Resiliency in Systems Engineering

Prepared for C-NO INCOSE Chapter – 18 August 2020

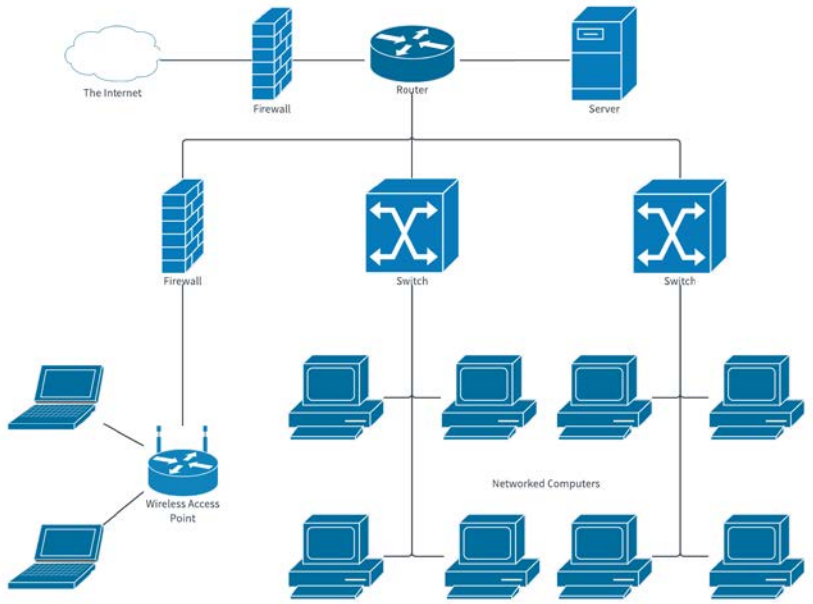
Rick Hefner, Ph.D.
California Institute of Technology
Center for Technology and Management Education
rhefner@caltech.edu, 626.395.4043

Background

- Resilience is the ability to provide required capabilities in the face of adversity - any condition that may degrade the desired capability of a system
- This presentation will discuss the characteristics of a resilient system and its supporting design techniques
- Presentation is based on Systems Engineering courses at Caltech *Center for Technology and Management Education*, https://ctme.Caltech.edu

Resilience

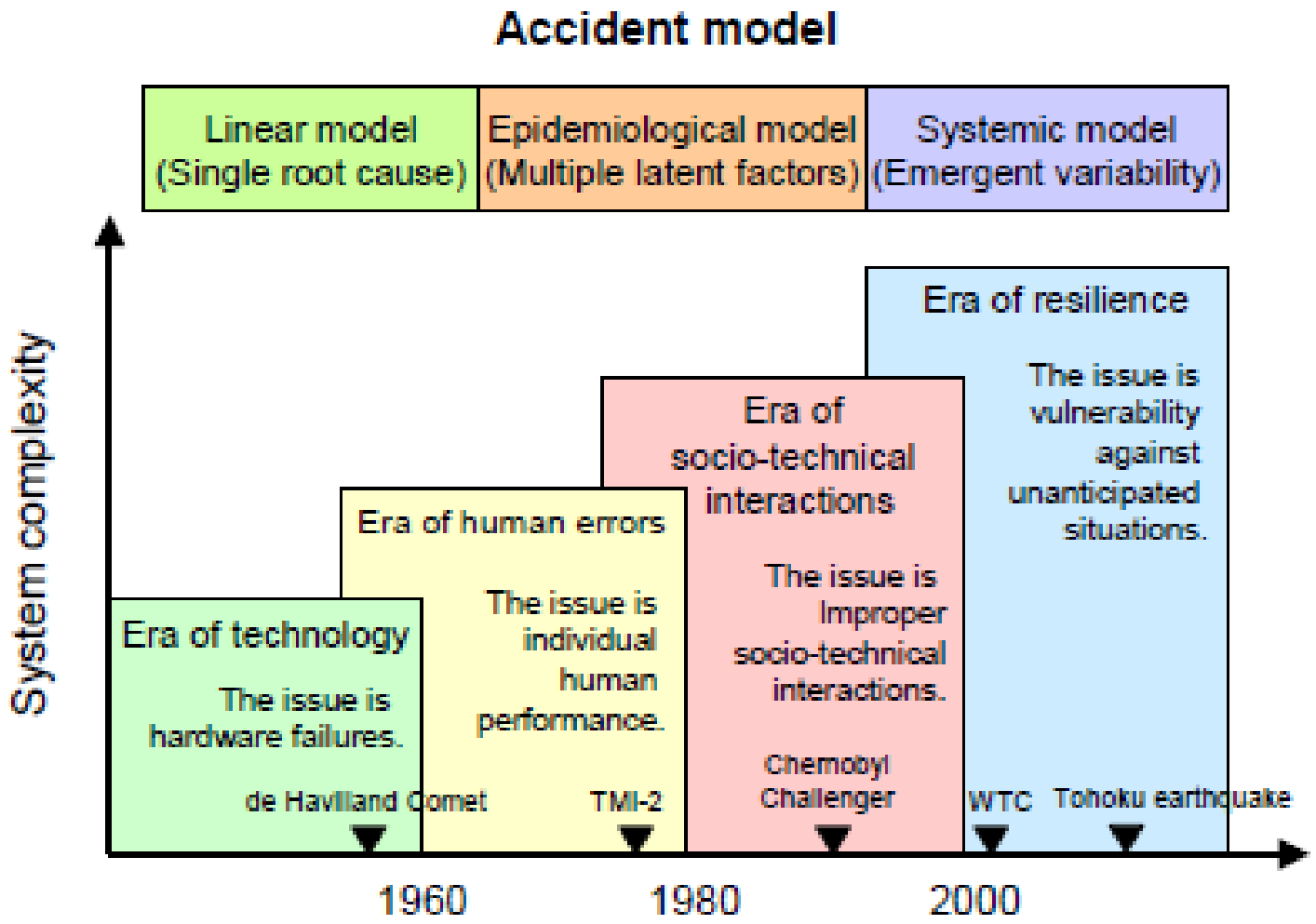
- Resilience is the ability to provide required capability in the face of adversity
- Adversity is any condition that may degrade the desired capability of a system
  - Environmental sources
  - Normal failure
  - Human sources - malicious or accidental



