33rd Annual INCOSE international symposium

hybrid event

Honolulu, HI, USA
July 15 - 20, 2023

PANEL 15:

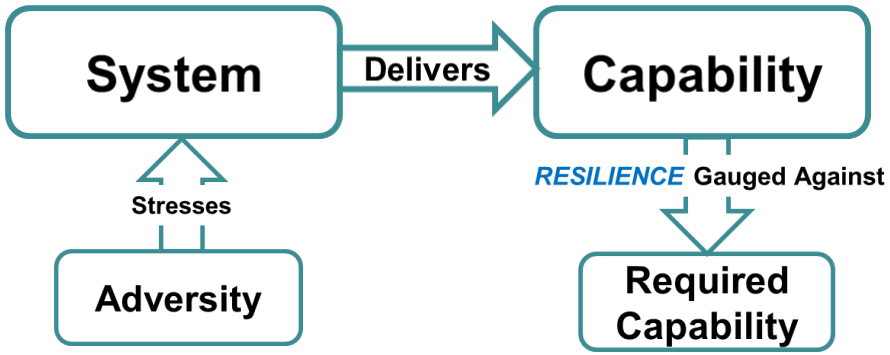
Methods of Resilience Engineering

Moderator: Mr. Kenneth Cureton, Co-Chair, Resilient Systems Working Group (RSWG)
kenneth.cureton@incose.net

PANEL 15: METHODS OF RESILIENCE ENGINEERING

INCOSE Systems Engineering Handbook and SEBoK Definition:

Resilience is the ability of the system to provide required capability when facing adversity



3 Objectives to obtain the Value of Resilience:

- ***Avoid adversity***
- ***Withstand adversity***
- ***Recover from adversity***

Many different means of achieving Resilience Objectives

Many different Architecture, Design, & Operational Techniques to Achieve Resilience Objectives

Sources: INCOSE Systems Engineering Body of Knowledge (SEBoK) https://sebokwiki.org/wiki/System_Resilience
Brtis, J.S. and M.A. McEvilley. 2019. Systems Engineering for Resilience. The MITRE Corporation. MP 190495. Used with permission.

PANEL 15: METHODS OF RESILIENCE ENGINEERING

This panel examines best-practices and advances in the state-of-the-art for Resilience Engineering via four panel presentations:

- **Dr. Scott Jackson: “Resilience as a Markov Chain”**
- **William Scheible: “Resilience and Quality Management”**
- **Dr. Ivan Taylor: “Modelling Cybersecurity Operations to Improve Resilience”**
- **Dr. Mark Winstead: “Resilience Relationship with Systems Security (and Safety and …)”**

