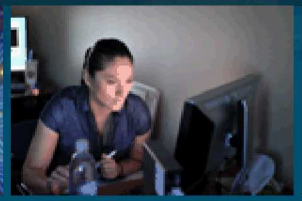
Operational Resilience



PRESENTED BY

Timothy Berg, DPhil (tberg@sandia.gov)

Acknowledgement: Eric Vugrin, SNL Cyber Resilience

SAND2018-12869PE

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

Topics

1. Why resilience for freight?
2. Approaches to improving resilience
3. Examples of the science and engineering of resilience
4. Cyber resilience research

The Continuity of Road Freight is a National Priority

Transportation is one of sixteen named US critical infrastructures

- "…whose assets, systems, and networks, whether physical or virtual, are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety…" (DHS)
- Many of the other fifteen depend upon transportation, e.g. agriculture and food, military, manufacturing, emergency services
- The current national cybersecurity plan names seven priority areas for risk reduction, including transportation

The continuity of freight traffic is also critical to… freight business success

- The goal of resilience planning is the discovery of superior business strategies
- Resilience investments are tied to meeting objectives under varying operating conditions
- Transportation resilience impacts many downstream customers

Operational Resilience is a Best Business Practice

Critical infrastructure resilience depends upon resilient civilian operations

Why Operational Resilience?

Transportation resilience is not a new concept

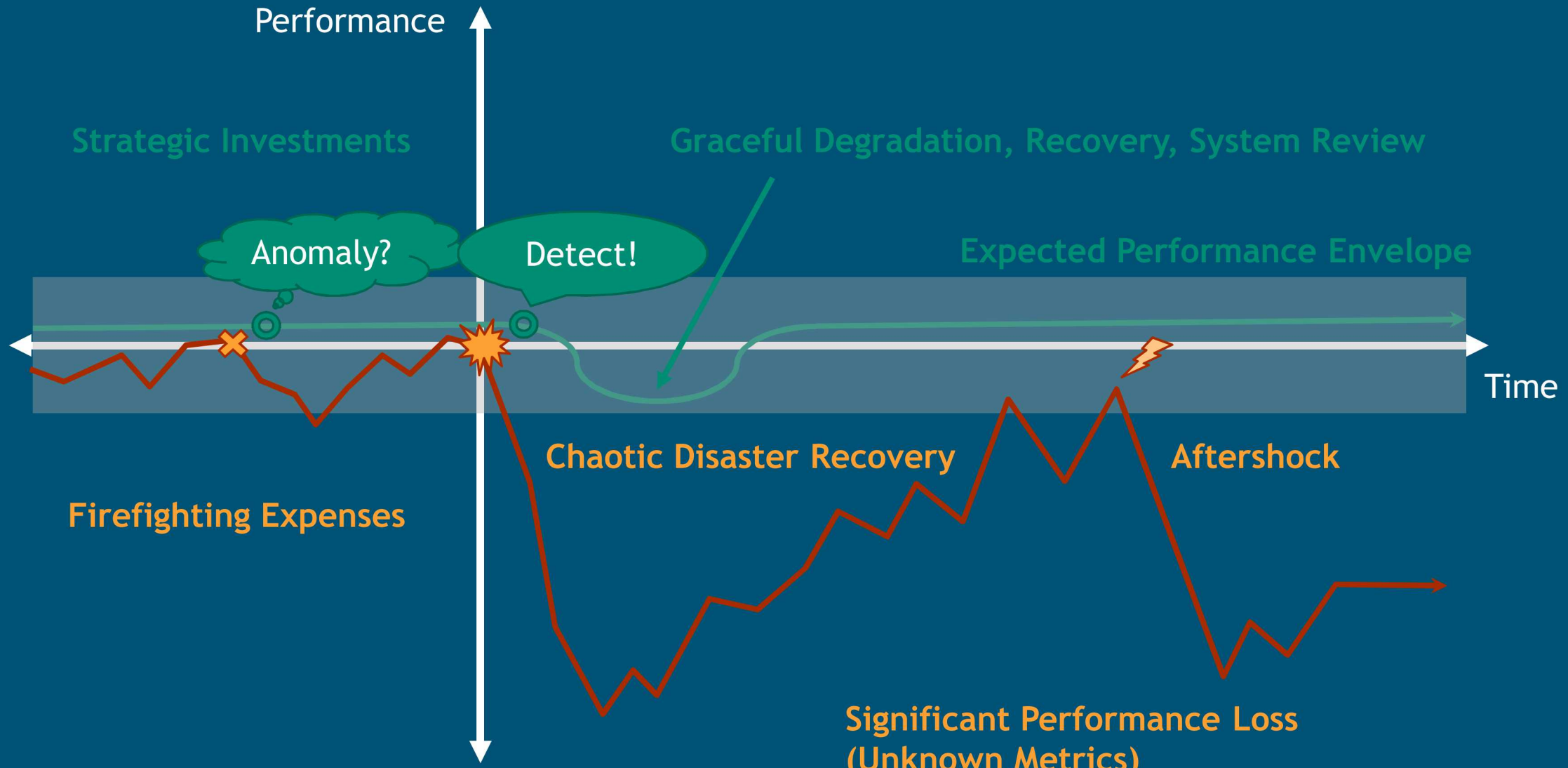
Resilience **is** the ability to withstand, adapt to, or recover from disruptions

