CYBER SECURITY SUMMIT 2017

Securing Critical Infrastructure in an Uncertain World

S. Massoud Amin, D.Sc.
Director & Honeywell HW Sweatt Chair, Technological Leadership Institute
Professor, Electrical & Computer Engineering & University Distinguished Teaching Professor, University of Minnesota

Chairman, IEEE Smart Grid | Fellow, IEEE & ASME

October 24, 2017

The Infrastructure Challenge

Will today's national and local infrastructure systems be left behind as a relic of the 20th century, or become the critical infrastructure supporting the digital society, a self-healing infrastructure?

Why systems fail?

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

There are many challenges facing the energy and power infrastructure

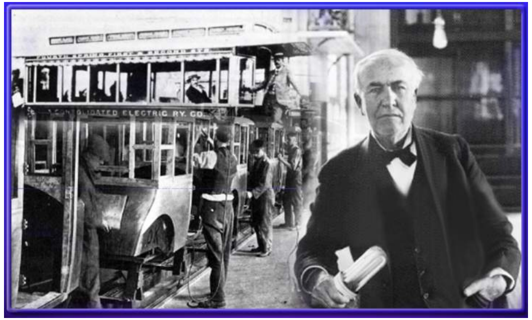
- Severe Weather Events
- Physical and Cyber attacks
- Aging Assets
- Dependencies and inter-relationships with other infrastructures (gas, telecommunications, etc.)
- Market and Policy including recovery of investments

Source: IEEE report to the U.S. DOE for the White House's Quadrennial Energy Review (QER) to guide U.S. energy policy. See Chapter 4, on implications and importance of aging infrastructure and the options for addressing them: http://www.ieee-pes.org/final-ieee-report-to-doe-qer-on-priority-issues

Electric Power Infrastructure: Interdependencies, Security, and Resilience

The vast networks of electrification are the greatest engineering achievement of the 20th century

– U.S. National Academy of Engineering



- Presidential Policy Directive 21: “*Energy and communications infrastructure especially critical because of their enabling functions across all critical infrastructure areas*”
- DOE: “*A resilient electric grid… is arguably the most complex and critical infrastructure.*”

Industry Drivers

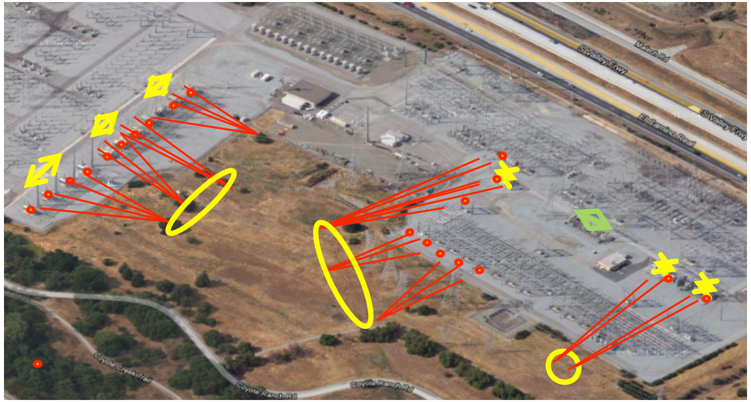
Source: IEEE report to the U.S. DOE for the White House's Quadrennial Energy Review (QER) to guide U.S. energy policy. See Chapter 4, on implications and importance of aging infrastructure and the options for addressing them: http://www.ieee-pes.org/final-ieee-report-to-doe-qer-on-priority-issues

Grid Resiliency

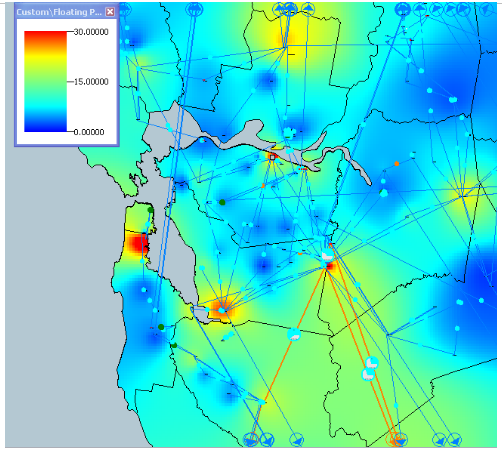
- Cost of Major Outages
- Public Safety & Security
- Critical Infrastructure Protection
- *Physical vulnerability*

Physical Vulnerability

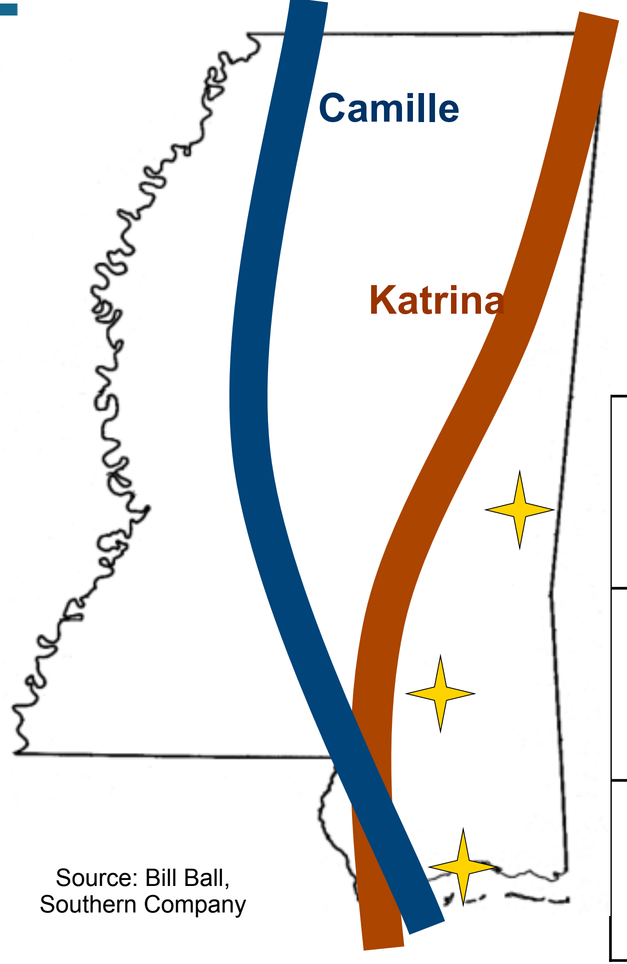
- Transmission Equipment
- System - Selecting critical substations
- Standards



Equipment with gunshot damage



Peak Wind Speed Comparison (MPH)



Source: Bill Ball, Southern Company

	Katrina 08.29.05	Camille 08.17.69
Meridian	90	55
Hattiesburg	110	
Gulfport	140	190

	CAMILLE	IVAN	KATRINA
Landfall Date	08.17.69	09.16.04	08.29.05
Landfall	Waveland/BSL, MS	Eastern Mobile Bay	MS/LA State Line
Category at Landfall	Category 5	Category 3	Category 4
Wind Speed/Gusts	190 / 220 mph	115 / 135 mph	140 / 180 mph
Tidal Surge (Maximum)	20-28’	10-15’	35-40’
Hurricane Winds (Size of Storm)	60 miles	35-40 miles	125 miles
Forward Motion	NNW at 15 MPH Sustaining at Landfall	NNE at 12 MPH Weakening at Landfall	NNE at 15 MPH Strengthening & Expanding at Landfall
System Outages	104,000*	1.7 million	971,000
System Companies Most Affected	MPC - 77% Loss	Gulf - 90% Loss APC - 65% Loss	MPC - 100% Loss APC - 49% Loss
Others Impacted	APC	MPC, GPC	APC, Gulf, GPC
Service Restoration	15 days	2 weeks	2 weeks

