A Collision of Two Infrastructures

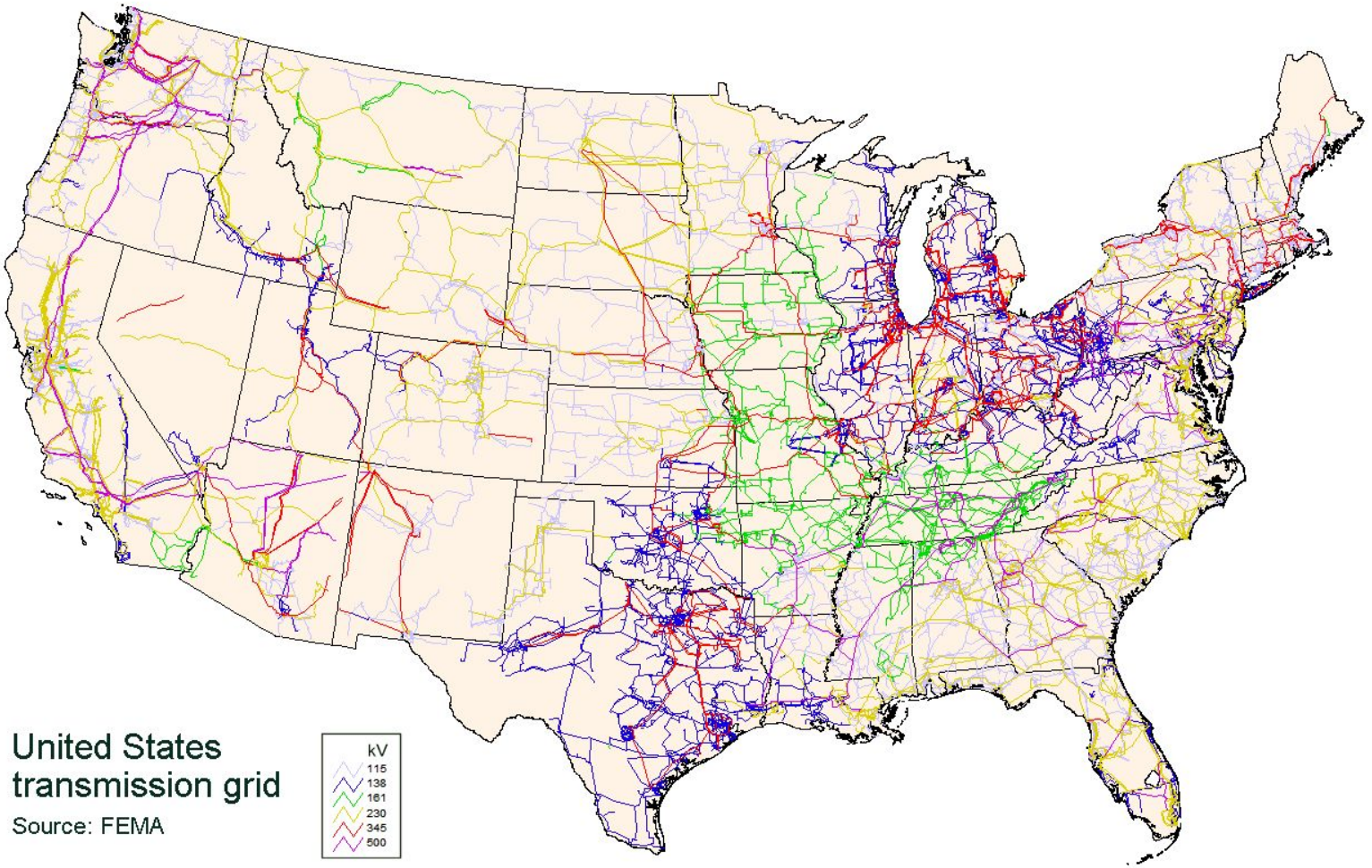
or Energy, delivered by Google

Jimmy Jia
jimmy@jimmyjia.com
