34th Annual INCOSE international symposium

hybrid event

Dublin, Ireland
July 2 - 6, 2024

Session 2.2 Security

Building a Scientific Foundation for Security: Multilayer Network Model Insights for System Security Engineering

Security threats are not always what or who you expect…

Linda Davidson/The Washington Post/Getty Images

A REPORTER AT LARGE https://www.newyorker.com/magazine/2015/03/09/break-in-at-y-12

BREAK-IN AT Y-12

By Eric Schlosser

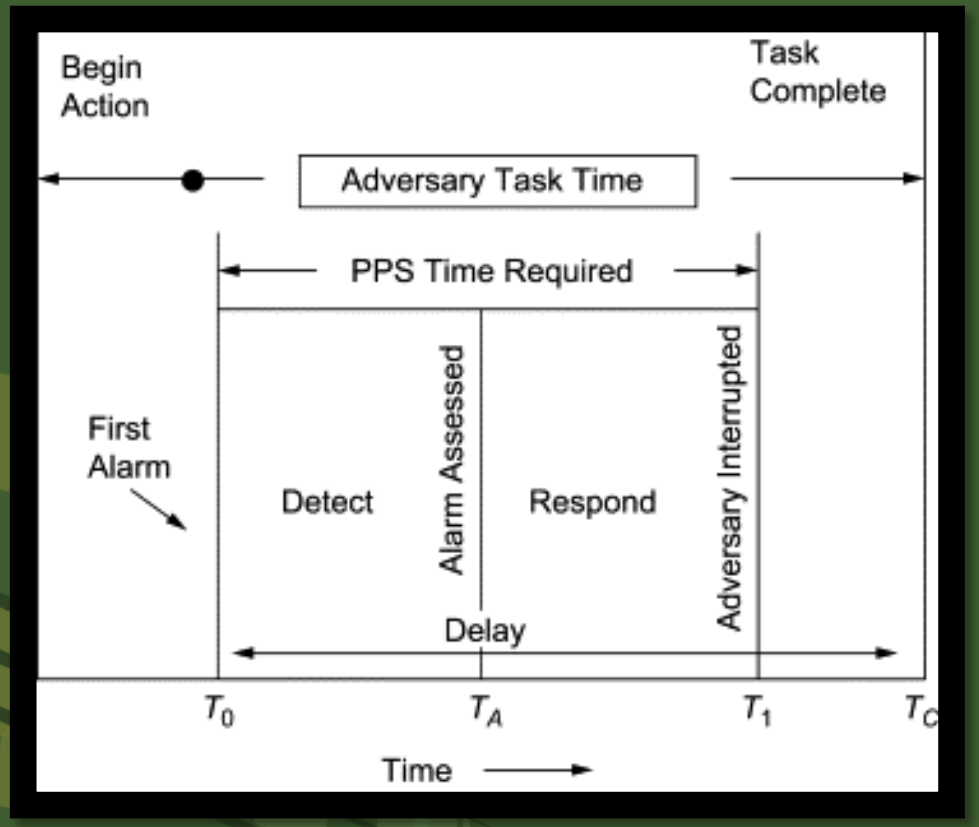
March 1, 2015

The Plowshares movement was inspired by Dorothy Day, a Greenwich Village bohemian who converted to Catholicism and urged resistance to all wars. In the Vietnam era, Philip Berrigan led actions to symbolically destroy the nuclear arsenal. Illustrations by Alex Williamson; Left to Right: Getty (Dorothy Day); Bettman / Corbis (Philip Berrigan and Protest March)

The Y-12 National Security Complex sits in a narrow valley, surrounded by wooded hills, in the city of Oak Ridge, Tennessee. Y-12 and Oak Ridge were

Traditional/Historical World View

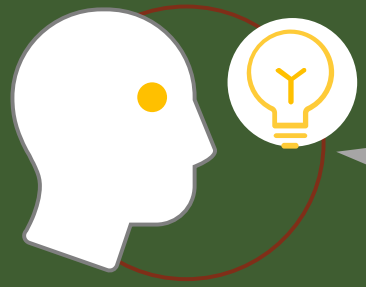
Security System Performance



(Smith & Brooks, 2013)

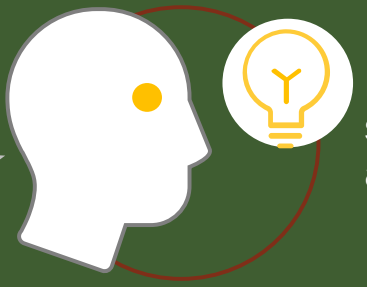
Time for a paradigm shift

Human-machine interactions for security expert



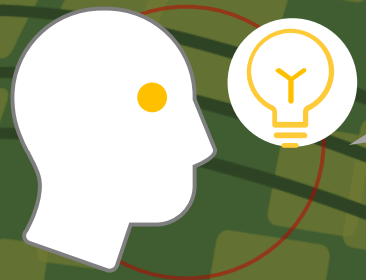
"Historically, [it is] likely [that we] had rich conversations about the [security assessment] framework and associated caveats and assumptions…[while] the framework has been passed on, ***the continuous improvement process has not been retained***"

"… a systematic view is needed that looks **beyond compliance** with the regulations, but also considers emergency response, cyber vulnerabilities, as well as safety and security issues."



