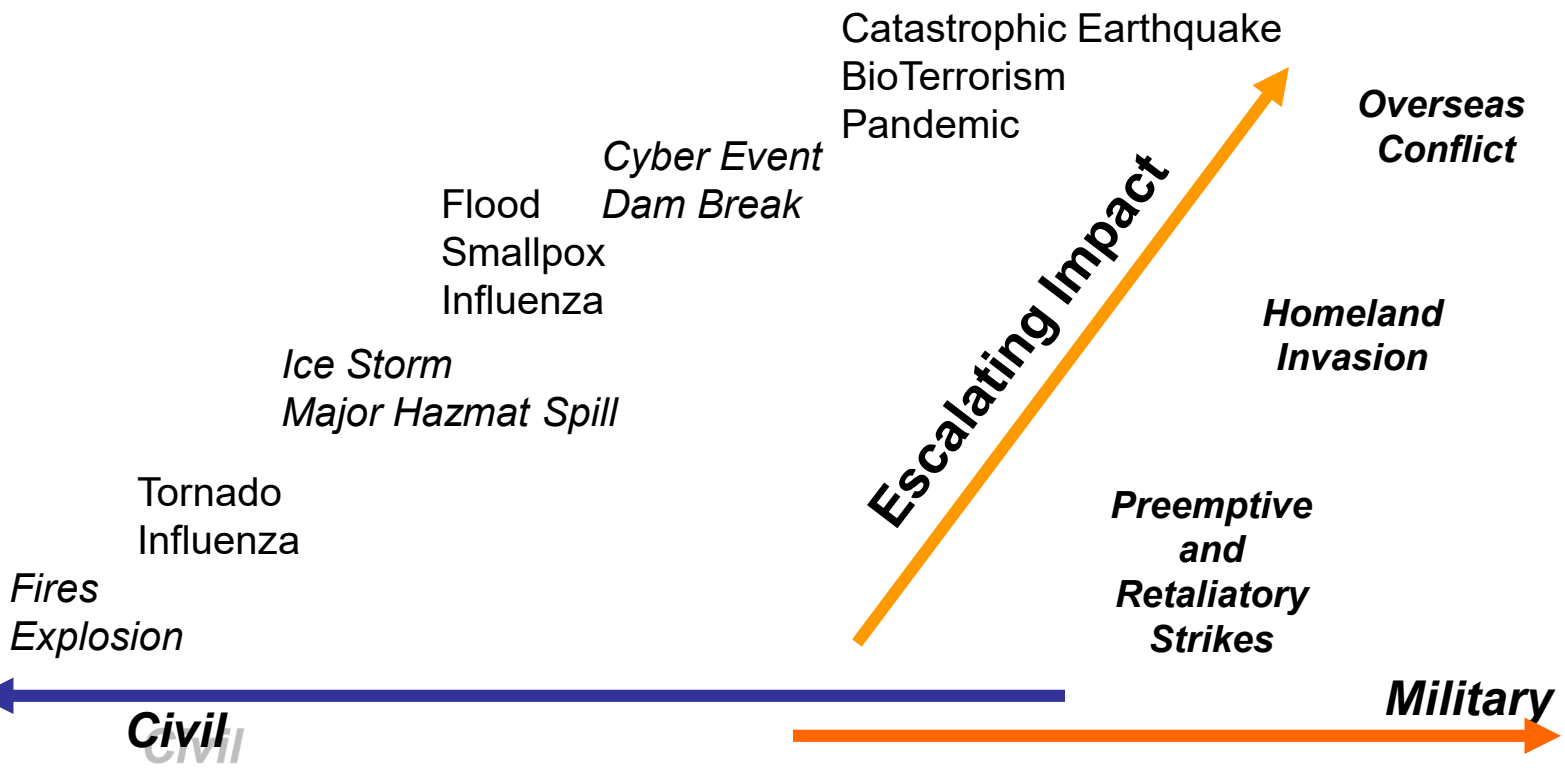
Resilience:
All Hazards and Layered Responsibilities

Global: Surveillance,Intelligence, Intervention

National: Federal, Other Entities

Mutual Aid: Regional, State, Local

Local: City, County, Private, Non-Governmental



18 (now 16) Critical Infrastructures

- Agriculture and Food
- Defense Industrial Base
- Energy
- Public Health and Healthcare
- Banking and Finance
- Drinking Water and Water Treatment Systems
- Transportation System
- Government Facilities
- Chemical
- Commercial Facilities
- Dams
- Emergency Services
- Commercial Nuclear Reactors
- Materials and Waste
- Information Technology
- Communication
- National Monuments and Icons
- Postal and Shipping

Currently, there are 16 industry sectors defined as critical infrastructure

85% of critical infrastructure is in private sector *hands*[1]

Trends exposing industry to increased risk

- Interconnectedness of sectors
- Proliferation of exposure points
- Concentration of assets

Critical infrastructure sectors

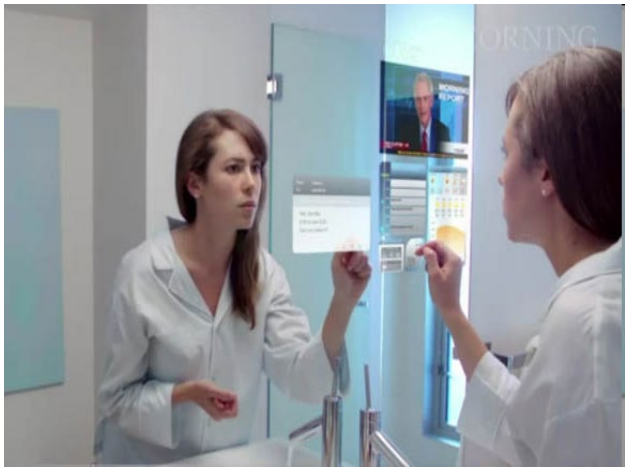
1 GAO Report, Critical Infrastructure Protection: Sector Plans and Sector Councils Continue to Evolve. July 2007, http://www.gao.gov/assets/100/95010.pdf

Example: Interdependencies

- Transportation
- Water, Natural Gas, Fuel Supply
- Electricity/Power/Energy
- Telecom Networks
- More

More “Things” are being connected

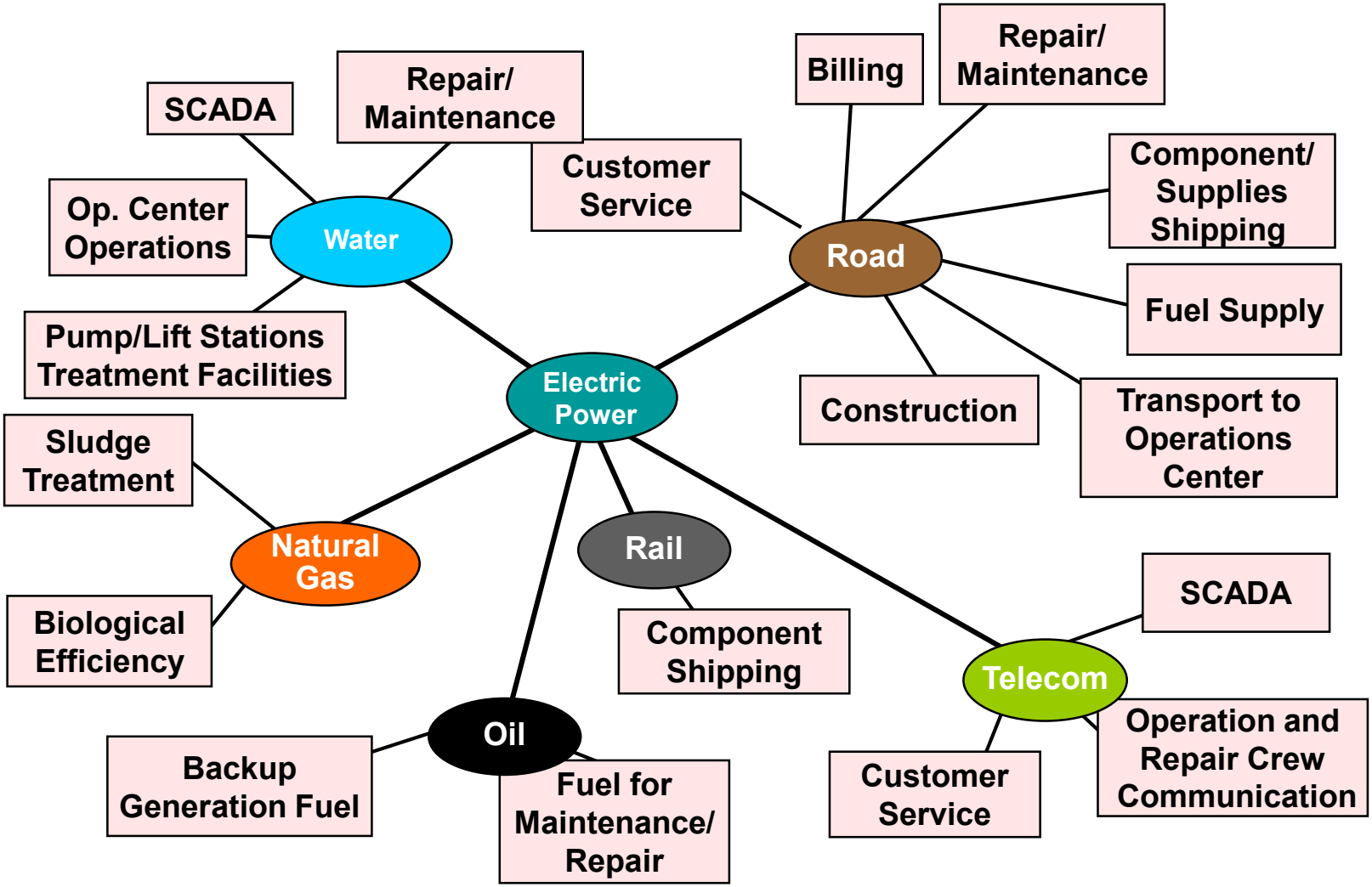
Home/daily-life devices
Business and
Public infrastructure
Health-care
Environment & Climate
Security vs. Privacy
…