Disruptions, especially cyber disruptions, will happen

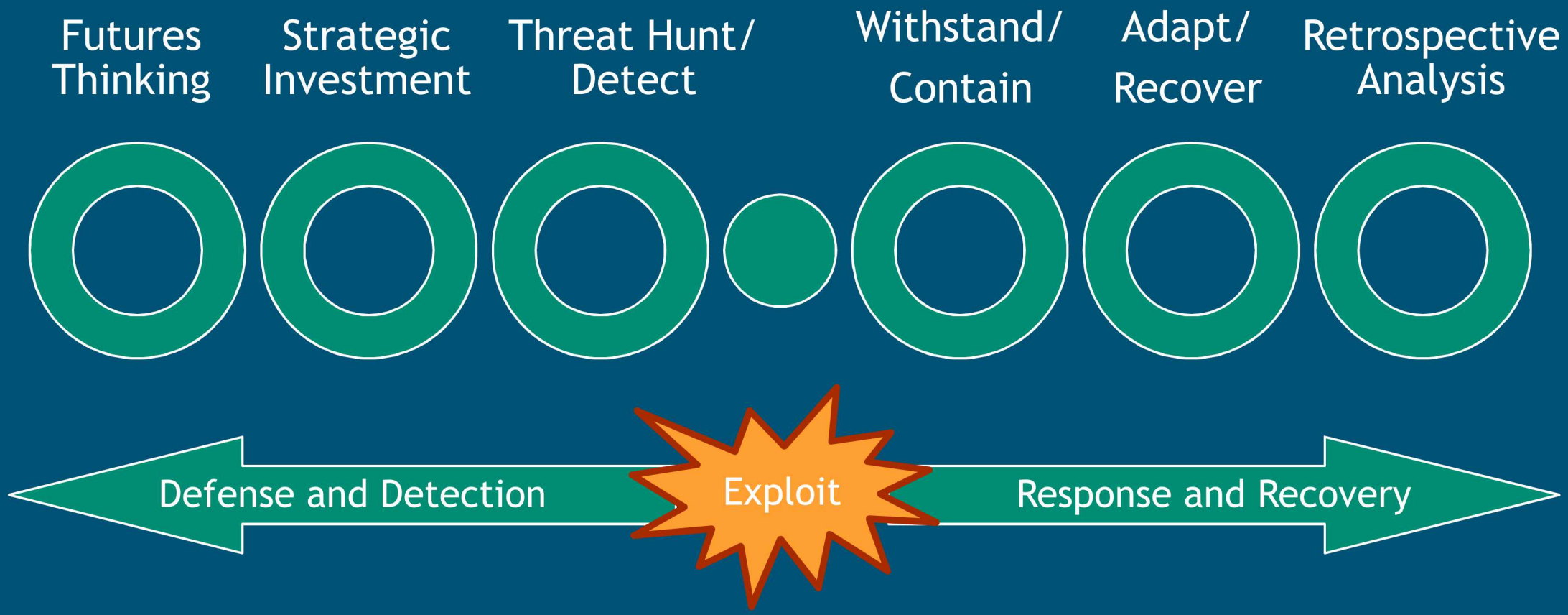
The lack of catastrophic transportation events paradoxically creates a false sense of security (National Academy of Sciences)

Security + Resilience = Comprehensive Risk Management Strategy

Two Business Continuity Journeys



Invest Strategically "Pre-Bang" to Maximize Resilience "Post-Bang"



Does the system suffer similar vulnerability to exploitation elsewhere?

Resilience Based on Attributes and Attribute Analysis

- **Prevention**: "A dollar in prevention is worth four in recovery"
- **Recoverability**: How to pre-position for response and return to "normal"
- **Resilience**: It happened, now what?
- **Response**: What are the best actions to take with the available resources
- **Robustness**: Investments to withstand and minimize impacts, e.g. CA earthquake building codes
- **Security:** Protect the "inside"
- **Sustainability**: How long is the current approach tenable?
- **Threat based**: What is being protected, from what, how likely is the scenario, and what would be the impacts?

