National Institute of Standards and Technology
U.S. Department of Commerce

PCAST Cyber Resilience Panel Nov 9, 2022

Physical and Cyber Resilience of the Built Environment

Therese McAllister, PhD, PE, F.SEI, Dist.M.ASCE

Acting Chief, Materials and Structural Systems Division

Engineering Laboratory

Community and Cyber Resilience

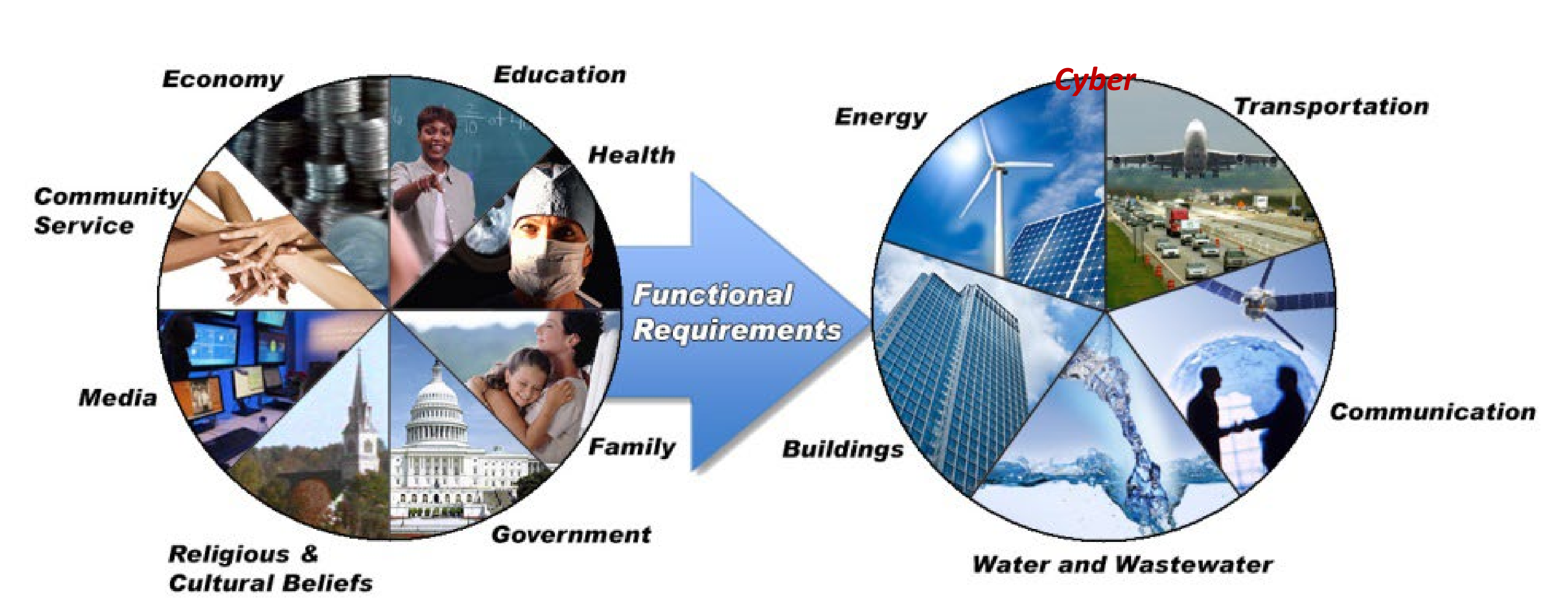
Resilience is the ability to ***prepare for*** and ***adapt to*** changing conditions and to ***withstand*** and ***recover rapidly*** from disruptions.

Community resilience goes beyond risk and includes recovery of functions in a specified timeframe.

NIST SP 1190
Community Resilience Planning Guide for Buildings and Infrastructure Systems

Cyber resilience addresses adverse conditions, stresses, attacks, or compromises of systems enabled by cyber resources.

NIST.SP.800-160
Engineering Trustworthy Secure Systems



Key Concepts for Infrastructure Resilience

Context

Role in the community, including recovery.

- How does it support community functions?
- What are appropriate performance goals and metrics?
- Which mitigation and recovery concepts best provide optimal resilience?