Can the corporate network function effectively under:

- Flood, earthquake
- Failure of any component
- Human error in configuration
- Cyber attack

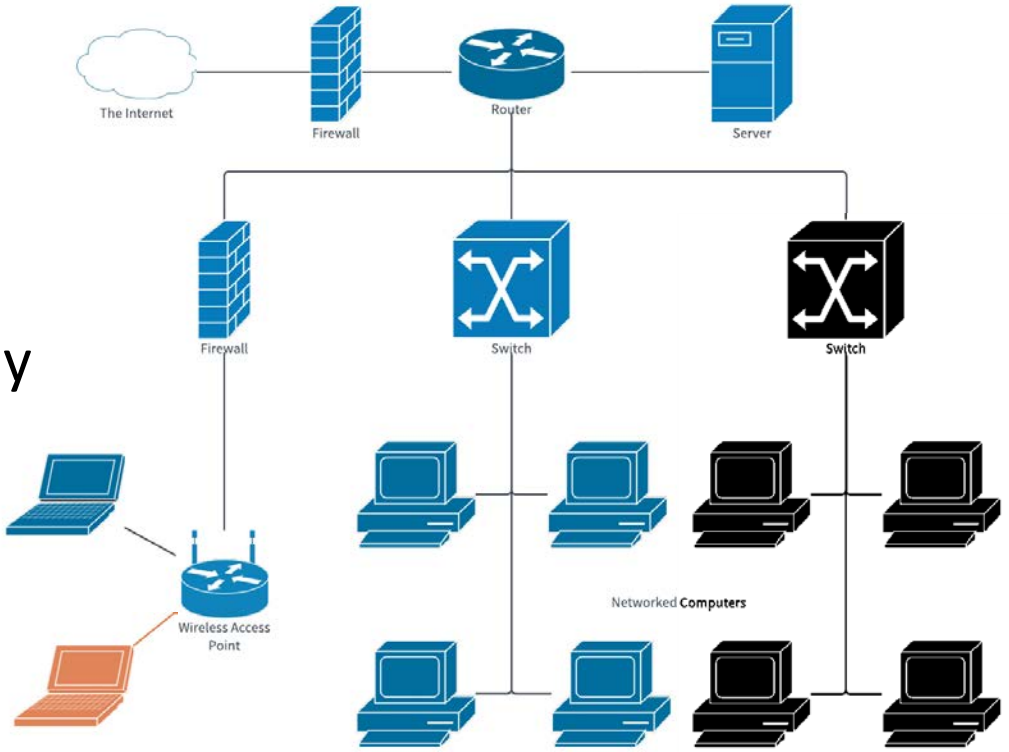
Resiliency Emerging as a Major Design Consideration