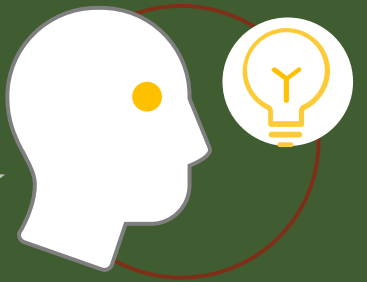
Evaluation of security assessments

Resilience frameworks and systems analysis expert



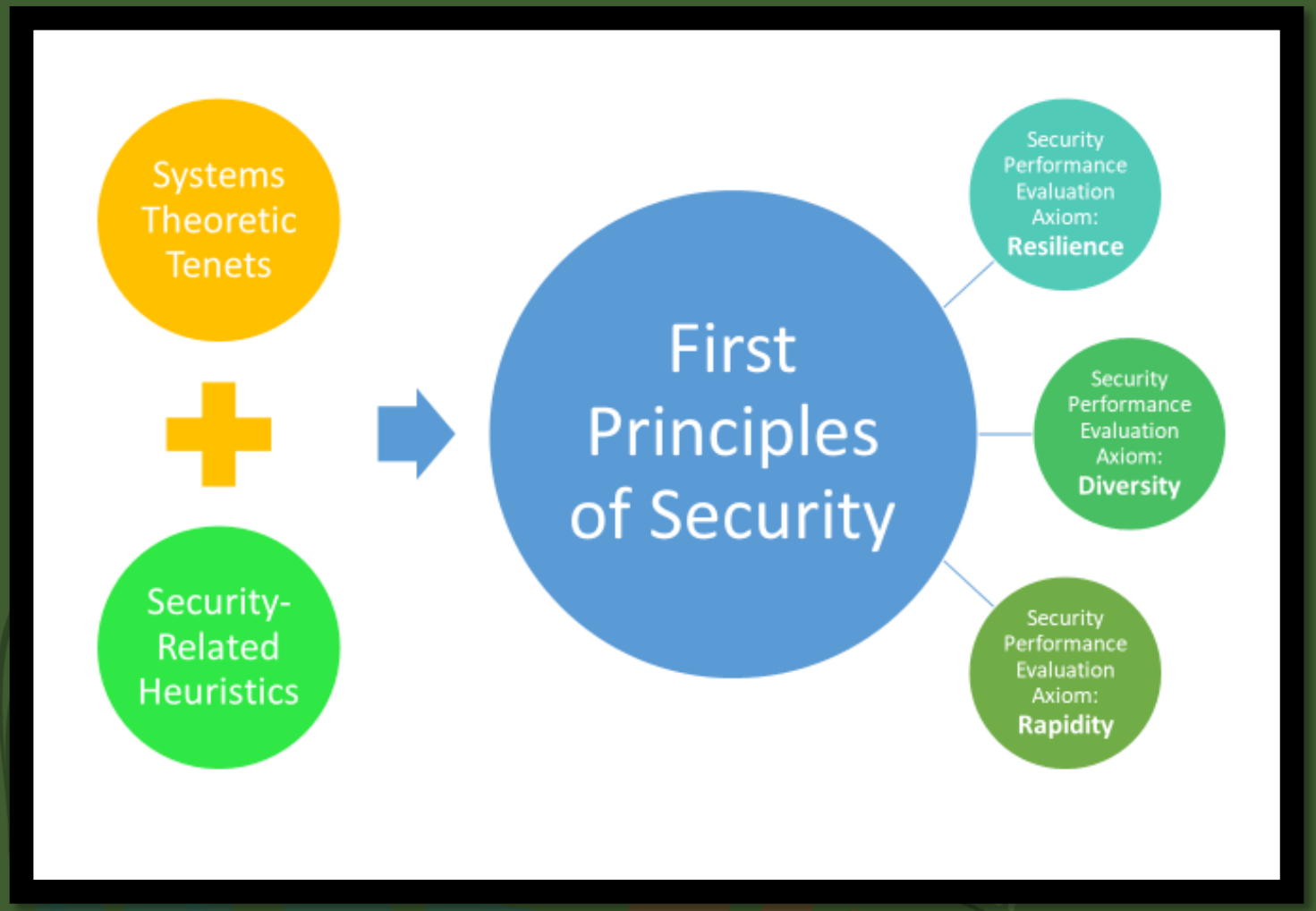
"…ensure that consequences are looked at **over time**: temporal disconnects between threats and consequences are **assessed dynamically**."

"We need to consider changing the end state from just stopping the bad guys to **include considering how they may be changing**…and **measure the overall system stability and flexibility**."