Example: Fire under the 500 kV Lines

Example: Midway – Vincent 500 kV line tower damage

Midway – Vincent 500 kV line damage

Vincent Substation before Transformer Explosion & Fire

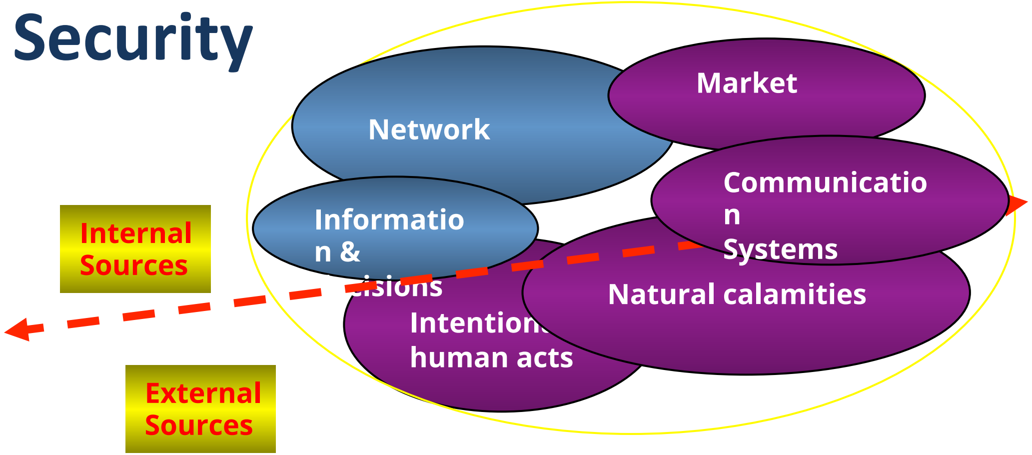
Source CA-ISO

500 / 230 kV Transformer Explosion & Fire: Vincent Substation

Source CA-ISO

Context: Threats to Security

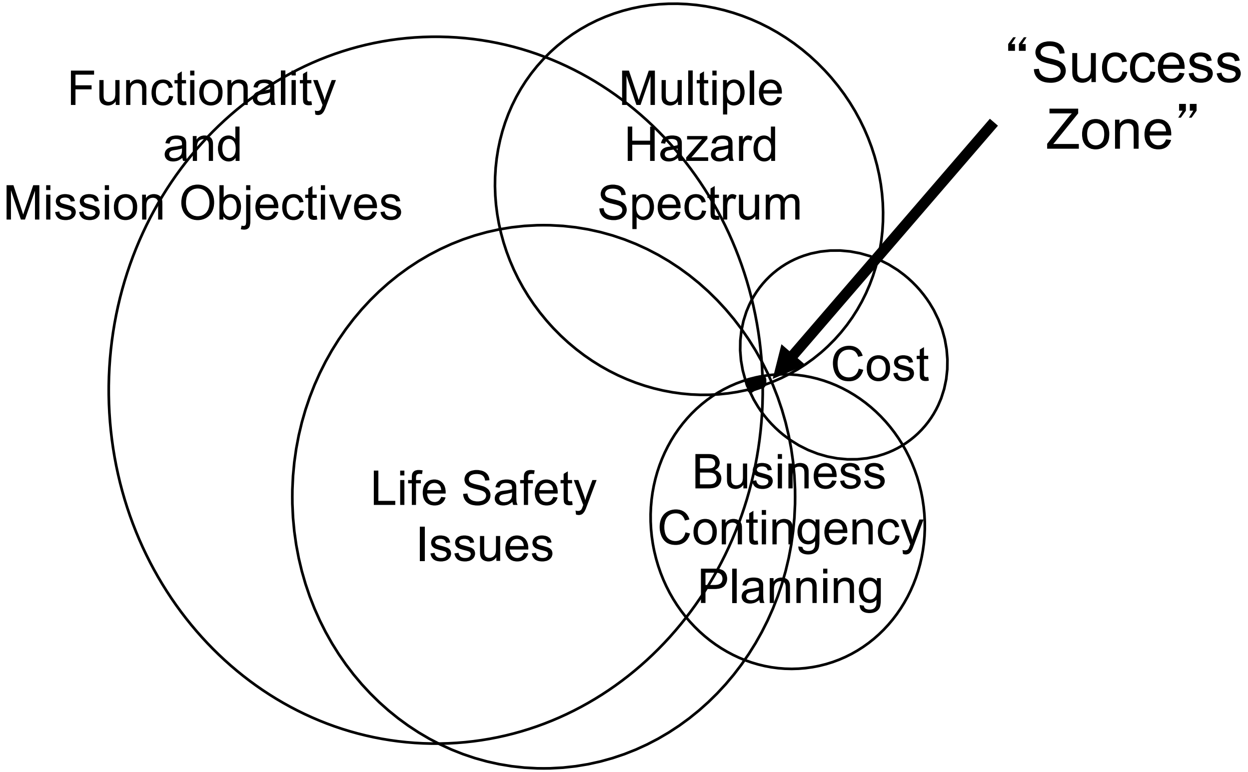
Sources of Vulnerability



- Transformer, line reactors, series capacitors, transmission lines...
- Protection of ALL the widely diverse and dispersed assets is impractical
  - 202,835 miles of HV lines (>230 kV)
  - 6,644 transformers in Eastern Intercon.
- Control Centers
- Interdependence: Gas pipelines, compressor stations, etc.; Dams; Rail lines; Telecom – monitoring & control of system
- Combinations of the above and more using a variety of weapons:
- Truck bombs; Small airplanes; Gun shots – line insulators, transformers; more sophisticated modes of attack...

- EMP
- Hijacking of control
- Biological contamination (real or threat)
- Over-reaction to isolated incidents or threats
- Internet Attacks – > 120,000 hits a day at an ISO
- Storms, Earthquakes, Forest fires & grass land fires
- Loss of major equipment – especially transformers...

Real world solutions may be elusive

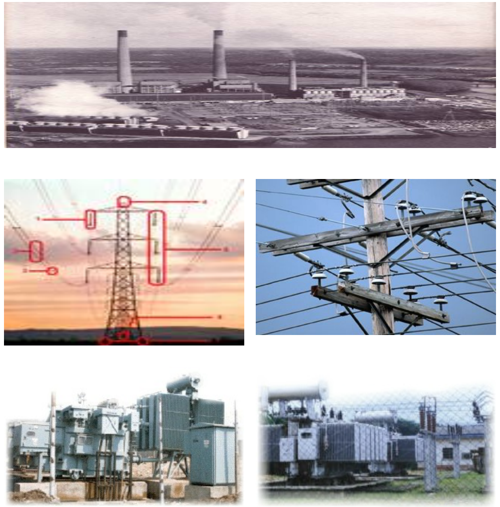


Modern society depends on a secure and reliable energy and power infrastructure

Generation | Delivery | Customer

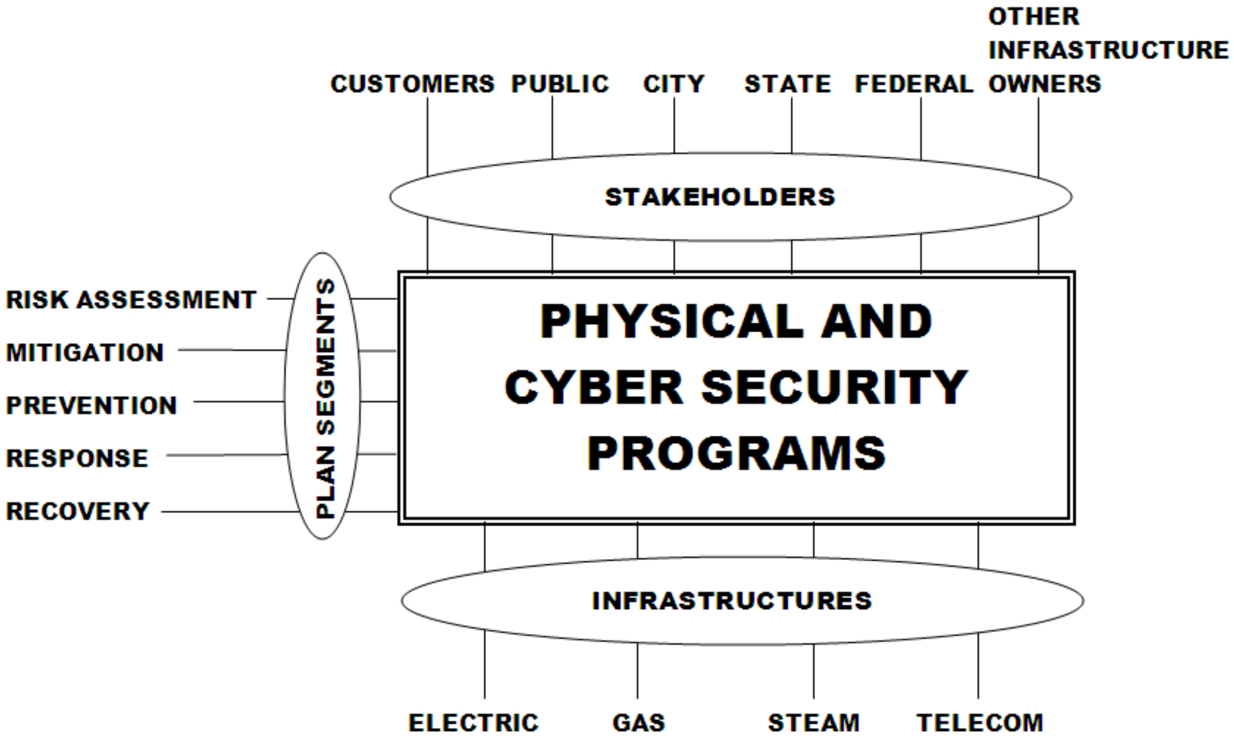
Interface of Smart Grid and Microgrids

- Fossil Fuel
- Long Distance Central Station
- An Aging Infrastructure
- Out of Capacity



- Renewable Power
- On-site
- Zero Energy Building
- Smart Grid

CIP programs in the industry



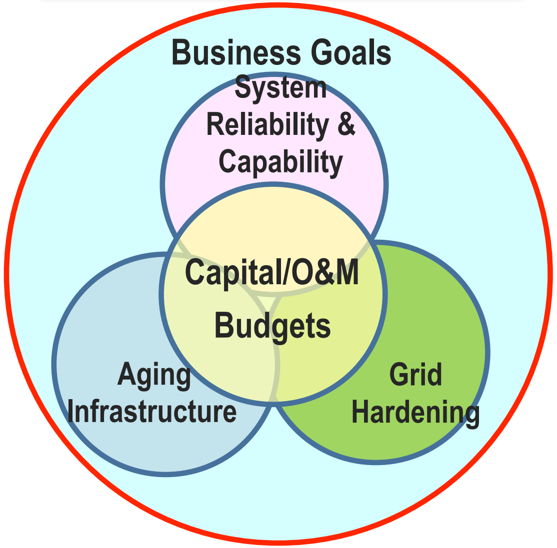
Holistic Asset Management

**Asset management:
Predictability of Cost
& Reliability**

Average systems 40 to 60 years old

25% of electric infrastructure is of an age and situation where condition is a concern

Demand for maintenance double over the next 10-20 y

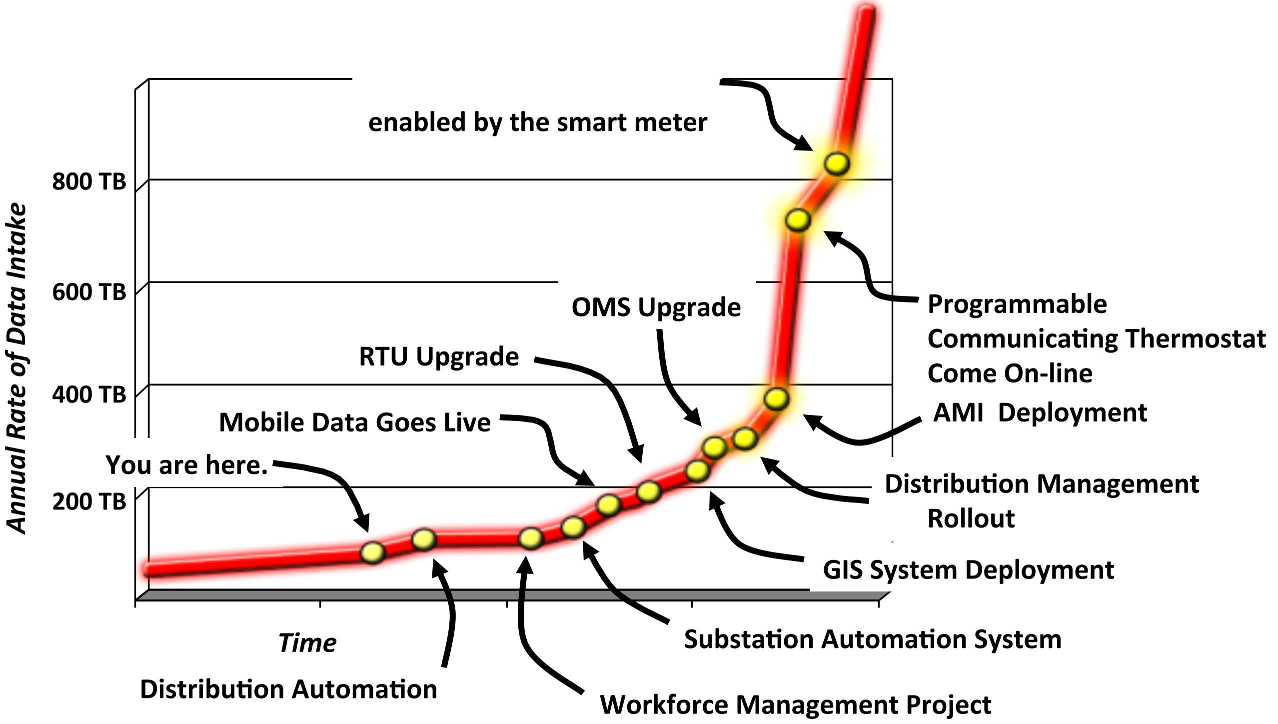


- As system ages, operating cost increases and reliability decrease - limited resources for wholesale replacements
- How to manage Smart Grid assets?
- Need for sound strategy for controlling the symptoms of aging within the utility's overall business plan - maintain ***accepted levels of performance (Metrics!)***