Resilience can also be addressed using science and engineering

Two Resilience Approaches

	Attribute Based "Qualitative"	Performance Based "Quantitative"
Central Question	What makes the system resilient? - Assumes certain characteristics do	How resilient is the system? - Assumes metrics can be developed
Analyzes system…	Attributes to identify strengths	Outputs via quantitative metrics
Advantages	Limited data required Links outputs to defined attributes	Data driven objectivity Metrics allow cross-system comparisons
Limitations	Inherent subjectivity Missing link from attributes to performance	Does not explain "why?" Quantities may be too abstract Can be model specific
Example	Mapping of framework controls, e.g. do you have evacuation plan and how often do you execute it?	Freight model scenario 'what-if' analyses, e.g. hurricane of x mph with y storm surge causes z damage under scenario

Performance + Attribute = Comprehensive Process

An Integrated Process Designed to Yield Useful Results

Iterative Process:

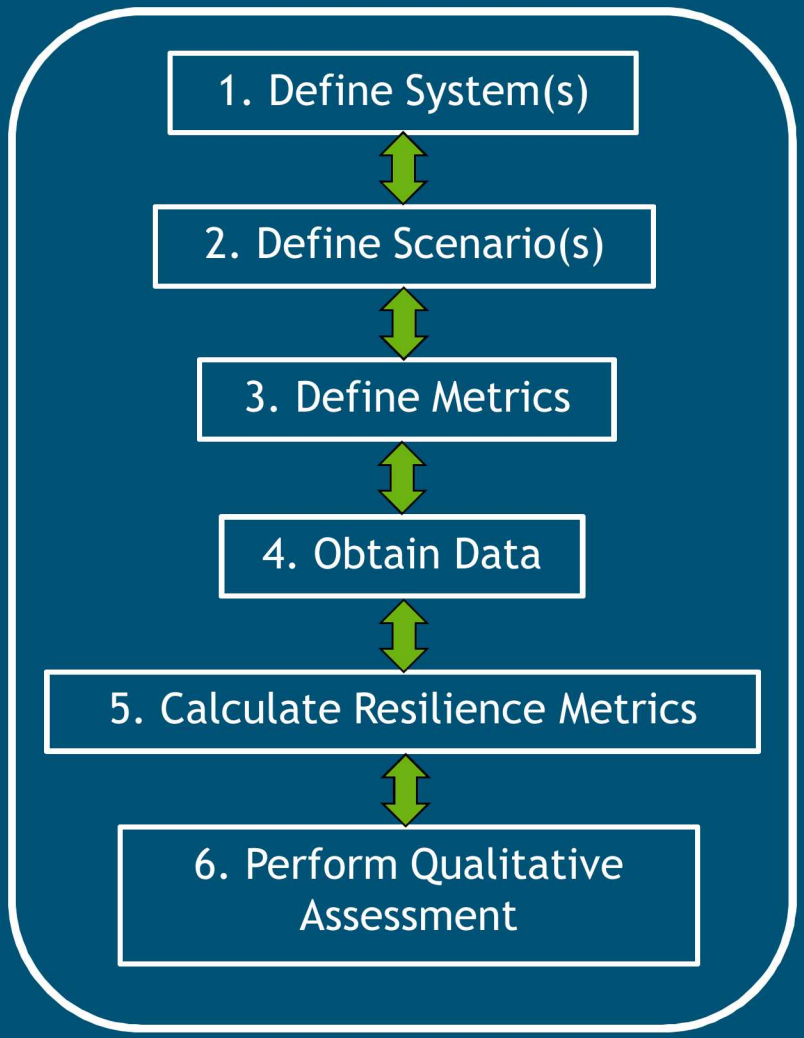
1. System objectives, boundaries, components, resources to include

2. Choose hazards; time, location; affected system components; extent of physical and functional damage; cascading impacts; spectrum of responses, resource requirements; when is recovery complete

3. System performance and recovery metrics, system performance targets

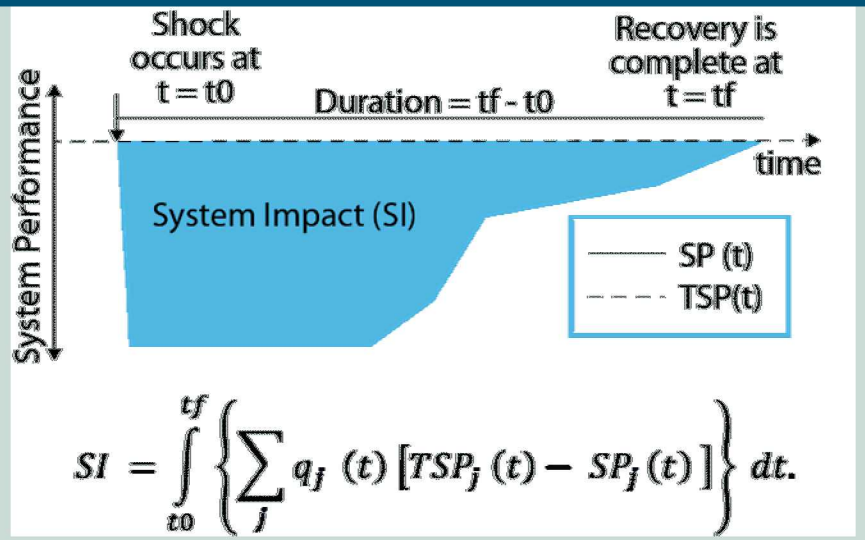
4. Obtain performance and resource usage data. Use historical, simulated, expert judgement derived data

