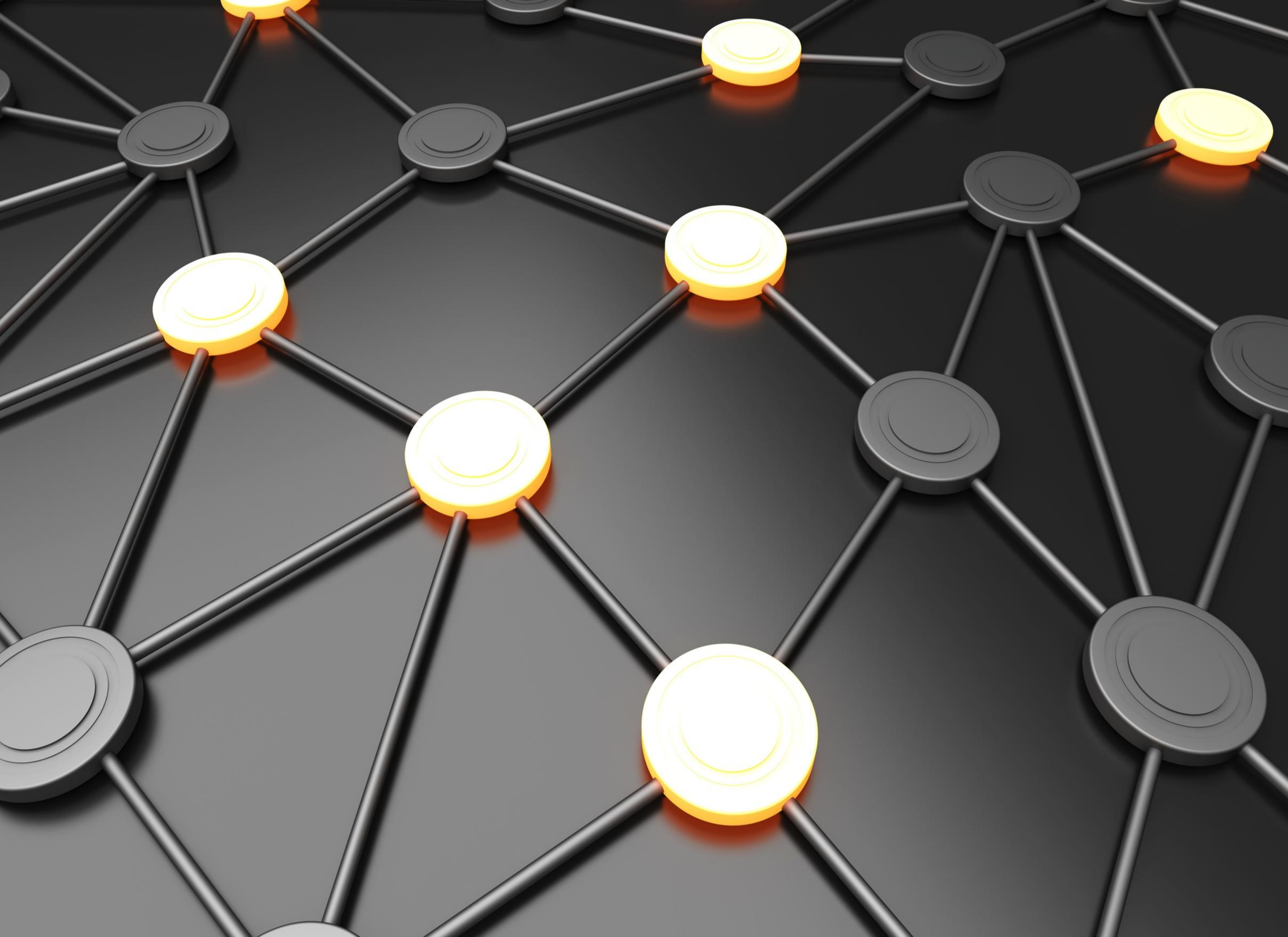
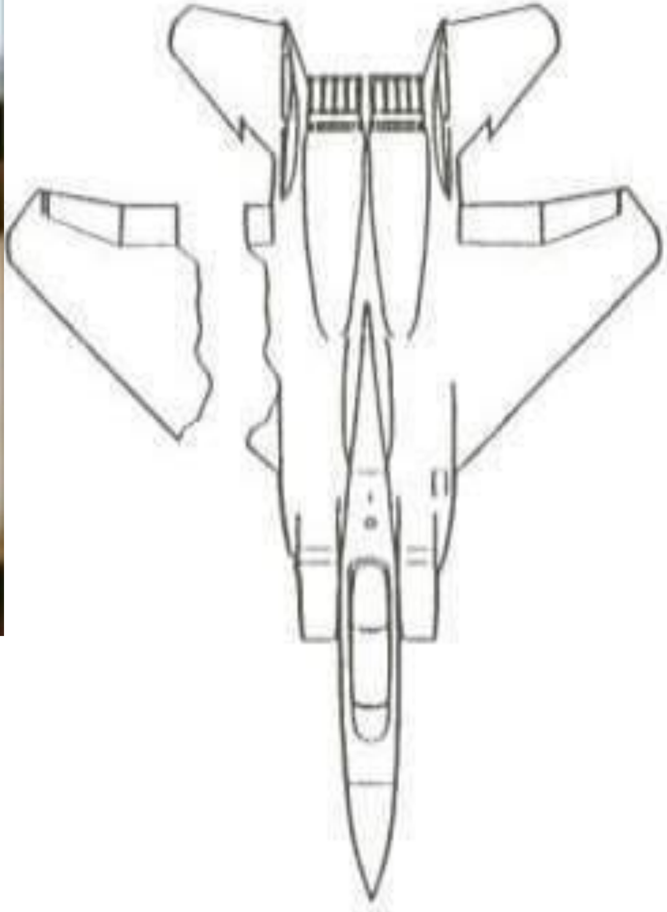
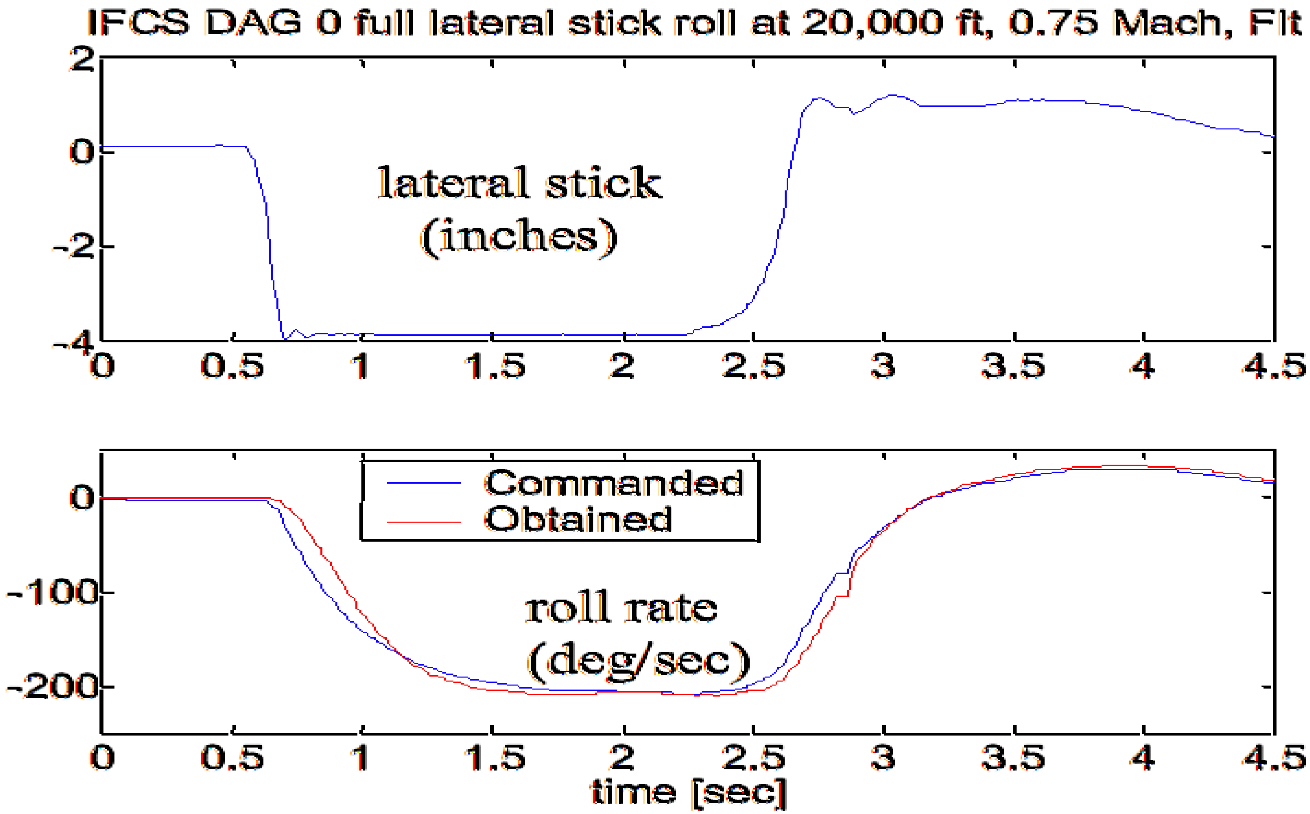
So, Where are we exactly?