Recovery of Function

Time to recovery and community social needs

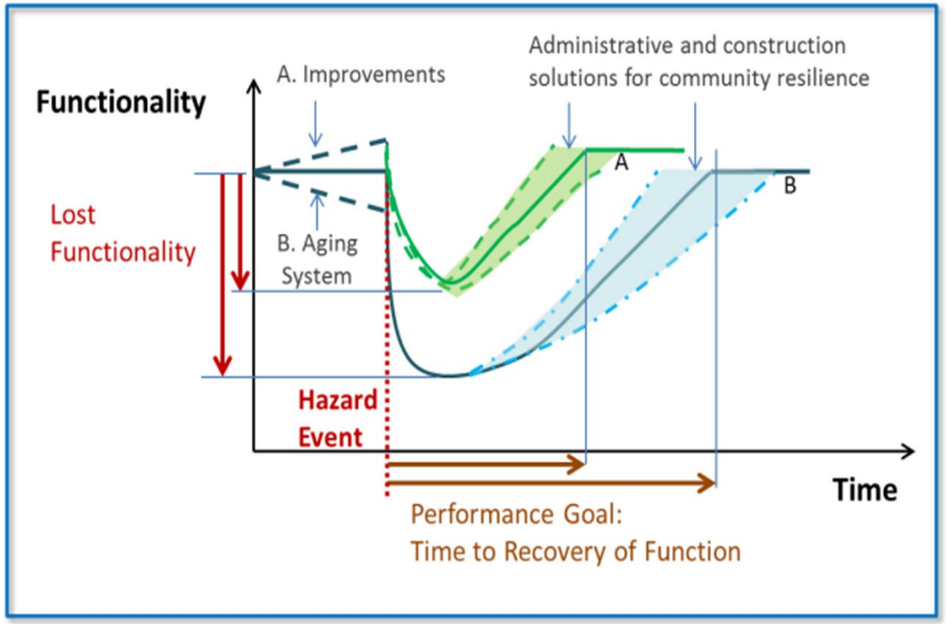
- Can recovery of function be met with temporary measures?
- Does function change over time during recovery?

Interdependencies

No system is an island.

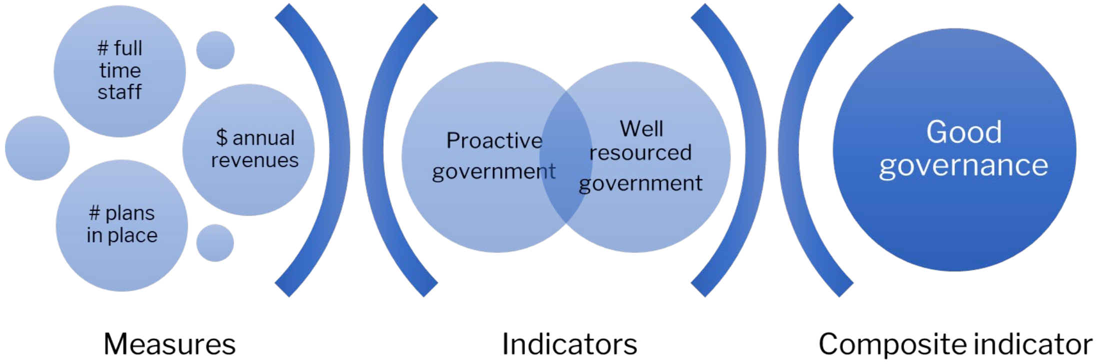
- What other systems depend on this system?
- What can be done to reduce dependencies during recovery?

New Orleans Flooding in 2005 (FEMA)



System Functionality vs Time

Telecommunication Metrics



Availability - the percentage of time a system is accessible for use. The best communications networks have 99.999 % availability (unavailable for ~ 5 minutes/year).

Reliability is the probability of successfully performing an intended function over a given time period (the complement to frequency of downtime).

- For a series of short service disruptions, a network may have high availability and reduced reliability (i.e., increased frequency of service failure).

Resilience includes the ability of a system to prepare for anticipated hazards, adapt to changing conditions, and withstand and *recover rapidly* from disruptions.

- *Recovery* may include plans to rebuild infrastructure to improve network availability and reliability.

Capacity is the volume of calls, texts, and other transmissions that can be reliably transmitted.

- After hazard events, the demand may exceed system capacity during *recovery*.