33rd Annual INCOSE international symposium

hybrid event

Honolulu, HI, USA

July 15 - 20, 2023

33rd Annual INCOSE international symposium

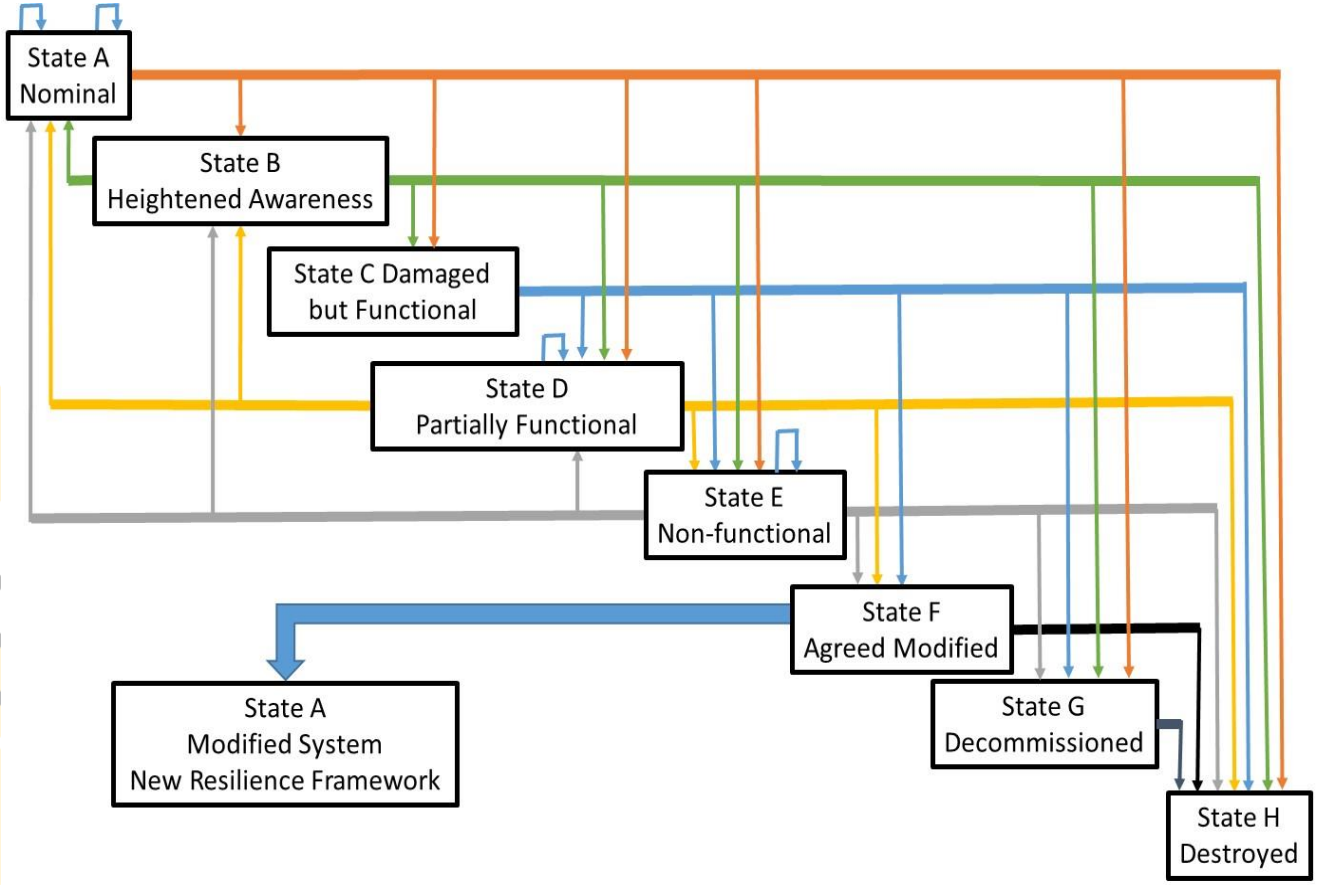
hybrid event

Honolulu, HI, USA
July 15 - 20, 2023

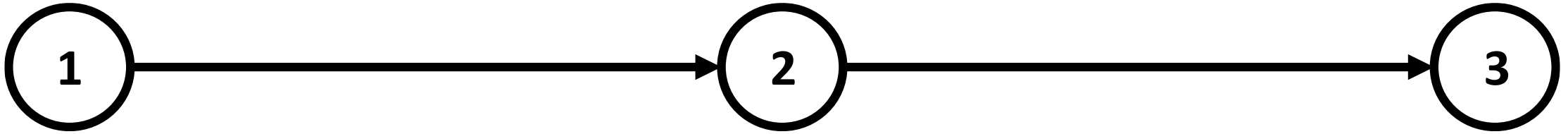
The Resilience State Model as a Markov Chain

Scott Jackson, PhD
Burnham Systems
(jackson@burnhamsystems.net)

State Model of Resilience

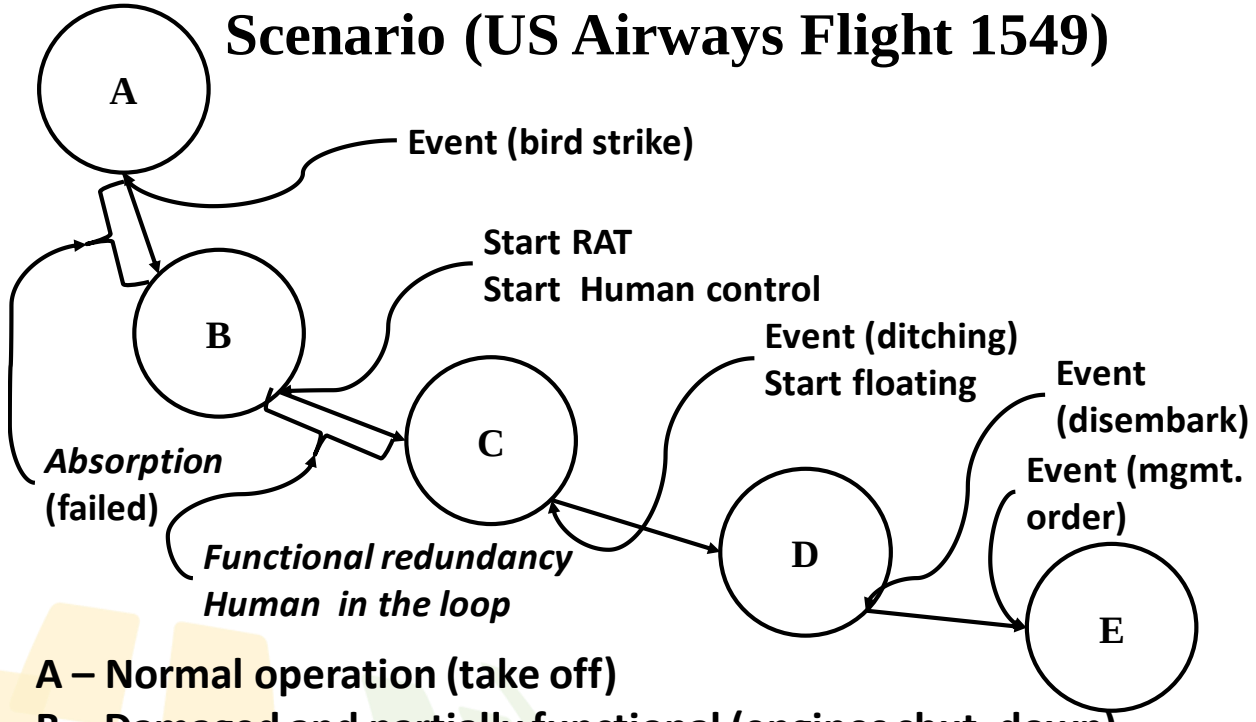


The Markov Chain



A rule of Markov analysis is that the probability of any transition cannot be dependent on prior decisions. Each technique is independent of all other decisions and the probability resulting from it is also independent of all other probabilities. Therefore, all the independent transition probabilities can be combined using standard probability analysis to determine the final probability of the final state.