Systems safety and security analysis expert

Needed: a scientific foundation for security



A generalized description of science – based on established theory and principles that explain—and can be validated by—observation and experimentation

INCOSE's systems security engineering working group's world view

Trustworthiness

Systems security tends to have a singular focus on risk

A return to modeling trust as an evidentiary core aspect of system security

Loss-Driven

Systems security tends to focus on risk & too late in the development process

An approach to include security earlier in development & focus on preventing "loss"—not risk

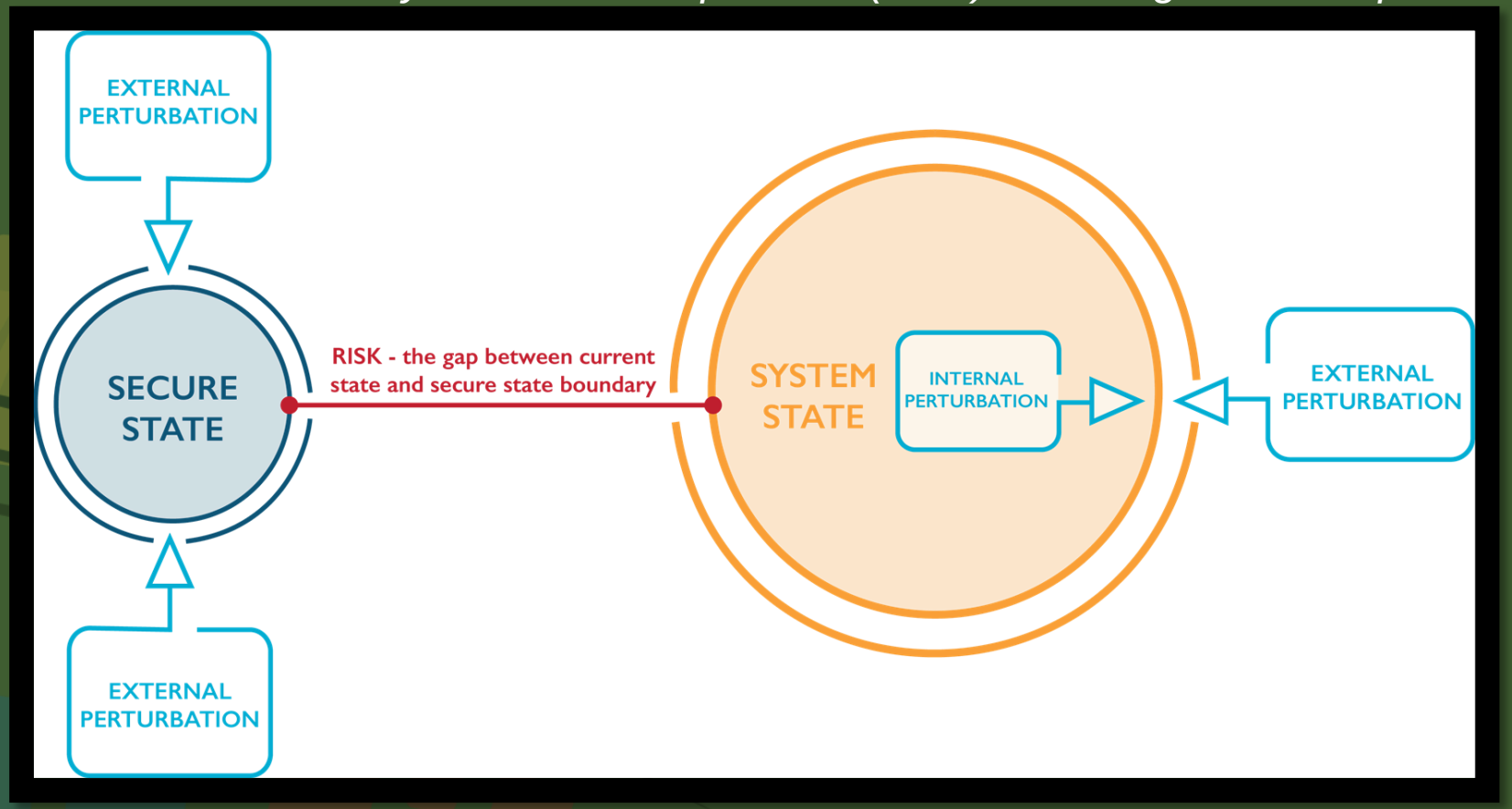
Capabilities-Based

Systems security too often starts with available solutions rather than desired results

A top-down paradigm that defines systems security in terms of desired results

A proposed definition for security risk

a failure to mitigate vulnerabilities that could intentionally be exploited to allow for the successful theft of or destruction of structures, systems, or components (SSC), resulting in unacceptable loss



(Caskey et al., 2021)

Security System Heuristics

Without resilience, security risk will grow

Without assessment and response there is no detection

Must have current data, information, and intelligence

Without detection, barriers are only a deterrence

Decision-making requires knowledge

No weak links

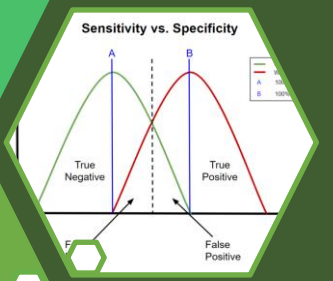
Must be consistent in time, space, and application