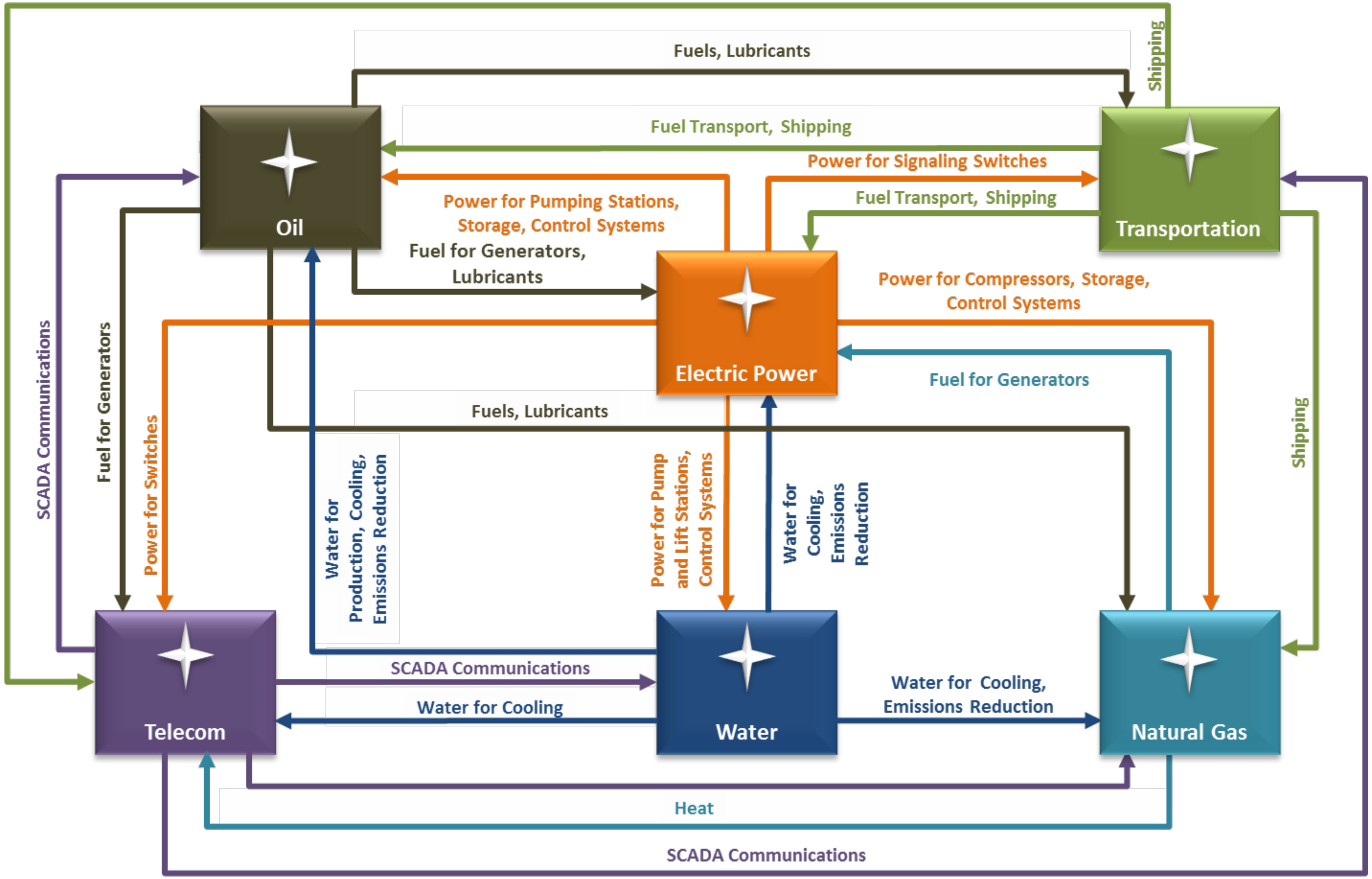
Interdependencies

NIST

Types (internal, external, source, spatial, temporal)

Spatial (national, regional, local)

Temporal (hours, days, weeks, months)



Example of External Dependencies

NIST SP 1190

Critical Infrastructure – 2012 Hurr Sandy

Data Centers

- After ConEdison proactively turned off power, batteries provided power until fuel arrived for generators.
- Mechanical/electrical equipment in basements were destroyed.