What is Resiliency Engineering?, Kazuo Furuta

Resiliency Challenges are Amplified in Systems of Systems

- Systems acquired at different times, from different providers
- Total system not designed top-down, so emergent behaviors may be unknown
- Impact of individual failures of system performance



Framing the Resiliency Problem

- The capability(s) of interest (note: a system may deliver several capabilities each of which may have different levels of resilience)
  - The measure(s) (and units) of the capability(s)
  - The target value(s) of the capability(s), perhaps by level (e.g., nominal, degraded mode, minimum useful, objective, threshold, etc.).
- System modes of operation (e.g., operational, training, exercise, maintenance, update…)
- The adversity(s) being considered for this resilience scenario
  - The ways that the adversity(s) affect(s) the system and how the system reacts in terms of its ability to deliver capability
  - The timeframe of interest
- The required resilience (performance) of the capability in the face of each identified resilience scenario
  - E.g., expected availability, maximum allowed degradation, maximum length of degradation, etc.
  - Note there may be several resilience goals (e.g., threshold, objective, As Resilient as Practicable (ARAP))

System Resilience, sebokwiki.org

Types of Disruptions

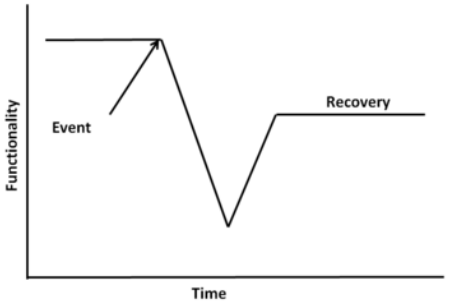
Type A – A disruption of input

- An unexpected or unknown (to the designer) phenomenon
  - *NY twin towers attack*
  - *Tacoma Narrows bridge*
- A change in environment
  - *Katrina hurricane and flood*

Type B – A degradation in function, capability or capacity

- Software error
- Human error (in the system)
  - *Nagoya*
  - *Metrolink 111*
- Component failure
  - *Challenger*
- Interaction Between Components
  - *Helios 522*
  - *Mars Polar Lander*

Failure States



State A
Nominal

State B
Heightened awareness

State E Damaged
but functional

State D Partially
functional disrupted

State C
Non-functional
disrupted

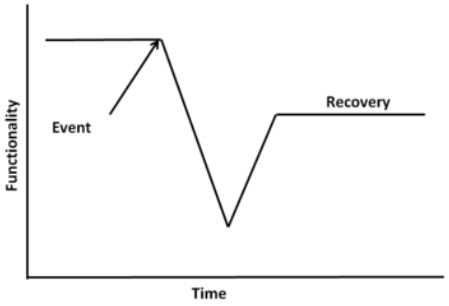
State F
Agreed modified

State A
Modified system
New resilience framework

State G
Decommissioned

State H
Destroyed

Means of Achieving Resilience



- **Avoiding** – Keep the adversity from happening or from effecting the system
  - E.g., shielding, hardening
- **Withstanding** – Accept the adversity's impact but continue operating despite it (perhaps at a reduced level)
  - E.g., redundancy
- **Recovering** – Accept the adversity's impact and reconfigure afterwards to continue operating
  - E.g., serviceable system
- **Evolving and adapting** – Sense the approaching adversity and adjust over time to lessen/eliminate it's impact
  - E.g., failure detection

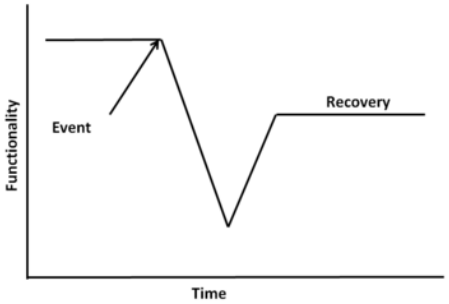
System Resilience, sebokwiki.org

Attributes of a Resilient System

Robustness • Ability of a system to withstand a threat in the normal operating state	**Adaptability** • Ability of a system that allows it to restructure itself in the face of a threat
Tolerance • Ability of a system that allows it to degrade gracefully following an encounter with adversity	**Integrity** • Property of being whole or cohesive

Jackson, S., & Ferris, T. (2013). Resilience Principles for Engineered Systems. Systems Engineering, 16(2), 152-164. doi:10.1002/sys.21228.

