Designing Resiliency into Critical Infrastructure Systems

NDIA Systems Engineering Conference

Springfield, VA

28-30 October 2014

Dr. Warren K. Vaneman
Department of Systems Engineering
Naval Postgraduate School
Monterey, CA
wvaneman@nps.edu

Dr. Kostas Triantis
Grado Department of Industrial and Systems Engineering
Virginia Polytechnic Institute and State University
Falls Church, VA
triantis@vt.edu

Problem Statement

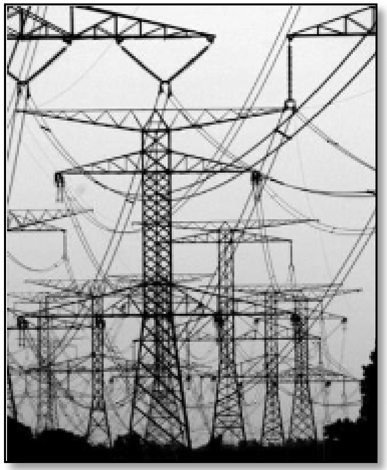
- As today's critical infrastructure systems become more complex and interconnected, the probability of widespread and prolonged service disruptions increase.
- One has to look no further than the devastation that Super Storm Sandy caused to many New Jersey seaside municipalities, or envision the loss of communication capabilities due to a catastrophic event to our space-based or terrestrial infrastructure.

Critical Infrastructure Systems

The U.S. PATRIOT Act (P.L. 107-56, Sec. 1016(e)) defined critical infrastructure as:

" systems and assets, whether physical or virtual, so vital to the United States that incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."

Example of Critical Infrastructure Systems



Critical Civil Infrastructures

- Highly decentralized and dynamic with interlocking parts.
- Permanent and durable, usually dependent on other infrastructures (interdependencies).
- Disruption of electrical power impacts water, government services, finance, and emergency services.

Space-based Infrastructures

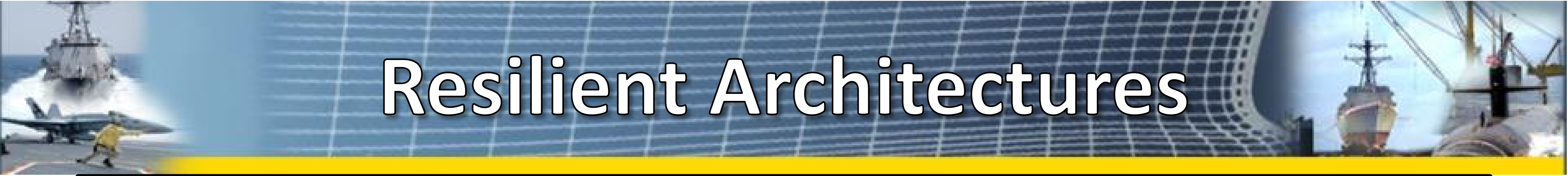
- Centralized and static with strong interlocking parts.
- Permanent but fragile in a contested environment, but critical to other infrastructures (interdependencies).
- Disruption of service has wide-spread implications with impacts to communications or other space-based services.

Resiliency

Resiliency is the ability to adapt to changing conditions (natural or man-made) through planning on how to absorb (withstand) and rapidly recover from adverse events and disruptions.

Definition Fundamentals:

- **Adapt** - to restructure before, during, or after an encounter with an adverse condition or threat.
- **Plan** - to architect and engineer the system or SoS, in advance, to absorb or rapidly recover from an encounter with adverse events or disruptions.
- **Absorb** - to retain full or partial functionality during an encounter with adverse conditions or disruptions.
- **Rapidly Recovery** - to restore the system or SoS to full or partial functionality following an encounter with an adverse condition or threat that caused a degradation.



Resilient Architectures

An architecture is resilient if it can provide the necessary operational functions, with a higher probability of success and shorter periods of reduced capabilities during and after an adverse condition or disruption through avoidance, robustness, recovery, and reconstitution.