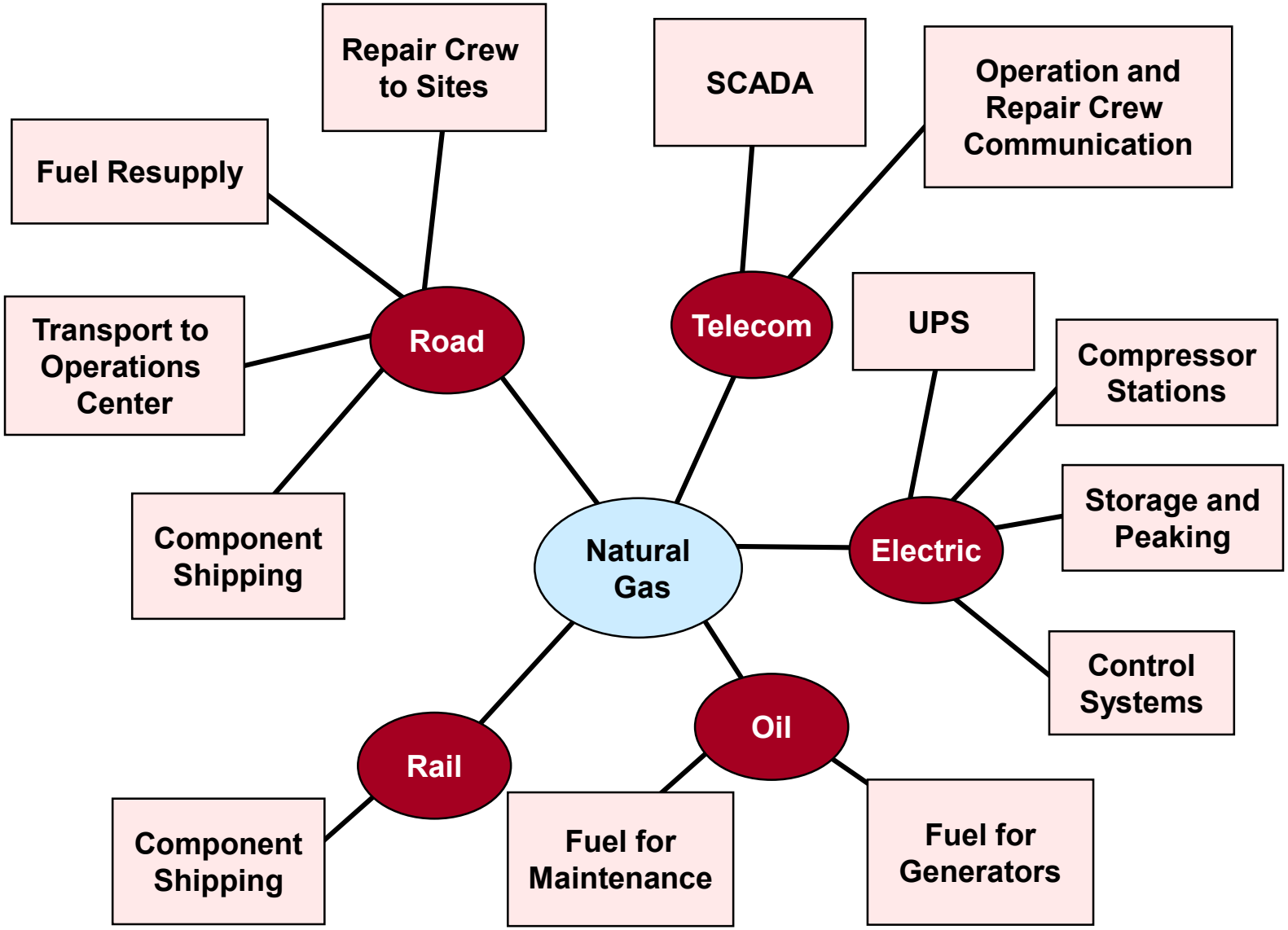


Types of Interdependencies

- Physical (e.g., material output of one infrastructure used by another)
- Cyber (e.g., electronic, informational linkages)
- Geographic (e.g., common corridor)
- Other (e.g., dependency through financial markets)

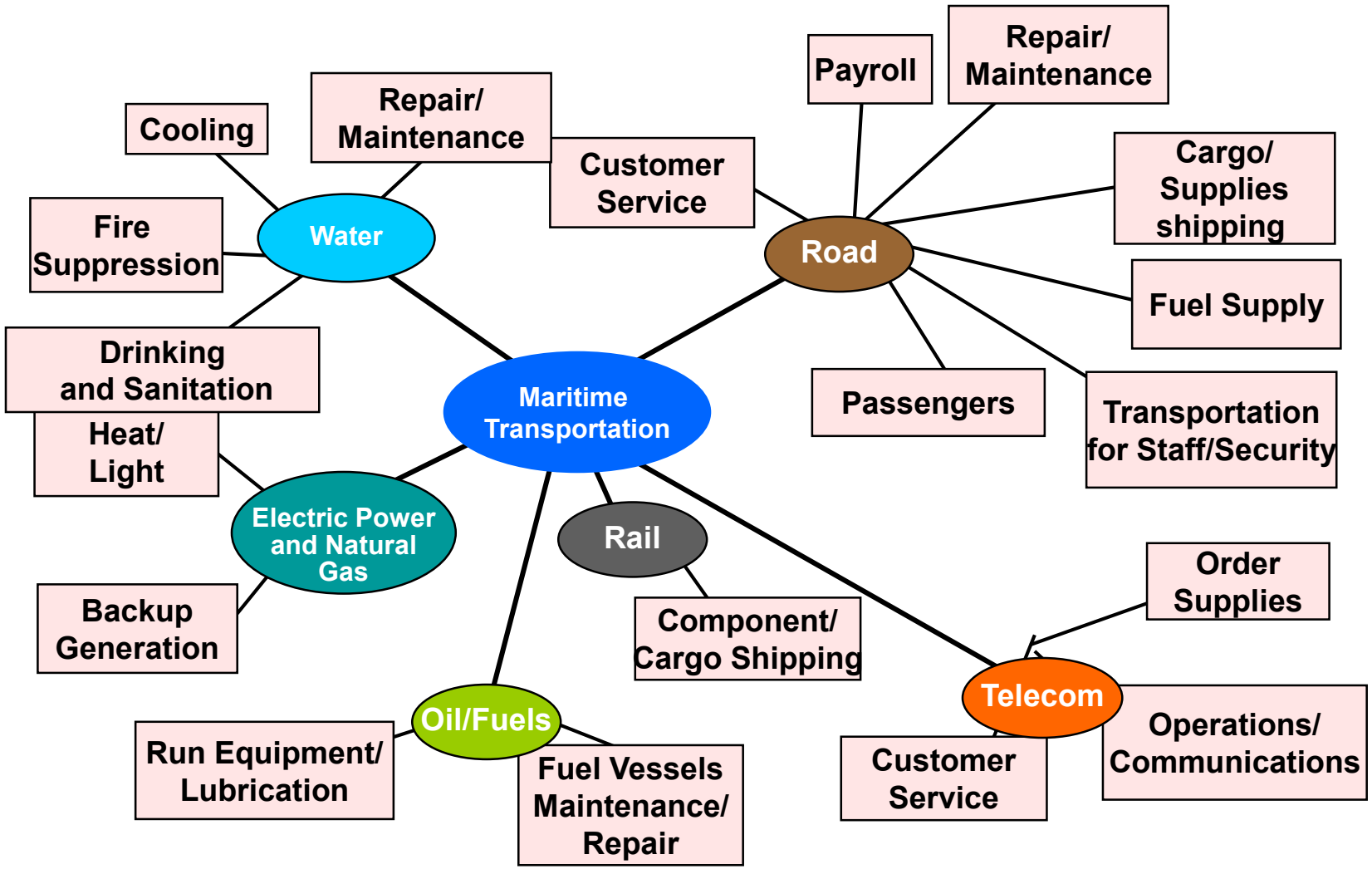
Illustrative Infrastructure Dependencies
Electric Power