Robustness

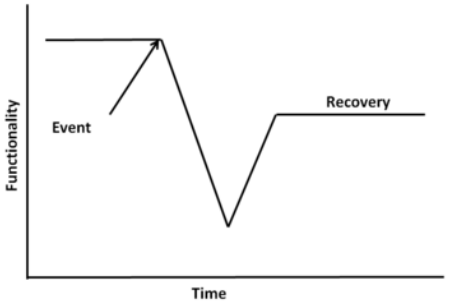


Ability of a system to withstand a threat in the normal operating state

Design techniques:

- Absorption – Withstand a disturbance without a fundamental breakdown in the system's performance or structure
- Physical redundancy – Two or more independent and identical components to perform critical tasks
- Functional redundancy – Two or more different ways to perform a critical task

Adaptability

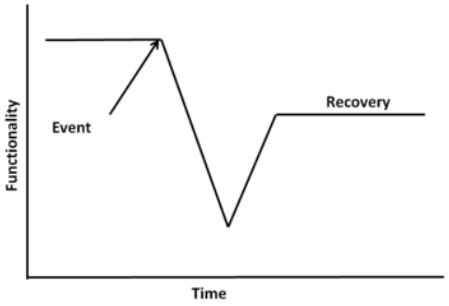


Ability of a system that allows it to restructure itself in the face of a threat

Design techniques:

- Restructuring
- Human in the loop
- Complexity avoidance – System no more complex than required
- Drift correction – System senses an approaching failure and takes corrective/ preventative action

Tolerance

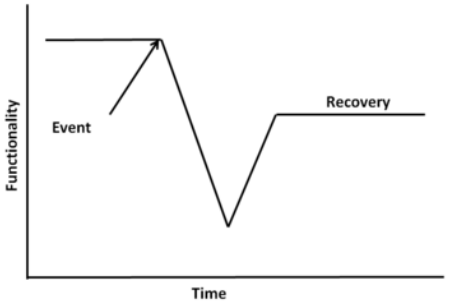


Ability of a system that allows it to degrade gracefully following an encounter with adversity

Design techniques:

- Modularity – Functionality is distributed through multiple nodes, so if one node is damaged, others continue to function
- Loose coupling – Events in various elements can occur independently
- Neutral state - System is put into neutral state, if possible, following a disruption
- Reparability – System can be brought to partial or full capability, over a specified period of time, in a specified environment
- Defense in depth – Two or more ways to address a vulnerability

Integrity



Property of being whole or cohesive (acting as a unified whole in the face of a threat)

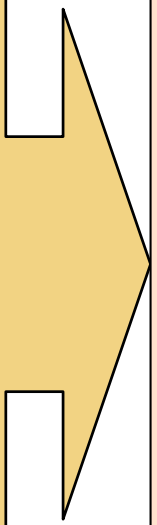
Design techniques:

- Internode interaction – Every node, or element, of a system should be capable of communicating, cooperating, and collaborating with every other node
- Reduce hidden infrastructures – Potentially harmful interactions between nodes of the system are reduced

Other Perspectives

Engineering techniques

- adaptive response
- analytic monitoring
- coordinated defense
- deception
- distribution
- detection avoidance
- diversification
- dynamic positioning
- dynamic representation
- effect tolerance
- non-persistence
- privilege restriction
- proliferation
- protection
- realignment
- reconfiguring
- redundancy
- replacement
- segmentation
- substantiated integrity
- substitution
- threat suppression
- unpredictability