NASA/MDA/WU IFCS: NASA Ames Research Center, NASA Dryden, Boeing Phantom Works, and Washington University in St. Louis.


IFCS DAG 0 full lateral stick roll at 20,000 ft, 0.75 Mach, Flt 126
lateral stick
(inches)
2
0
-2
-4
0
0.5
1
1.5
2
2.5
3
3.5
4
4.5
Commanded
Obtained
roll rate
(deg/sec)
0
-100
-200
time [sec]

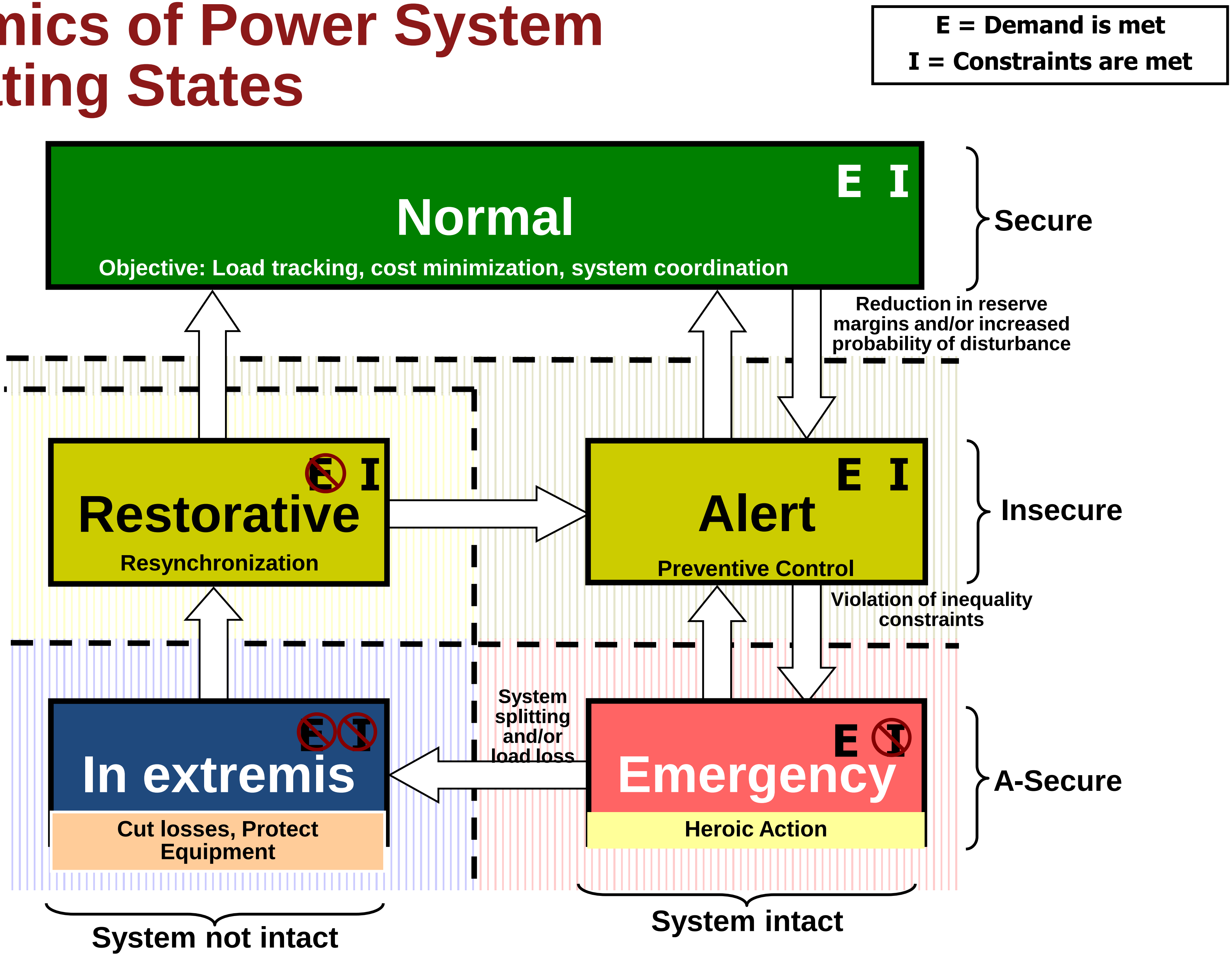
Critical System Dynamics and Resilience Capabilities

- **Anticipation of disruptive events**
- **Look-ahead simulation capability**
- **Fast isolation and sectionalization**
- **Adaptive islanding**
- **Self-healing and restoration**

re·sil·ience, *noun,* 1824: The capability of a strained body to recover its size and shape after deformation caused especially by compressive stress; An ability to recover from or adjust easily to misfortune or change