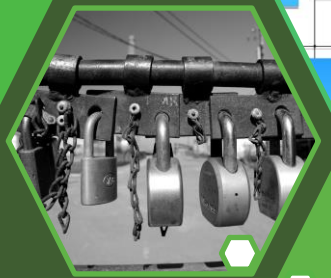
No ‘back doors’

Context is critical

Sociological basis specific to the organization

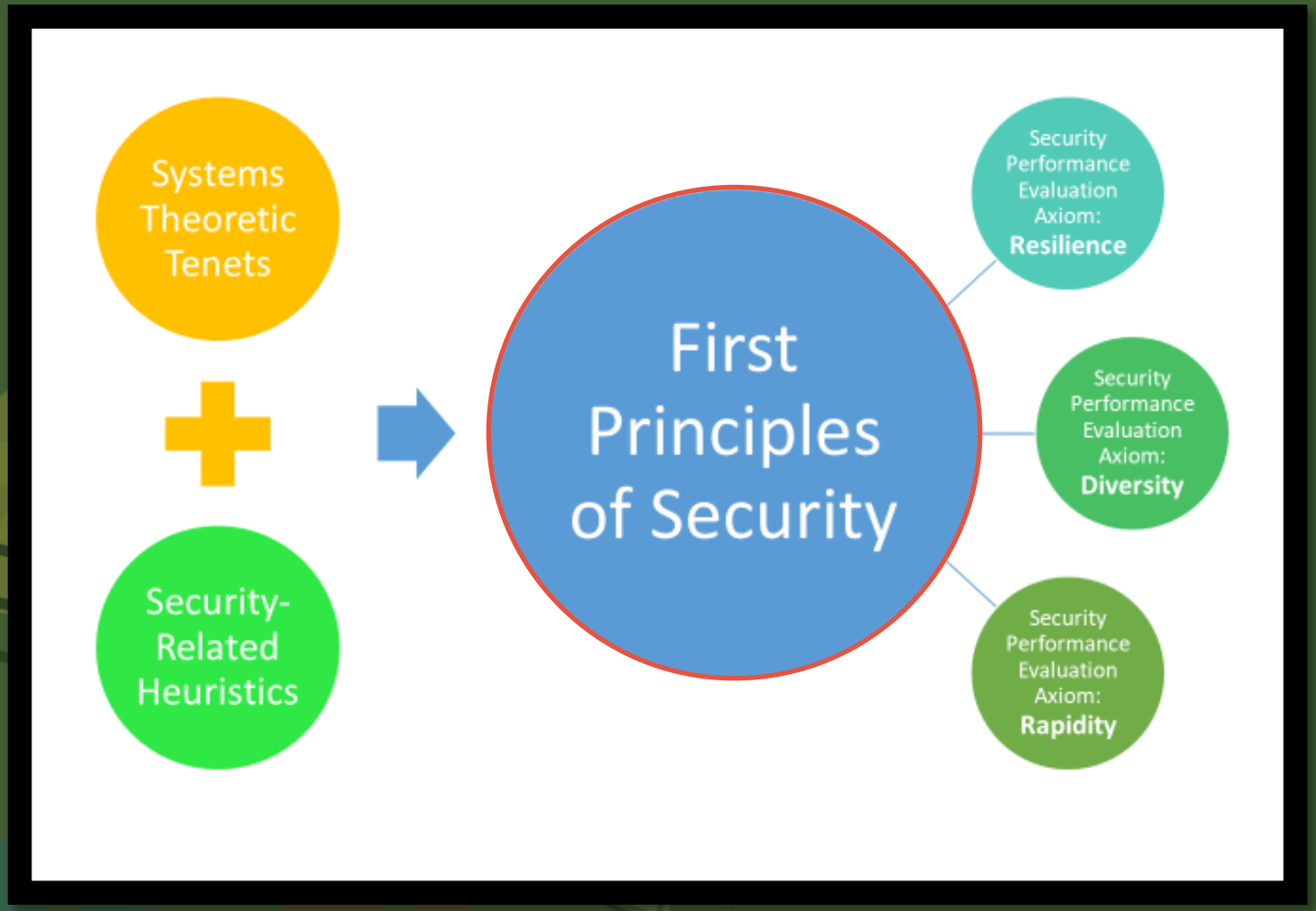
Support sufficient specificity





Designed with layers

Needed: a scientific foundation for security



Proposed 1st Principles of System Security

Detection

- Known or estimated specificity and sensitivity based on normal operations
- Be resilient to environmental and internal perturbation
- Evaluated within each layer of protection and across the entire system to decide if and where weaker detection elements or gaps may exist

Signaling

- Must be prompt, resilient, and provide clear information regarding time and space
- Evaluated within each layer of protection and across the entire system to determine if and where weak signaling or gaps may exist
- Confidence in data signals and detectors impacts the sensing and assessment, driving a need to know specificity and sensitivity over time and space