Examples of Smart Grid Technologies & Systems

Electric Transmission Systems	Electric Distribution Systems	Advanced Metering Infrastructure	Customer Systems
			
• Synchrophaser technologies • Communications infrastructure • Wide area monitoring and visualization • Line monitors	• Automated switches • Equipment monitoring • Automated capacitors • Communications infrastructure • Distribution management systems	• Smart meters • Communications infrastructure • Data management systems • Back-office integration	• In-home displays • Programmable communicating thermostats • Home area networks • Web portals • Direct load controls • Smart appliances

Smart Grid: Tsunami of Data Developing



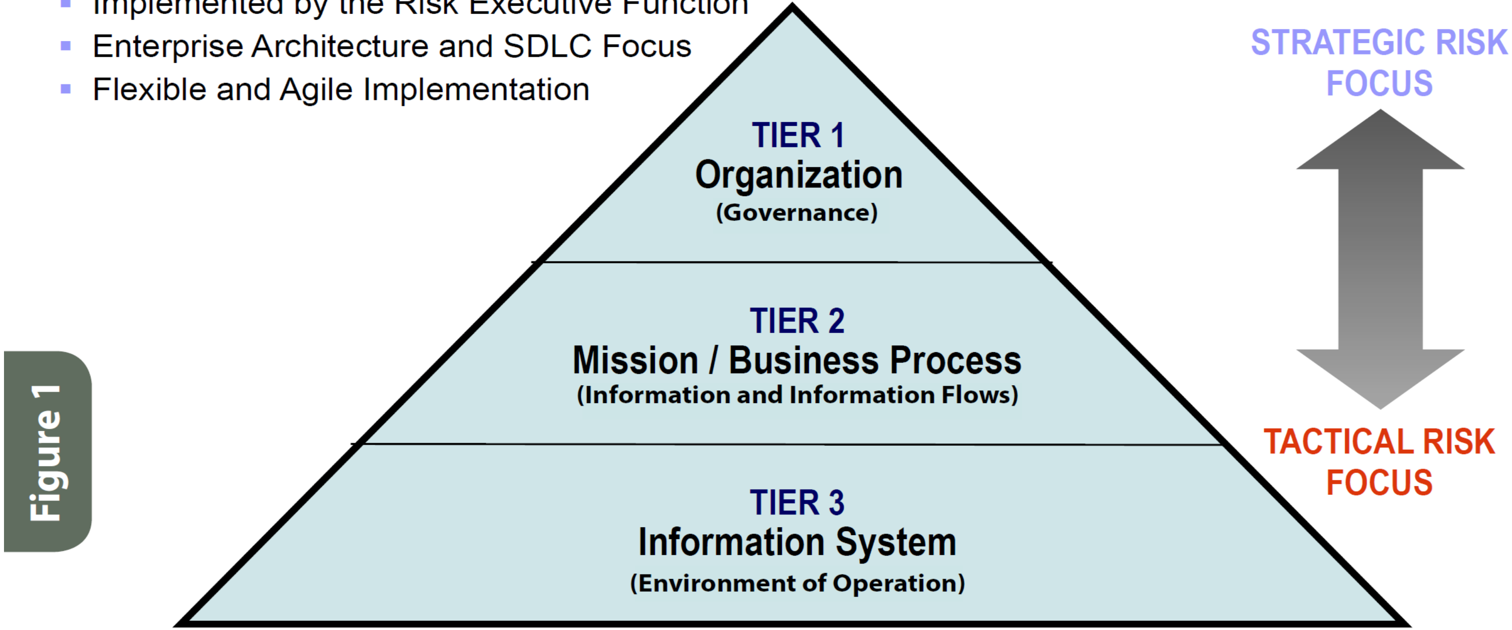
Tremendous amount of data coming from the field in the near future - paradigm shift for how utilities operate and maintain the grid

Industry Needs to Connect 50 Billion Devices by 2020

An unsolved problem costing billions per year in wasted resources requires radically improved wireless performance and lower cost

NIST: Enterprise-Wide Risk Management

- Multi-tiered Risk Management Approach
- Implemented by the Risk Executive Function
- Enterprise Architecture and SDLC Focus
- Flexible and Agile Implementation



Enterprise risk management (conceptual model)
Source: *National Institute of Standards and Technology (NIST)*

Approach

- **Vulnerability mapping**

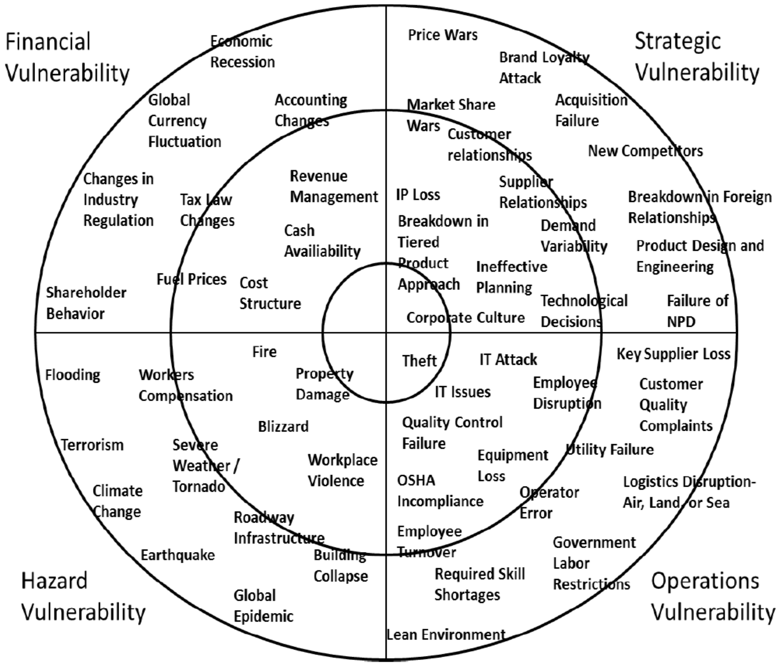


Figure 2

Figure 3

Example of In Depth Analysis: Critical Contingency Situations

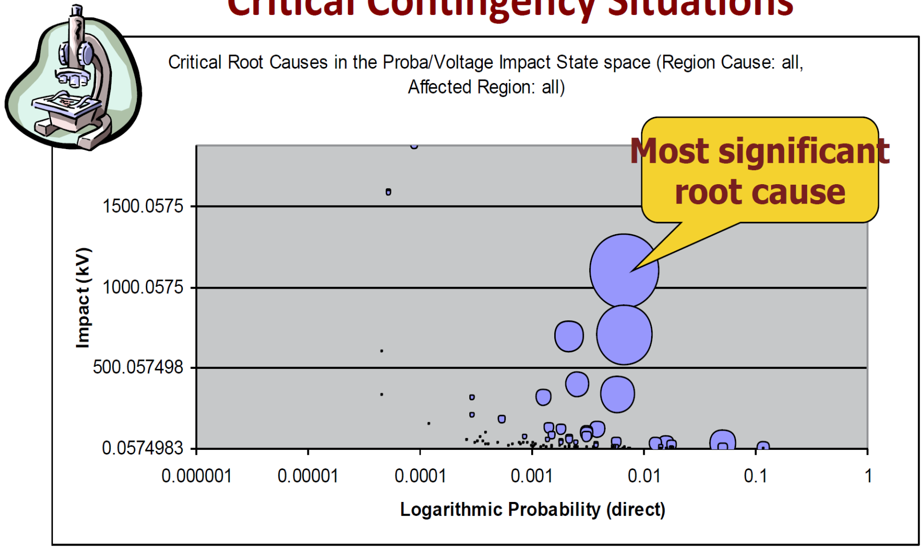


Illustration of how probability and voltage factors can be combined to determine high-priority investments; It is taken from the author's work on adopting the methods discussed in Professor Yossi Sheffi's book, "*The Resilient Enterprise*", for a holistic risk assessment/asset management tool for utility decision-makers