Last Edit: April 14, 2019

Agenda

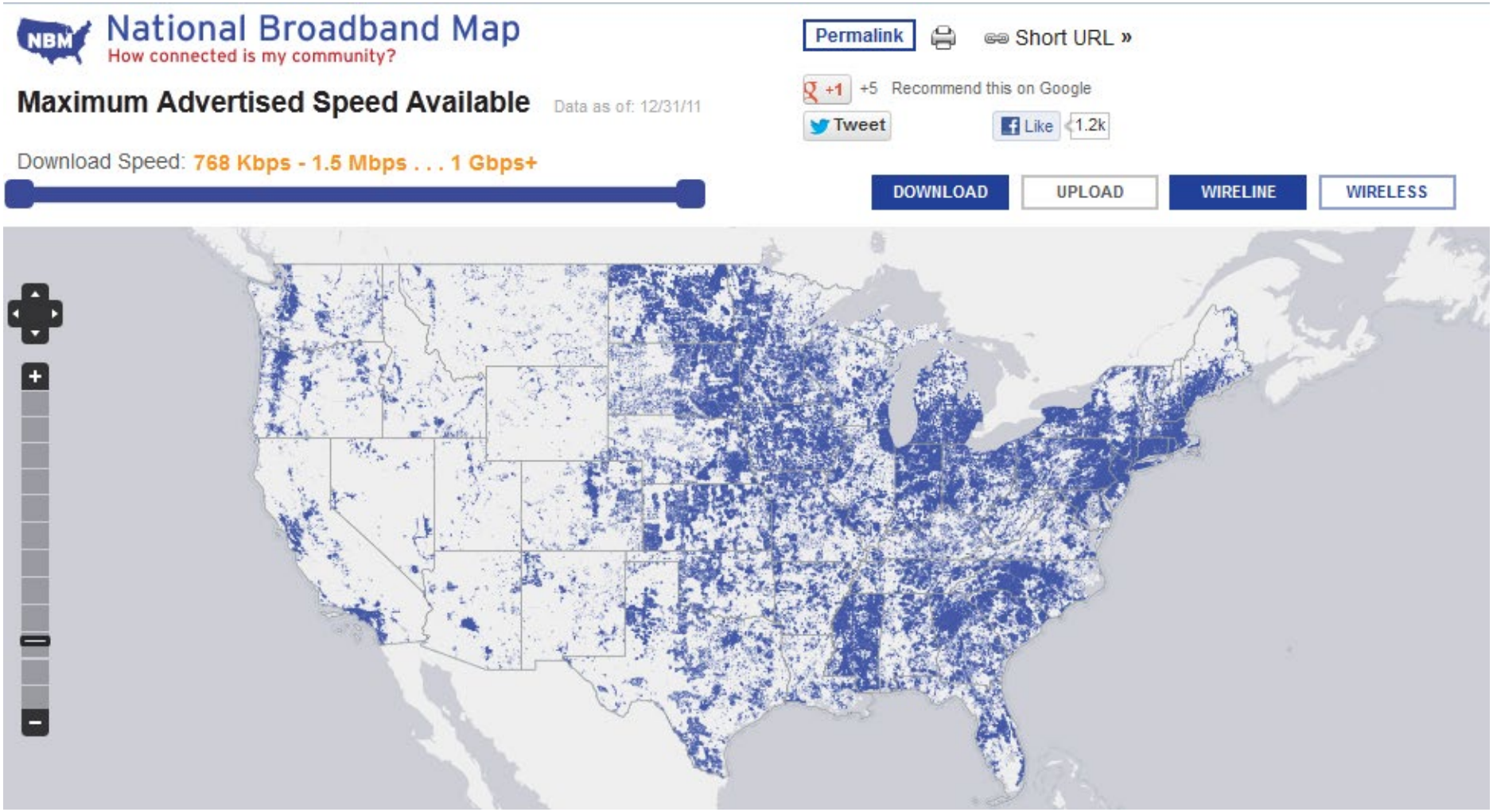
- The Collision of Two Infrastructures
- Cyber-Physical Security