Wastewater Treatment Plants (WWTP)

- WWTP sites had not flooded previously, even with proximity to water bodies.
- Pre-event planning included de-energizing systems to reduce damage.
- The 12-ft storm surge rapidly inundated the WWTPs before proactive actions could be taken. Damage units included transformers, switchgear, communication, SCADA systems, electronic controls, etc.
- Local power was restored within 2 days but damaged power systems required extended use of emergency power.

“At one flooded gas station, personnel … said that because their fuel company required a data link for all sales transactions, cash sales could not have been completed even if they had generator power for the fuel pumps.”

FEMA P-942

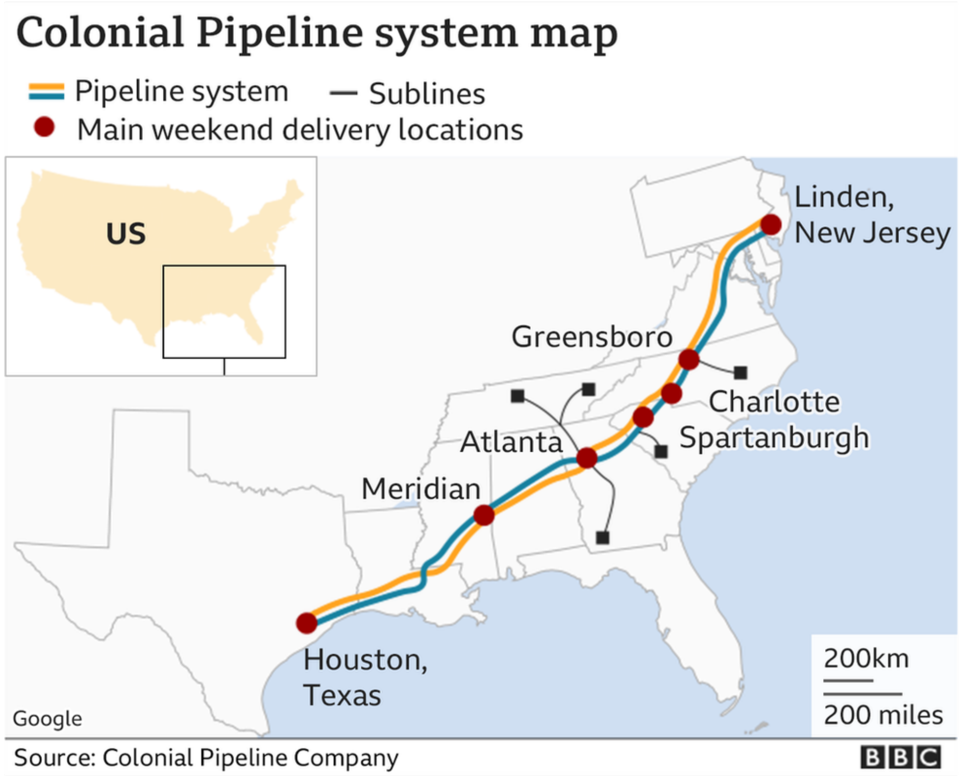
Generators to replace failed basement generators at a data center

Subgrade WWTP electric systems damaged by floodwater

Colonial Pipeline – 2021 Cyber Attack

NIST

- May 7 cyberattack on business systems.
- To ensure the safety of the pipeline, systems that monitor and control physical pipeline functions were proactively disconnected, halting pipeline operations.
- May 13 pipeline/product delivery resumed.
- Fuel supply disruption – e.g., 10,000s spent hours in gas lines.
- Subsequently, Congress passed cyber requirements for critical infrastructure firms — obligating them to alert the government within 3 days if hacked and within 1 day if ransom paid to hackers.
- Hackers never reached the operational technology systems but caused so much panic by locking up IT systems that operators shut down the pipeline anyway.



https://www.bbc.com/news/technology-57063636

Data and Metrics

Organizations should err on the side of reporting any cybersecurity incidents they experience to the Cybersecurity and Infrastructure Security Agency, even if they seem small or inconsequential, according to an agency official discussing a rule CISA must publish to implement the Cyber Incident Reporting for Critical Infrastructure Act.