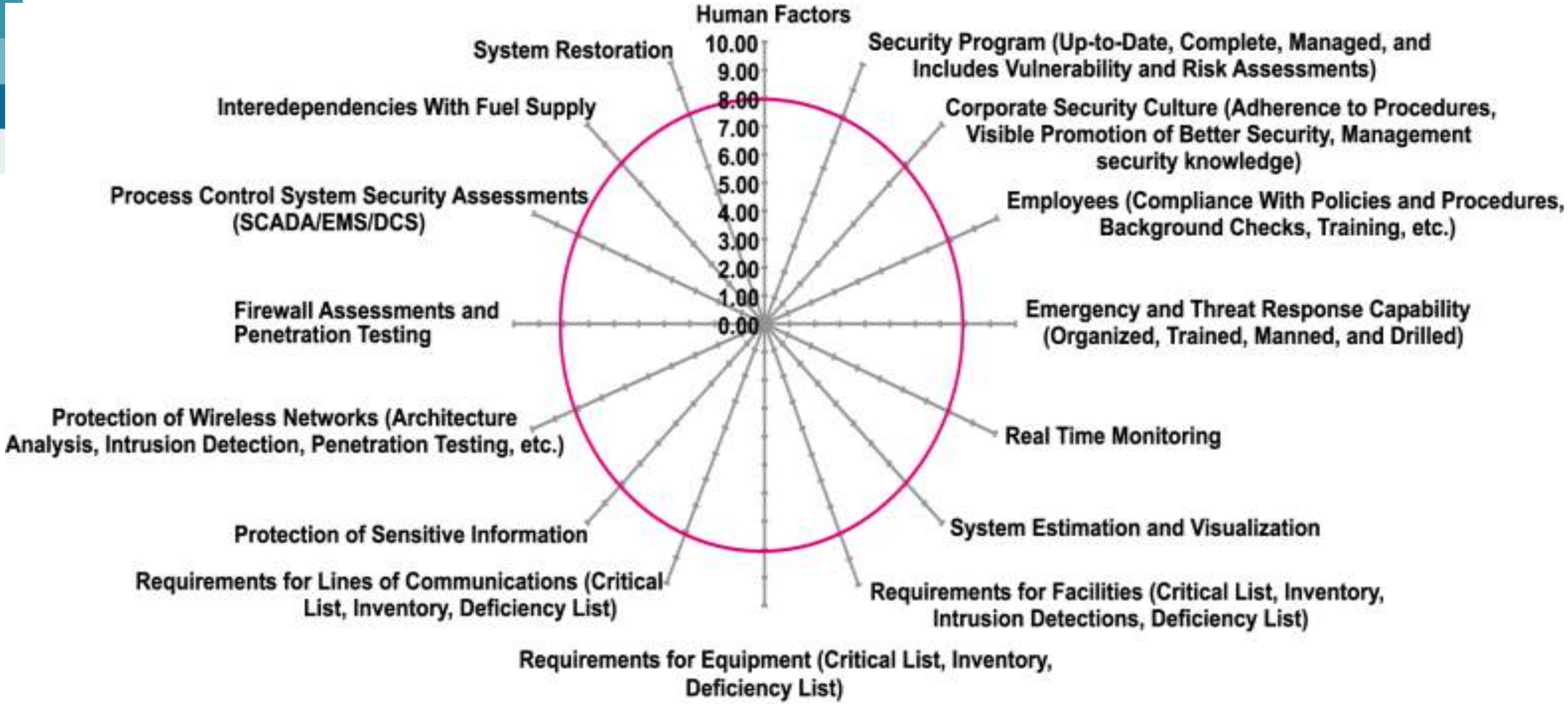
This illustration provides a target-and-crosshairs model for vulnerability mapping to prioritize risk factors across four sectors, including operational, hazard, financial and strategic vulnerabilities

Prioritization: Security Index

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



A "Better" Connected Interdependent Smart Grid

Grid data sharing

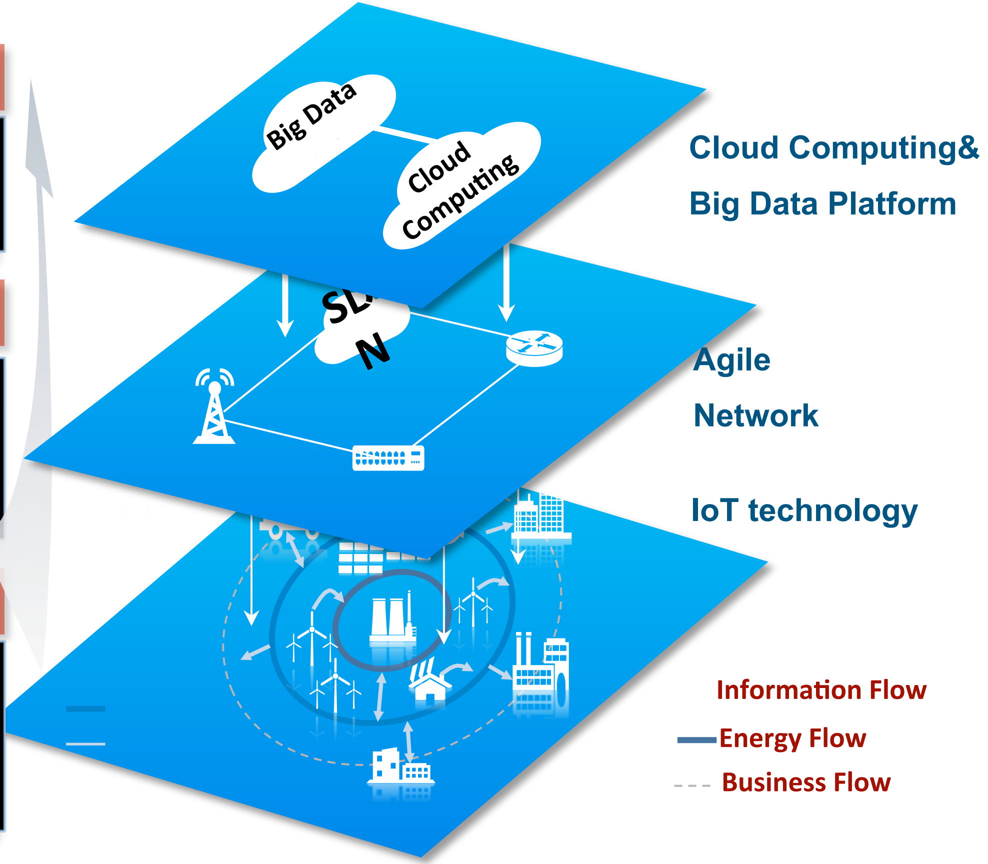
Resource-sharing cloud data centers provides an effective IT platform for business applications like BI, Big Data, decision support & analytics;

Agile communication networks

Fast and robust backbone network , flexible and converged access network offers ubiquitous access to smart devices, achieving real-time bi-directional interaction

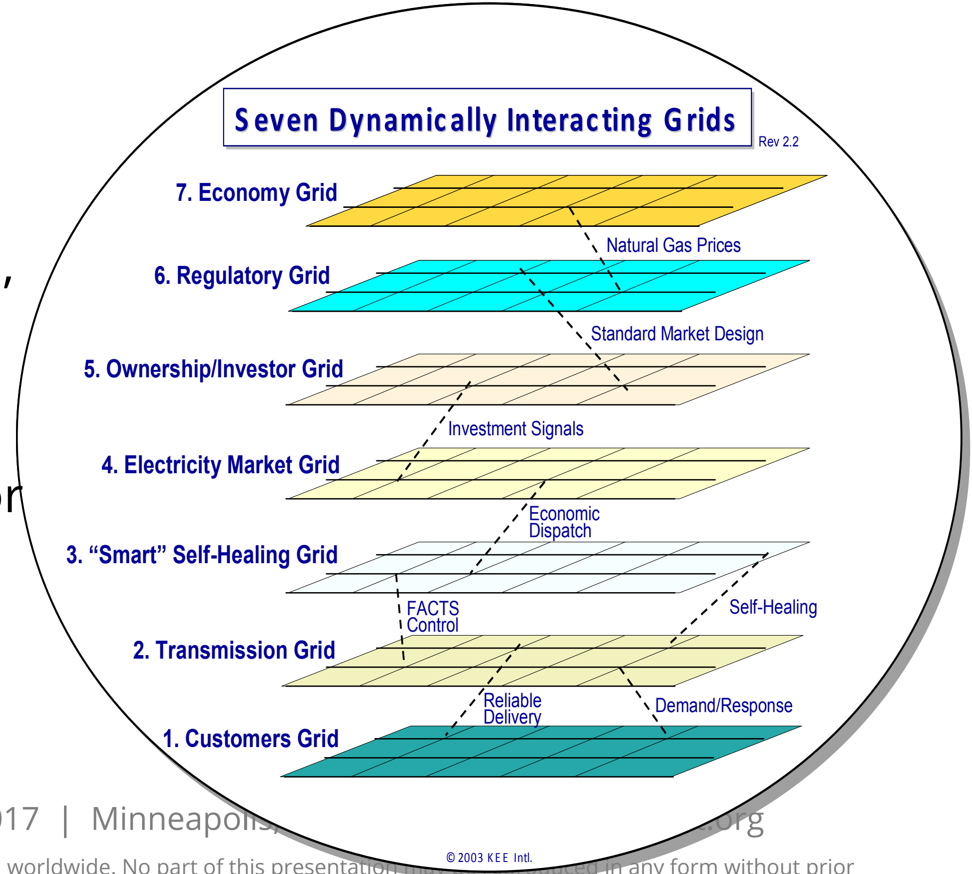
Better-connected smart terminals

With rich interface the IoT gateway implements high-speed two-way interconnection for intelligent meters, sensors, and controllers everywhere, providing communication channel to an open M2M platform