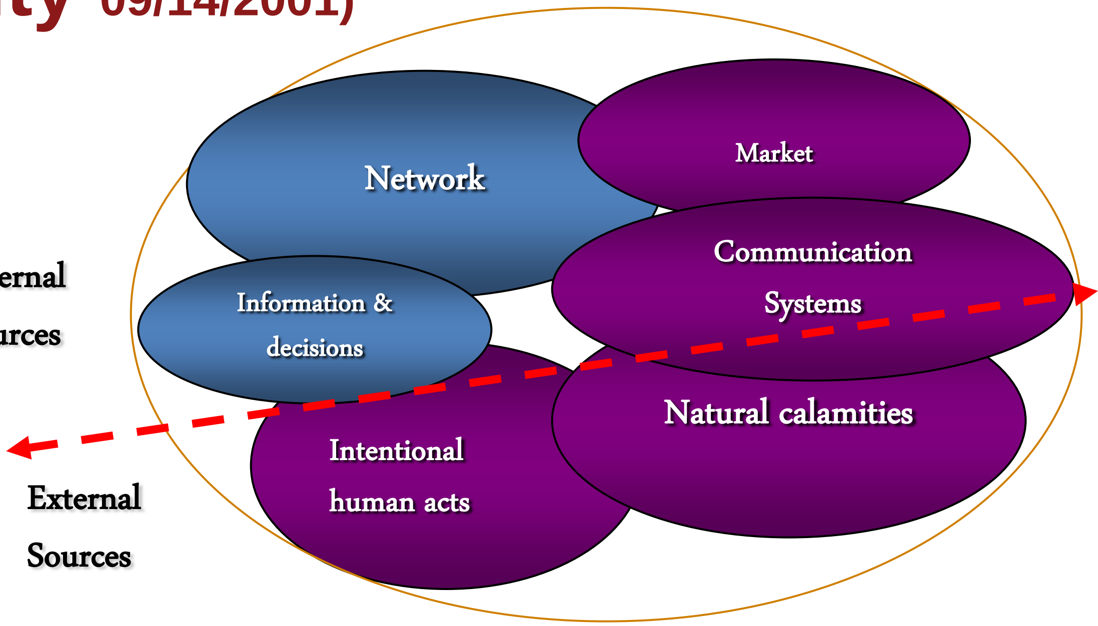
Resilience enables "Robustness": A system, organism or design may be said to be "robust" if it is capable of coping well with variations (internal or external and sometimes unpredictable) in its operating environment with minimal damage, alteration or loss of functionality.

Dynamics of Power System Operating States



Context: Threats to Security 09/14/2001)

Sources of Vulnerability



- Transformer, line reactors, series capacitors, transmission lines...
- Protection of ALL the widely diverse and dispersed assets is impractical

-- over 215,000 miles of HV lines (230 kV and above

-- 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
- Biological contamination (real or threat)
- Over-reaction to isolated incidents
- Internet Attacks
- Over 80,000 hits/day at an ISO
- Hijacking of control
- Storms, Earthquakes, Forest fires & grass land fires… Loss of major equipment – especially transformers…

“… for want of a horseshoe nail … "

Utility Telecommunications

- Electric power utilities usually own and operate at least parts of their own telecommunications systems
- Consist of backbone fiber optic or microwave connecting major substations, with spurs to smaller sites
- Media:
  - Fiber optic cables
  - Digital microwave
  - Analog microwave
  - Multiple Address Radio (MAS)
  - Spread Spectrum Radio
  - VSAT satellite
  - Power Line Carrier
  - Copper Cable
  - Leased Lines and/or Facilities
  - Trunked Mobile Radio
  - Cellular Digital Packet Data (CDPD)
  - Special systems (Itron, CellNet)

New Challenges for a Smart Grid

- Need to integrate:
  - Large-scale stochastic (uncertain) renewable generation
  - Electric energy storage
  - Distributed generation
  - Plug-in hybrid electric vehicles
  - Demand response (smart meters)

- Need to deploy and integrate:
  - New Synchronized measurement technologies
  - New sensors
  - New System Integrity Protection Schemes (SIPS)