6. What features led to the results (absorptive, adaptive, restorative). How to improve the system?

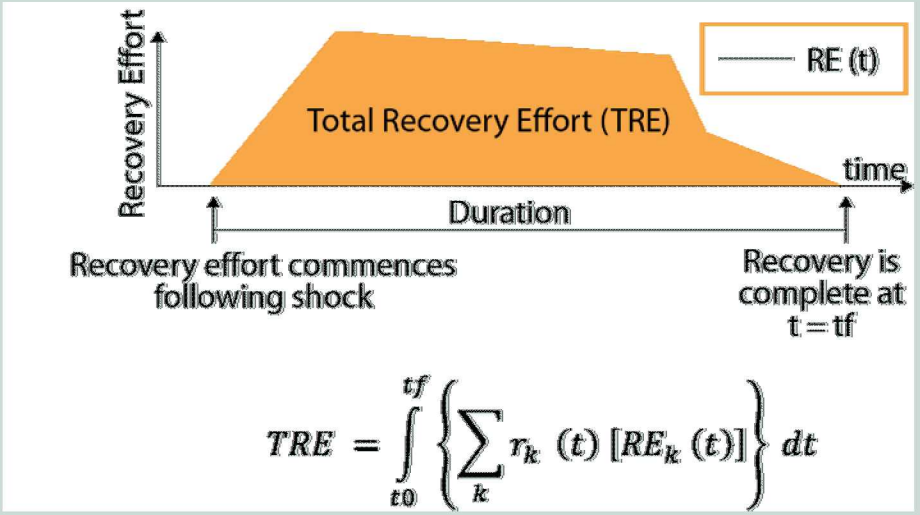


Performance: Resilience Represented Mathematically

"Given the occurrence of a particular, disruptive event (or set of events), the resilience of a system to that event (or events) is the ability to reduce efficiently both the magnitude and duration of the deviation from targeted system performance levels." (Vugrin et al. 2010)



$$SI = \int_{t0}^{tf} \left\{ \sum_{j} q_j\ (t) \left[TSP_j\ (t) - SP_j\ (t) \right] \right\} dt.$$



$$TRE = \int_{t0}^{tf} \left\{ \sum_{k} r_k\ (t) \left[RE_k\ (t) \right] \right\} dt$$

Control-Theoretic Metrics (Vugrin et al.)

Performance-based measures can inform trade-off and design analyses using existing models

Attribute Analysis: Three Capacities

	Absorptive Capacity	Adaptive Capacity	Restorative Capacity
Directly Impacts	Systemic Impact	Primarily Systemic Impact, but also TRE	Total Recovery Effort
Distinguishing features	Automatic manifestation after disruption	Reorganization and change from standard operating procedures	System repair
Temporal Sequencing	First line of defense	Second line of defense	Final line of defense
Post-disruption event required	Automatic/little effort	Increased effort	Greatest effort
Duration of changes	Permanent	Temporary	Permanent
Resilience enhancement feature examples	Stored inventory; robustness; redundancy; segregation	Substitution; rerouting; conservation; reorganization; ingenuity	Advance warning and monitoring systems; pre-positioning; reciprocal aid agreements

Example Steps 1 and 2: Rail Network Recovery Sequence Optimization

Central Question:

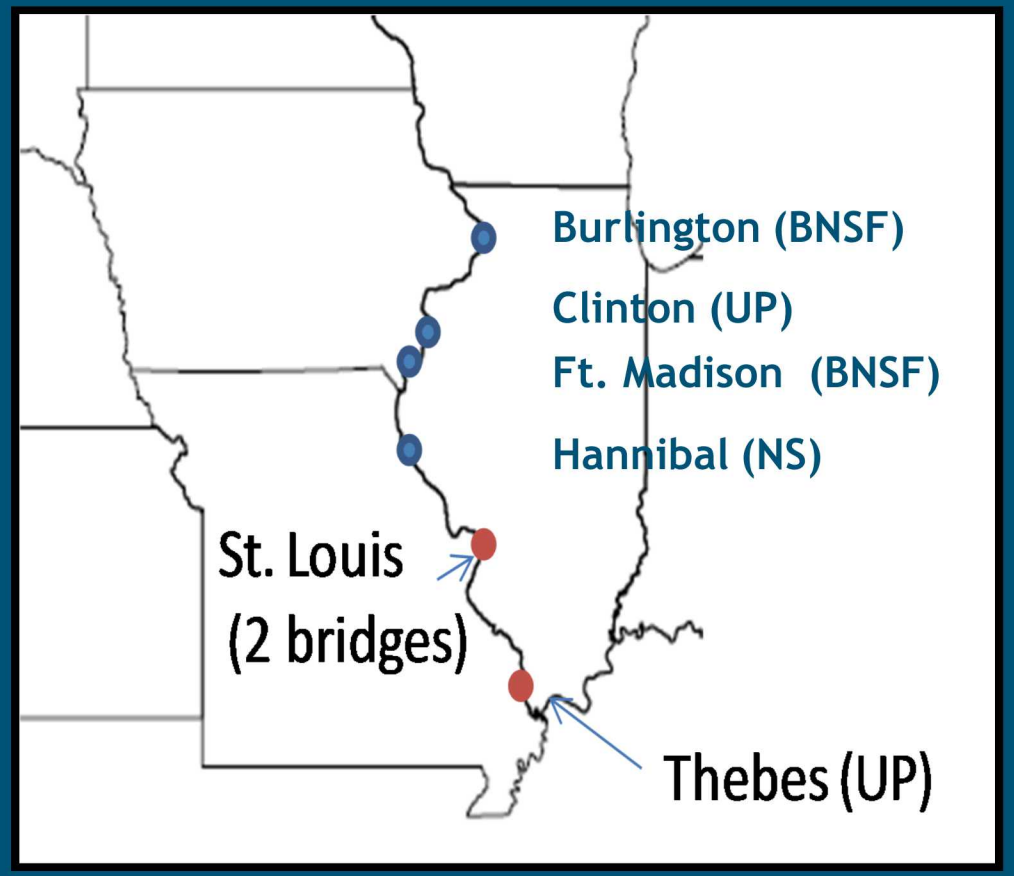
"What optimal recovery sequence maximizes rail carrier flooding event resilience, given limited recovery resources, multiple recovery modes, and multiple restoration sequences?"

System:

- US freight rail system

Scenario:

- 4 flooded rail bridges on northern Mississippi
- 3 bridges unaffected
- East-West rail traffic significantly affected
- Chicago is the largest east-west interchange point
- Disrupted traffic between Chicago and Kansas City
- Disrupted traffic between Omaha and Denver



Step 3: Identify System Performance Metrics and Recovery Costs

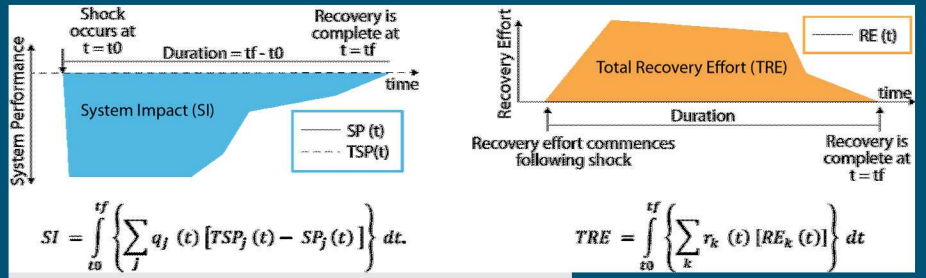
System Performance (SP)= daily revenue from carload movement Iowa, Illinois, Nebraska, Kansas and Missouri

- TSP = "nominal" daily revenue from carload movement
- SI = lost revenue from carloads not moved

Total Recovery Effort (TRE): cost of rerouting plus recovery activities

- Additional operating costs from increased time
- Additional operating costs from increased distance
- Bridge repair costs

Category	Variable	Cost
Additional car-miles	ACM	$1.50/car-mile
Additional Transit Time	ATT	$38/car-day
Carloads not moved	CNM	$1770/load
Bridge Repairs	BR	TBD



$$SI = \int_{t0}^{tf} \left\{ \sum_j q_j(t) \left[TSP_j(t) - SP_j(t) \right] \right\} dt.$$

$$TRE = \int_{t0}^{tf} \left\{ \sum_k r_k(t) \left[RE_k(t) \right] \right\} dt$$

$$SI = \sum_t \left[1770\, CNM(t) \right]$$

$$TRE = \sum_t \left[1.5\, ACM(t) + \frac{38}{24} ATT(t) \right] + BR$$

Step 4: Obtain Data (Adapted Existing Simulation Tools)

Adapted existing rail network model for dynamic simulation of recovery

Performed two level optimization over recovery sequences and costs

Employed simulated annealing and computational efficiency adjustments

Commodity Group	Additional Car-Miles	% Change	Additional Car-Hours	% Change	Not Moved
Coal	169929	2.9	294479	97.2	58
Grain	-26182	-2	6892	3.2	700
Chemicals	28220	1.6	14234	3.3	819
Intermodal	213801	15.4	31928	48	1146
Motor Veh	45550	3.2	61109	87.1	355
Other	88613	1.6	15616	1	2539
Total	519931	3	424258	15.9	5617