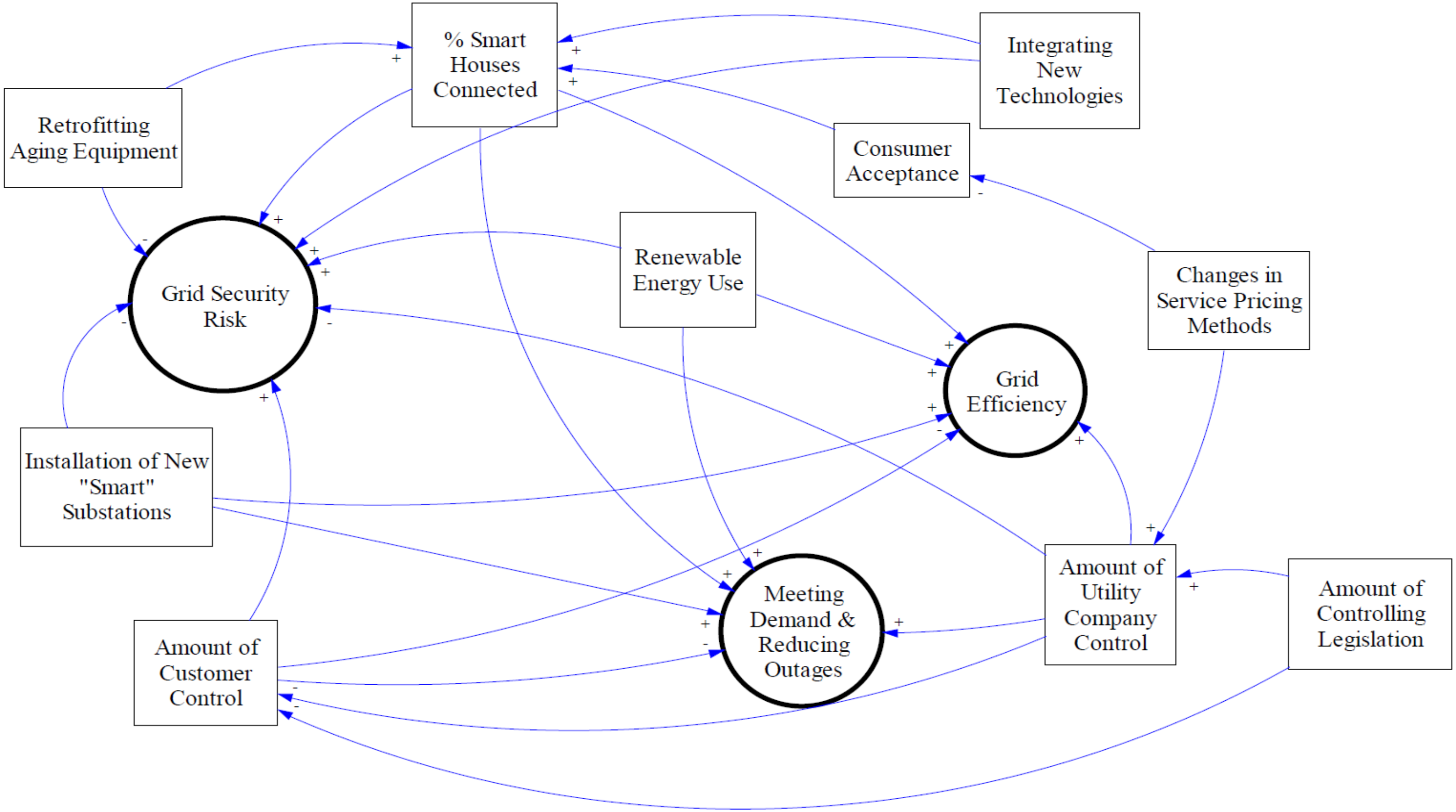


Technology Development, Transition and Implementation: … the really hard part

- STEM-based R&D to enable secure, efficient, resilient and adaptive infrastructure
- Markets and Policy framework, implementation, and evaluation
- Wind-tunnel testing of designs, markets and policy
- Making the business case for the opportunity
- Decision Support Dashboard: Have a plan … Metics .. Foresight…



Critical Infrastructure Interdependencies
Security, Efficiency, and Resilience



Resiliency Metrics

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

Smarter about education, safety, energy, water, food, transp., e-gov. Innovative Cities:

- **Smarter transportation**
  Stockholm, Dublin, Singapore and Brisbane are working with IBM - smart systems ranging from predictive tools to smart cards to congestion charging in order to reduce traffic and pollution.
- **Smarter policing and emergency response**
  New York, Syracuse, Santa Barbara and St. Louis are using data analytics, wireless and video surveillance capabilities to strengthen crime fighting and the coordination of emergency response units.
- **Smarter power and water management**
  Local government agencies, farmers and ranchers in the Paraguay-Paraná River basin to understand the factors that can help to safeguard the quality and availability of the water system. Malta has a smart grid that links the power and water systems, and will detect leakages, allow for variable pricing and provide more control to consumers. Ultimately, it will enable this island country to replace fossil fuels with sustainable energy sources.
- **Smarter governance**
  Albuquerque is using a business intelligence solution to automate data sharing among its 7,000 employees in more than 20 departments, so every employee gets a single version of the truth. It has realized cost savings of almost 2,000%.

"Cities are perfect for promoting change and renewable energies. Cities can serve as innovation platforms, creating clusters of business around green energy."

Top 10 cities

Rank	Country	City	Rating
1	Canada	Vancouver	98.0
2	Austria	Vienna	97.9
3	Australia	Melbourne	97.5
4	Canada	Toronto	97.2
5	Canada	Calgary	96.6
6	Finland	Helsinki	96.2
7	Australia	Sydney	96.1
8=	Australia	Perth	95.9
8=	Australia	Adelaide	95.9
10	New Zealand	Auckland	95.7

The Connected City: Trends and Developments Driving Smart City Innovation

"The Connected City: Trends and Developments Driving Smart City Innovation," produced by MIT Technology Review and IEEE Collabratec:

… vision, efficient use of technology, an environment that attracts a talented workforce, and an enabling infrastructure…

Powering Progress

The Connected City: Trends and Developments Driving Smart City Innovation

IEEE Collabratec

Join the Smart Cities community on IEEE Collabratec

I-35W bridge

Just after 6:00 p.m. on Aug. 1, Prof. Massoud Amin was at work in his office on the University of Minnesota's West Bank, where he heard and watched the unthinkable happen—the collapse of the I-35W bridge about 100 yards away.

"As an individual, it was shocking and very painful to witness it from our offices here in Minneapolis," says Amin, director of the Center for the Development of Technological Leadership (CDTL) and the H.W. Sweatt Chair in Technological Leadership. Amin also viewed the tragedy from a broader perspective as a result of his ongoing work to advance the security and health of the nation's infrastructure.

In the days and weeks that followed, he responded to media inquiries from the BBC, Reuthers, and the CBC, keeping his comments focused on the critical nature of the infrastructure. He referred reporters with questions about bridge design, conditions, and inspections to several professional colleagues, including Professors Roberto Ballarini, Ted Galambos, Vaughan Voller, and John Gulliver in the Department of Civil Engineering and the National Academy of Engineering Board on Infrastructure and Constructed Environment.

For Amin, Voller, and many others, the bridge collapse puts into focus the importance of two key issues—the tremendous value of infrastructure and infrastructure systems that help make possible indispensable activities such as transportation, waste disposal, water, telecommunications, and electricity and power, among many others, and the search for positive and innovative ways to strengthen the infrastructure.

To improve the future and avoid a repetition of the past:

Sensors built in to the I-35W bridge at less than 0.5% total cost by TLI alumni

Terry Ward Heidi Hamilton Val Svensson Joe Nietfeld

Technological Leadership Institute

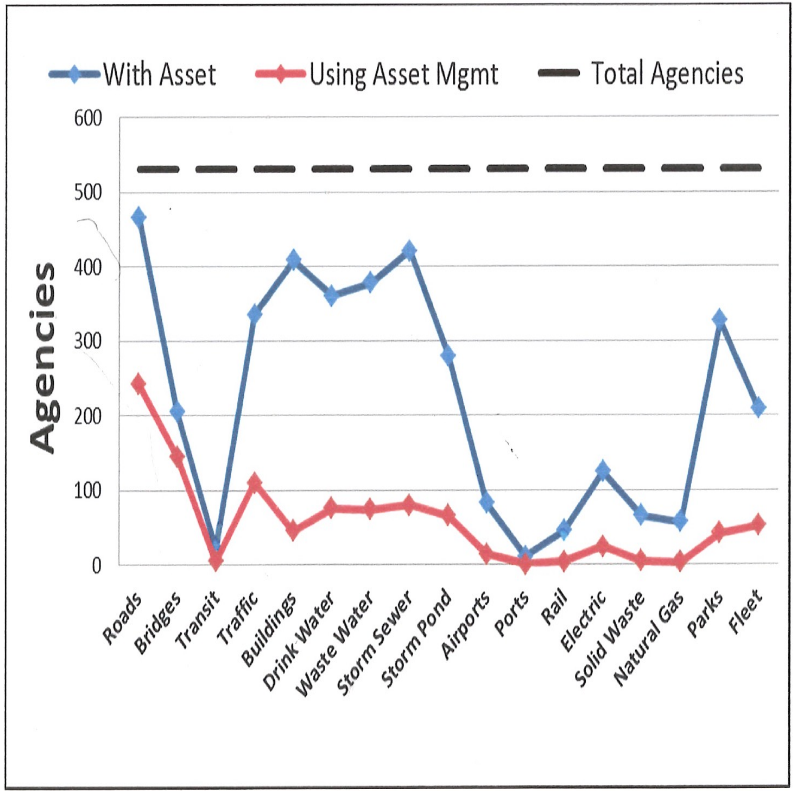
University of Minnesota
Driven to Discover℠

Not Just Utilities … Our Role in Minnesota: 2015 MN2050 Survey

	2015 Values				
	Small City	Large City	County	State	Total
Roads	$4,174,022,424	$10,517,476,430	$27,647,815,260	$29,338,312,840	$71,677,626,954
Bridges	$1,151,894,172	$807,350,570	$1,456,009,206	$6,592,940,562	$10,008,194,510
Transit	$0	$0	$0	$0	$0
Traffic	$14,168,440	$138,820,460	$59,985,398	$0	$212,974,298
Buildings	$7,583,657,510	$13,724,959,690	$4,869,723,674	$501,696,056	$26,680,036,930
Water	$1,499,020,952	$6,279,799,230	$0	$0	$7,778,820,182
Waste Water	$1,704,463,332	$4,244,983,540	$0	$6,494,782,638	$12,444,229,510
Storm sewer	$0	$2,085,960,070	$0	$0	$2,085,960,070
Storm ponds	$150,185,464	$65,757,060	$5,453,218	$0	$221,395,742
Airports	$1,240,446,922	$1,344,366,560	$0	$0	$2,584,813,482
Ports	$0	$0	$0	$0	$0
Rail	$0	$0	$3,173,772,876	$0	$3,173,772,876
Electrical	$0	$10,564,967,640	$0	$0	$10,564,967,640
Solid Waste	$0	$94,982,420	$796,169,828	$0	$891,152,248
Natural Gas	$2,056,549,066	$2,747,183,840	$0	$0	$4,803,732,906
Total	**$19.5B**	**$52.6B**	**$38.0B**	**$42.9B**	**$153B**

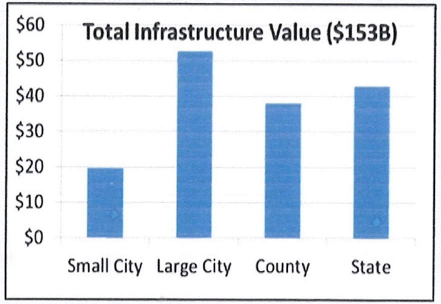
Not Just Utilities … Our Role in Minnesota:

2015 MN2050 Survey



2015 Values

	Small City	Large City	County	State	Total
Roads	$4,174,022,424	$10,517,476,430	$27,647,815,260	$29,338,312,840	$71,677,626,954
Bridges	$1,151,894,172	$807,350,570	$1,456,009,206	$6,592,940,562	$10,008,194,510
Transit					$0
Traffic					$212,974,298
Buildings					$26,680,036,930
Water					$7,778,820,182
Waste Water					$12,444,229,510
Storm sewer					$2,085,960,070
Storm ponds					$221,395,742
Airports					$2,584,813,482
Ports					$0
Rail					$3,173,772,876
Electrical					$10,564,967,640
Solid Waste					$891,152,248
Natural Gas					$4,803,732,906
Total	$19.5B	$52.6B	$38.0B	$42.9B	$153B



Assets Managed by Cities, Counties and State Agencies

	Assets Managed	Road	Bridge	Transit	Traffic	Buildings	Drink Water	Waste Water	Storm Sewer	Storm Pond	Airports	Ports	Railways	Electrical	Solid Waste	Natural Gas	Total
Small Cities	14	97	11	1	55	71	92	92	89	54	15	0	7	18	5	9	616
Large Cities	15	187	88	4	112	109	128	139	137	133	19	2	9	54	9	7	1137
Counties	14	132	99	4	64	45	7	5	36	18	8	0	4	4	18	3	447
State Agencies	7	9	3	0	3	7	0	4	2	2	0	0	0	0	0	0	30
Totals =		425	201	9	234	232	227	240	264	207	42	2	20	76	32	19	2230

Providing reliable and resilient systems requires organizations that can

- ⌘Anticipate
- ⌘Plan
- ⌘Implement
- ⌘Adapt and improvise

Coordination and Communication:

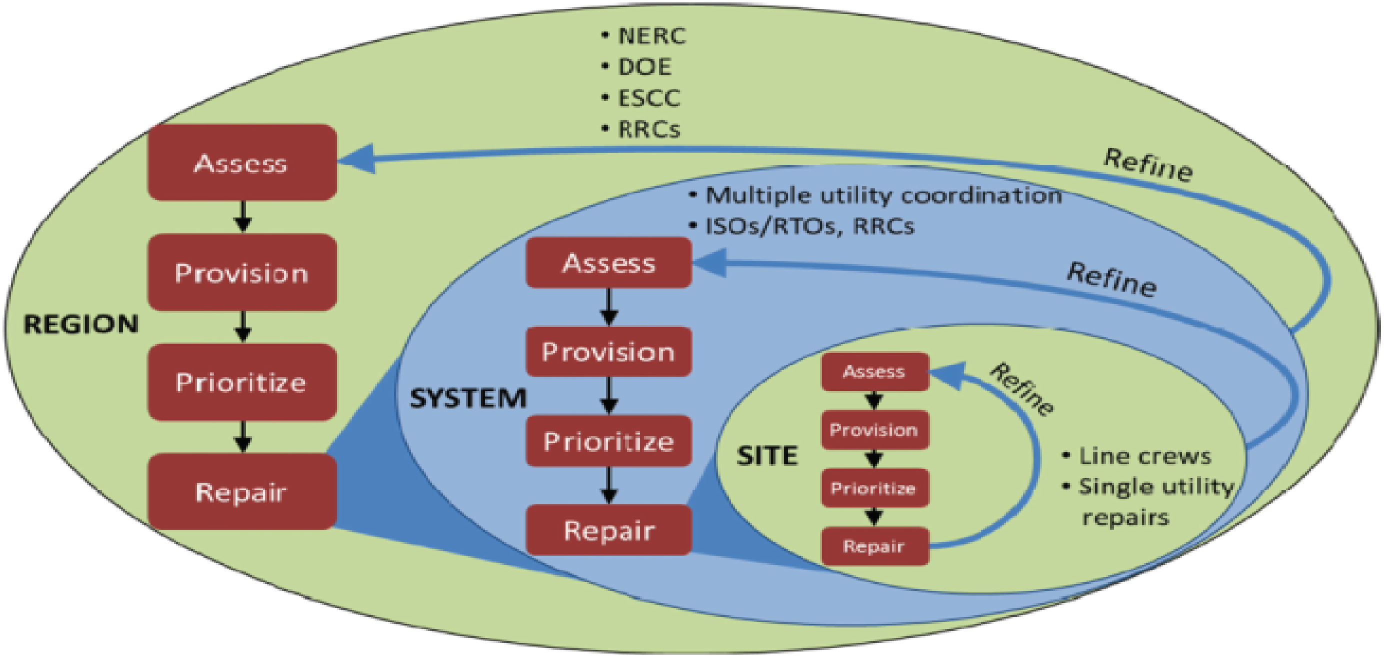
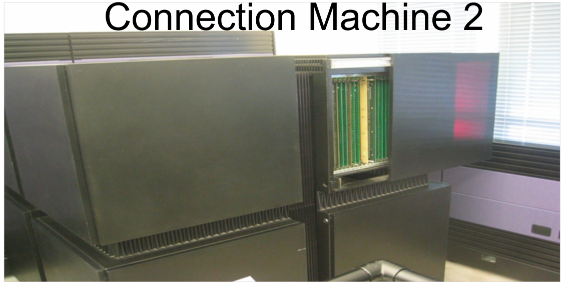


FIGURE 6.1 Illustration of the general processes of restoration that occur on multiple levels by different institutions with responsibility for electricity restoration.
NOTE: NERC, North American Electric Reliability Corporation; DOE, Department of Energy; ESCC, Electricity Subsector Coordinating Council; RRC, Regional reliability coordinator; ISO, Independent system operator; RTO, Regional transmission operator.