The National Electric Grid:



http://www.geni.org/globalenergy/library/national_energy_grid/united-states-of-america/americannationalelectricitygrid.shtml

The National Telecommunications Grid:



http://broadbandmap.gov/

Historical timeline

Ages of Man	"Physical" Energy	Fuel	Available Technology
Stone Age 1.5M BCE – 2400 BCE	N/A	300 °C Wood	350 °C Campfire 800 °C Pit Kiln
Bronze Age 3000 BCE – 1500 BCE	850 °C Bronze	2000 °C Oil	1000 °C Bloomery
Iron Age 1300 BCE – 500 AD	1538 °C Iron	2000 °C Coal	2000 °C Blast Furnace

Historical timeline

Ages of Man	"Physical" Energy	Fuel	Available Technology
Stone Age 1.5M BCE – 2400 BCE	N/A	300 °C Wood	350 °C Campfire 800 °C Pit Kiln
Bronze Age 3000 BCE – 1500 BCE	850 °C Bronze	2000 °C Oil	1000 °C Bloomery
Iron Age 1300 BCE – 500 AD	1538 °C Iron	2000 °C Coal	2000 °C Blast Furnace
Information Age 1900 AD – Present	Pure Energy	Electricity	Data Centers

Energy is Information

The grid is run by computers

Our society needs computers

Computers need electricity

http://www.spurgeonworld.com/blog/archives/2007/03/build_your_own.html

http://en.wikipedia.org/wiki/File:NetworkOperations.jpg

http://en.wikipedia.org/wiki/Electronic_trading_platform

Energy is Information

The grid is run by computers

Our society needs computers

Computers need electricity

http://www.spurgeonworld.com/blog/archives/2007/03/build_your_own.html

http://en.wikipedia.org/wiki/File:NetworkOperations.jpg

http://en.wikipedia.org/wiki/Electronic_trading_platform

Merge the two infrastructures

Internet now is essential to:

- Banking and Finance
- Insurance
- Chemical
- Oil and Gas
- Electric
- Law Enforcement
- Higher Ed
- Transportation (Rail)
- IT and Telecom
- Water

Information is Energy:

- How much money do you have in your bank account?
- What was your favorite photo from your last vacation?
- What did you do at work last week?

A history lesson: Sam Insull

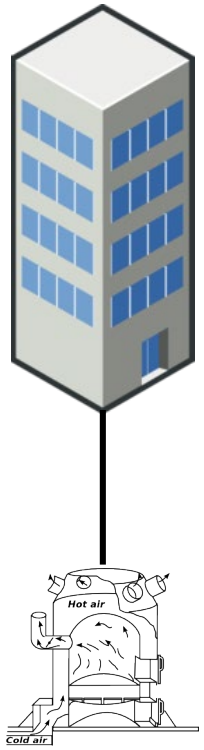
- Edison's personal secretary
- Vice President at General Electric
- Founder of Chicago Edison Company

- Believed in a centralized system in order to minimize ***marginal*** costs of delivering electric power