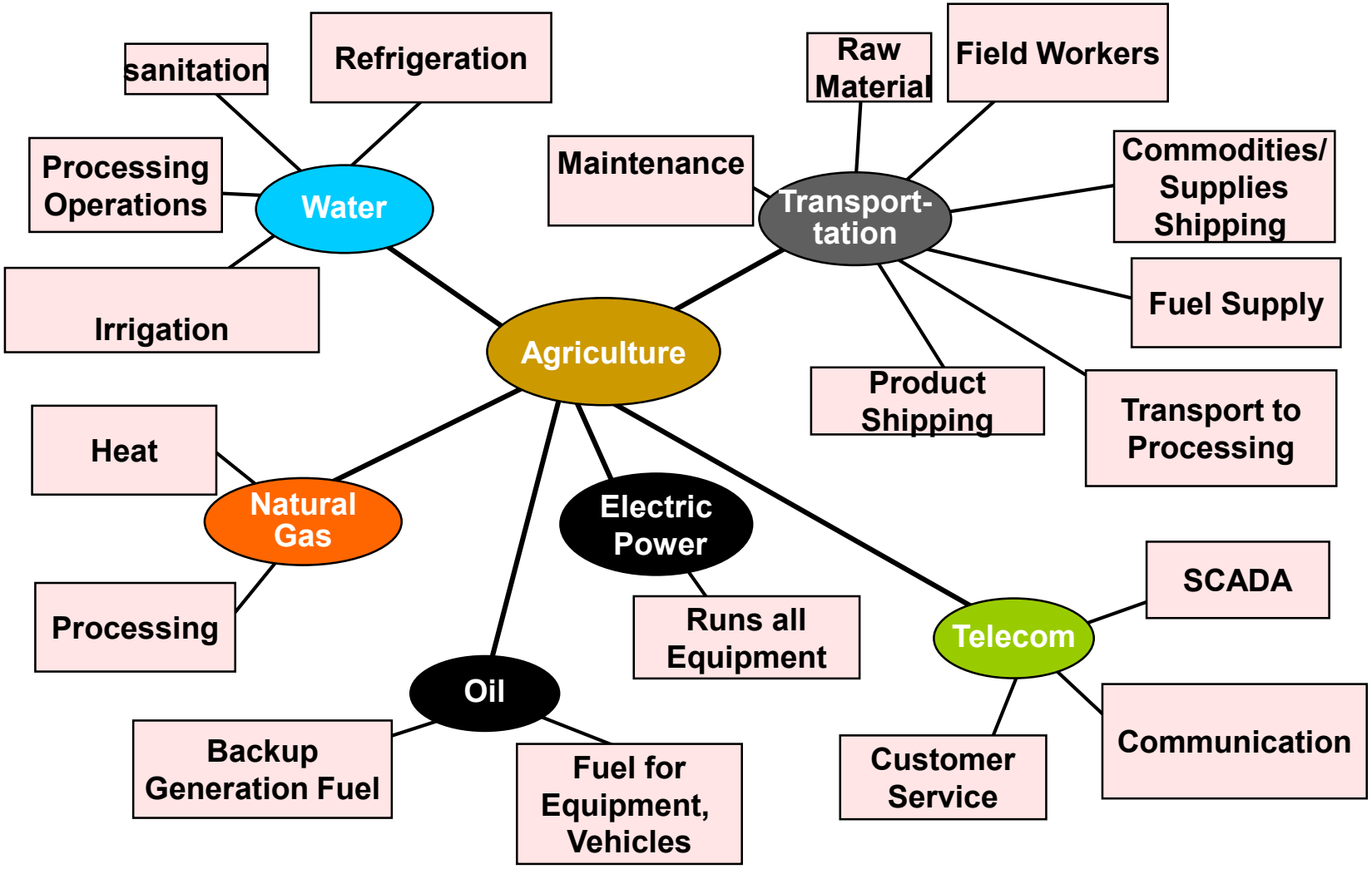


ANL

Illustrative Infrastructure Dependencies
Maritime Transportation



Illustrative Agriculture Dependencies



Types of Interdependence Failures

- Cascading failure – a disruption or unavailable product of service in one infrastructure or organization causes a disruption in a second

- Escalating failure – a disruption or unavailable service or product in one infrastructure or organization exacerbates, or impedes recovery of an independent disruption elsewhere

- Common cause failure –disruption of two or more components or assets simultaneously because of a common cause (e.g., natural disaster, right–of–way corridor)

“Things” Connected to the Internet

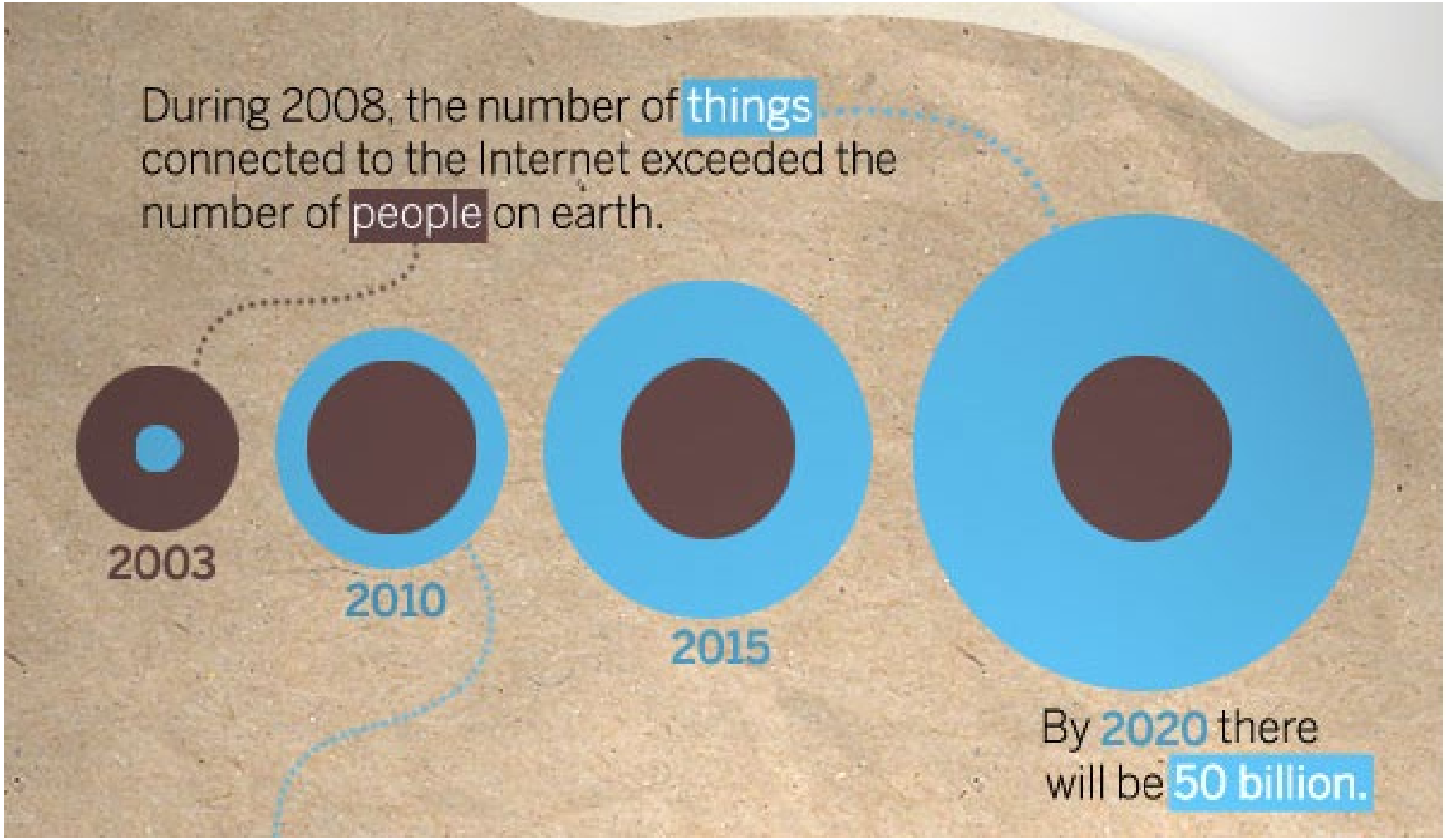
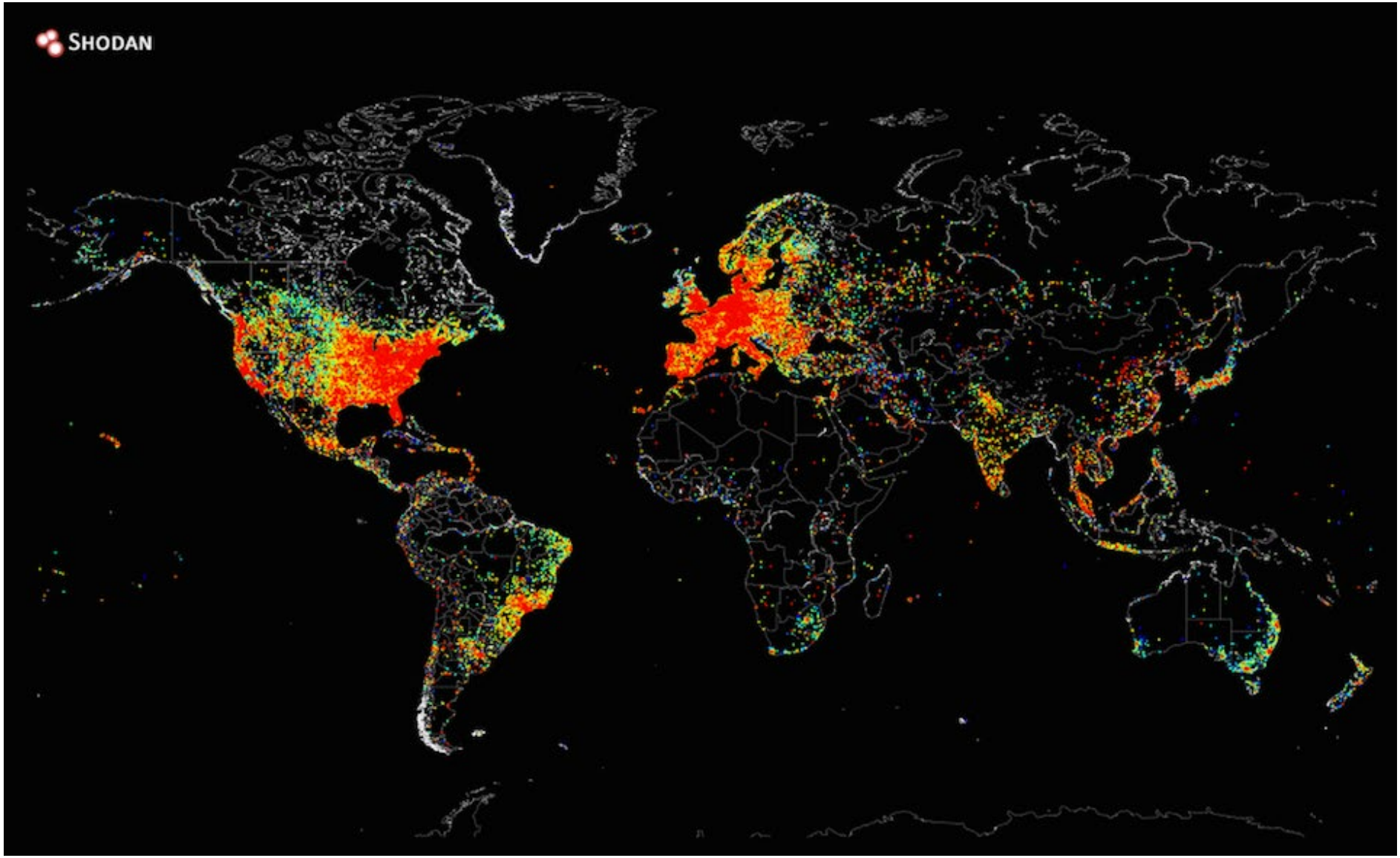