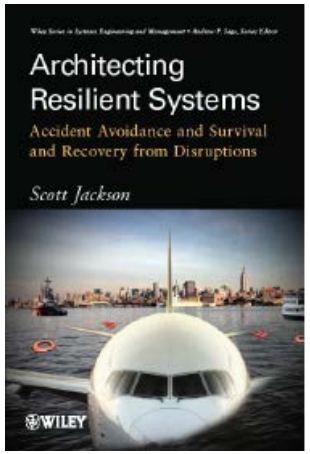


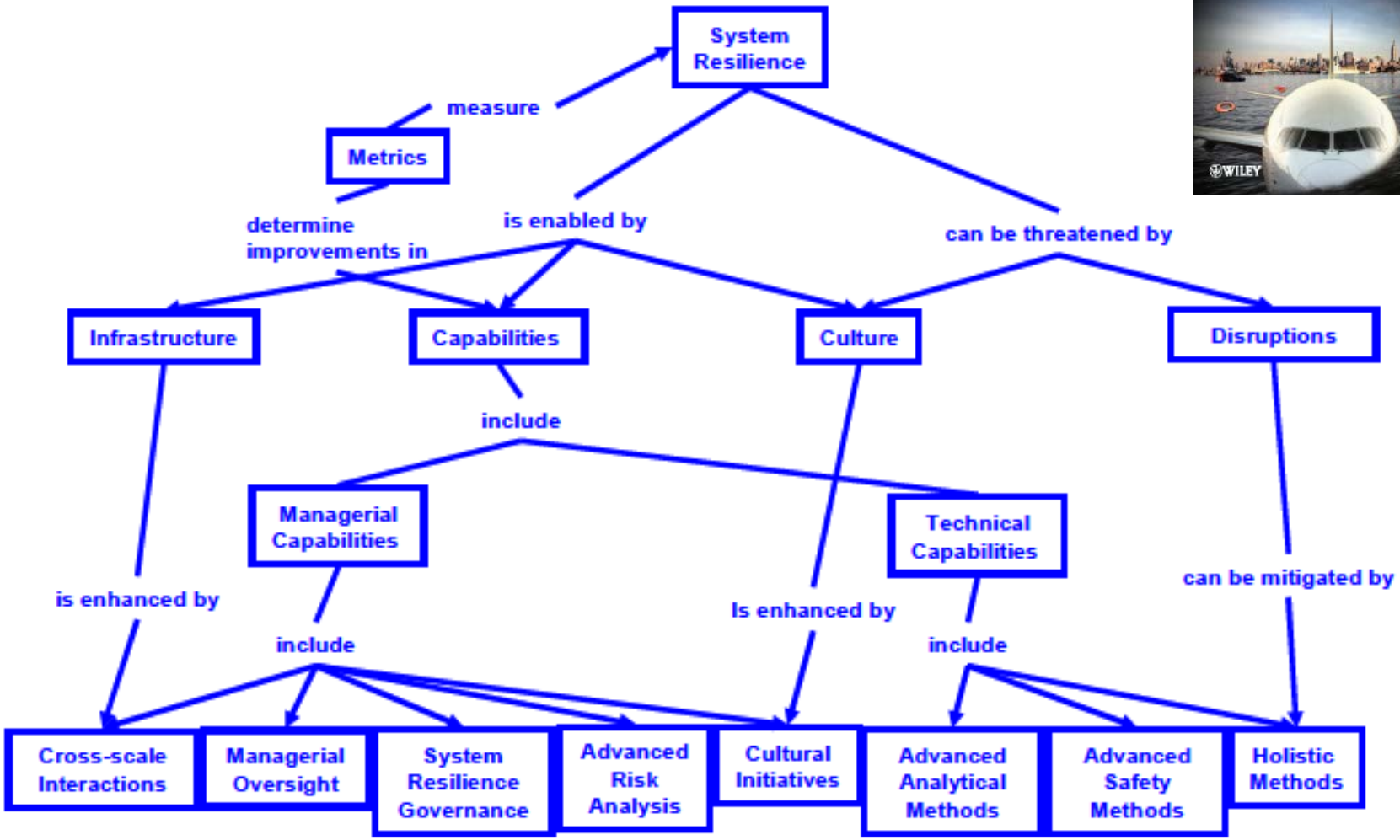
Objectives

- Adapt
- Anticipate
- Understand
- Disaggregate
- Prepare
- Prevent
- Continue
- Constrain
- Redeploy
- Transform
- Re-architect

Brtis, J. S., and McEvilley, M. A. (2019). Systems Engineering for Resilience, MITRE Technical Report

System Resilience Relationships





Summary

- System engineers must increasingly consider resiliency in designing systems
- Multiple design principles exist – selecting and applying the right one(s) requires experience and judgement