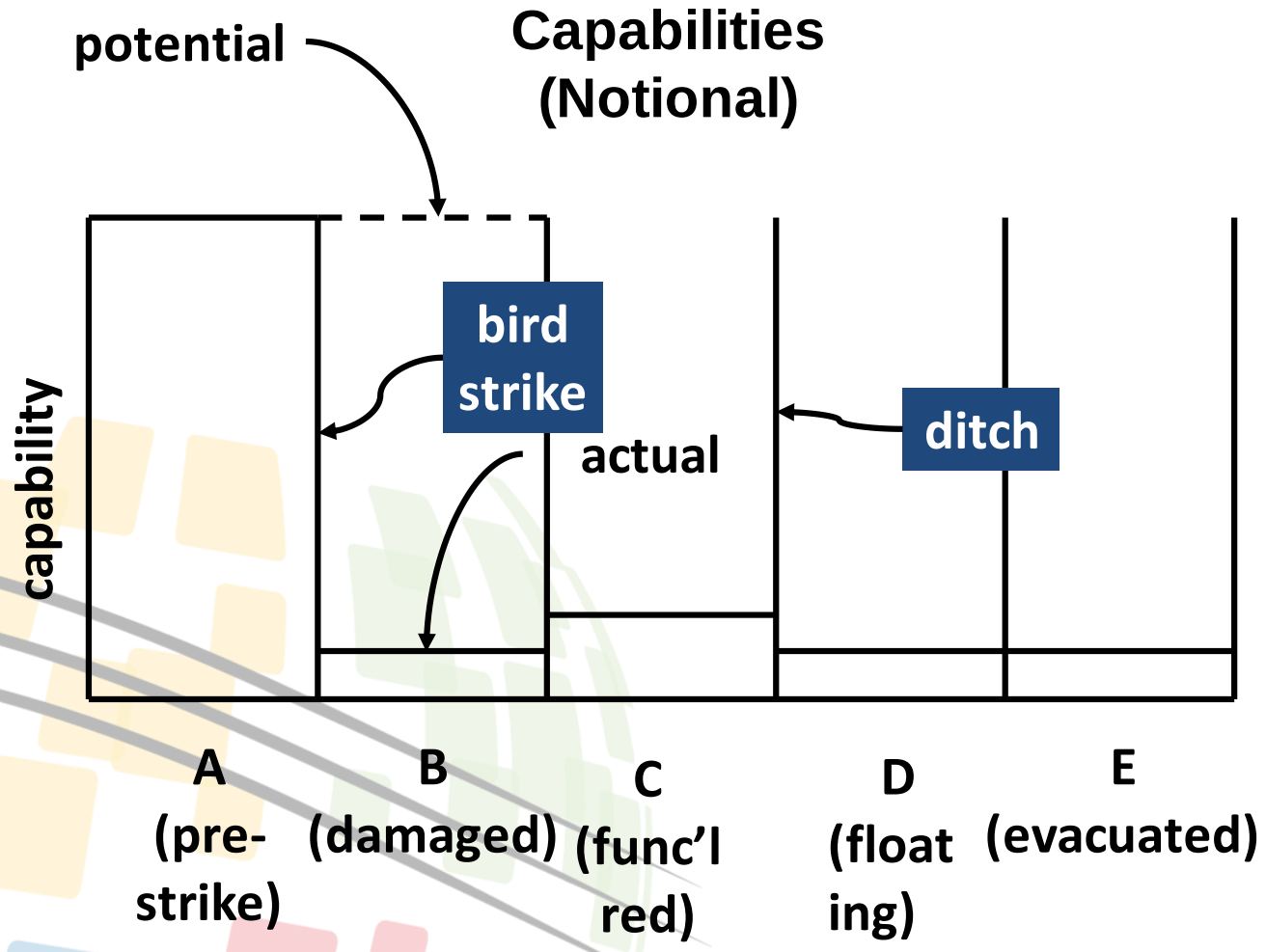
Example Resilience State Model Scenario (US Airways Flight 1549)



A – Normal operation (take off)
B – Damaged and partially functional (engines shut down)
C - Damaged and partially functional (control by RAT and pilot)
D - Damaged and partially functional (floating in water)
E - Decommissioning

Primary techniques: (1) Absorption (States A and B) and (2) Functional redundancy (states B and C) (Thrust plus Human)

Timeline of Capabilities from Birdstrike to Ditching



References

Jackson, Scott, Stephen C. Cook, and Timothy Ferris. 2015. "Towards a Method to Describe Resilience to Assist in System Specification." IS 2015, Seattle, 15 July.

Jackson, Scott, and Timothy Ferris. 2013. "Resilience Principles for Engineered Systems." *Systems Engineering* 16 (2):152-164.

Brtis, John. "How to think about Resilience in a DoD Context." Mitre Report. 2016/

33rd Annual INCOSE international symposium

hybrid event

Honolulu, HI, USA

July 15 - 20, 2023

33rd Annual INCOSE international symposium

hybrid event

Honolulu, HI, USA
July 15 - 20, 2023

Resilience and Quality Management

William Scheible

bill.scheible@incose.net

Resilience and Quality Management

- If Resilience focuses on providing required capability when facing adversity, including disruptive events, then a follow on discussion could be “What is a suitable approach to determining those possible events, reactions and outcomes”?
- One approach would be the adoption and use of known quality concepts and methodologies.
  - Establish policy, procedures, test labs and organizations to make quality happen
  - Focused to specific activities and sections of an business or company to accomplish this.
- This often is translated to additional testing or more procedures rather than a culture change
  - Quality Control (QC) often employed but focuses on eliminated defects. An after action response
  - Quality Assurance (QA) attempts to design the quality into the product or service. Can drive whole lifecycle development. Statistical probabilities and failure calculation are key tools. Still a focused effort.

Resilience and Quality Management

- Quality Management (QM) however is a larger picture and includes QA and QC but adds other management and cultural concepts to what is known as a Quality Culture.
- Conformance to requirements is a common definition of both QM and Systems Engineering
  - What the Customer Needs, Wants or Expects in a Product, Service or system
  - Balancing between the Cost of doing things wrong vice the Cost of doing things right.
- The Challenge for Leadership is a key consideration for Quality Management
  - (1) Keeping the promise to your customers
  - (2) Hiring and retaining reliable people and
  - (3) Developing a QM culture

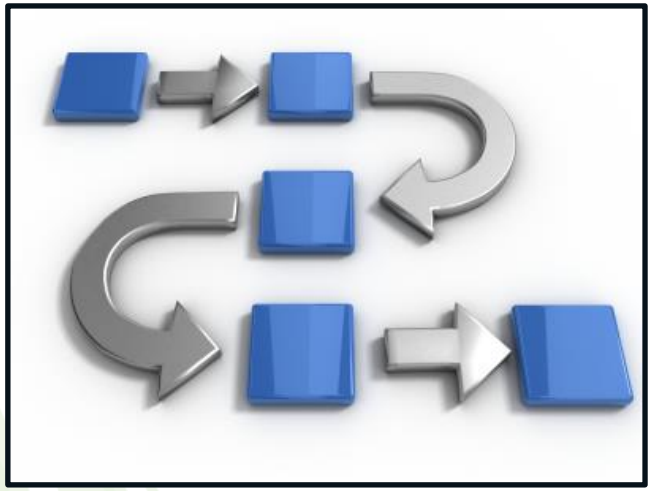
Values: Keys to Quality Management Adoption