- **NOTE**: Power (*MW)*! Not Energy (*MWH)!*

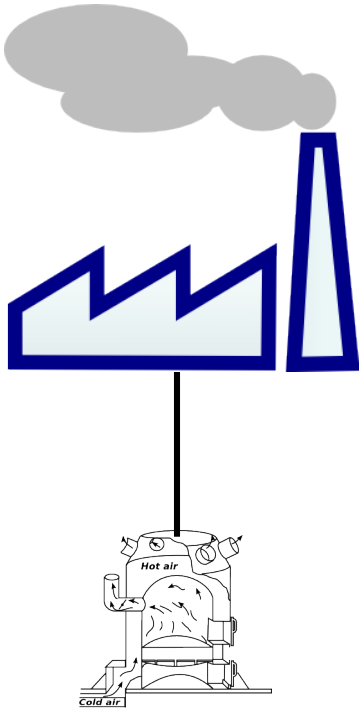
Load Diversification

10 MW Load



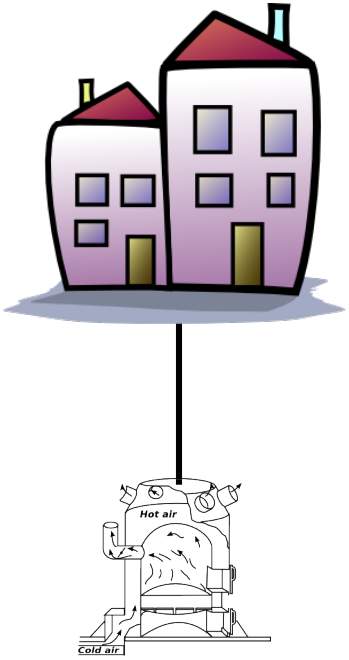
10 MW Generator

10 MW Load



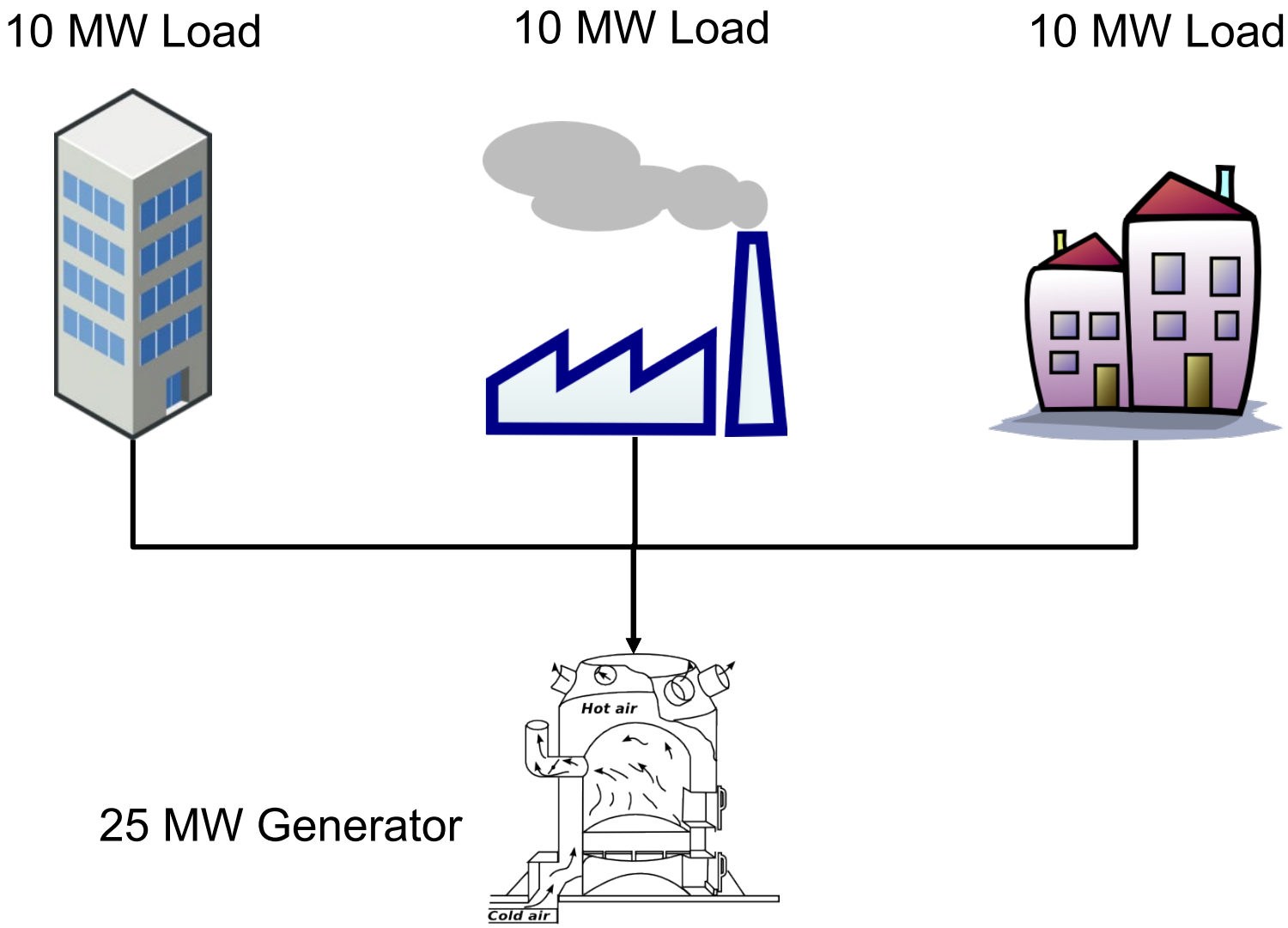
10 MW Generator

10 MW Load



10 MW Generator

Load Diversification



Insull used *load diversification* to serve clients

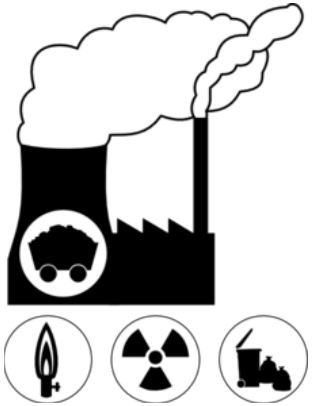
In a Chicago block with 193 customers,

- The calculated required load was 92 kW
- He served the clients with a 29 kW substation
- The more diverse the load, the more money he could make!
- Or the lower cost it would cost the end client.

Electric Grid: Centralized or Decentralized?

- In the 1890's there were 1,500 individual power plants operating independently.
- Why did they connect with each other to create a centralized system?

Turns out, Insull's math works on generation as well!