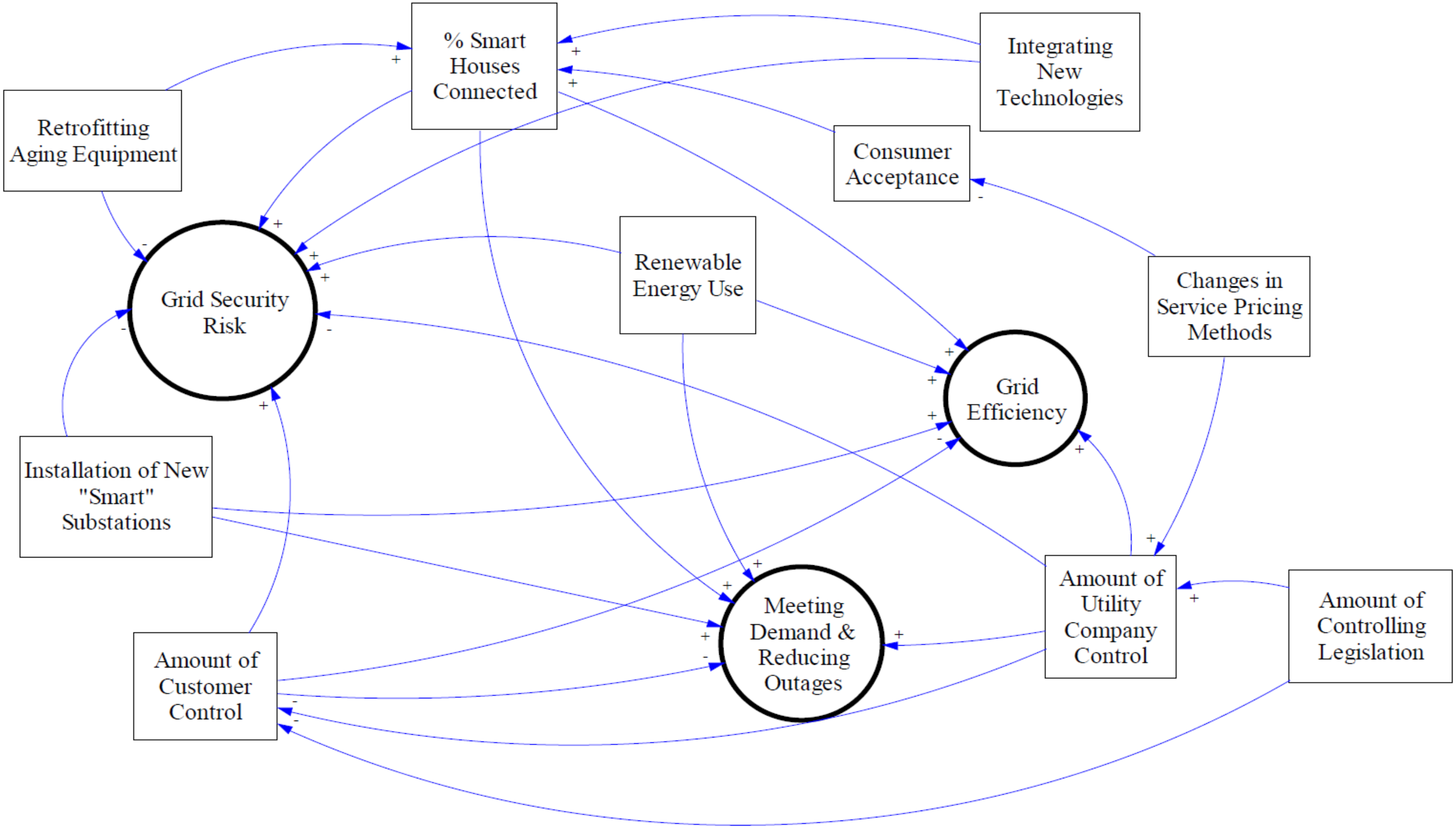
- Critical Security Controls

Smart Grid Vulnerabilities

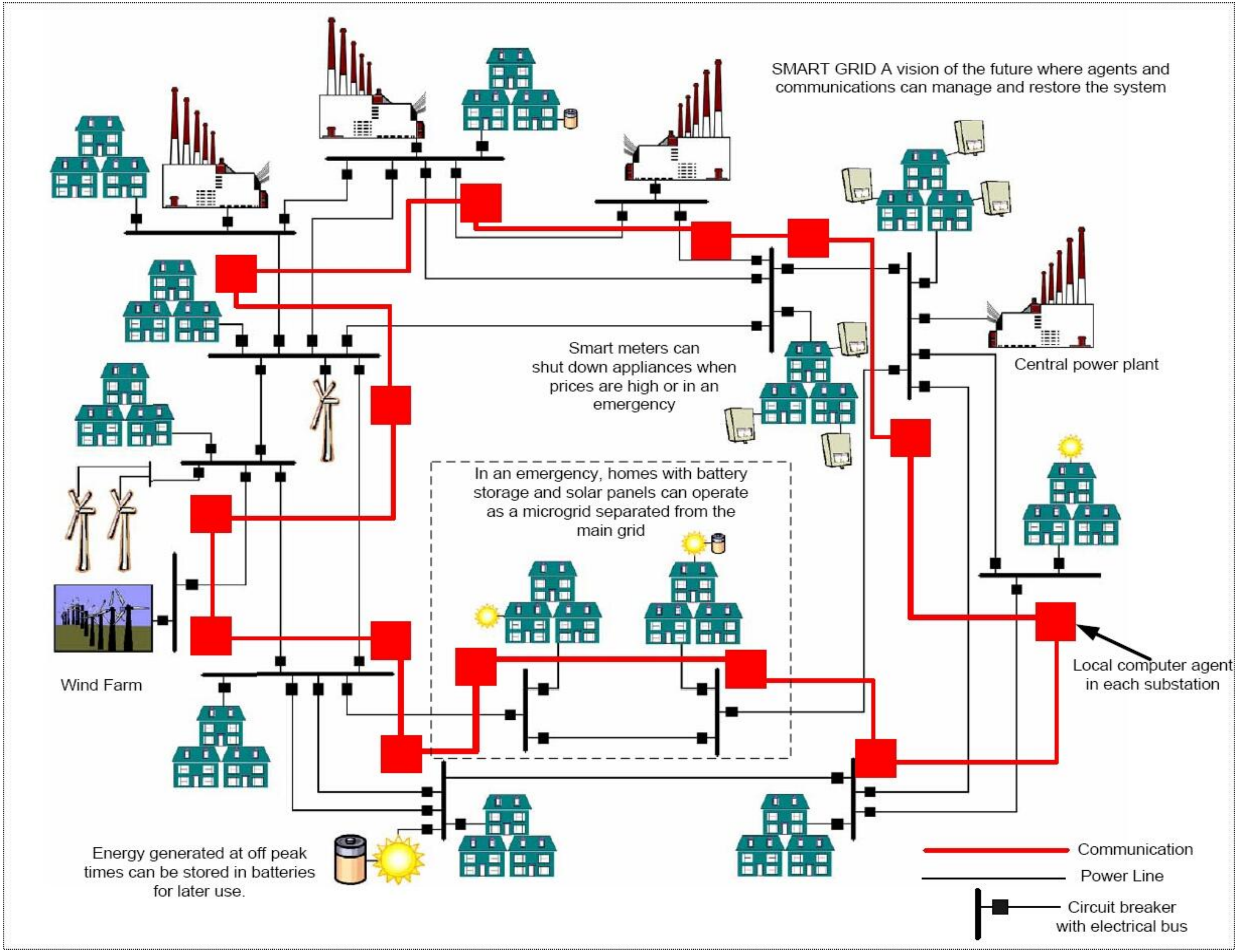
- Cyber:
  - Existing control systems were designed for use with proprietary, stand-alone communications networks
  - Numerous types of equipment and protocols are used
  - More than 90% of successful cyber attacks take advantage of known vulnerabilities and misconfigured operating systems, servers, and network devices
  - Possible effects of attacks:
    1) Loss of load
    2) Loss of information
    3) Economic loss
    4) Equipment damage

Smart Grid Interdependencies

Security, Efficiency, and Resilience



Our team's Smart Grid Research



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

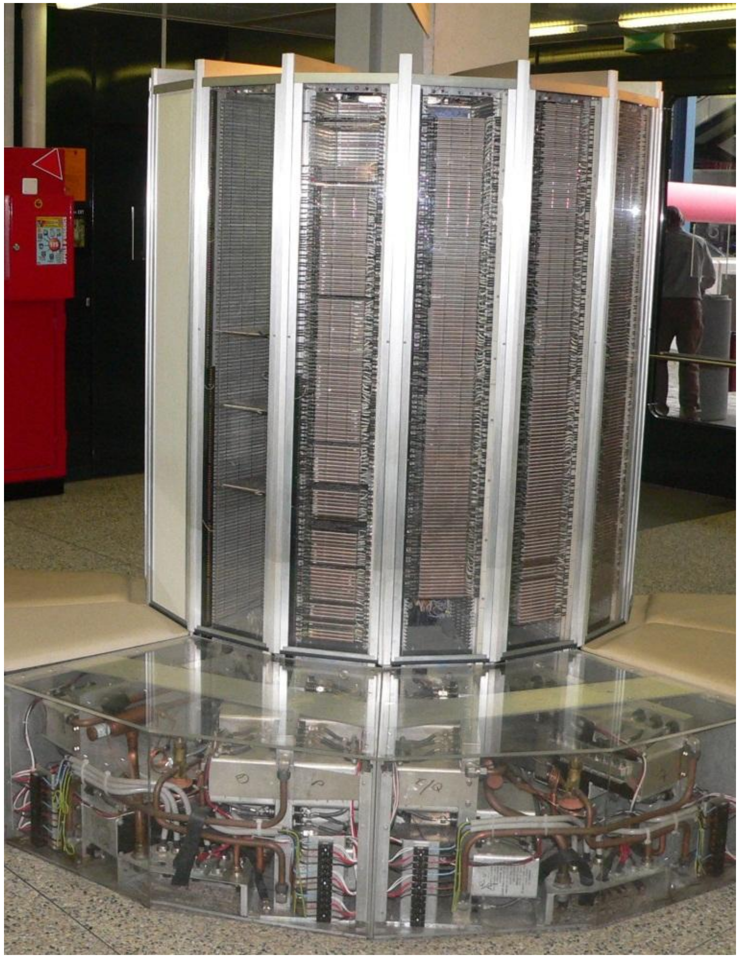
NVIDIA Tesla C870: $1300 in 2009, over 5 million sold