- Managing Quality requires:
  - QM Methods, QM Values and Reasonable Discussions with involved parties.
  - Quality Management is a cultural adoption based upon 8 attributes

QM and Systems Engineering

- Quality Management is Systems Thinking
  - An approach to problem solving, that considers and evaluates “facts and events” as parts of an overall system.
  - Avoids the failures created by reacting to specific parts, outcomes or events in isolation.
  - Considers specific strategies and tactics to overcome known limitations.
- Quality Management can also have significant staff impacts
  - QM trained and adoptive people are Engaged
    - Learn the facts and take action to create reliable solutions within scope and resources
  - QM People are Productive
    - Utilize the right processes and tools with improved outcomes
- QM culture and discipline supports System Engineering practices

Complete QM is People, Processes and Tools



Work Culture

Team of Engaged, Well-Trained High-Performers

Policy / Procedure

Artfully Designed and Deployed Work Standards

Technology

Fully-Utilized Tools and Efficiencies

Resilience solutions can be helped by QM!

If Resilience focuses on providing required capability when facing adversity, including disruptive events, then what is a suitable approach to determining those possible events, reactions and outcomes?

Strong Resilience solutions can be helped by adopting a Quality Management Culture!

The INCOSE Systems Engineering Quality Management (SEQM) working group was formed and dedicated to supporting other INCOSE working groups to understand and implement QM concepts into the efforts of other INCOSE working groups.

33rd Annual INCOSE international symposium

hybrid event

Honolulu, HI, USA

July 15 - 20, 2023

33rd Annual INCOSE international symposium

hybrid event

Honolulu HI USA

Ivan Taylor and Keith Willett

Modelling Cybersecurity Operations to Improve Resilience

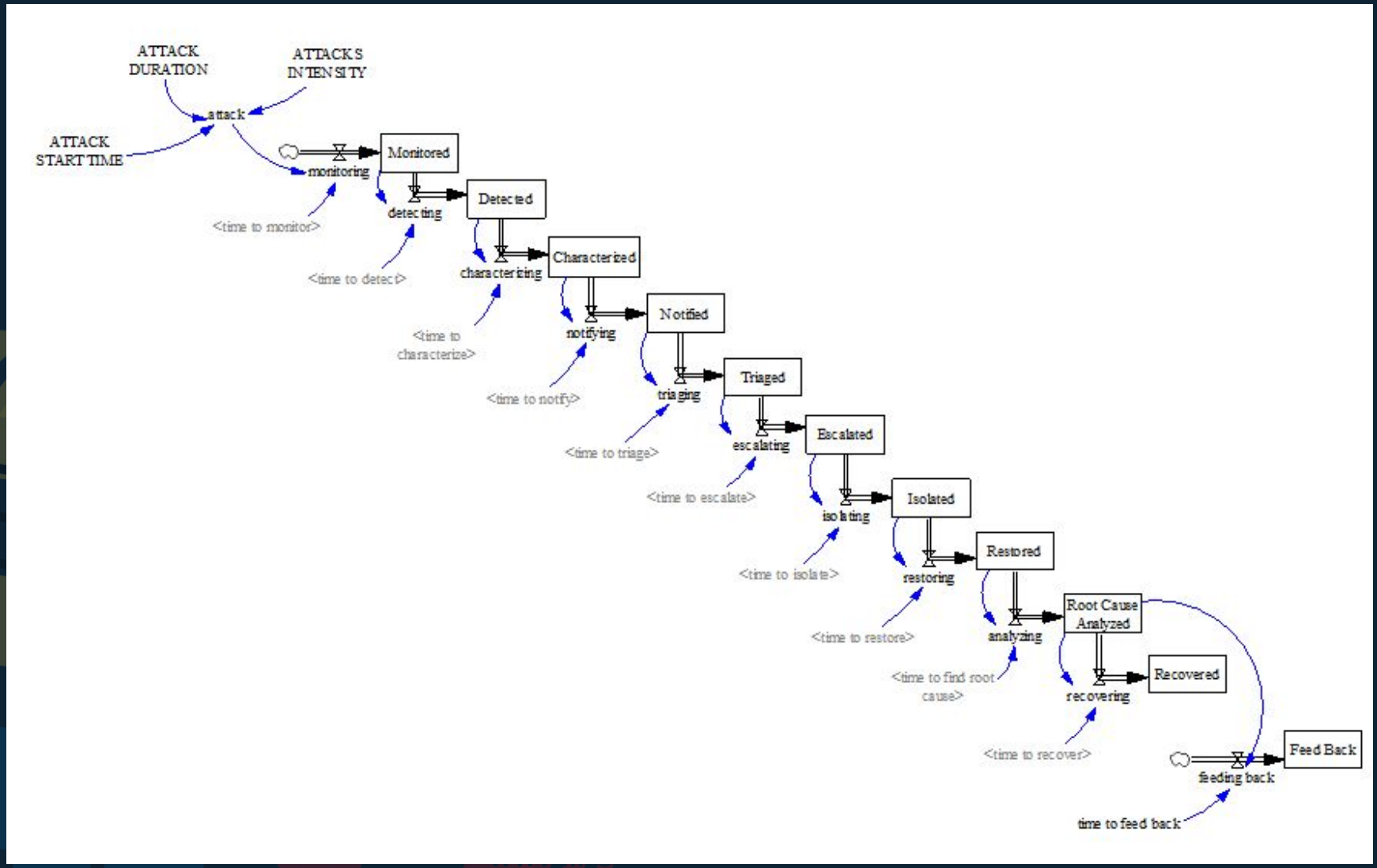
Purpose

Demonstrate How System Dynamics Modelling Can Be Used to Improve Cybersecurity Operations