Image Courtesy: : CISCO

A Map of every Connected Device on Earth



Sandstorm

Wildfire

Drought

Hoover Dam turbines set for upgrade to cope with drought

April 19, 2010

The US Bureau of Reclamation has awarded a $3.4 million contract to Andritz Hydro Corporation to upgrade generating facilities at the Hoover Dam.

The Hoover Dam's water store, Lake Mead, has record low water levels because of the drought downstream

Andritz Hydro, which is based in Charlotte, North Carolina, will design and manufacture a new "wide head" turbine runner for the Number Eight generating unit at the power plant on the Nevada side of the Colorado River.

Drought & extreme temps

Drought could shut down nuclear power plants

Southeast water shortage a factor in huge cooling requirements

jump to discuss
comments below

Below: Discuss Related

Recommend 3
Tweet 0
+1 0
Share 1

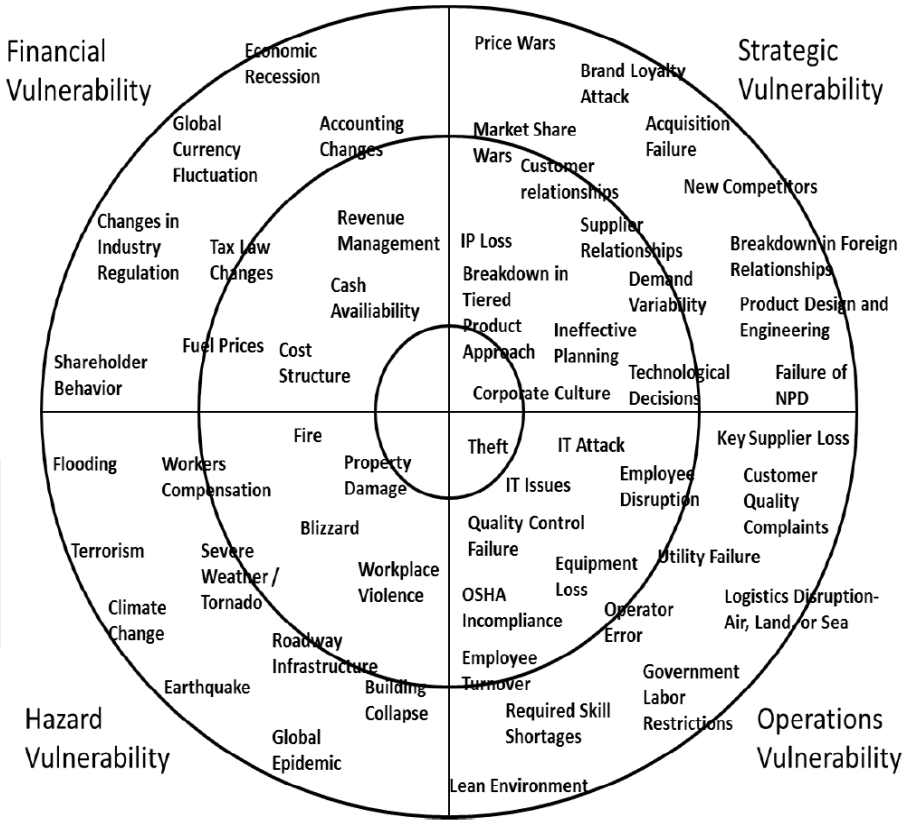
Jason E. Miczek / AP

A man fishes next to the water outflows of the McGuire Nuclear Station near Lake Norman, N.C., on Monday. Lake Norman has dropped to about a foot above the minimum level needed for a backup system at the plant.

Flood

Approach

- **Vulnerability mapping**



- **Scenario analysis**
  - **The green movement**
    - Resilience requirement for new suppliers
  - **Middle East embargo**
    - New projects require improved delivery
  - **Non-renewable energy abundance**
    - Supplier and product distribution will provide snapshot of product portfolio health

Figure 2

This illustration provides a target-and-crosshairs model for vulnerability mapping to prioritize risk factors across four sectors, including operational, hazard, financial and strategic vulnerabilities

TABLE 2.2 Example Resilience Metrics Proposed by the DOE-supported Grid Modernization Laboratory Consortium

Consequence Category	Resilience Metric
Direct	
Electrical Service	Cumulative customer-hours of outages
	Cumulative customer energy demand not served
	Average number (or percentage) of customers experience an outage during a specified time period
Critical Electrical Service	Cumulative critical customer-hours of outages
	Critical customer energy demand not served
	Average number (or percentage) of critical loads that experience an outage
Restoration	Time to recovery
	Cost of recovery
Monetary	Loss of utility revenue
	Cost of grid damages (e.g., repair or replace lines, transformers)
	Cost of recovery
	Avoided outage cost
Indirect	
Community function	Critical services without power (e.g., hospitals, fire stations, police stations)
	Critical services without power for more than N hours (e.g., N> hours or backup fuel requirement)

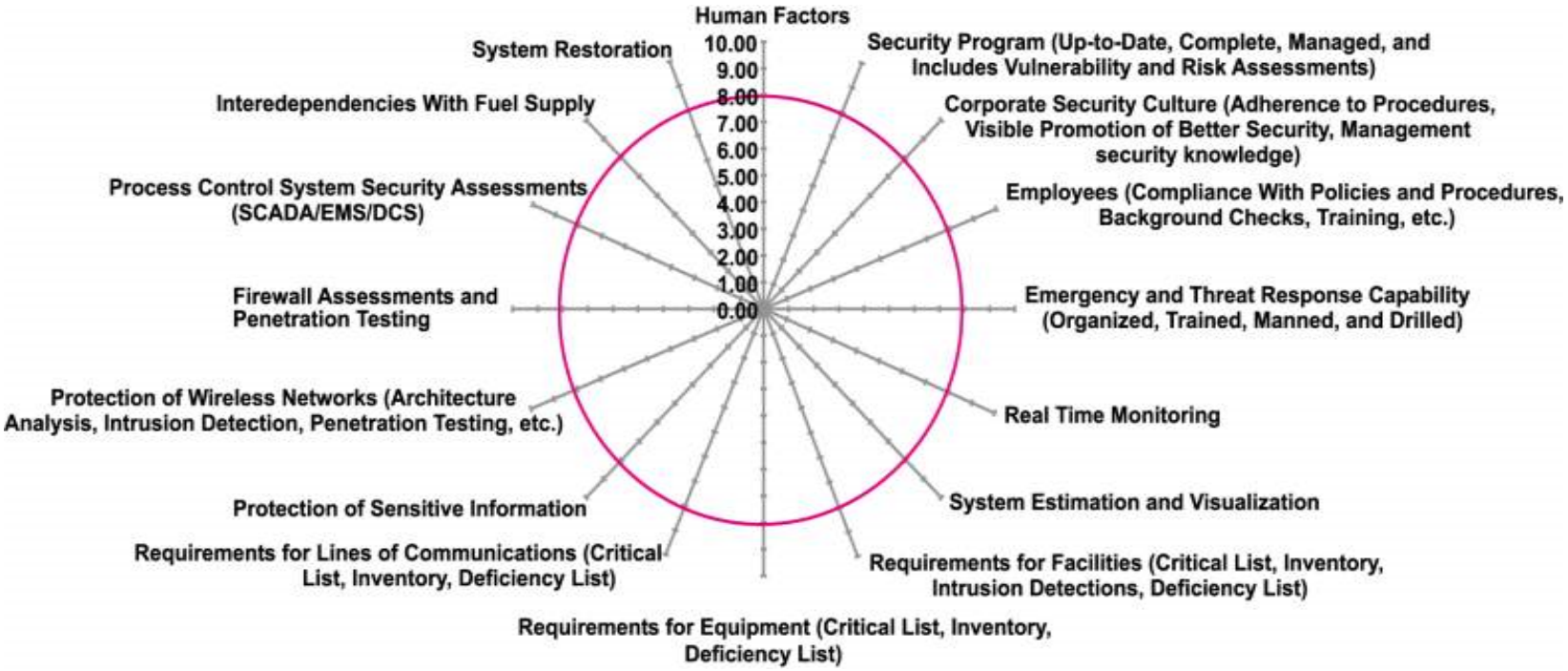
SOURCE: GMLC (2017).