https://www.nextgov.com/cybersecurity/2022/11/cisa-leaning-toward-lower-threshold-mandatory-cyber-incident-reporting/379370/

Resilience Measurement Challenges

Metrics

- Indicators and metrics for resilience goals vs project status
- V&V of indicators and metrics

Data

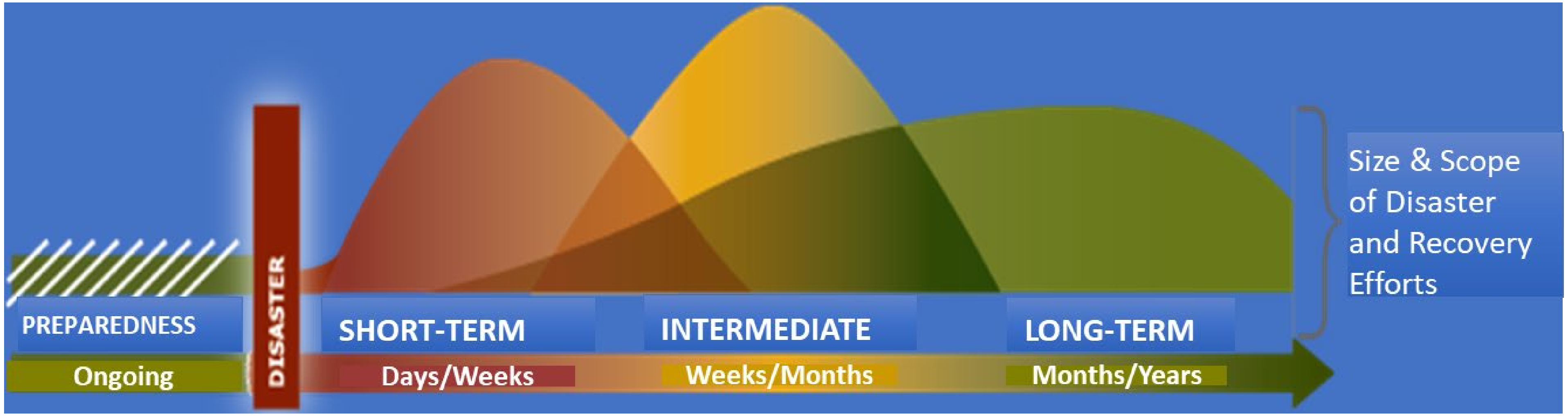
- Varying spatial and temporal scales of data
- Lack of data, especially for recovery

Models

- Integrated physical/cyber, social, economic data and analyses
- Systems of systems interdependent performance
- V&V systems of sytems models

Decision Support

- Short and long-term decisions, before and after disruptive events
- Uncertainty in model outputs and metrics



Questions?

The Resilience Paradigm Shift

Resilient physical and cyber systems require functional recovery:

- Critical functions are immediately available.
- Housing, schools/daycare, and businesses are functional and operating shortly after disruptive events.
- Recovery is equitable across districts and demographics.

Social functions depend on the built environment:

- Housing comprises 70% of all buildings (with 80% single family homes and 15% multi-occupant).
- Small businesses employ ~47 % of the population.
- People cannot work if their children are not in school or daycare.

- **Assessments and design practices:**
  - Need to address both of these interdependent requirements.

Lumberton, NC Water Treatment Plant Inundation from Hurricane Matthew in 2016

Designing for Resilience

A Physical-Cyber Systems Approach

- **Engage with system design team early**
  - Identify hazard scenarios causing physical damage
  - Identify cyber damage scenarios
  - Identify reliability, risk, and recovery goals
- **Incorporate resilience goals in the system design**
  - Develop trustworthy secure cyber systems
  - Consider interdependencies
  - Consider system role in recovering community social and economic functions
- **Minimize damage, losses, and recovery time**
  - Plan for redundancy and back-up options
  - Reduce and manage cyber system complexity
  - Limit damage to being repairable within a specified time