Key Elements:

- **Avoidance** - proactive or reactive measures taken to reduce the likelihood or impact of adverse conditions or threats.
- **Robustness** - design feature to resist functional degradation and enhance survivability.
- **Recovery** - actions and design features that restore a a lost capability to meet a specific mission set (perhaps the most critical mission set),
- **Reconstitution** -actions and design features a measure of how much the total capability can be replaced, and the time it takes to achieve it.

Attributes of a Resilient Architecture

Avoidance	Robustness	Recovery	Reconstitution
Operational Flexibility	Physical Redundancy	Reduce Complexity	Repairability
Policy and Procedures Flexibility	Functional Redundancy	Repairability	Replacement
Loose coupling	Distributed	Reorganization of system or SoS	Logistical solvency
Extendibility	Reduce Complexity		
	Disaggregation		
	Diversified		

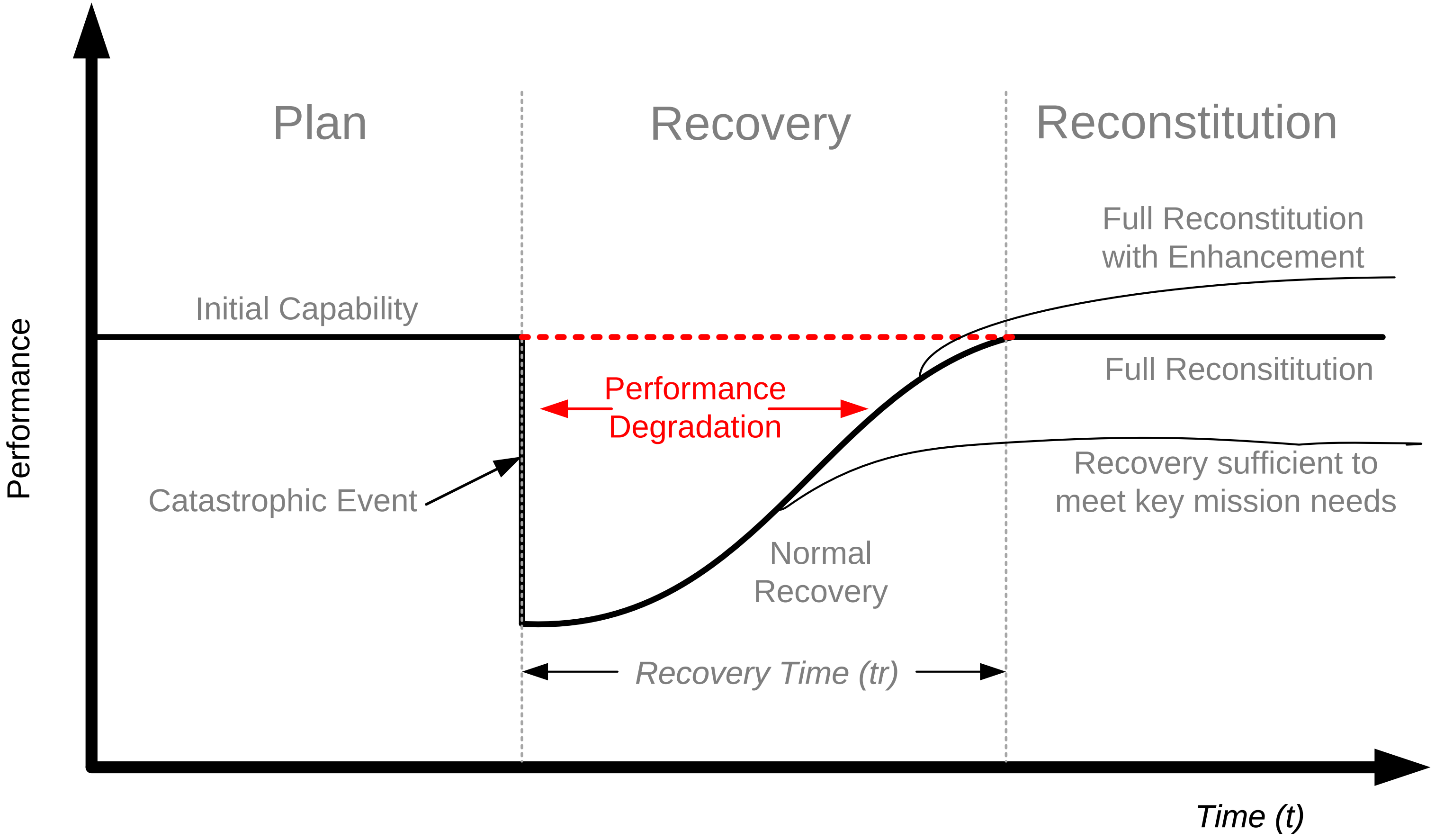
Resilient Architectures exhibit one or more of these architectural attributes.