Building a super computer from many small processors

Up to 65,536 processors

- The IBM Blue Gene computer

Fast Power Grid Simulation



CRAY Supercomputer

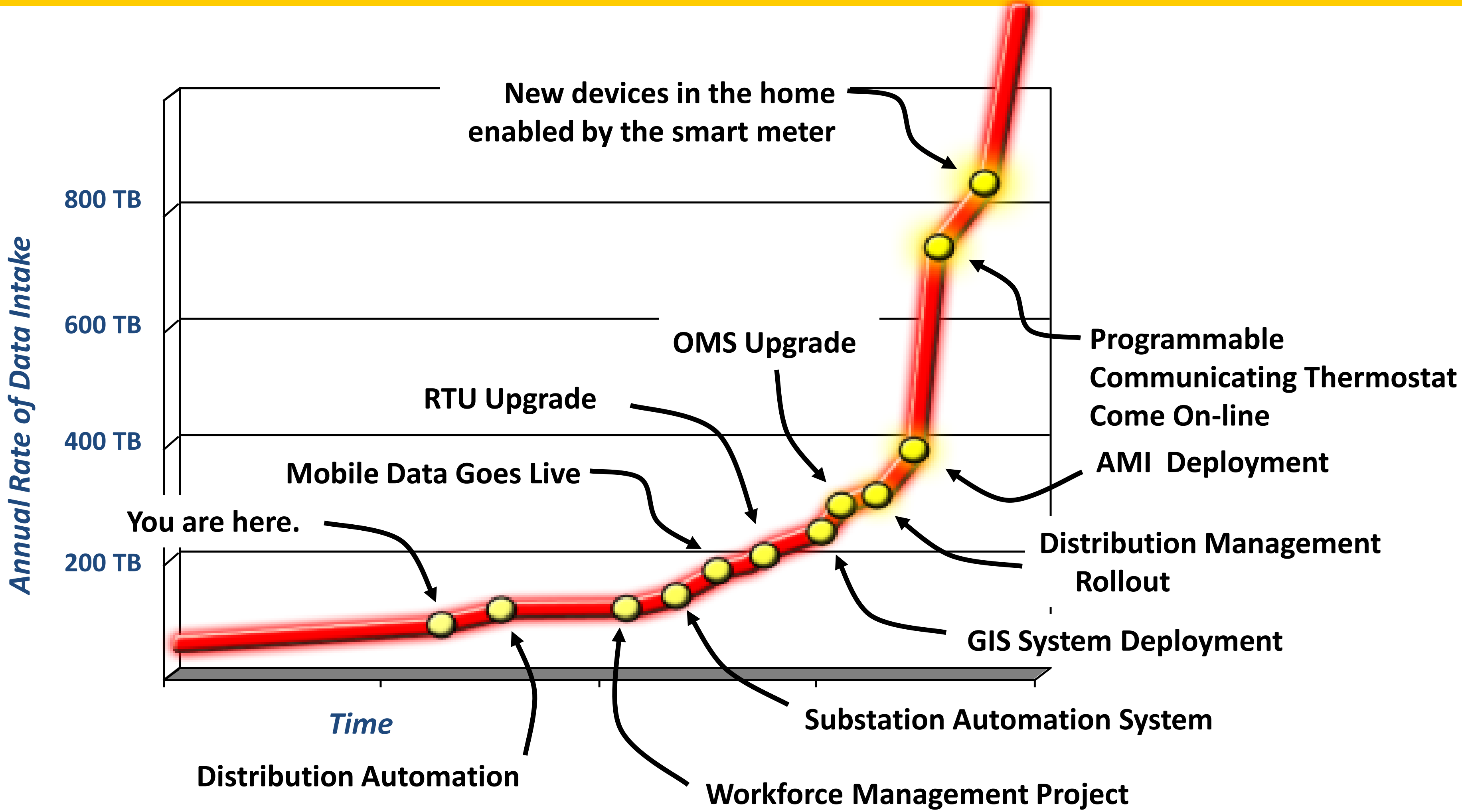
Nvidia GeForce GPU card for PC

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

Smart Grid Protection Schemes & Communication Requirements

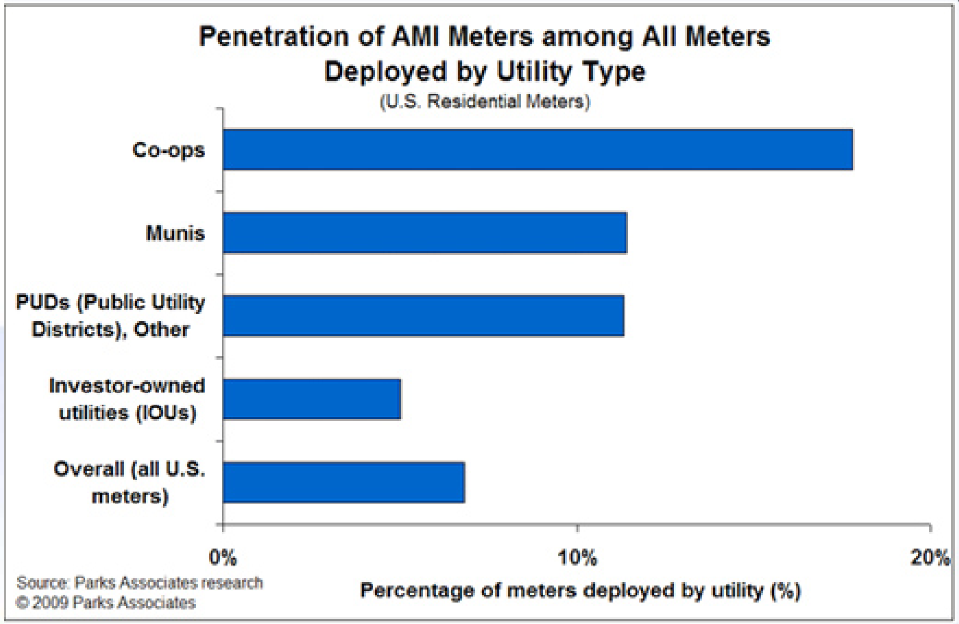
Type of relay	Data Volume (kb/s)		Latency	
	Present	Future	Primary (ms)	Secondary (s)
Over current protection	160	2500	4-8	0.3-1
Differential protection	70	1100	4-8	0.3-1
Distance protection	140	2200	4-8	0.3-1
Load shedding	370	4400	0.06-0.1 (s)	
Adaptive multi terminal	200	3300	4-8	0.3-1
Adaptive out of step	1100	13000	Depends on the disturbance	