2018 Camp Fire


2013 Moore Medical Center, OK


2011 Fukushima Tsunami (PDH Engineer)

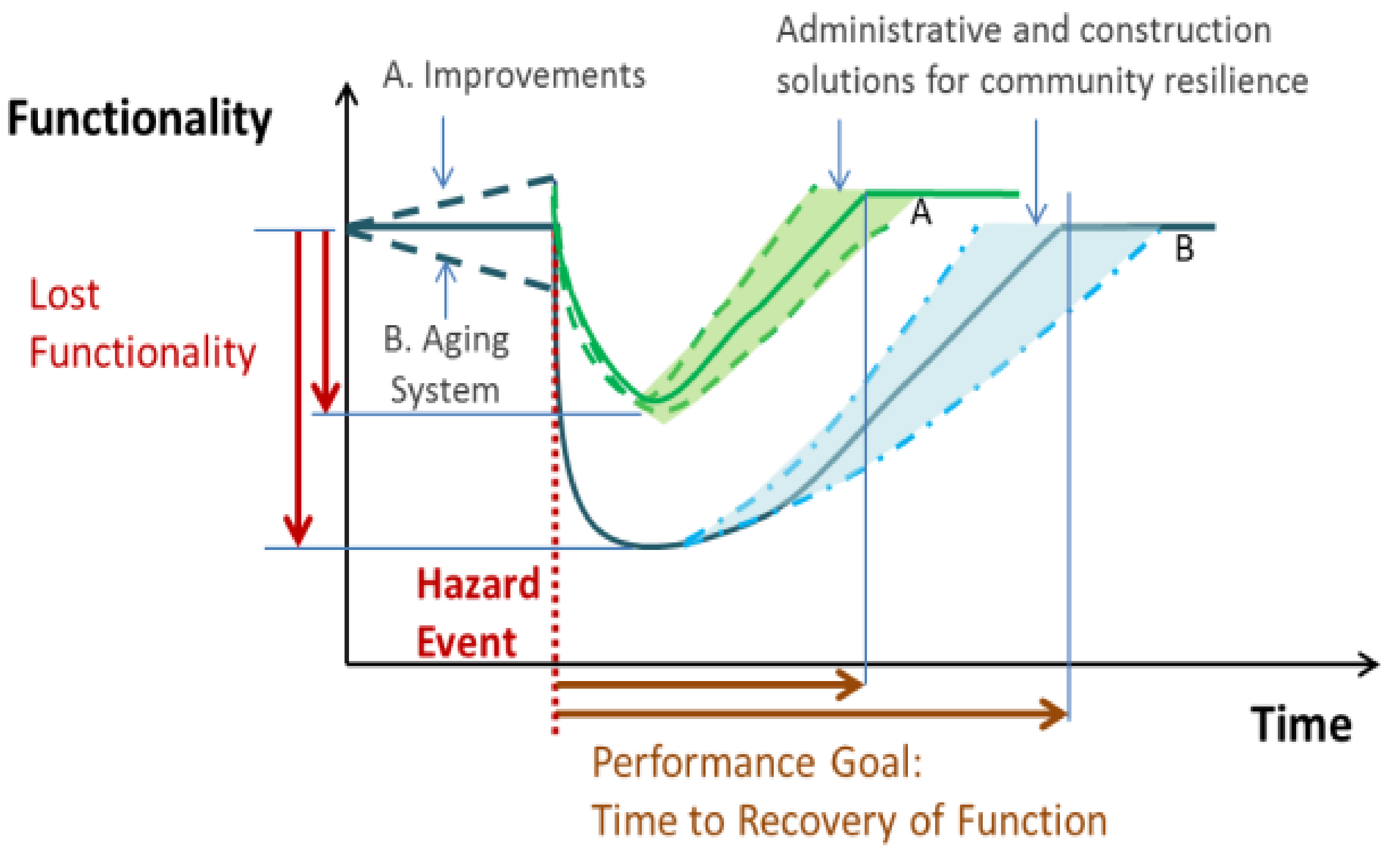
Cyber Resiliency

A Systems Engineering Perspective

- Adopt a multi-dimensional protection strategy.
- Employ design principles to develop trustworthy secure systems that are resilient.
- Reduce and manage system complexity.
- Incorporate assurance arguments to verify and validate system designs.
- Focus on mission success.