Assessment

- The assessment process must be resilient to internal and operator perturbations and provide rapid reporting

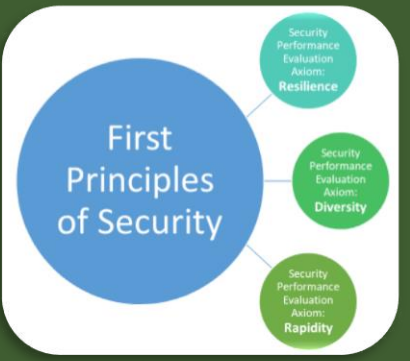
Response

- Systems security response is only effective with rapid and resilient communication and actions

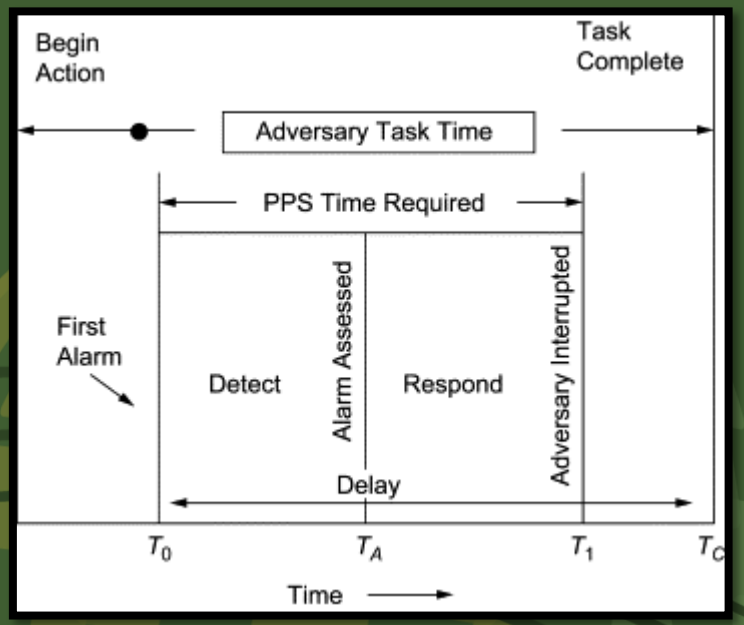
System

- System security must support rapid and resilient communication between all related organizational systems
- System security must support the organization and its mission

Security Performance Evaluation Axioms



Traditional Performance Evaluation

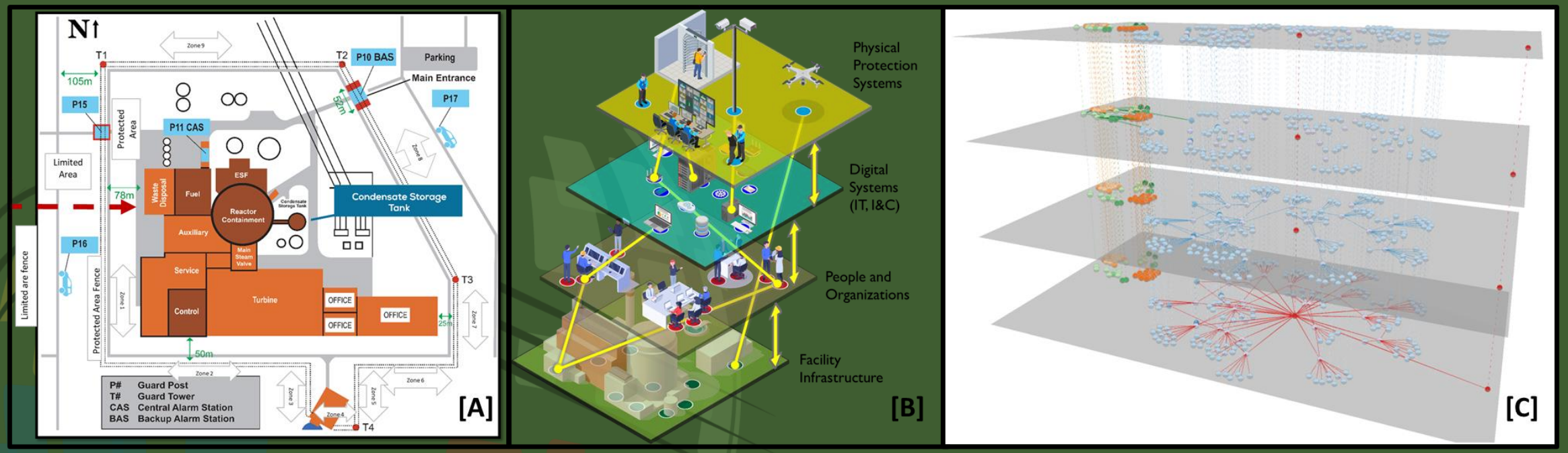


Axiomatic Approach

Axiom Name	Axiom Description
Confidence	The level of trust in the information being generated and transmitted to support systems security decision-making.
Criticality	The importance of various components or elements within the systems security solution to ensure adequate performance
Diversity	The ability to balance the use of the same technology for different systems security purposes and the use of different technologies to support the same security function
Human Performance	Incorporates human actors' role(s) on systems security solutions in terms of security "performance influencing factors."
Rapidity	The speed, accuracy, and structure of information flow throughout systems security solutions
Reliability	How well a component correctly provides valuable information (e.g., sensitivity) and how well a component does not provide incorrect information (e.g., specificity)
Resilience	The ability of the systems security solution to maintain (e.g., absorb, adapt, or recover) desired performance levels against a range of perturbations