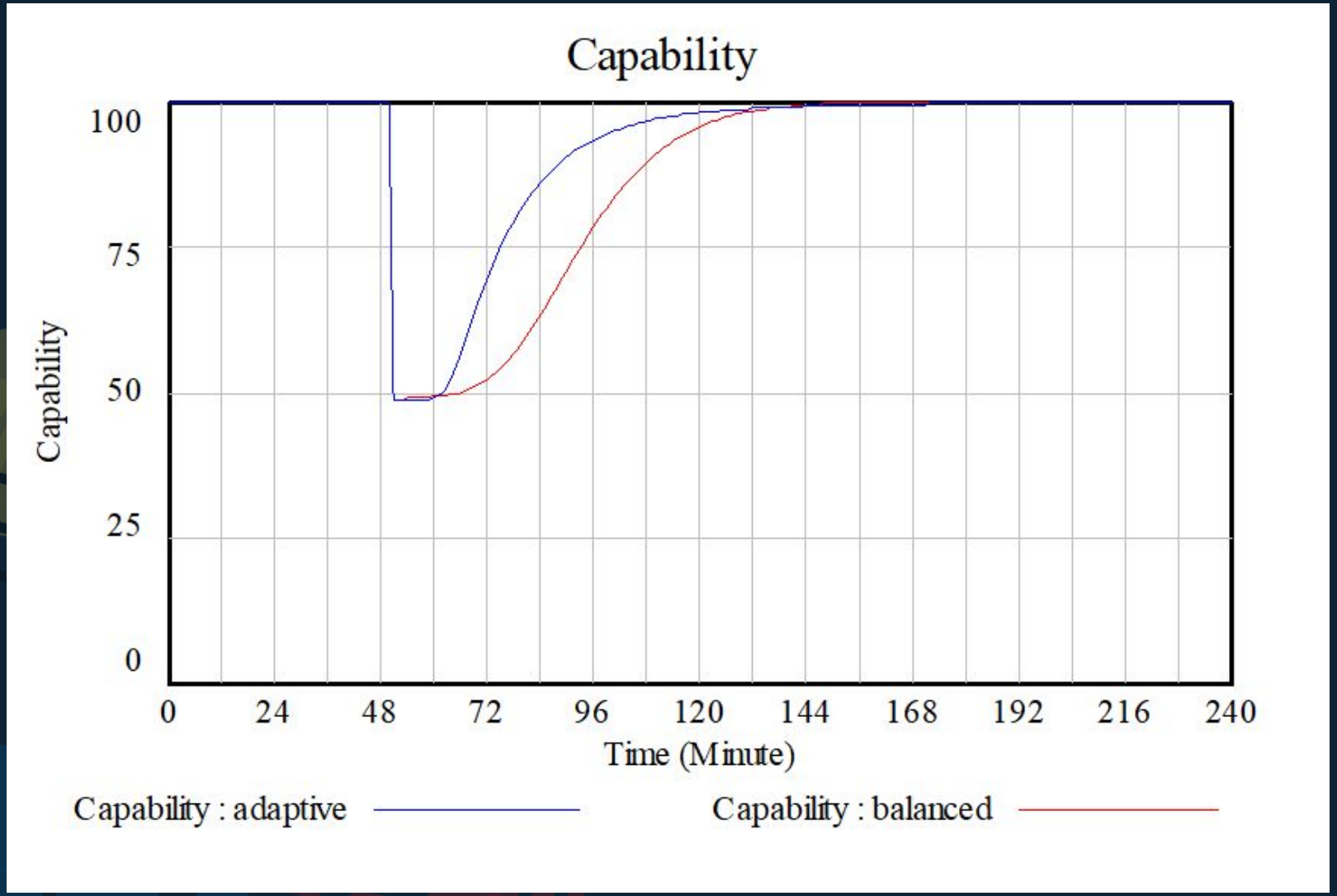
Cybersecurity Operations Phases

Phase	Description
Monitor	Ongoing observation with intent to raise awareness
Detect	Indicator of anomaly where an anomaly is something unexpected
Characterize	Known-known, known-unknown, unknown-unknown, unknown-known
Notify	Tiered support
Triage	Determine priorities
Escalate	Send to subject matter expert(s)
Isolate	Contain adversity or effects of adversity
Restore	Restore effective operations even if at diminished capacity
Root Cause Analysis	Identify the root cause of the problem
Recover	Recover operations to *desired* performance level
Feedback	Minimize anomaly/adversity recurrence and effects of recurrence