Daily lost revenue = $9.9 M/day
Cars moved decreases by > 1/3

Daily Additional Car Moves= $830k

Daily Additional Transit Time= $700k
Average additional car-hours increase: 16%
Nearly double for coal and motor vehicles

Steps 5 and 6: Calculate Recovery Costs and Compare Strategies

	Days To Complete Recovery	Systemic Impact	Total Recovery Effort
Cooperative Approach	24	$96M	$43m
Non-cooperative Approach	30	$176M	$48M

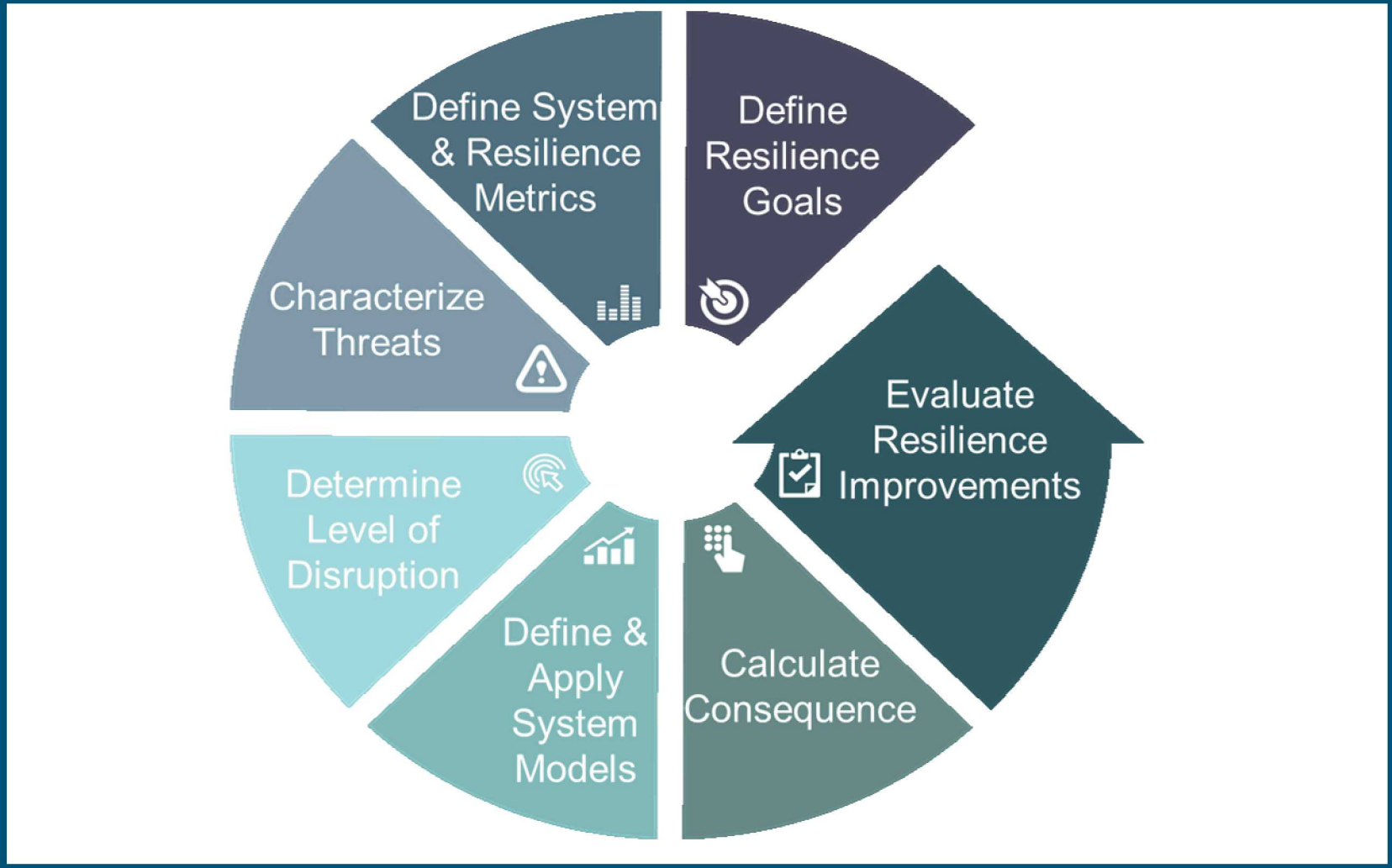
Cooperative approach is the superior strategy, improves:

- Time to recovery by 6 days and costs by $85M
- System Impact by 45% ($80M)
- Total Recovery Effort by 10% ($5M)