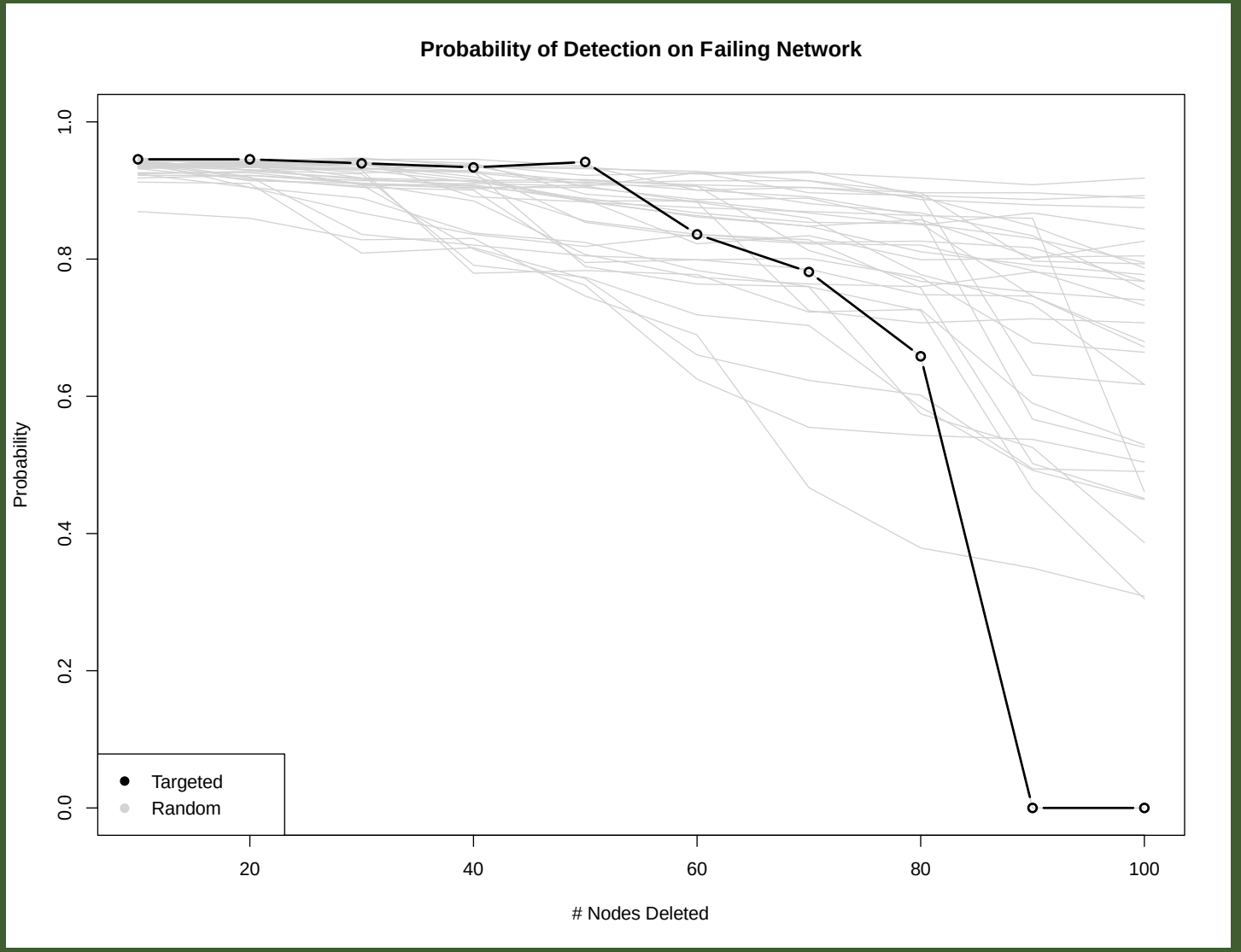
A generalized description of science – based on established theory and principles that explain—and can be **validated by—observation and experimentation**

Experiment: Utilize an MLN reflecting the physical, digital, infrastructure, and people that create a security system for a hypothetical nuclear power plant and use observations and metrics to consider the proposed security performance axioms