Smart Grid: Tsunami of Data Developing

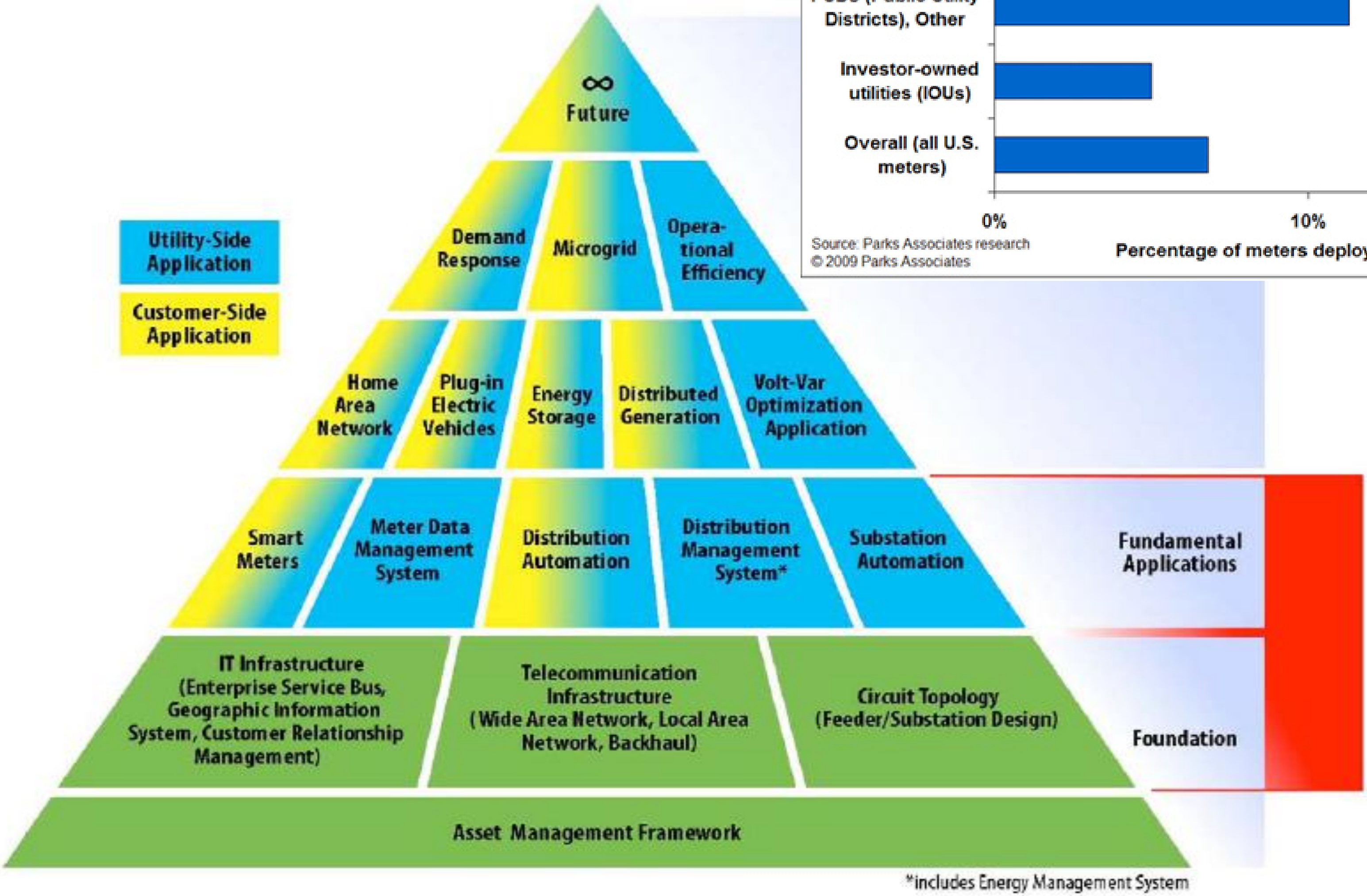


Tremendous amount of data coming from the field in the near future - paradigm shift for how utilities operate and maintain the grid

End-to-End Smart Grid Opportunities



Smart Grid framework

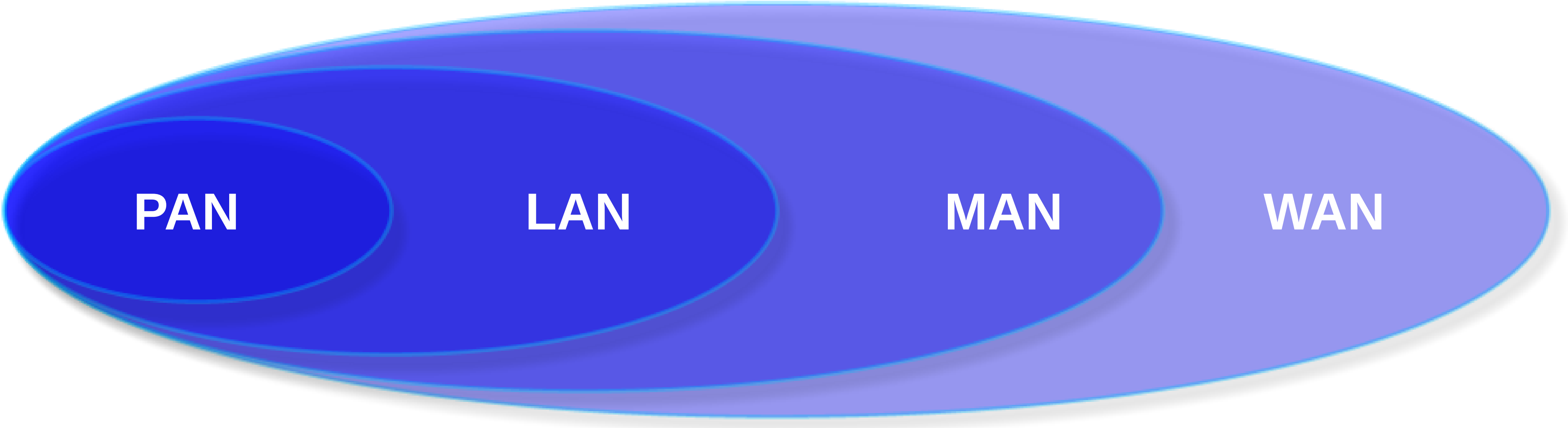


Source: BC Hyrdo

Connecting Everywhere – the wireless revolution

Interface of Smart Grid and Buildings

Personal Space | On-Campus / Public | City, Community | Cellular/ PCS /Satellites



Bluetooth, Zigbee
(Feet to 10's of feet)