- NIST SP 800-160, Volume 1
  Engineering Trustworthy Secure Systems
- NIST SP 800-160, Volume 2
  Developing Cyber Resilient Systems

Recovery of Functionality



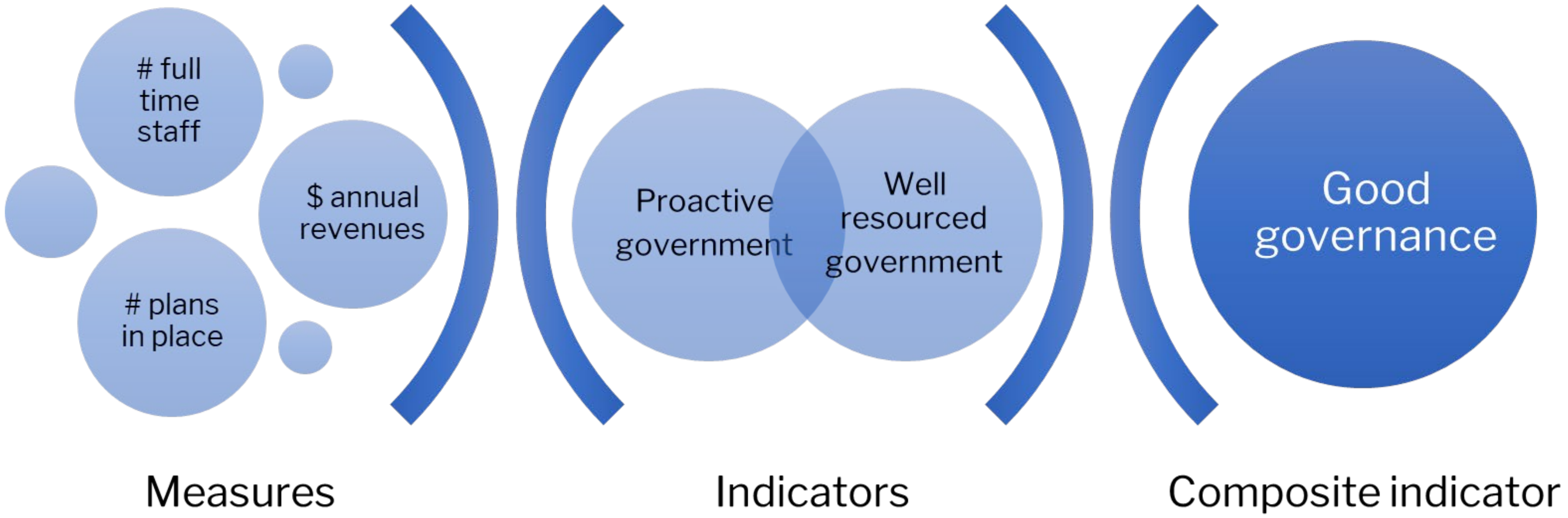
Source: NIST SP-1190

Functionality is a measure of how well a building or infrastructure system operates, delivers its required services, or meets its intended purpose.

Time to recovery of function is a measure of how long it takes before a building or infrastructure system is functioning after a hazard event.

FEMA P-2090/NIST SP-1254
Recommended Options for Improving the Built Environment for Post-Earthquake Reoccupancy and Functional Recovery Time

Resilience Measurement Science



- Commonly used data/measures and indicators for physical, social, and economic systems
  - Is there data/measures of system performance for recovery of functionality?
- Data dependencies (and correlations)
- Methodologies for combining measures for indicators
- Validation methodologies

https://www.nist.gov/community-resilience/assessment-products

Resilience Time-Based Metrics

Performance Gaps

- Difference in time to ***functional recovery***
- Informs **prioritization** of projects

Summary Performance Goals Matrix

Summary Resilience Table	Design Hazard Performance								
	Phase 1: Short-Term			Phase 2: Intermediate			Phase 3: Long-Term		
	Days			Weeks			Months		
	0	1	1-3	1-4	4-8	8-12	4	4-24	24+
Critical Facilities									
Buildings	90%							X	
Transportation		90%	X						
Energy		90%	X						
Water			90%		X				
Wastewater				90%				X	
Communication	90%			X					