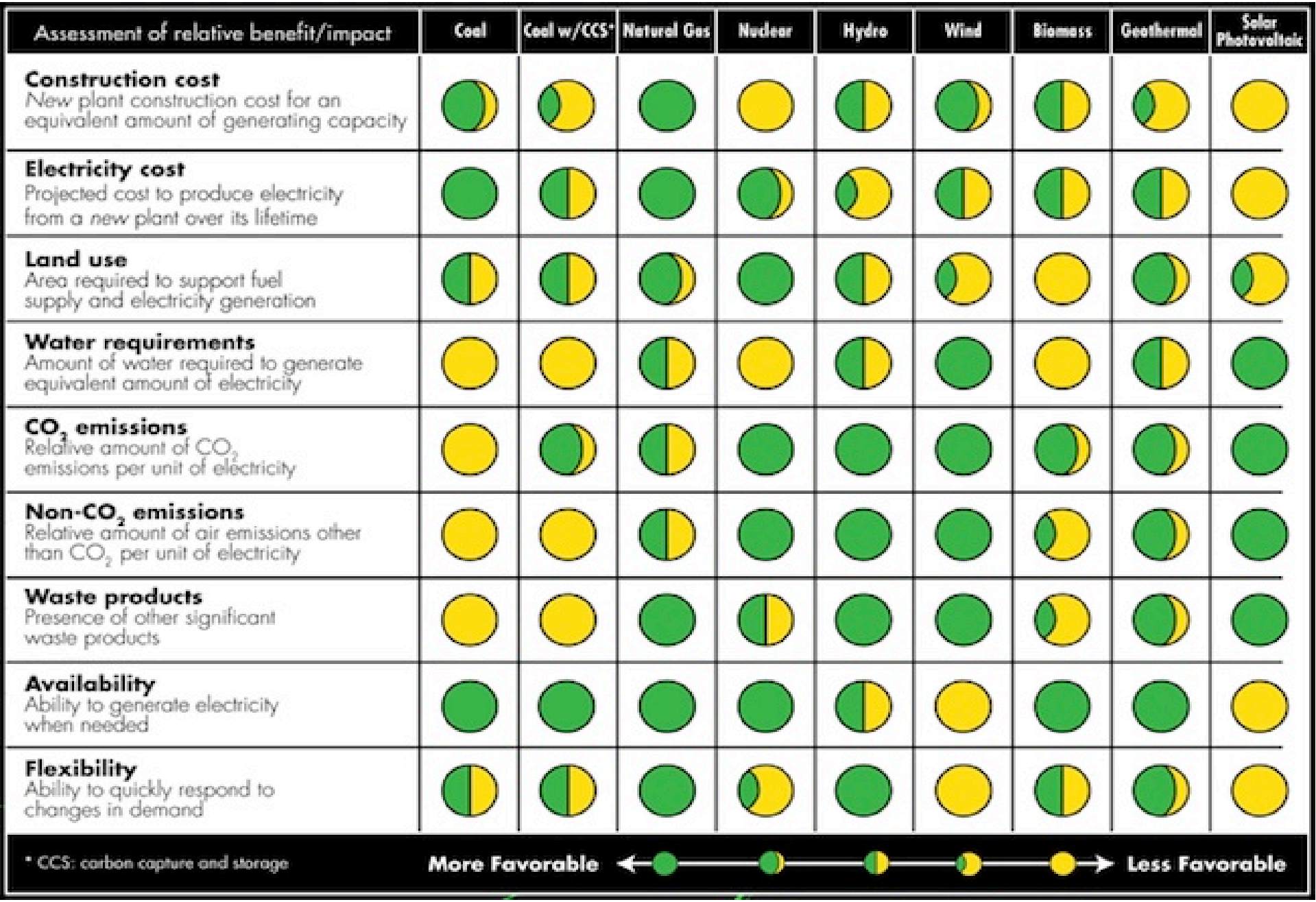
Source: Forthcoming "Enhancing the Resilience of the Nation's Electricity System," NAP, 2017

General	Corporate culture
	Security Program
	Employees
	Emergency and threat response capability
Physical	Requirements for facilities, equipment and lines of communication
	Protection of sensitive information
Cyber and IT	Protection of wired and wireless networks
	Firewall assessments
	Process control system security assessments

Assessment & Prioritization:

A Composite Spider Diagram to Display Security Indices



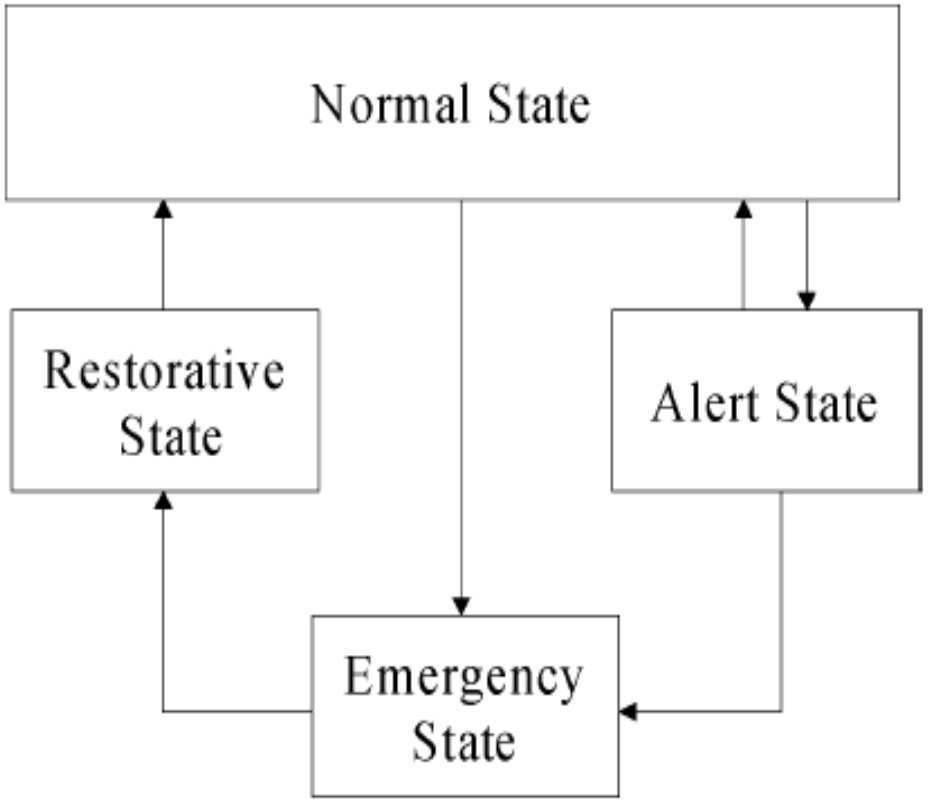


Source: EPRI http://sites.epri.com/refcard/comparison.html

Understanding Complex Dynamical Systems

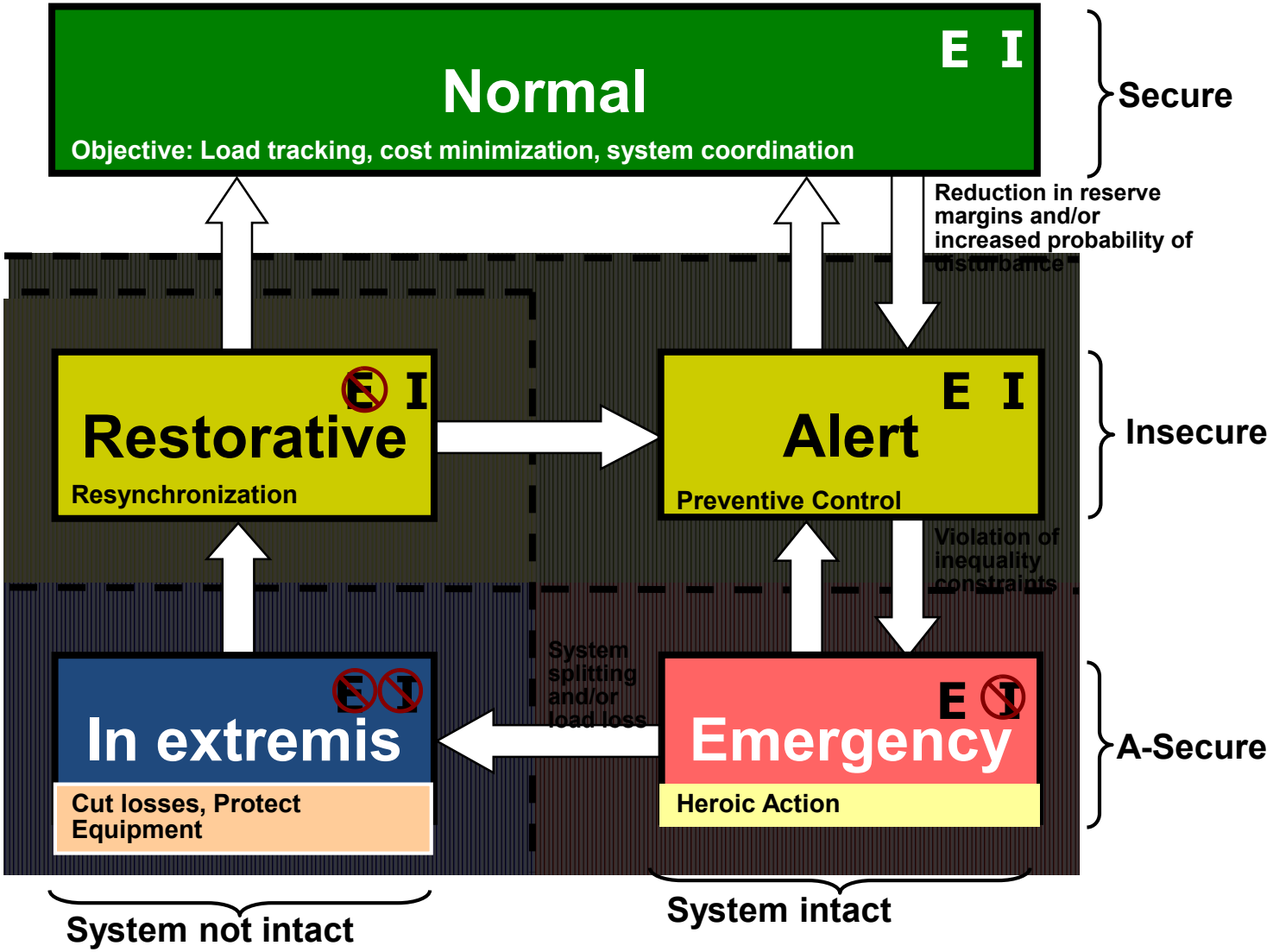
Modes of Electric Power Systems:

- *Normal mode:* economic dispatch, load frequency control, maintenance, forecasting, etc.;
- *Alert mode:* red flags, precursor detection, reconfiguration and response;
- *Emergency/Disturbance mode:* stability, viability, and integrity -- instability, load shedding, etc.;
- *Restorative mode:* rescheduling, resynchronization, load restoration, etc.