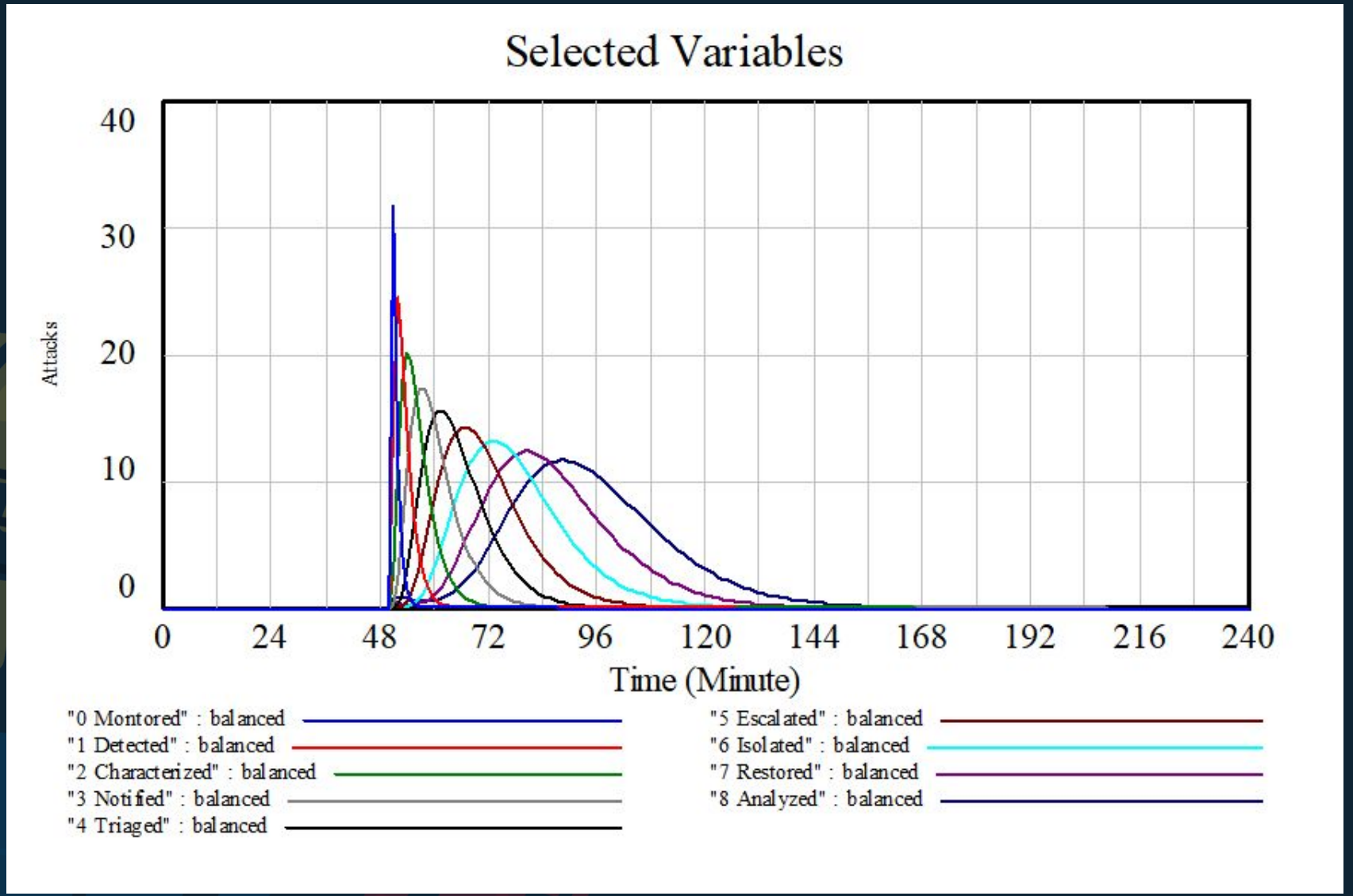
Cascade System Dynamics Model



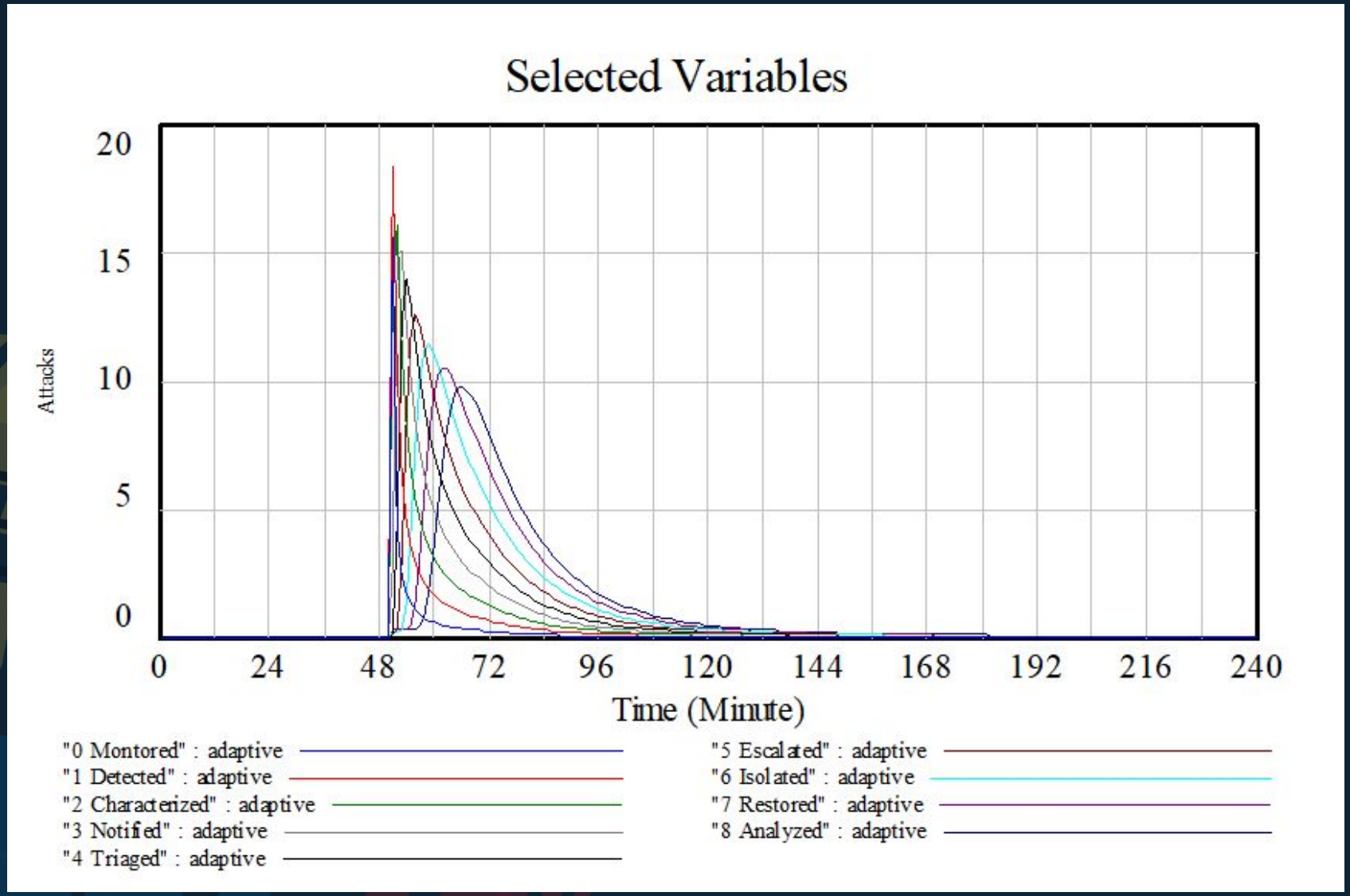
Capability with Balanced and Adaptive Resource Allocations