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

Fast Power Systems Risk Assessment

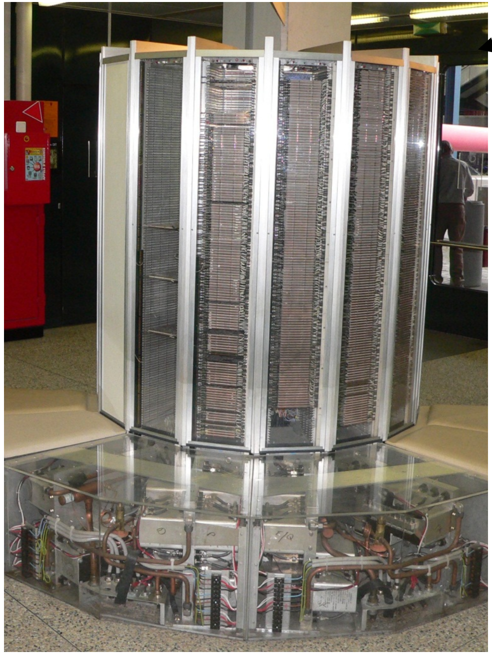
1987 → **2010**



$5,000,000 → **$350**

Only a dozen built → **100 million sold**

Fast Power Grid Simulation

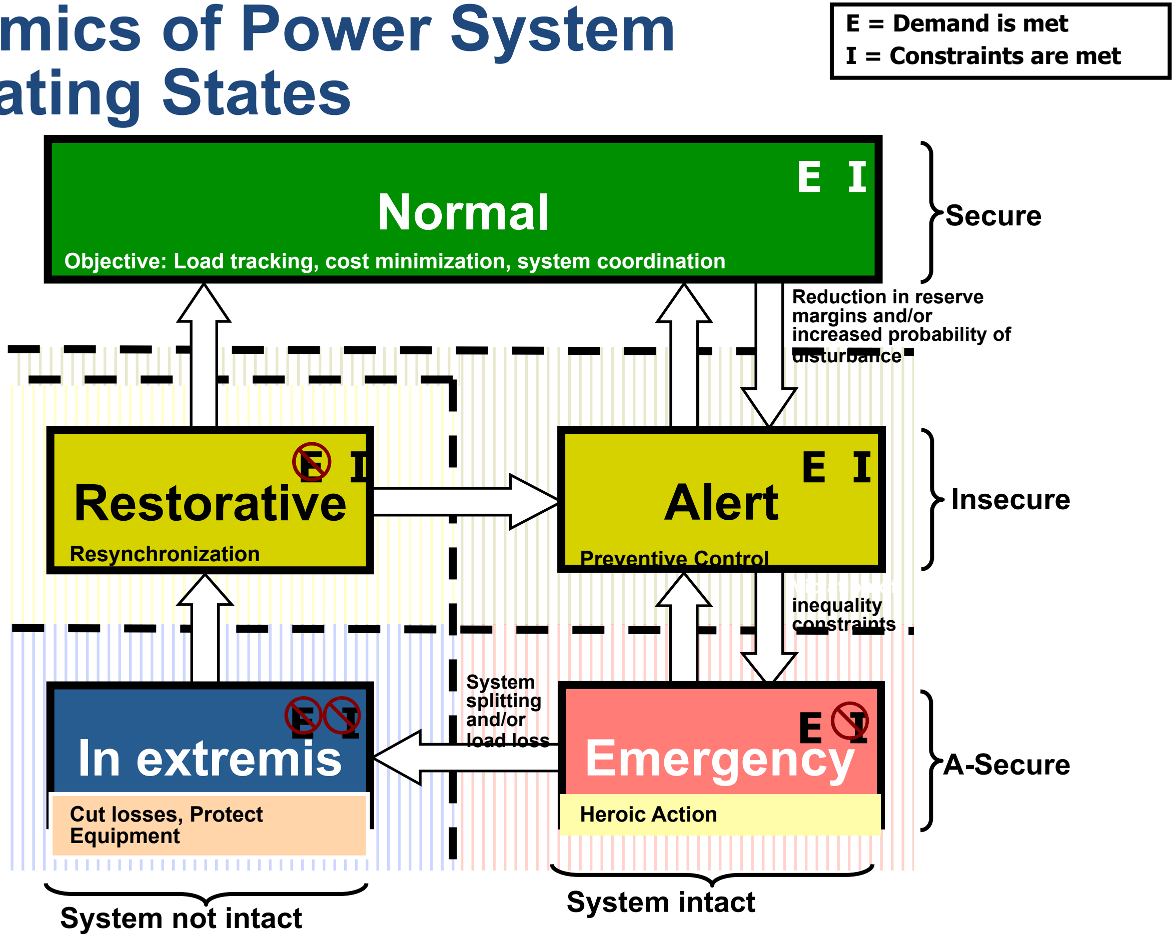


CRAY Supercomputer

Nvidia GeForce GPU card for PC

Use Nvidia GeForce GPU card to gain 15 times faster power flow calculation on PC

Dynamics of Power System Operating States

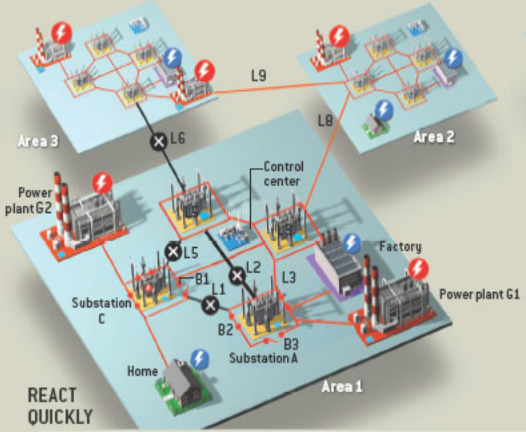


Smart Self-Healing Grid

"Preventing Blackouts," Scientific American, May 2007

THE SOLUTION: A SMART GRID THAT HEALS ITSELF

Imagine that a thunderstorm knocks out power lines L5 and L6. This occurrence would typically cause a chain reaction of line faults that would black out Area 1. But a smart grid would isolate and correct the problem as depicted below. The action begins as a look-ahead computer at the control center simulates corrective actions in less than half a second and sends instructions to control computers around the grid.



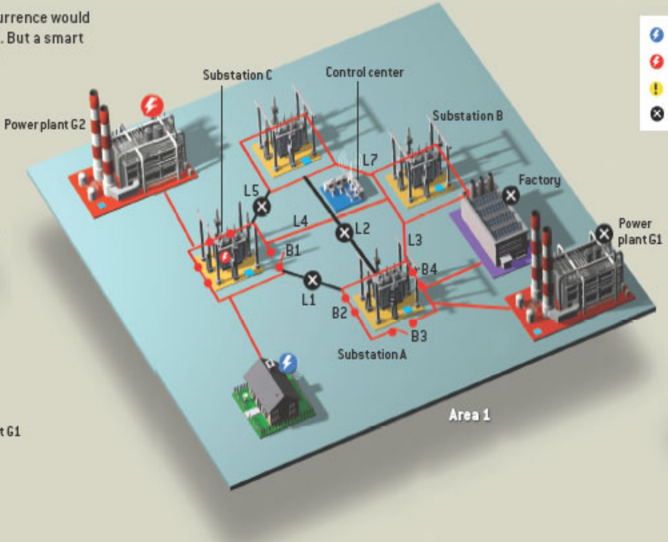
REACT QUICKLY

0.04 second later
The loss of L5 and L6 causes a fault in line L1. Control computers tell circuit breakers B1 and B2 to open to isolate the fault, but B2 becomes stuck in the closed position.

0.1 second
Power generator G1 automatically accelerates to meet demand from the loss of G2 caused by problems on lines L5 and L1. G1 also accelerates to attempt to keep line voltage throughout Area 1 at the required 60 hertz (cycles per second).

0.4 second
The control computer-simulator in substation A tells breaker B3 to open to protect the substation against damage from excessive current flow through it. B3 opens, shutting down line L2. G1 accelerates further to compensate.

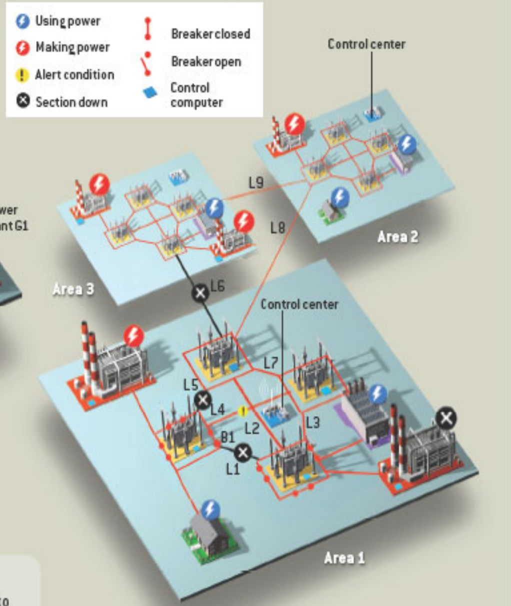
0.5 second
The control center shuts down generator G1 to prevent damage to it from excessive acceleration.



MAKE DECISIONS

0.6 second
The control computer in substation B would typically shut down line L3 to reduce demand if generator G1 were accidentally lost, but because it was stopped deliberately, computers across Area 1 communicate and decide instead to shut down a big factory, lowering demand considerably. This action reduces the mismatch between generation and demand so critical functions such as streetlights and hospitals can stay powered.

10 seconds
After several seconds, however, the substation B computer detects that the voltage there is beginning to oscillate beyond safe tolerances because the mismatch is still significant, threatening to damage equipment on lines L3, L4 and L7. Rather than shutting down those lines (the old-fashioned response), the area computers change control of generator G2 to manual, advising human operators at the Area 1 control center to raise generation or reduce load. They do some of both.

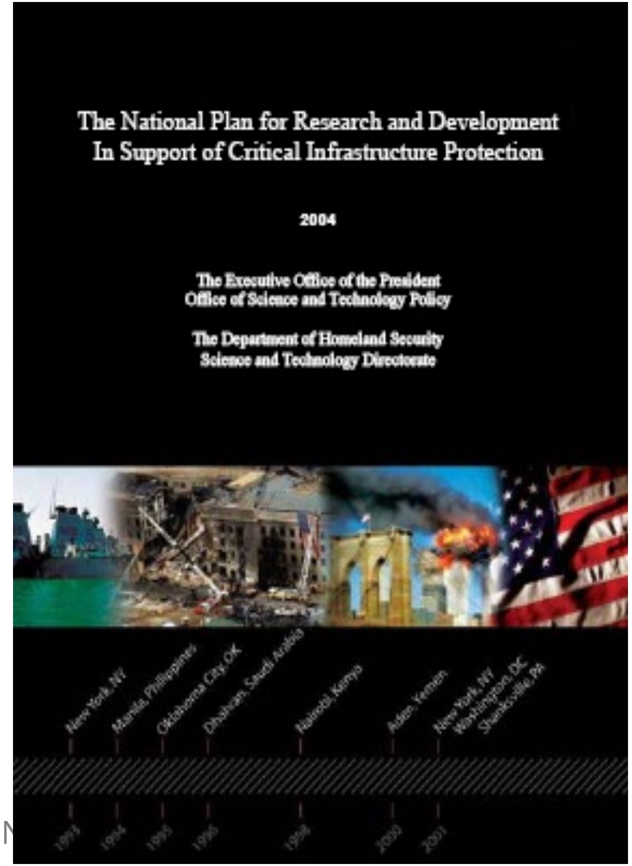


RETURN TO NORMAL

60 seconds
Lines L3, L4 and L7 have been spared, but L4 is becoming overloaded. Human operators at the control center communicate via satellite to operators in the Area 2 control center, asking for help. Operators in Area 2 send power over line L8; they also instruct the control computers in their sector to modify power flows slightly to compensate for the sudden export. Once road crews fix damaged lines L5 and L6, the computers will bring L1 and power plant G1 back into service. Power in the three areas returns to normal flow.

THE NATIONAL PLAN FOR RESEARCH AND DEVELOPMENT IN SUPPORT OF CIP

- The area of **self-healing infrastructure** has been recommended by the White House Office of Science and Technology Policy (OSTP) and the U.S. Department of Homeland Security (DHS) **as one of three thrust areas for the National Plan for research and development in support of Critical Infrastructure Protection (CIP).**



prior

BASIS OF FUTURE COMPETITION

The speed at which an Enterprise can

- Gather
- Collate
- Analyze
- Apply information

Looking Beyond Interdependencies: Other Pressing Infrastructure Security Issues

Current focus on technical, practitioner-related challenges—Tyranny of the In-Box

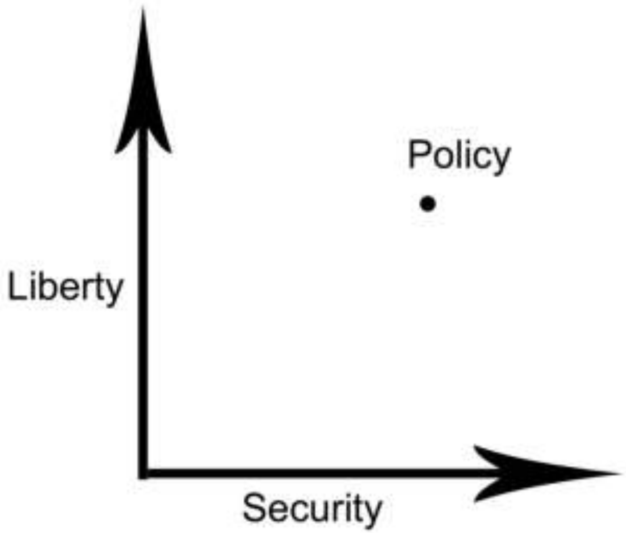
Not Being Adequately Addressed:

1. Building the necessary policy foundation that addresses legal, ethical, and defense in depth issues in assuring Local/State/National/Global infrastructures
2. Long-term analysis of what technology, political and economic developments will have far-reaching repercussions for securing infrastructures and keeping them secure (with Economic Growth opportunities)

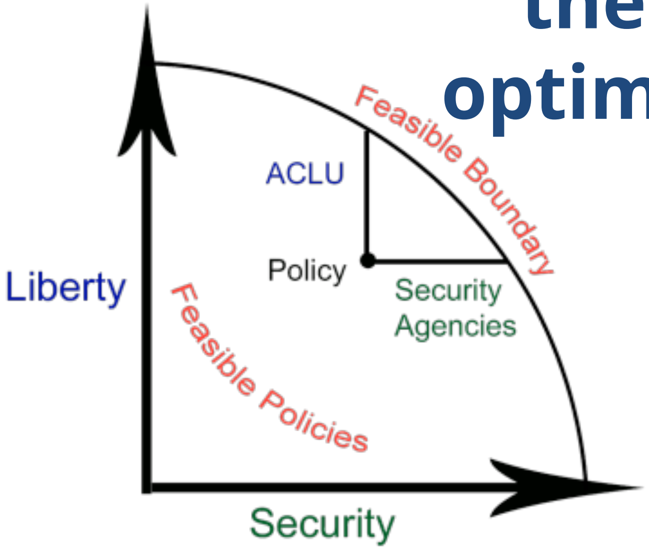
Can we build non-intrusive yet high confidence tools, systems, processes that increase our security AND preserve/extend our civil rights?

