metrics → quantify security orchestration

Multilayer networks → identify cross-domain connections → optimize security orchestration



Maturity of security orchestration → needs to capture humans, cyber & non-linear ops environments → address real-world SSE complexities

Multilayer networks → provide framework to capture cyber/ digital elements → security orchestration

Questions?