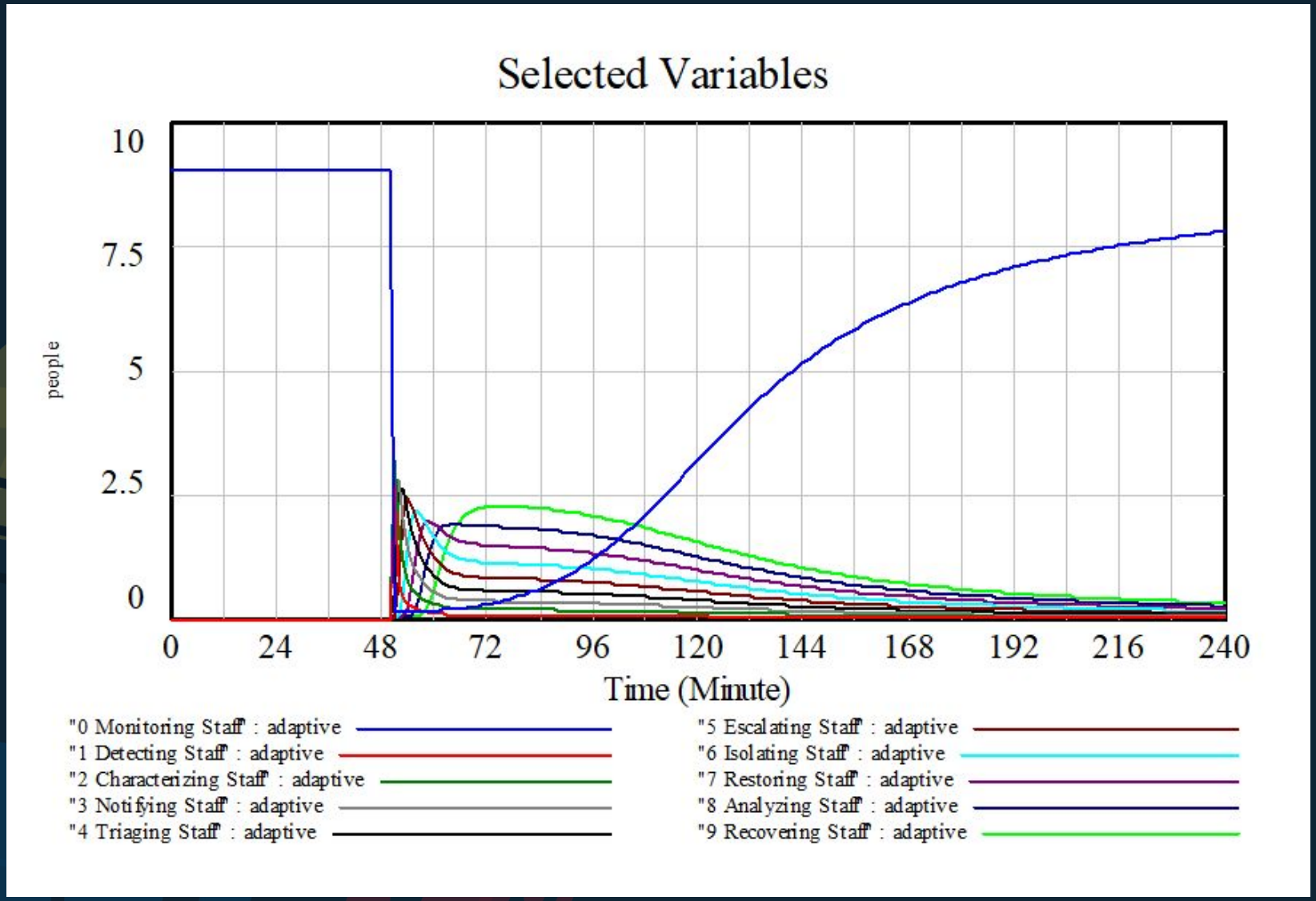
Activity with Balanced Resource Allocation



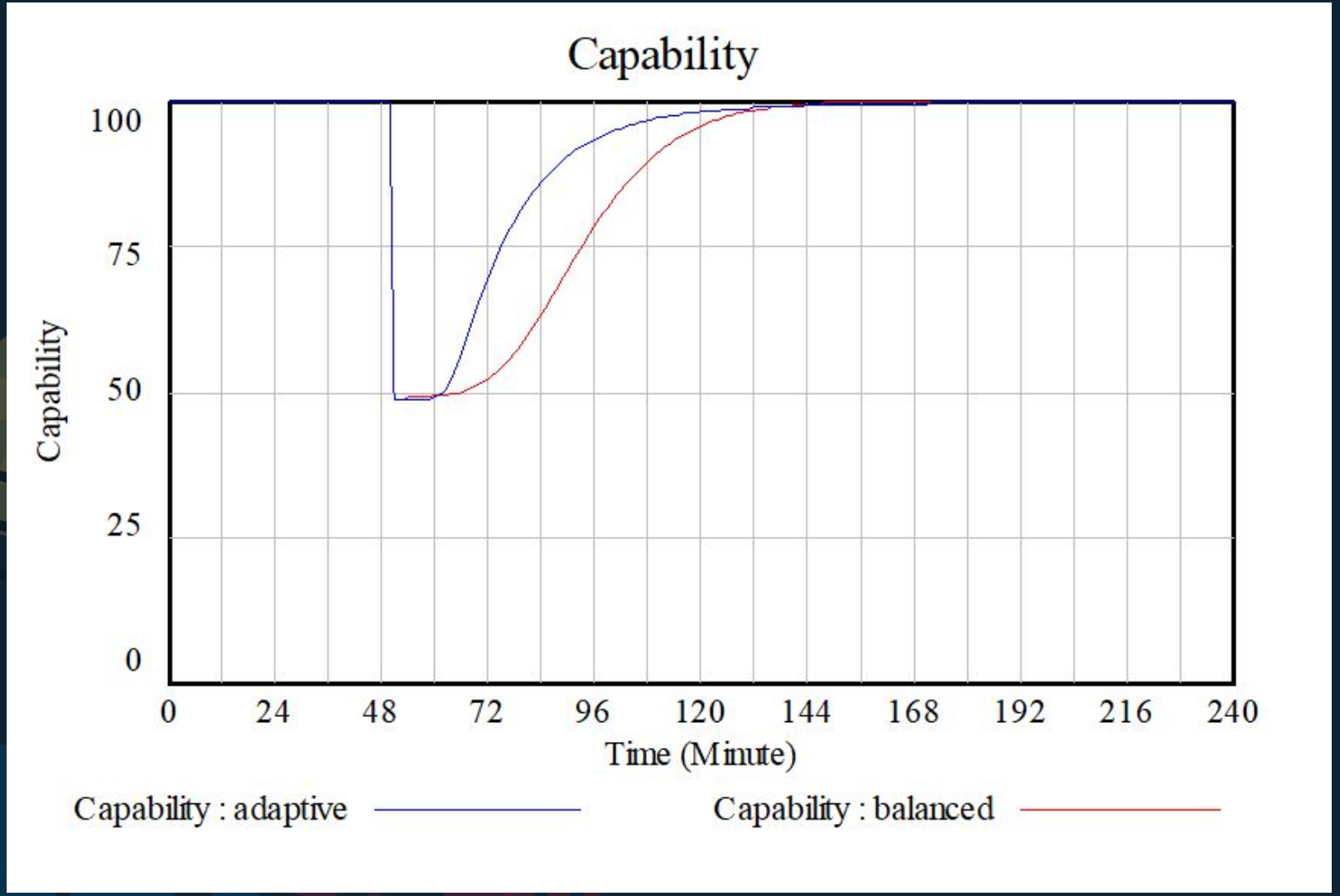
Activity with Adaptive Resource Allocation