Example Attribute based analysis

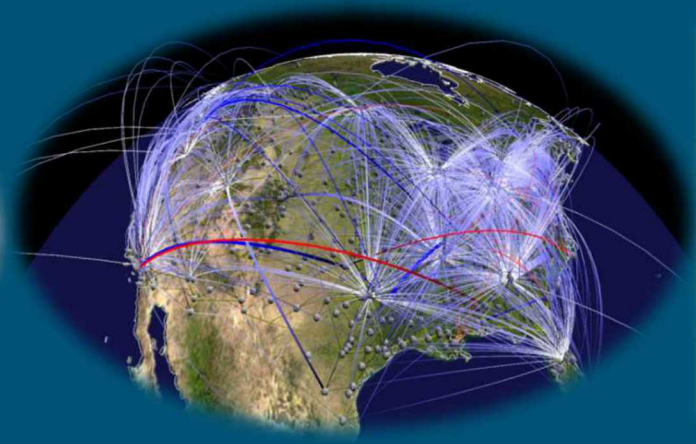
- What plans are in place that would enable use of this analysis?
- Are MOUs and government orders in place that would allow crisis cooperation?
- What mitigations could further improve recovery?

Performance Based Resilience for Quadrennial Energy Review



Watson et al. (2014) "Conceptual Framework for Developing Resilience Metrics for the Electricity, Oil, and Gas Sectors in the United States," *SAND 2014-18019*.

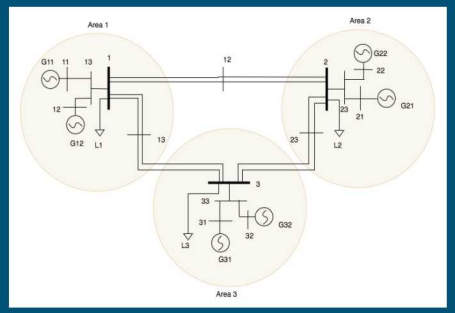
Many Different Kinds of Studies are Possible



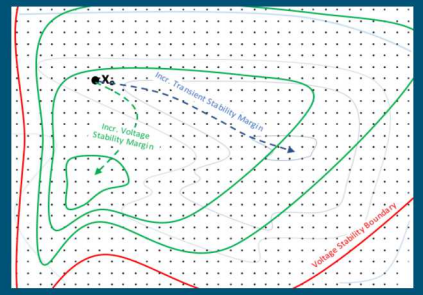
- **DHS Resilience Certification Study**: Resilience Star Building Certification. Energy Star Certifications show ROI through higher values, rents, and lower premiums. An assessed building is a better building
- **Shipping**: how to reroute marine/rail/road containers when bridges knocked out by floods? How well do routing algorithms work for recovering schedule and minimizing penalties?
- **Chemical Supply Chains**: How resilient are chemical supply chains to hurricanes?
- Many more: industrial control systems, security systems, cyber-physical systems, military systems

Research: Resilience Strategy Discovery With Machine Learning Assist

Grid Model
With Cyber Interface



Stability Calculations

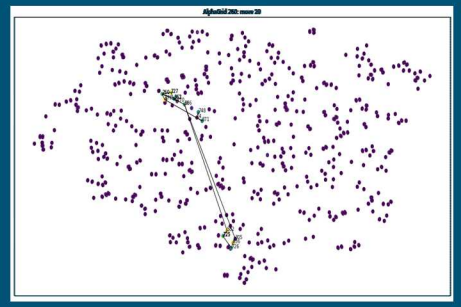


Stability Measures
12 dimensional model

Defender

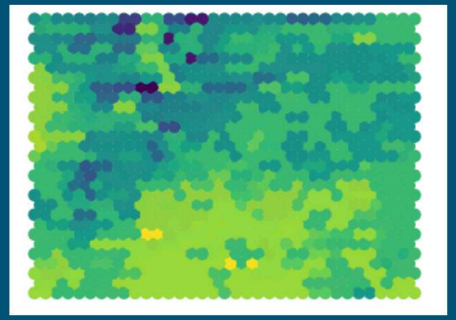
Attacker

Explore Game States
Random initially, then learns strategies



1. Learn Model

Rewards



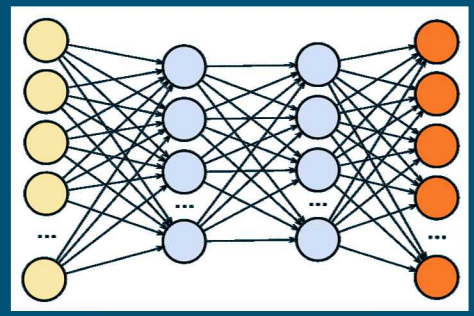
Game Play Data
Converges to playable game

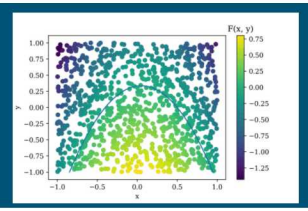
Game Play

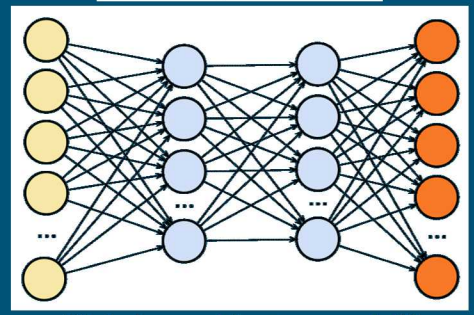
2. Rapid Self Play

3. Improve Networks

"Policy Network"
Probability distribution of possible moves







"Value Network"
Likelihood of win given board state

AlphaGrid: Uses AlphaGo AI engine to attack and defend a grid model. The goal is not automated response, rather preparing operators with scenarios and defense plans to use during incidents.