Key Issues to be Addressed by a Resilient Architecture

- The architecture’s resiliency attributes will determine how quickly, and completely, a system will recover from a disturbance.
- Key Questions:
  - Can the system withstand a disturbance with no loss of critical functions?
  - Can a disruption be isolated to prevent it from cascading to other interconnected systems?
  - Can the duration and magnitude of the disturbance be minimized?
- Recovery can be described with archetype of resilient behavior.

Archetype of Resilient Behavior

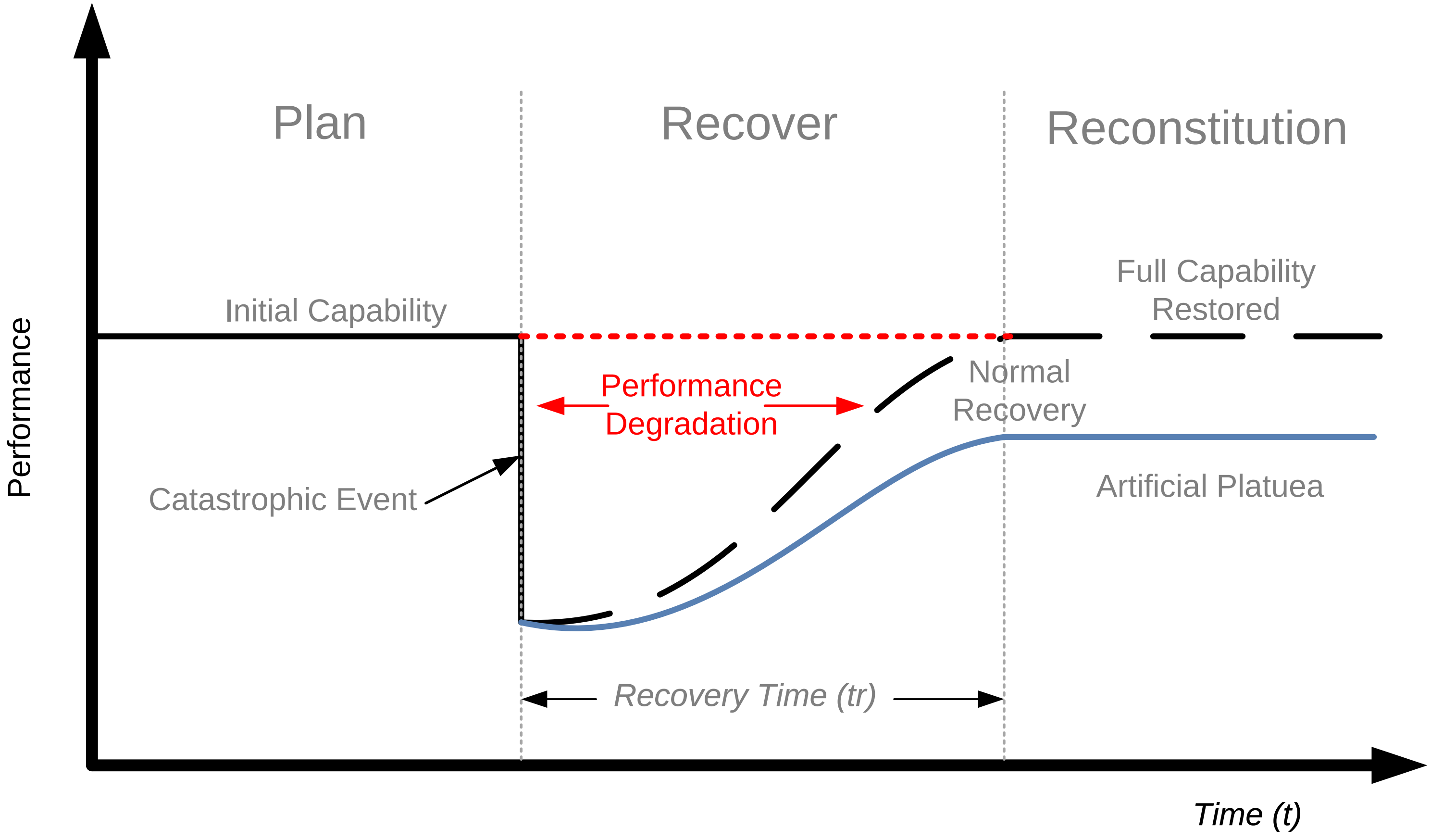
Generic Behavior



Recovery & Reconstitution After a Disturbance

Archetype of Resilient Behavior

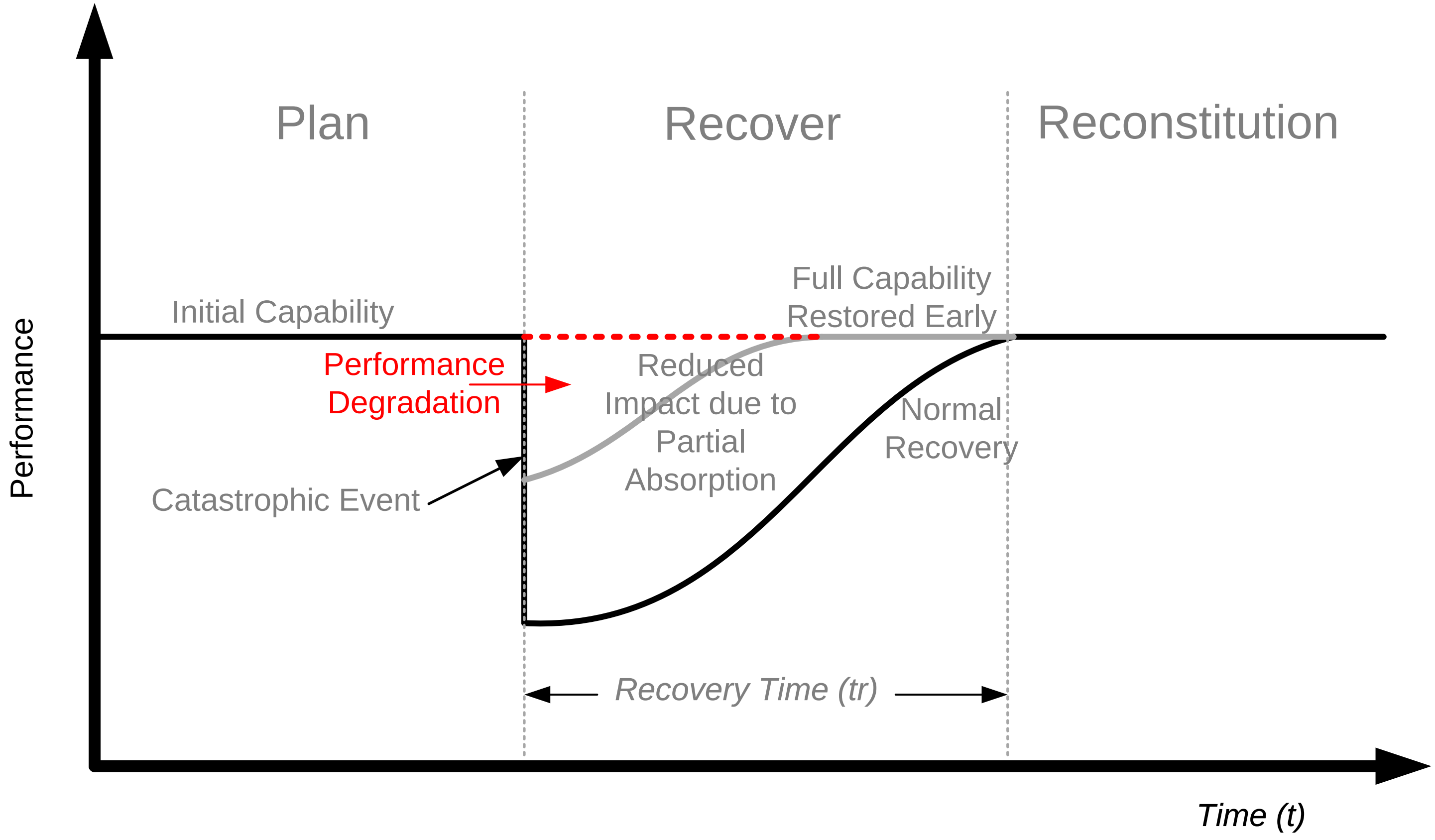
Artificial Plateau



<u>Artificial Plateau</u> - System does not recover to original performance level.