Desired Performance

Gap

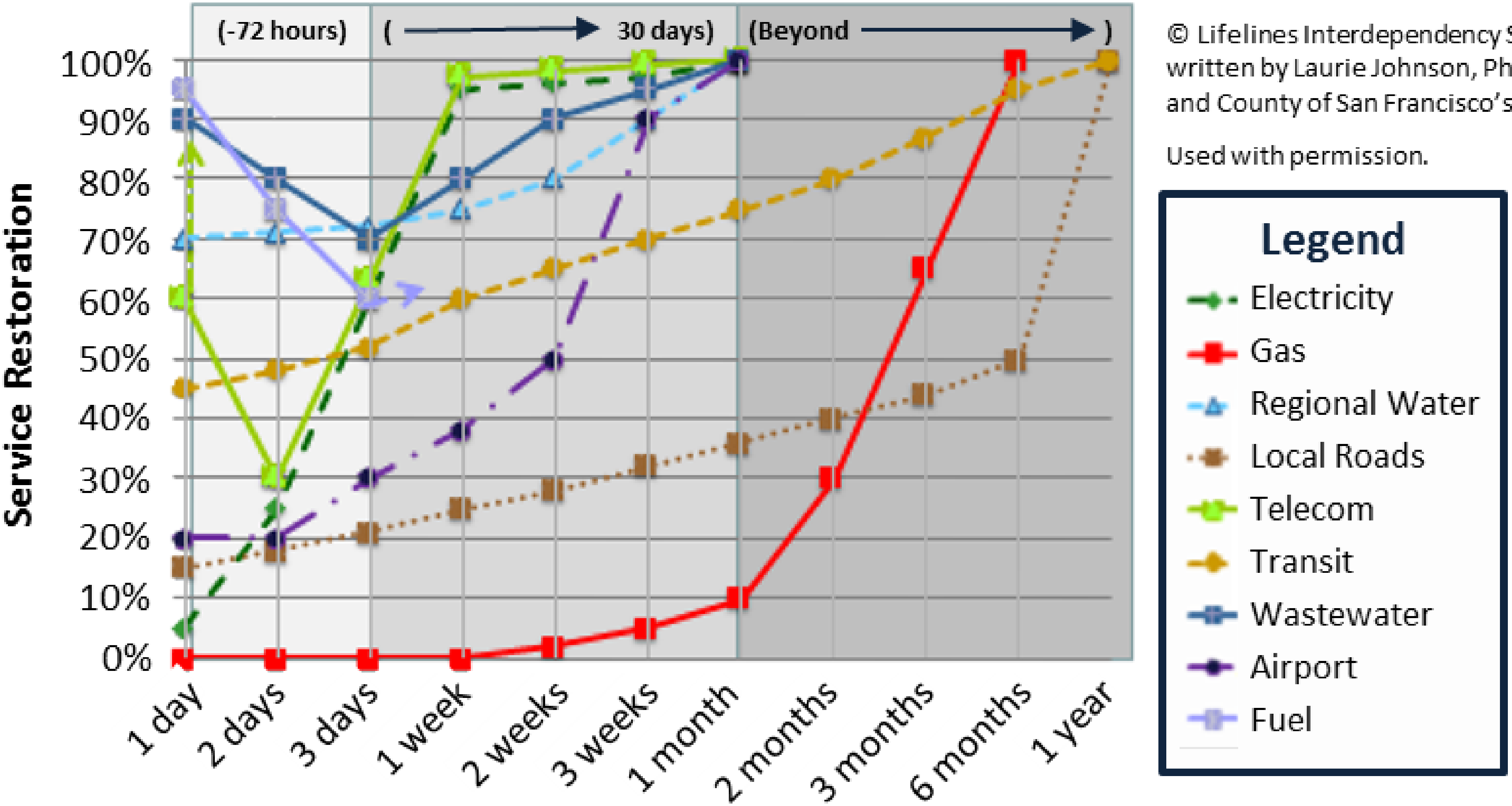
Anticipated Performance

NIST SP-1190

SEAOC 2020-08 Newsletter

Potential Service Recovery Times for EQ Event

- Identifying dependencies is a developing area of resilience planning. Empirical methods based on historical data is one approach to address dependencies during recovery. This method was used for the City and County of San Francisco Lifelines Council [The Lifelines Council, City and County of San Francisco 2014].



© Lifelines Interdependency Study, April 2014, written by Laurie Johnson, Ph.D. AICP for the City and County of San Francisco's Lifeline Council.

Used with permission.

NIST SP 1190