Dynamics of Power System Operating States

E = Demand is met
I = Constraints are met



Significant Goal-Setting Approaches/Tools

Approach/Tool	*Description*	*Unit of Analysis*
Management System Standards	**Management system standards that set benchmarks for a management system and objectives; specific performance standards left to the entity**	**Entity**
Scenario-Based Planning	**Identifies possible event, futures, and outcomes for planning; can have short and long-term horizons**	**Entity**
Risk Management	**Analysis and decision making to achieve an affordable, acceptable level of risk**	**Entity**
Capabilities-Based Planning and Assessment	**Identify capabilities to accomplish missions**	**Capabilities**

The Framework: National Preparedness Management System Standards

- *Standard*: a consensually-developed document that provides rules, guidelines or characteristics for activities or their results; provides uniform set of measures, conditions, or specifications between parties
- *Management system standards*: covers what an organization does to manage its processes or activities, applicable to any organization in any sector and is independent of products or services
  - ISO 9000 for quality management and ISO 14000 for environmental management
- *NFPA 1600* for public and private criteria to approach disaster management, emergency management, and business continuity; addresses mitigation, preparedness, response, and recovery
  - Endorsed by DHS and 9/11 Commission as national preparedness standard

NFPA 1600 Elements

- Laws and authorities
- Hazard identification, risk assessment, and impact analysis
- Hazard mitigation
- Resource management
- Mutual aid
- Planning
- Direction, control, and coordination
- Communications and warning
- Operations and procedures
- Logistics and facilities
- Training
- Exercises, evaluations, and corrective actions
- Crisis communication and public information
- Finance and administration

Grave New World: Security Challenges in the 21st Century

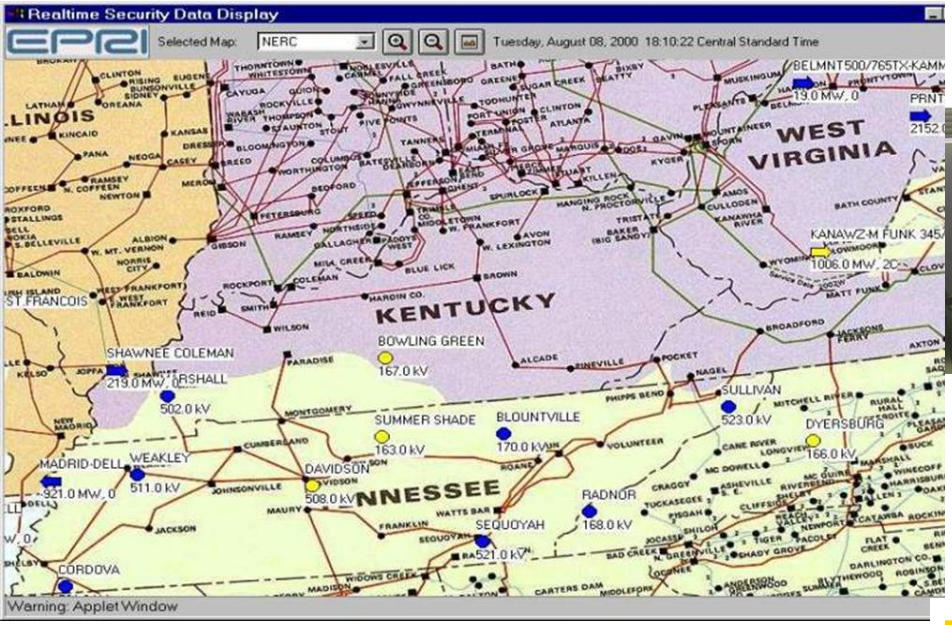
- Nuclear, Biological and Chemical Weapons
- Conventional Weapons
- Energy
- Environmental Change
- Demographic Developments
- Transnational Crime and Corruption
- Developing World
- Transnational Terrorism

The Greatest Challenge

- Putting aside the assumptions and the way you have always done business
- Being open and responsive to new ideas to meet the challenges of interdependence
- Cooperating across the stovepipes, beyond the fence, and working together

Think Regional!
Think Interdependencies!
Think Preparedness!

EPRI's Reliability Initiative-- Sample Screen of Real-time Security Data Display (RSDD)



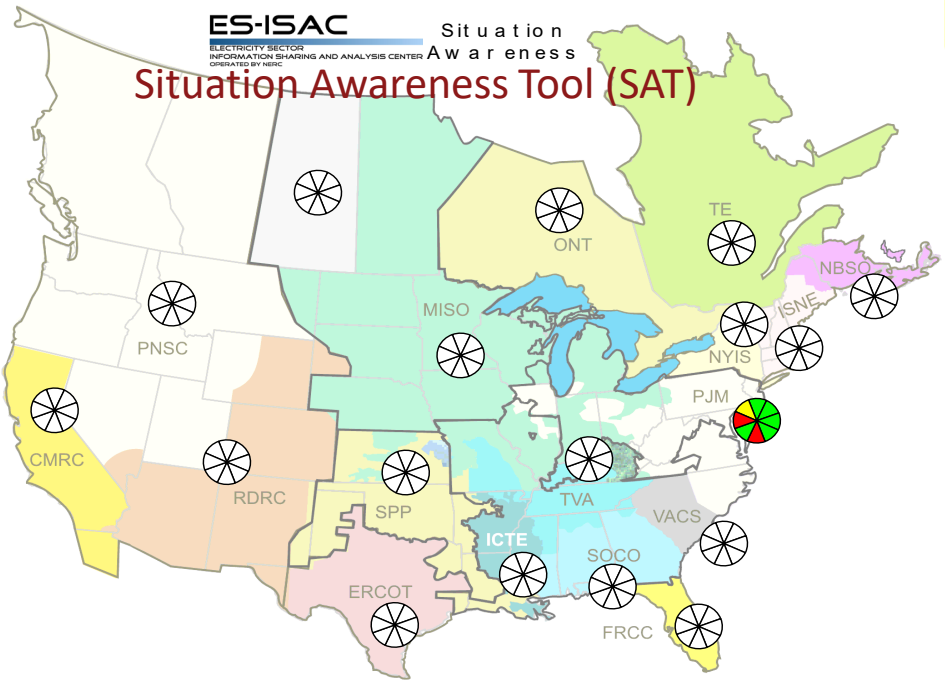
Fast Power Systems Risk Assessment

Doctoral Dissertation: Laurie Miller (June 2005-present)
ORNL contract, the U of MN start-up fund (2005-2008), and NSF grant (2008-2009), PI: Massoud Amin

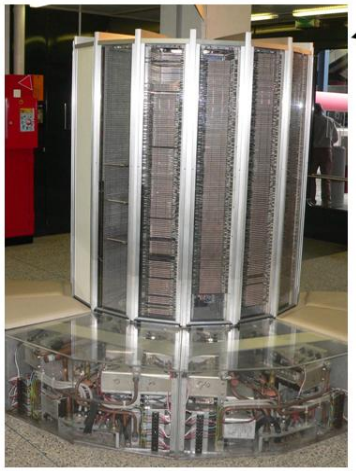
Connection Machine 2: $5 million in 1987, only a few dozen made

NVIDIA Tesla C870: $1300 in 2009, over 5 million sold

Situation Awareness Tool (SAT)



Fast Power Grid Simulation

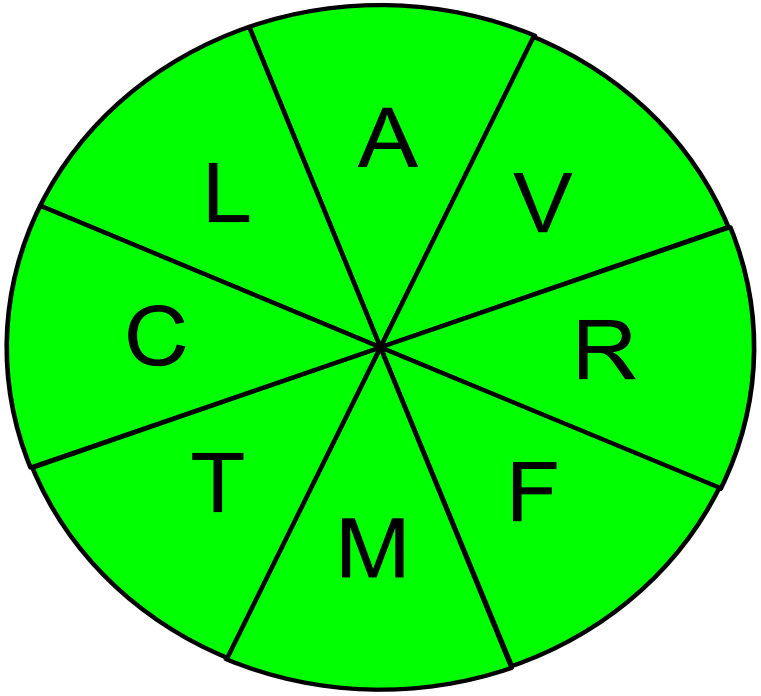


CRAY Supercomputer

Nvidia GeForce GPU card for PC

- Use Nvidia GeForce GPU card to gain 15 times faster power flow calculation on PC (Laurie Miller)