Adaptive Assignment of Resources



Capability with Balanced and Adaptive Resource Allocations



Conclusions

Built a System Dynamics Model of Cybersecurity Operations

Examined the Ability to Recover from a Cyber Attack with Balanced and Adaptive Resource Allocation to Improve System Resilience

Willett, Keith D. and Ivan Taylor, (2022) “Security Modeling and Simulation”, in *Handbook of Security Science*, A. J. Masys (ed.), Springer Nature Switzerland AG
https://doi.org/10.1007/978-3-319-91875-4_65

Thank you for listening - You can reach me at ivan@policydynamics.ca

Questions and Comments

33rd Annual INCOSE international symposium

hybrid event

Honolulu HI USA

www.incose.org/symp2023

33rd Annual INCOSE international symposium

hybrid event

Honolulu HI USA

Methods of Resilience Engineering

Mark Winstead, PhD, CSEP

Resilience Relationship with Systems Security (and Safety and …)

Approved For Public Release. Distributed Unlimited. Public Release Case Number 22-03738-8

Definitions

From Chapter 3 of **The Coupling of Safety and Security**, titled *Safety and Security are two Sides of the Same Coin* by Nancy Leveson

Definitions of the terms we use are necessary for effective communications. There is no right or wrong definition, only the one we choose to use. If we limit our definition of the terms “safety” and “security”, then we can effectively limit any overlap. Limited definitions, however, may also limit potential solutions to the problems. If we start from more inclusive and practical definitions, then overlap and common approaches to achieving the properties are possible … Safety and security can be considered using a common approach and integrated analysis process if safety and security are defined appropriately … Other limitations in how we handle these properties also need to be removed to accelerate success in achieving these two properties, which are really just two sides of the same coin

NIST SP 800-160 Volume 1 Revision 1
Engineering Trustworthy Secure Systems

Security: Freedom from those conditions that can cause the loss of assets with unacceptable consequences

Common asset classes in Vol 1 Rev 1:

- Material Resources and Infrastructure
- System Capability
- Human Resources
- Intellectual Property
- Data and Information
- Derivative Non-Tangibles

The definition of security expresses an ideal that encapsulates three essential characteristics of a secure system:

- It enables the delivery of the required system capability despite intentional and unintentional adversity
- It enforces constraints to ensure that only the desired behaviors and outcomes associated with the required system capability are realized while satisfying the first characteristic
- It enforces constraints based on a set of rules to ensure that only authorized human-to-machine and machine-to-machine interactions and operations are allowed to occur while satisfying the second characteristic

Authors of V1R1 – Ron Ross, Mark Winstead, Michael McEvilley

Approved For Public Release. Distributed Unlimited. Public Release Case Number 22-03738-8

Functionally Interpreting Systems Security

From **Functionally Interpreting Security** (McEvilley & Winstead) INCOSE Insight Vol 25 Issue 2:

Security: the expectation that a system does not, under defined conditions, exhibit behavior, produce outcomes, or lead to a state

- *that is in violation of rules that determine authorized and intended behaviors and outcomes*
- *that causes an unacceptable loss of assets*
- *that constitutes an unacceptable loss of assets*

Assets: anything of value to a stakeholder

Including *System Capability*

Approved For Public Release. Distributed Unlimited. Public Release Case Number 22-03738-8

Interpreting Resilience

- SEBoK: *Resilience is the ability to provide required capability despite adversity*

- Interpreting for a system (Security and Resilience Interpretation, OUSD(R&E) prepared by MITRE): *Resilience is the ability of a system to provide required capability despite the influence of adversity*

Approved For Public Release. Distributed Unlimited. Public Release Case Number 22-03738-8

Comparing Security, Safety, and Resilience

	Deliver required capability despite adversity	Deliver only the intended behavior and produce only the intended outcomes (based on required capability)	Enforce a set of rules governing authorized behaviors and outcomes
Resilience	x	-	-
Safety	x	x	-
Security	x	x	x

What may this look like with reliability, quality assurance, CIPR?
What new columns would be needed to distinguish?

33rd Annual INCOSE international symposium

hybrid event

Honolulu HI USA

www.incose.org/symp2023

Approved For Public Release. Distributed Unlimited. Public Release Case Number 22-03738-8