Archetype of Resilient Behavior

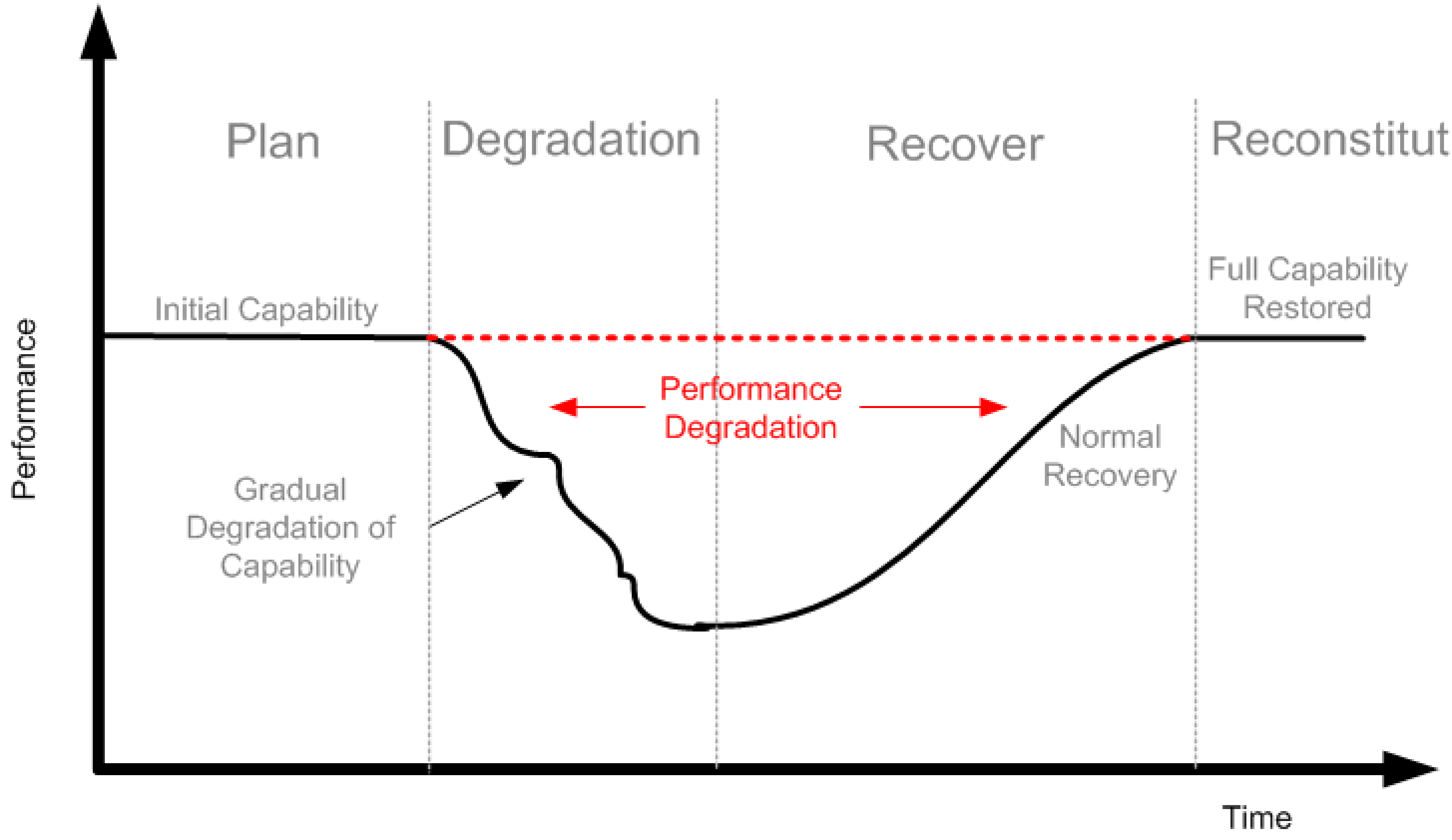
Partial Absorbtion



Normal Recovery after a Partially Absorbed Disturbance

Archetype of Resilient Behavior

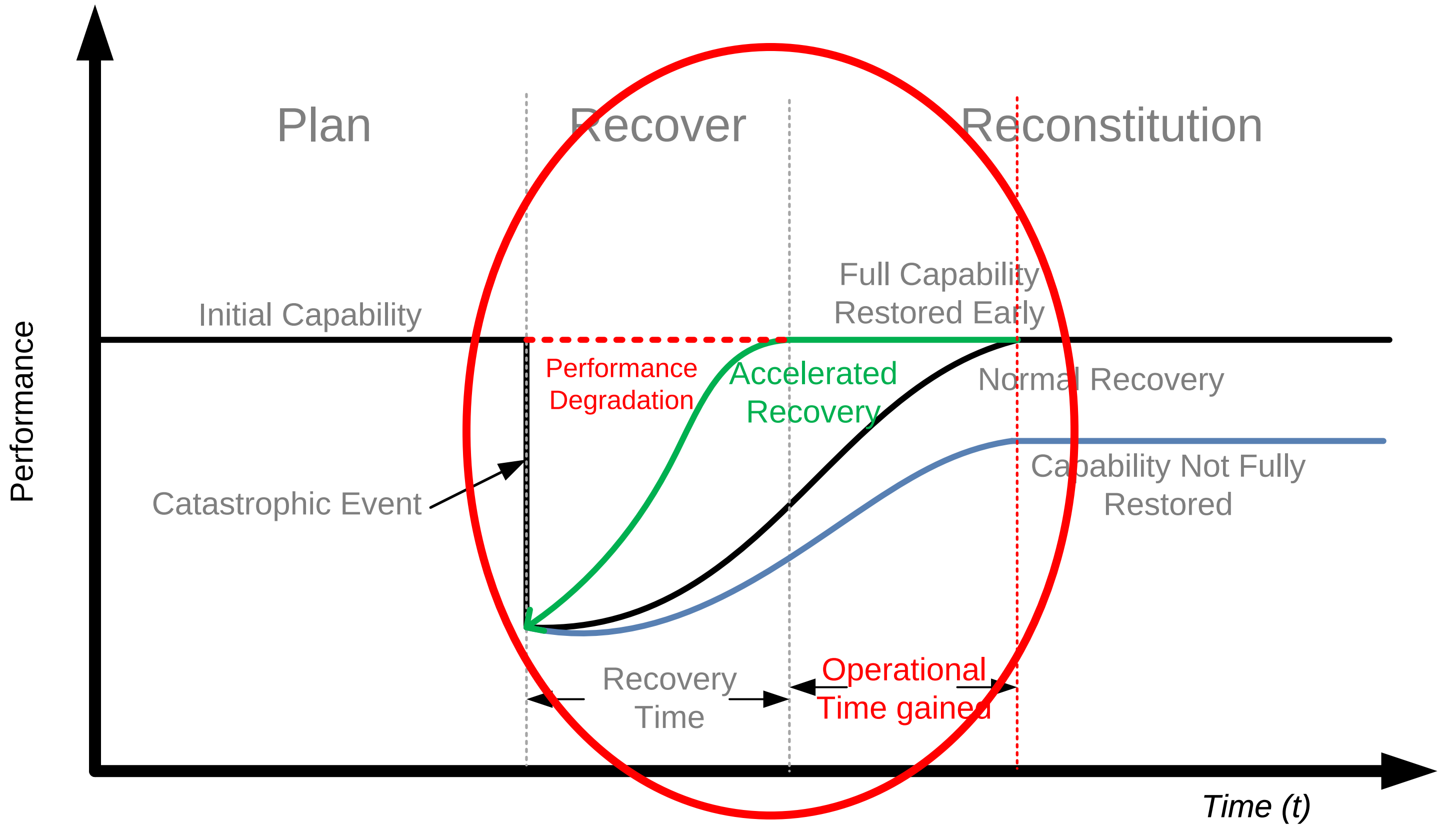
Gradual Degradation



Gradual degradation of capability, followed by recovery.

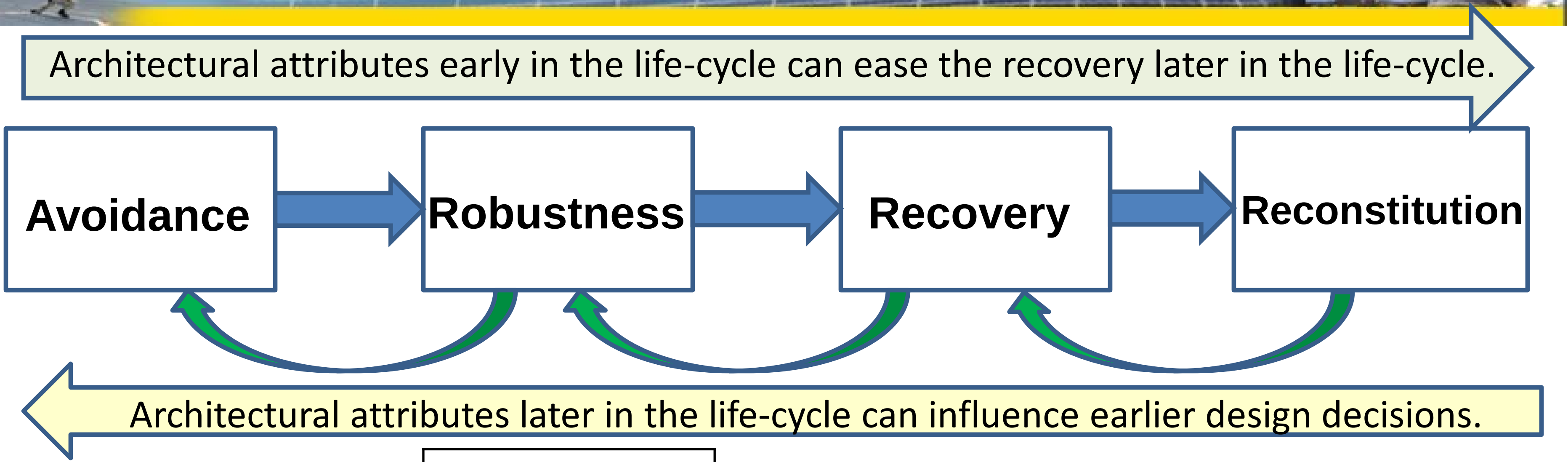
Archetype of Resilient Behavior

Accelerated Recovery



How is Accelerated Recovery Achieved?

Causal Relationships in Resiliency



Architectural attributes early in the life-cycle can ease the recovery later in the life-cycle.

Architectural attributes later in the life-cycle can influence earlier design decisions.

- Operational Flexibility
- Policy and Procedures Flexibility
- Loose coupling
- Extendibility

- Physical Redundancy
- Functional Redundancy
- Distributed
- Reduce Complexity
- Disaggregation
- Diversified

- Reduce Complexity
- Repairability
- Reorganization of System or SoS.

- Repairability
- Replacement
- Logistical Solvency

Research Overview

- Define, model, and investigate the attributes of resilient architectures
- Determine which architectural attributes are most important for a given system
- Determine the architectural drivers, and establish measurable goals during recovery periods
- Explore how causal relationships of architectural attributes can enhance the system throughout the resiliency life-cycle

Questions