Situation Awareness Tool (SAT)



No “Telemetry” Data

Data Value Nominal

Data Value Approaching Warning

Data Value in Warning Range

Data value Returned to Normal

A – ACE
L – Deviation from Forecasted Load
C – Reserve Real-power Capacity
V – Voltage Deviation from Normal
R – Reserve Reactive-power Capacity
M – Text Message
T – Transmission Constraint
F – Frequency

Threats … a subset

Challenges for Security and Mission Assurance

Need to identify:

- What "threats" are of greatest concern and what of risk is tolerable
- Components assets, products or services that, if lost, unavailable or degraded, could adversely affect other infrastructures and organizations
  - Under normal and stressed operations
  - During disruptions, including coincident events
  - Repair and restoration
- How backup systems or other mitigation mechanisms can reduce interdependence problems
- The linkages between critical infrastructures and community assets

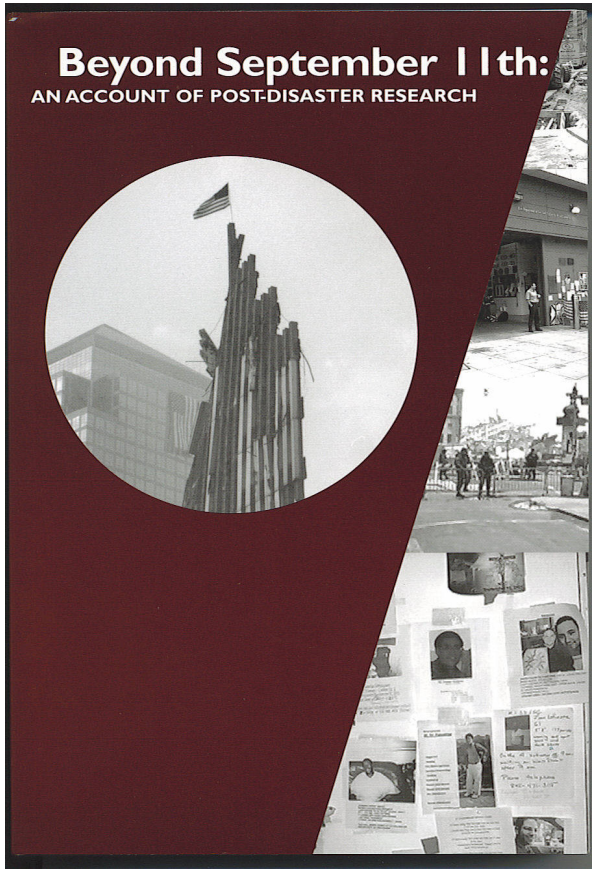
Why systems fail?

- Natural hazards
- Malevolent acts
- Wearout and breakdown
- Human error
- Close-coupling of system elements
- Focus on a single outcome

Providing reliable and resilient systems requires organizations that can

- Anticipate
- Plan
- Implement
- Adapt and improvise

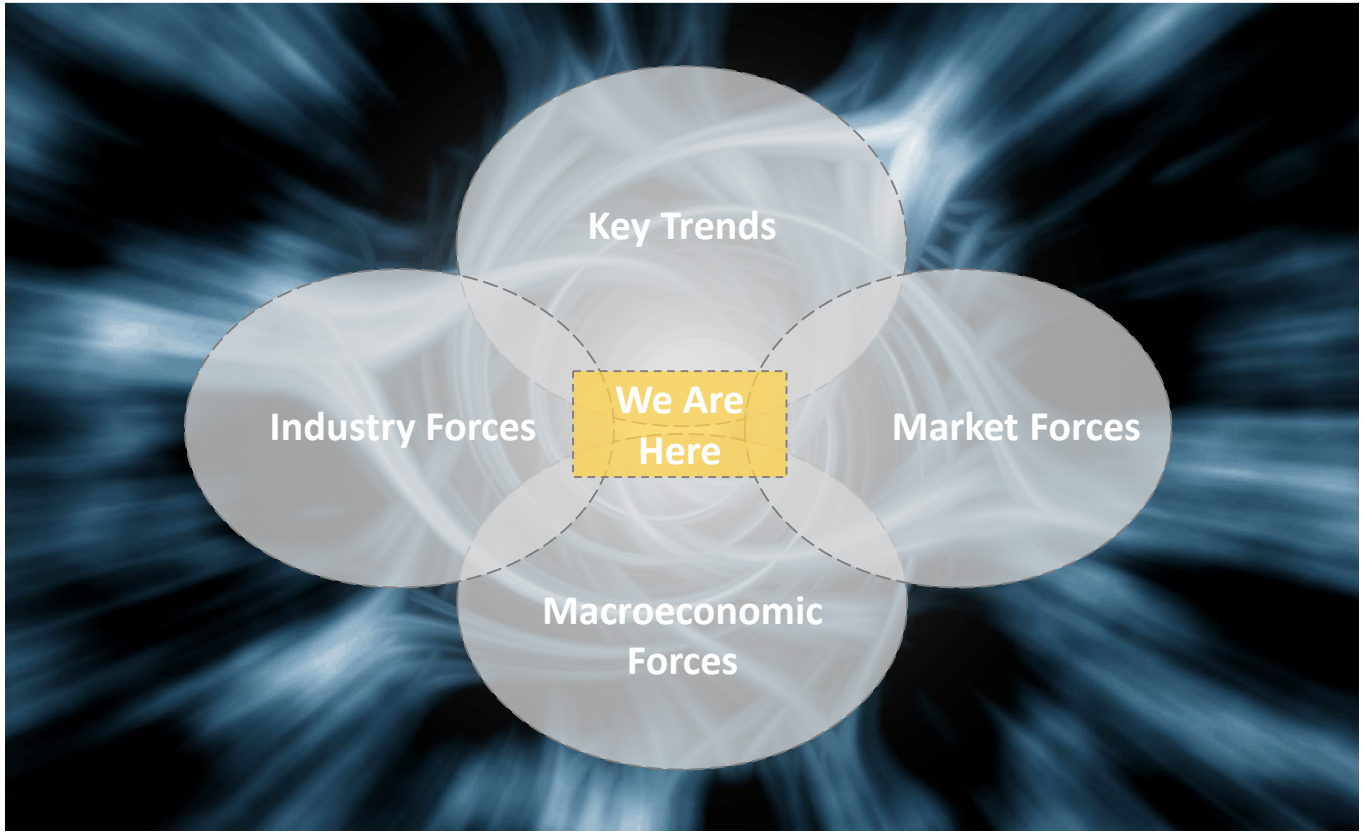
Critical Features of Survivable Systems: Lessons from September 11