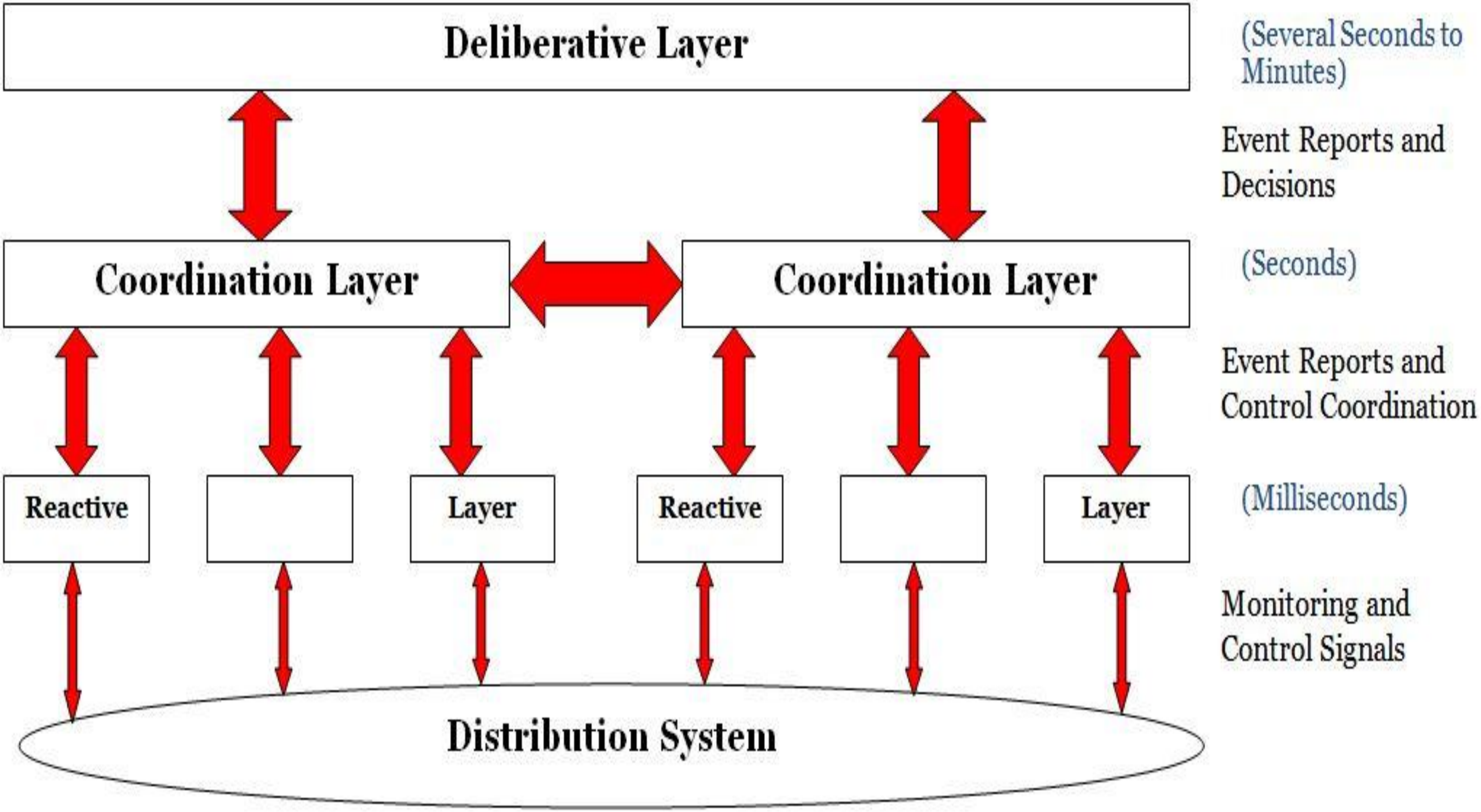
WLAN 802.11X
(10's, 100's of feet)