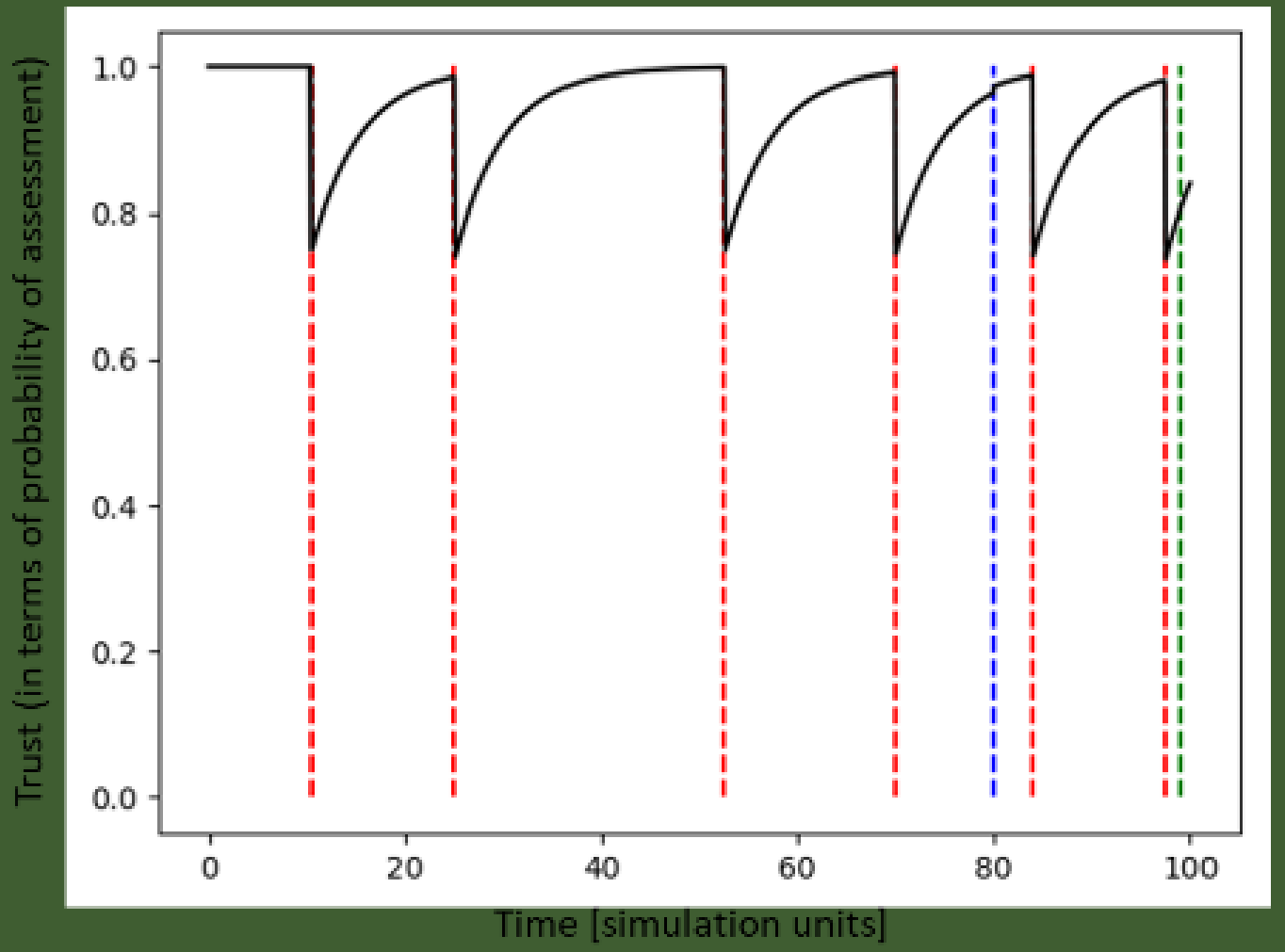
Example Results

Criticality



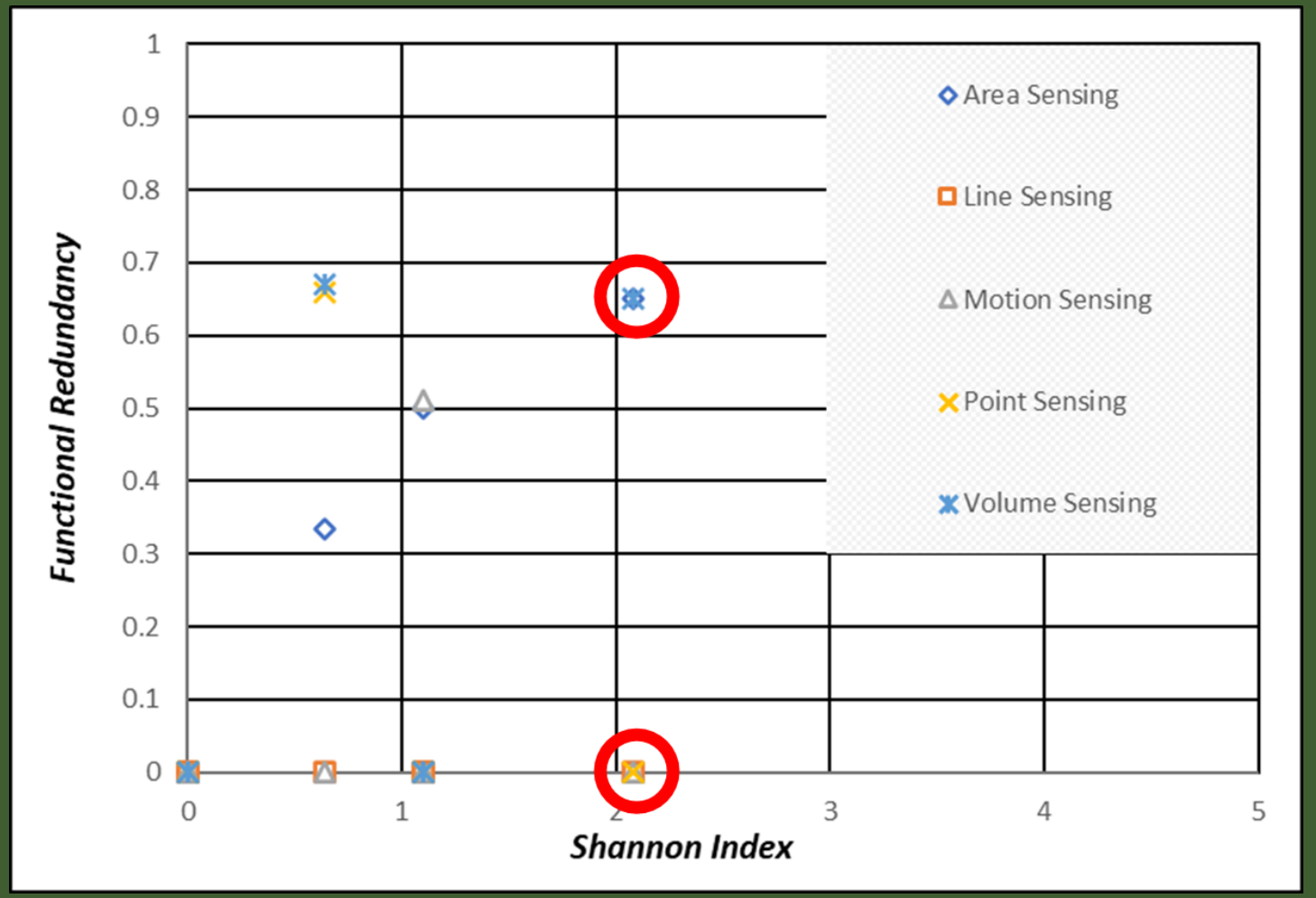
Example Results

Confidence



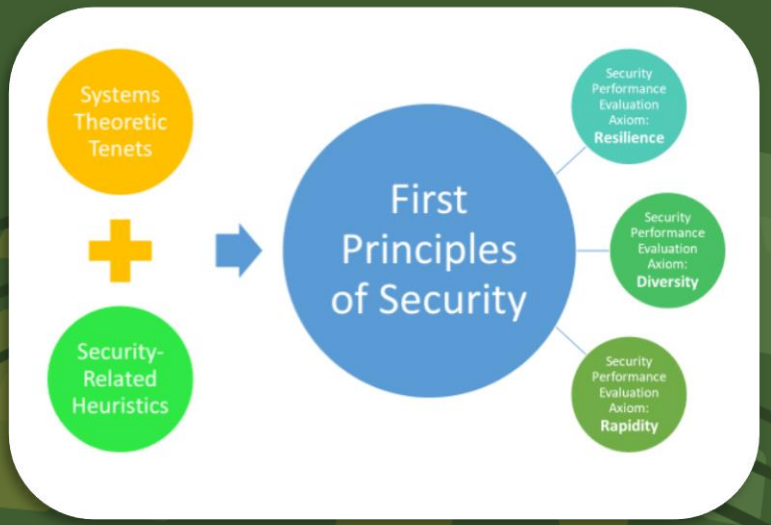
Example Results

Diversity



Conclusions

Our proposed 1st principles and security performance axioms create an opportunity to shift from “just stopping the bad guys” to “measur[ing] the overall system stability and flexibility”



Human-machine interactions for security expert

“Historically, [it is] likely [that we] had rich conversations about the [security assessment] framework and associated caveats and assumptions…[while] the framework has been passed on, ***the continuous improvement process has not been retained***”

“… a systematic view is needed that looks **beyond compliance** with the regulations, but also considers emergency response, cyber vulnerabilities, as well as safety and security issues.”

Evaluation of security assessments

Resilience frameworks and systems analysis expert

“…ensure that consequences are looked at **over time**: temporal disconnects between threats and consequences are **assessed dynamically**.”

“We need to consider changing the end state from just stopping the bad guys to **include considering how they may be changing**…and **measure the overall system stability and flexibility**.”

Systems safety and security analysis expert

34th Annual INCOSE international symposium

hybrid event

Dublin, Ireland
July 2 - 6, 2024

www.incose.org/symp2024
#INCOSEIS