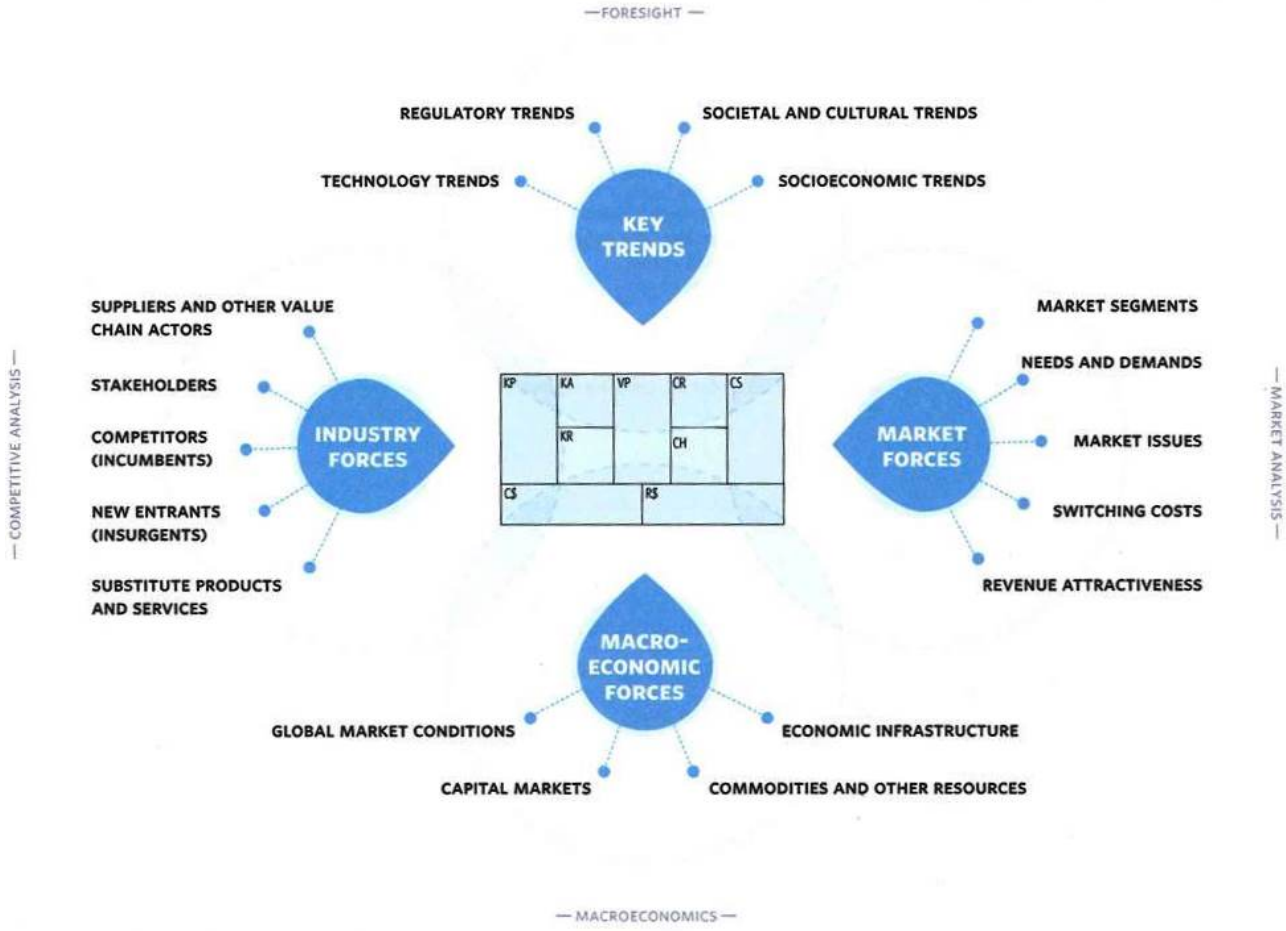


- ⌘ resilience: ability to recover quickly
- ⌘ robustness: failure-resistant through design and/or construction
- ⌘ redundancy: duplicative capacity for service delivery

Verizon, AT&T, ConEd, and MTA (among others) possessed all these attributes in equipment and people

Natural Hazards Research and Applications Information Center, University of Colorado, Boulder, 2003

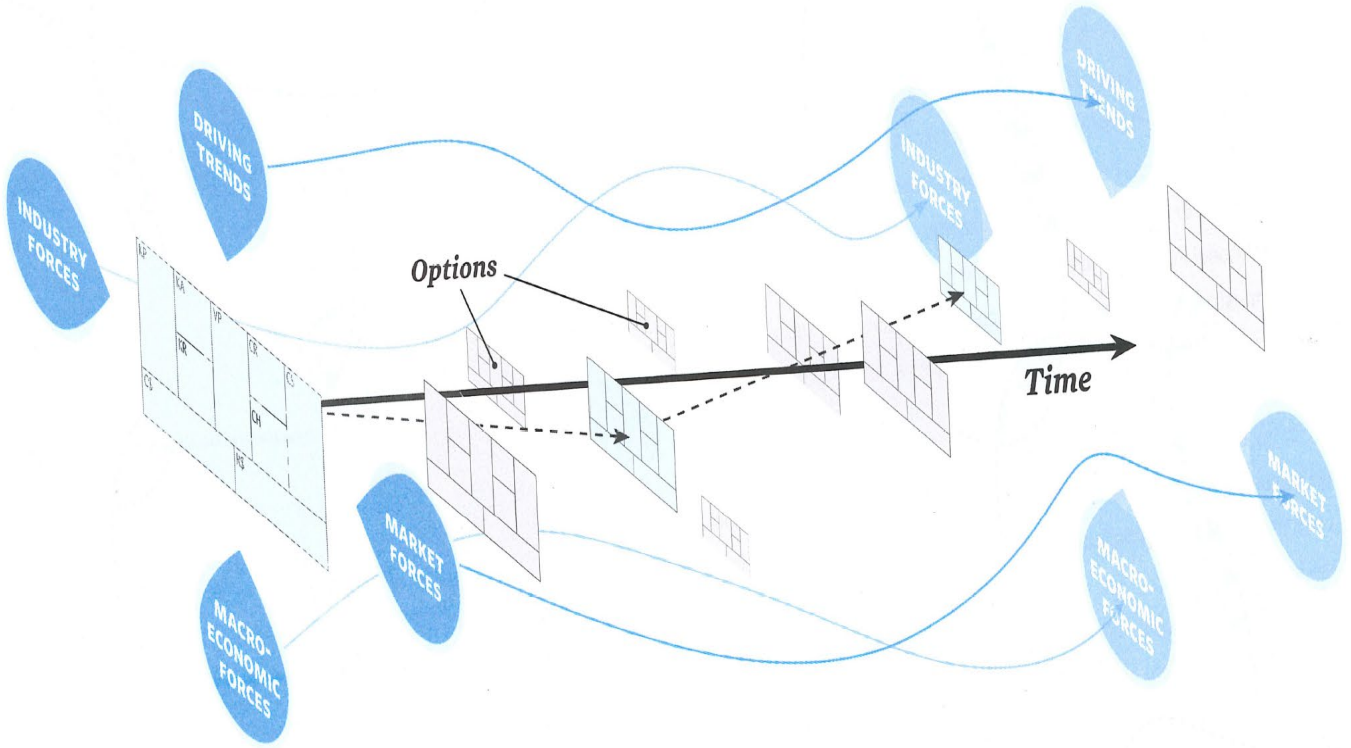




External context: The macro-environmental force field

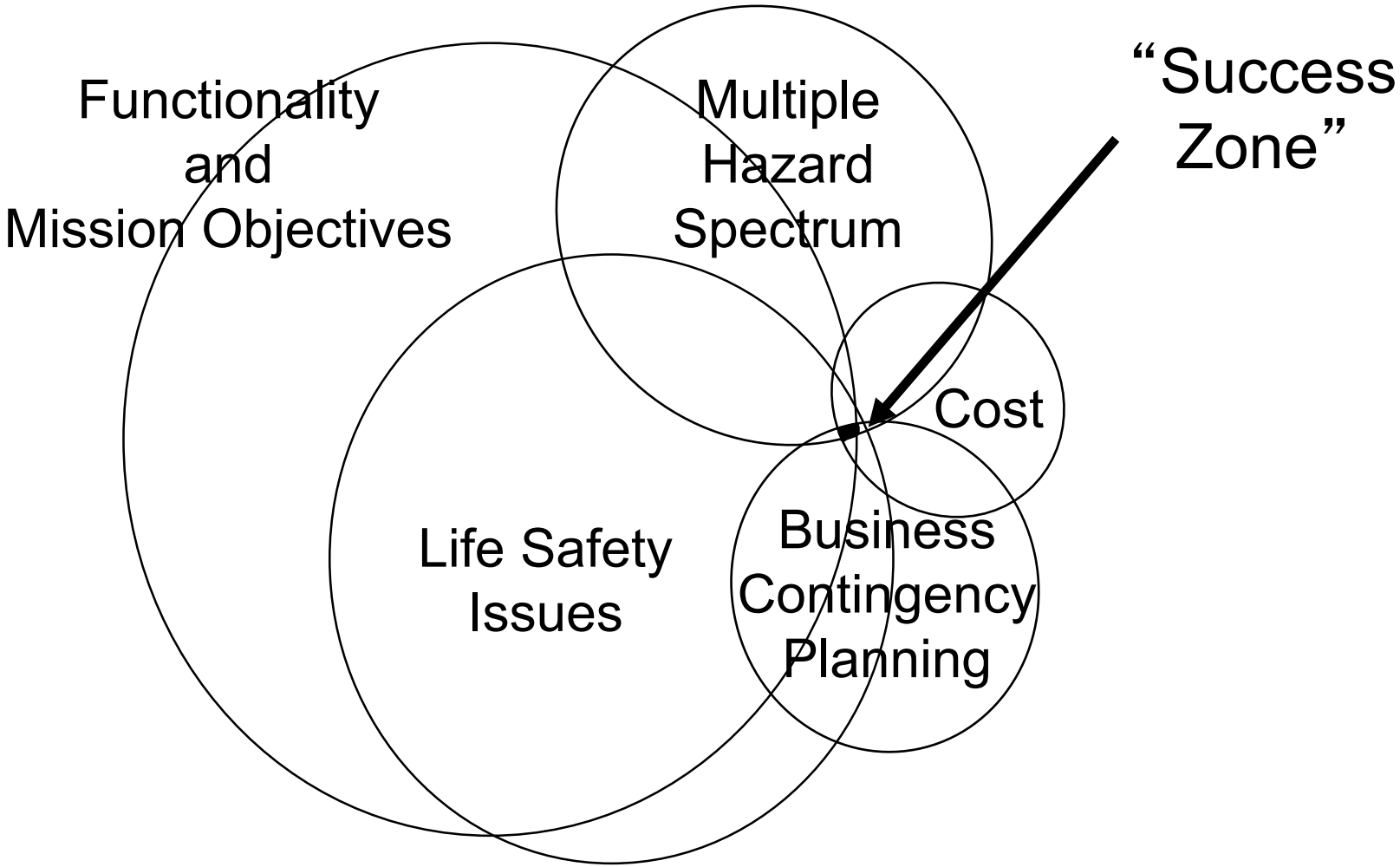
Source: Kirk Froggatt, TLI, UofM. ACS 2013, NOLA, with N. Rao for Nalco case study.

Macro-environmental Forces:
Strategic Technology Assessment and Foresight



Source: Adopted from *Business Model Generation,* by Osterwalder & Pigneur

Real world solutions may be elusive



Short-term Moves

BS = Business Strategy
CS = Corporate Strategy
IS = Innovation Strategy
GS =Government Strategy

Short-term focus is addressing high risks,
or defining the market niche and addressing its early needs

Strategy/Move	Who	What/Why	How	When	Cost/Risk

Long-term Moves

BS = Business Strategy
CS = Corporate Strategy
IS = Innovation Strategy
GS =Government Strategy

Long-term focus is satisfying strategic security (or customer) needs and reducing vulnerabilities (or expanding niche market for corresponding products)

Strategy/Move	Who	What/Why	How	When	Cost/Risk