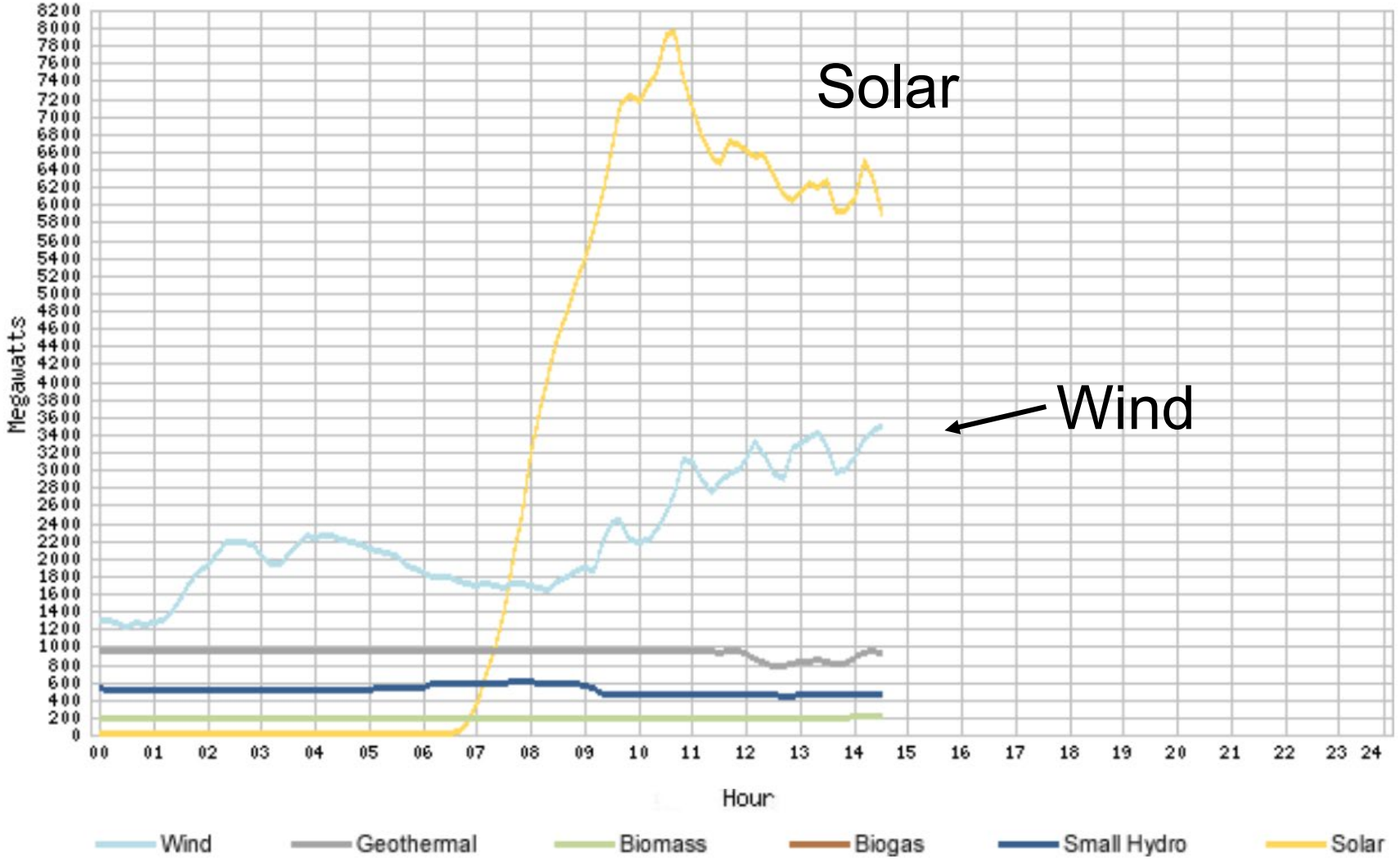
Reliable power: Always on

Variable power: can make statistically reliable if