WMAN 802.16, 802.20,
Ad-hoc, Beam Forming

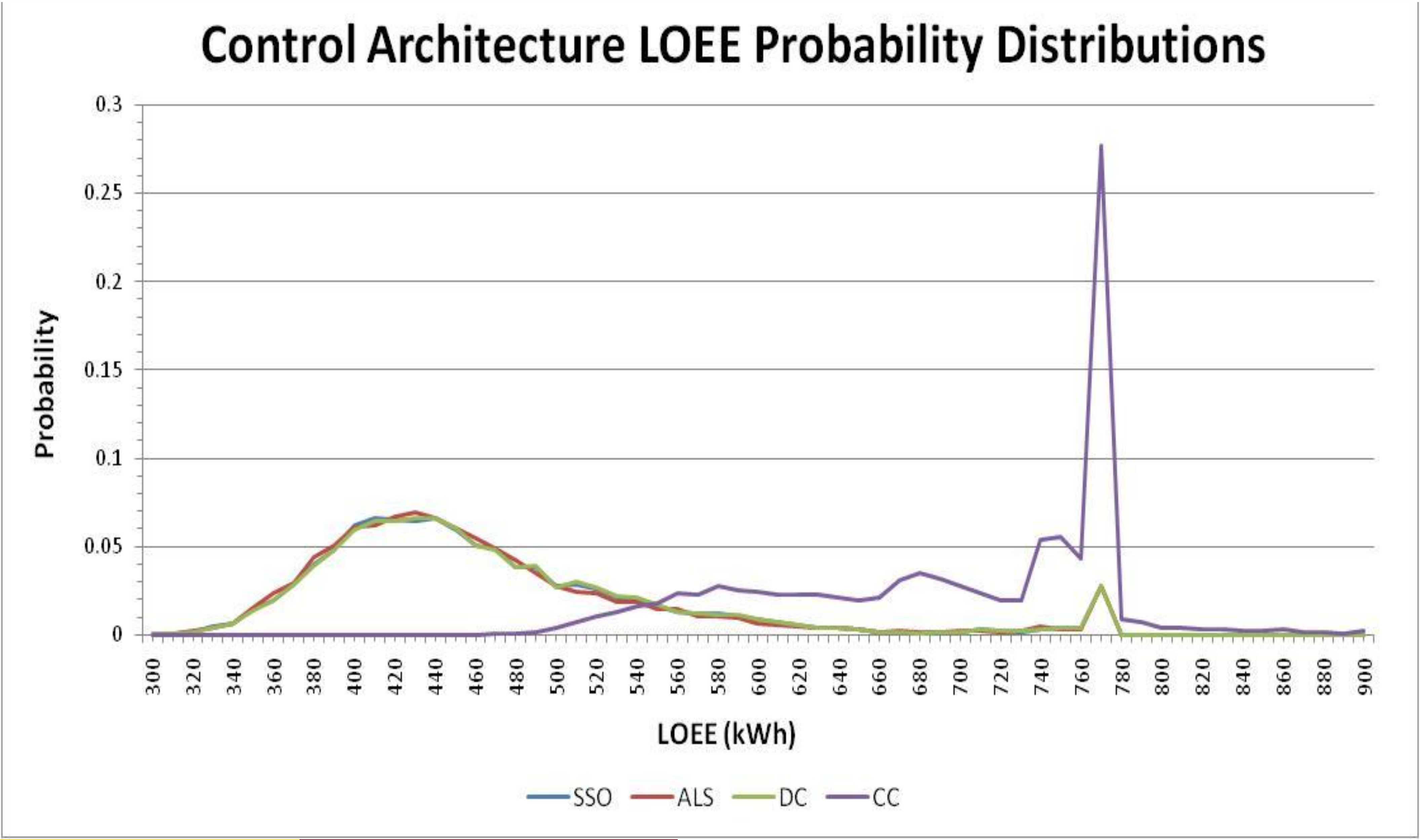
Cellular/Satellite

Source: IBM

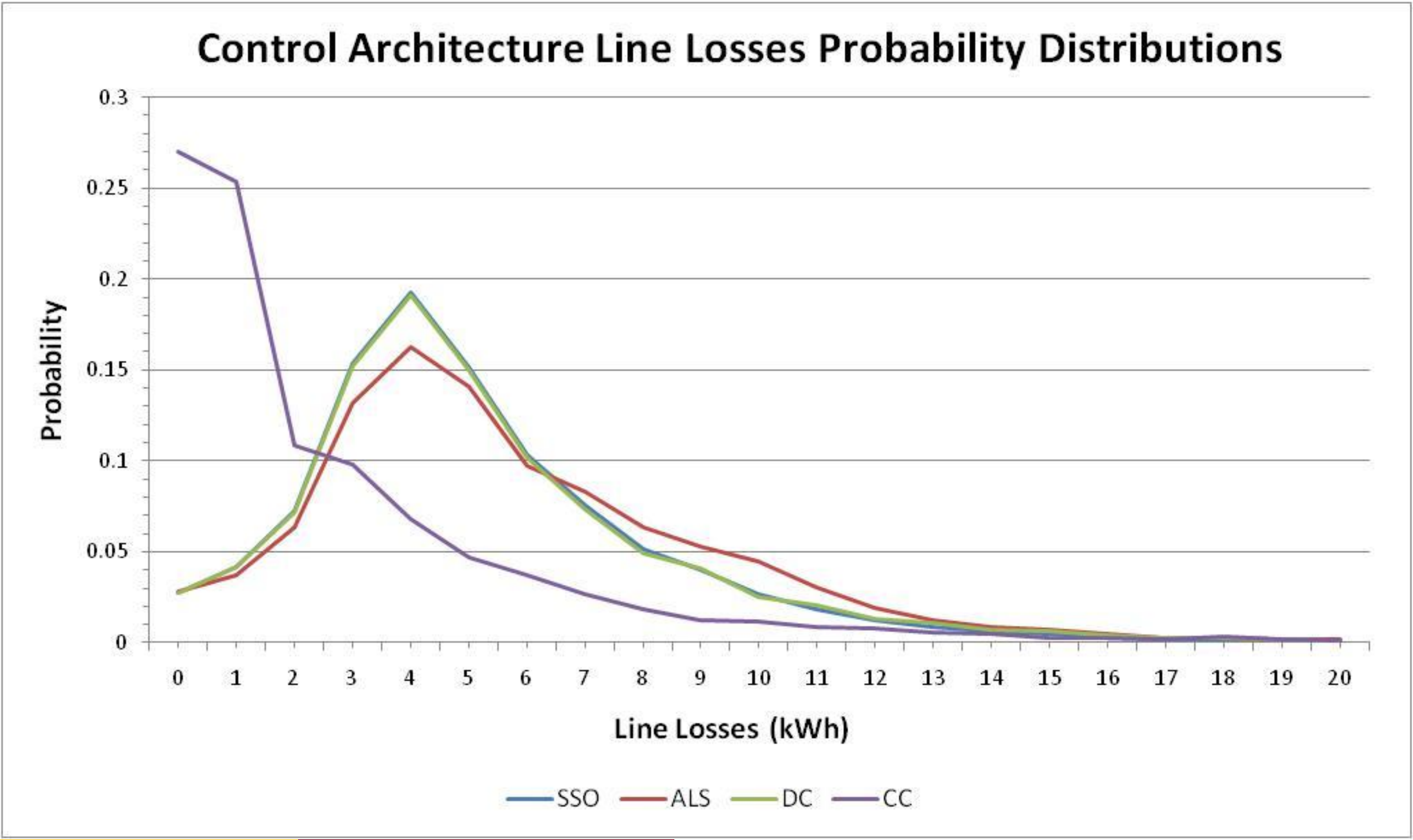
Intelligent Distributed Secure Distribution System Control Architecture



Centralized or Decentralized Control?



Centralized or Decentralized Control?



Observations

Threat Situation is Changing:

- Cyber has "weakest link" issues
- Cyber threats are dynamic, evolving quickly and often combined with lack of training and awareness.
- All hazard, including aging infrastructure, natural disasters and intentional attacks

Innovation and Policy:

- Protect the user from the network, and protect the network from the user: Develop tools and methods to reduce complexity for deploying and enforcing security policy.
- No amount of technology will make up for the lack of the 3 Ps (Policy, Process, and Procedures).
- Installing modern communications and control equipment (elements of the smart grid) can help, but security must be designed in from the start.
- Build in secure sensing, "defense in depth," fast reconfiguration and self-healing into the infrastructure.
- Security by default – certify vendor products for cyber readiness
- Security as a curriculum requirement.
- Increased investment in the grid and in R&D is essential.

Recommendations

- Facilitate, encourage, or mandate that secure sensing, "defense in depth," fast reconfiguration and self-healing be built into the infrastructure
- Mandate security for the Advanced Metering Infrastructure, providing protection against Personal Profiling, guarantee consumer Data Privacy, Real-time Remote Surveillance, Identity Theft and Home Invasions, Activity Censorship, and Decisions Based on Inaccurate Data
- Wireless and the public Internet increase vulnerability and thus should be avoided
- Bridge the jurisdictional gap between Federal/NERC and the state commissions on cyber security
- Electric generation, transmission, distribution, and consumption need to be safe, reliable, and economical in their own right. Asset owners should be required to practice due diligence in securing their infrastructure as a cost of doing business
- Develop coordinated hierarchical threat coordination centers – at local, regional, and national levels – that proactively assess precursors and counter cyber attacks
- Speed up the development and enforcement of cyber security standards, compliance requirements and their adoption. Facilitate and encourage design of security in from the start and include it in standards
- 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)
- Develop methods, such as self-organizing micro-grids, to facilitate grid segmentation that limits the effects of cyber and physical attacks

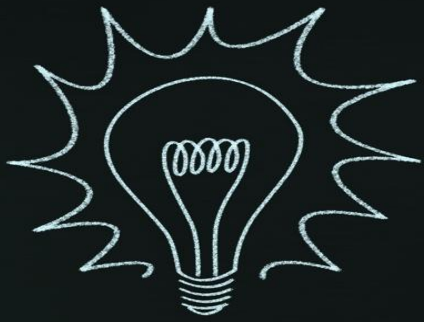
Enabling a Stronger, Smarter and more Secure Grid:

- Broad range of R&D including end-use and system efficiency, electrification of transportation, stronger and smarter grid with massive storage , cybersecurity and CIP

- Sensing, Communications, Controls, Security, Energy Efficiency and Demand Response *if architected correctly* could assist the development of a smart grid

- Smart Grid Challenge/Opportunity areas include:
  - Distributed Control
  - Grid Architectures
  - Cyber Security

Source: Massoud Amin, Congressional briefings, March 26 and October 15, 2009



1.
2.
3.
4.
5.
6.
7.
8.
9.


THANK YOU
MINNESOTA