Road Freight Example 1-2: Systems and Impacts

Operational Disruptions:

Data Systems
- Enterprise system cybersecurity
- Supply chain, logistics, billing, scheduling disruption
- Cloud services, personal device use
- IoT, OT, asset tracking, smart building systems
- Data centers and backup

People
- Insider threat, policy compliance, errors
- Smuggling, pilfering, sabotage, tampering

Vehicles
- Telematics
- Vehicle denial of service, safety systems
- Wireless vulnerabilities
- Maintenance prediction and operations
- Accidents, misuse

Other:
- Severe weather events, terrorism, epidemics

Infrastructure
- Reliance on chokepoints, unreliable infrastructure
- Terminals, distribution centers, multimodal
- Road quality, congestion, weather dependencies
- Reliance on communications, mapping, GPS
- Fuel and grid reliance
- Manufacturing disruptions

Emerging Trends
- Labor and leasing market trends
- Automated competitors, assisted driving
- Data driven, digital integration of everything
- Environmental drivers, electric power trains

Impacts:

Losses: Life, property, financial, penalties, data, customers, productivity, opportunity, time reputation, public health, jobs, competitiveness

Accountability: regulations, insurance, legal

Road Freight Example: 1-2 Define the System and Scenario

Clarify the central question to be answered by the resilience analysis

Central question may be triggered by a range of formal or informal sources:

- Risk assessment and management process
- Incident or problem management activity
- Operations "hot wash", stand up meeting, business capture discussion
- A continuous improvement process discovery, e.g. Lean IT, Lean Six Sigma, etc.
- Strategic planning process
- Systems study on emerging risks
- Governance issue
- Decision making process arbitration
- Trade off analysis
- Investment prioritization process
- Programmatic comparison
- Regulatory requirement

Iterate until necessary system and scenario boundaries are well defined

Example: What recovery strategy minimizes (lost miles, recovery costs) for fleets of sizes 10, 100, 1000 class 8 trucks under disruption circumstances X, Y, Z

Road Freight Example: 3-5: Propose Solutions and Work the Numbers

Many businesses have most of the tools, they just need to ask the right questions

Key Metrics:

- What is the quantitative or monetary benefit for day to day operations?
- What is the maximum tolerable downtime for various critical services

Develop solutions to evaluate in resilience context

- Assets: How many spares is enough, too much
- Information Technology: Value of COOP site, hot site, warm site, cold site, backups, cloud services, PODs
- Take advantage of existing models and business tools for resilience
- Additional supply chains create redundancy in acquisition and in the field
- Use subject matter experts: internal, NMFTA, Auto-ISAC, National Labs, Universities
- Remember the humans in the loop and provide training and awareness
- Rotate employees for cross training and to limit mischief

Road Freight 6. Resiliency Attributes May Include Preparing Several Plans

- **Incident Response Plan**
  - Detect, manage and learn from cyber incidents
  - May be a tiered process with tiered response, e.g. major outage definitions and responses including "pull the plug"
  - Preservation of forensic evidence including logs and malware is non-trivial and can be critical
- **Business Continuity Plan (BCP)**
  - Overarching, umbrella term
  - Governance, Sr. Management and IT planning and coordination essential
- **Continuity of Operations Plan (COOP)**
  - Approach for restoring mission-essential functions, which need to be identified
  - COOP site investments provide many opportunities for personnel and equipment testing and development
- **Crisis Communications Plan**
  - Very important to have clarity on who is authorized to speak for company
  - Key issues around law enforcement engagement and customer notifications
- **Disaster Recovery Plan (DRP)**
  - Triggered by major disruptions such as successful ransomware attack
  - Supports the BCP or COOP plans with prioritized service restoration requirements
  - Testing of backup services and failovers to hot, warm, or cold sites difficult but critical

Summary

The continuity of road freight is a national priority

Operational resilience is a best business practice

Proactively addressing resilience enables partnering with infrastructure providers and others who stand to gain along with you.

The best outcomes occur when investigating resilience options results in identifying ways to improve both resilience AND increase the efficiency/reliability of operations under normal conditions

There are many ways to approach operational resiliency and many resources

Choose the approach most likely to yield usable results

Remember the humans in the loop

Resilience requires a continuous process of learning and improvement