generators are in diverse environments!

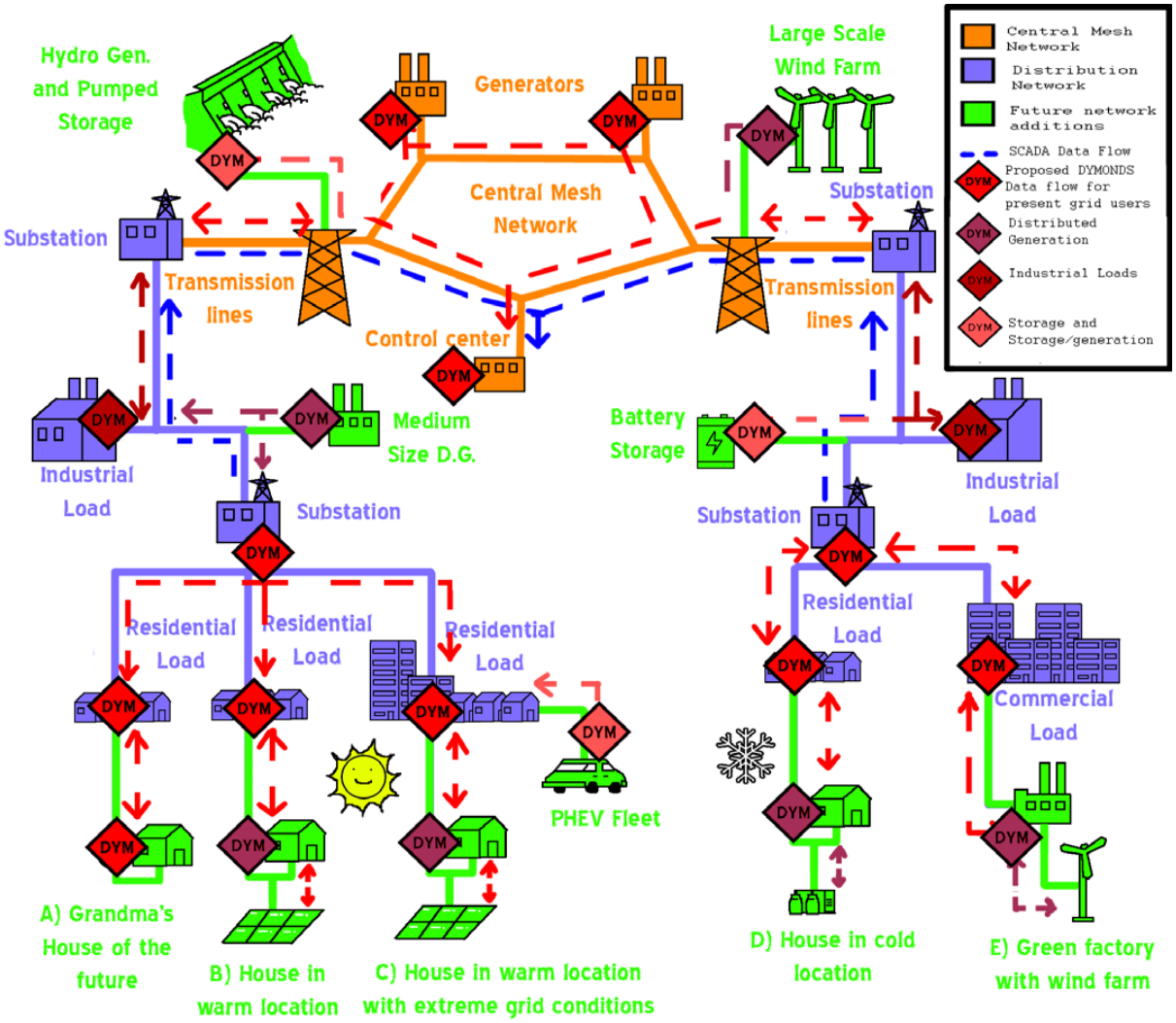
Variable Power are treated as ***Loads!***