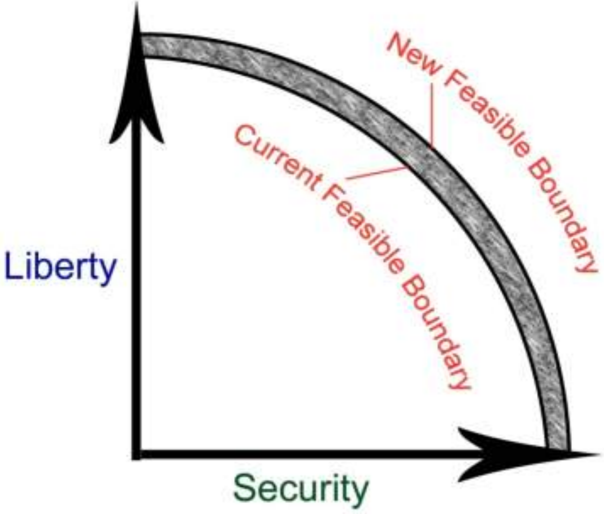
Synergy Between Security Technologies & Policy

- Incorporate security and privacy early as "design criteria"
- Provide policy impact statement
  - E.g. tradeoffs between "liberty & security"?
  - Non/low-intrusive but high confidence technologies analogous to "MRI"
  - Plot the space



Where is a given policy w.r.t. -a theoretically optimal front





Implications for new technologies -<u>some</u> offer more "L" or more "S"

- **-What if we offer both?**
- **-Can this be a design criteria?**

E.g. remote monitoring; anomaly detection; wide-area tamper detection

Recommendations - *Security, Privacy, and Resilience*

- Speed up the development and enforcement of **cyber security standards**, compliance requirements and their adoption. Facilitate and encourage design of security from the start and include it in standards.
- **Design communications and controls systems** for more limited failures including better EMP withstand capabilities
- Increase investment in the grid and in R&D areas that assure the security of the cyber infrastructure (algorithms, protocols, chip-level and application-level security).

Source: IEEE report to the U.S. DOE for the White House's Quadrennial Energy Review (QER) to guide U.S. energy policy. http://www.ieee-pes.org/final-ieee-report-to-doe-qer-on-priority-issues

New Business Opportunities

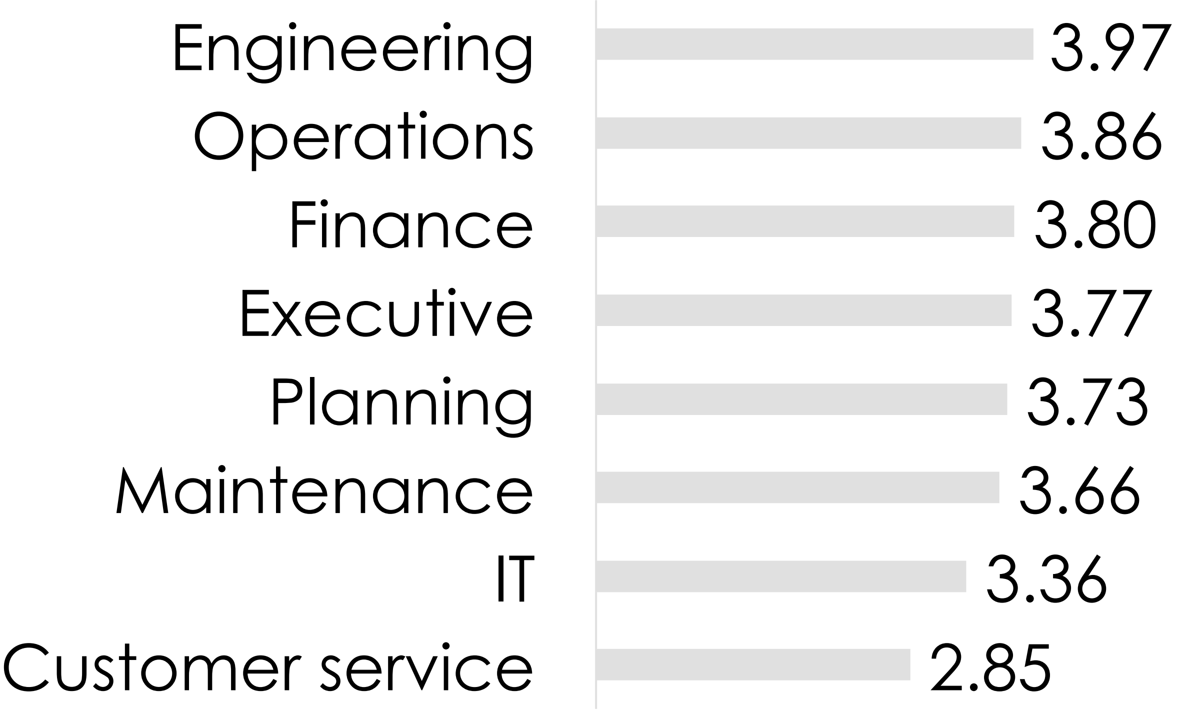
- Turnkey Smart Buildings
- Web-enabled Energy Systems
- Residential DR
- Turnkey Perfect Power Retailing
- Turnkey AMI
- Commercial Perfect Power Retailing
- Enhanced Distribution Reliability Zones
- Entrepreneurial Microgrids

Unlocking Smart Grid Benefits Requires

- Intelligent Technology
- Intelligent Policy
- Empowered Consumers & Communities

INTELLIGENCE = the ability to understand and deal successfully with new situations

Workforce: A VARIETY of people are needed…



…for a variety of things

(like data-driven asset management)

Role of groups in asset management (1 = no role, 5 = significant role)

Source: ABB – Zpryme survey of 150 utility executives, 2015-2016.

What to do? Pathways forward

1. **Create National Infrastructure Banks:**
   - Focused on addressing both the much-needed repairs today (to modernize existing aging infrastructure) AND also to bridge to more advanced, smarter, more secure and sustainable lifeline infrastructures envisioned for the next 10-20 years.
   - Created as public/private partnership enterprises that lend money on a sustainable basis and has clear cost/benefit, performance metrics and include fees for quality of services provided by the modernized infrastructures.

2. **Retool/re-train our best and brightest for this call to action:**
   - **Some of the best talents to help rebuild our critical infrastructure are our veterans of the Armed Forces.**

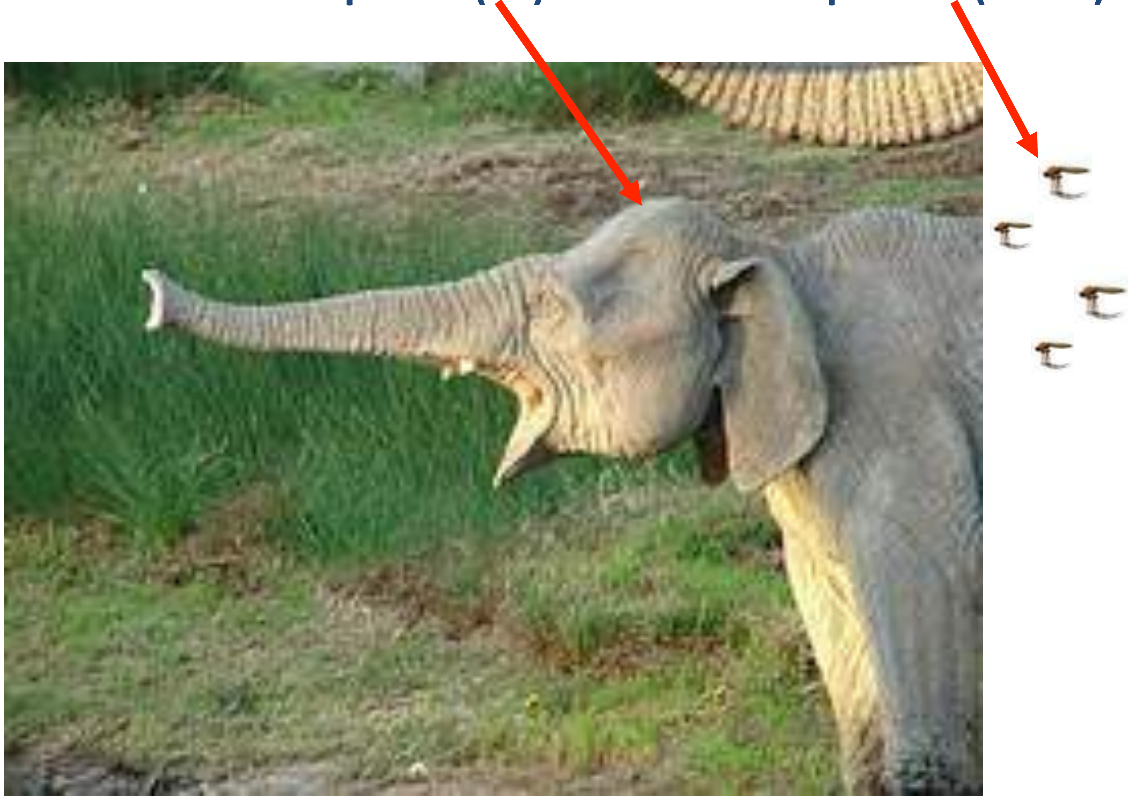
3. **Renew/Update the American Model:**
   - **Align innovation and policy: Focus, Alignment, Collaboration, and Execution to revitalize leadership in education, R&D, innovation and entrepreneurship.**

Embrace Change?

- Build Smarter, More Secure, Resilient, and Sustainable Lifeline Infrastructures
- Develop World-Class Human Capital
- Create Jobs - Grow The Economy - Power Progress

Bottom line

Elephant (us) …….and Mosquitoes (them)



Vision of future

...and

..and


THANK YOU
MINNESOTA