CAISO Renewable Resources 4/8/2017

MW



Dynamic monitoring and decision systems (DYMONDS)



http://pserc.wisc.edu/research/futuregrid/broadanalysis/gridenablers.aspx

Data

Interestingly, his math was based on statistics…

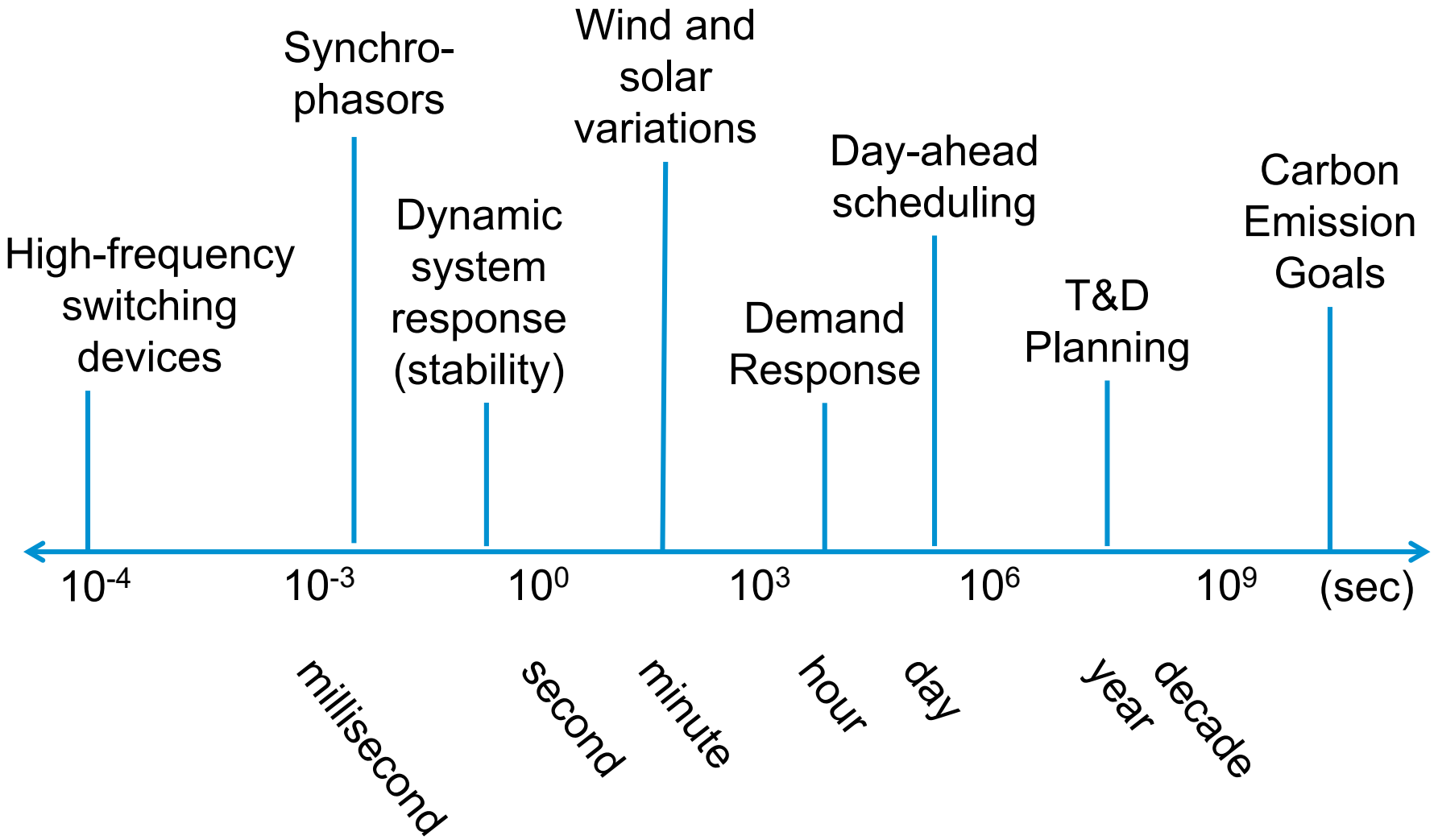
- …and statistics requires data. Lots of it.

The more sensors, the better

The more frequent sensor, the better

How *fast* do you think we can collect data?

Problems and issues faced by the Grid



http://www.gridwiseac.org/pdfs/te_framework_report_pnnl-22946.pdf

Synchophasor

- A device that collects data 30-60 *times per second*
- Install on substations
- Devices are $2,000 - $3,000 each
- But the data center cost….?

Connected devices generate a *lot* of data

Meters:

- kWh
- kW
- kVAR

Weather

- Temperature
- Humidity
- Etc.

Time

- Date
- Time
- Weekday

15 minute increments
x 8 data points

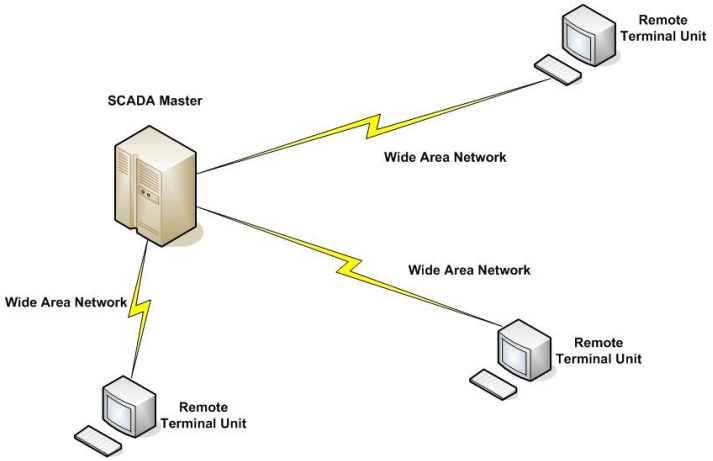
280,000 data points per year!

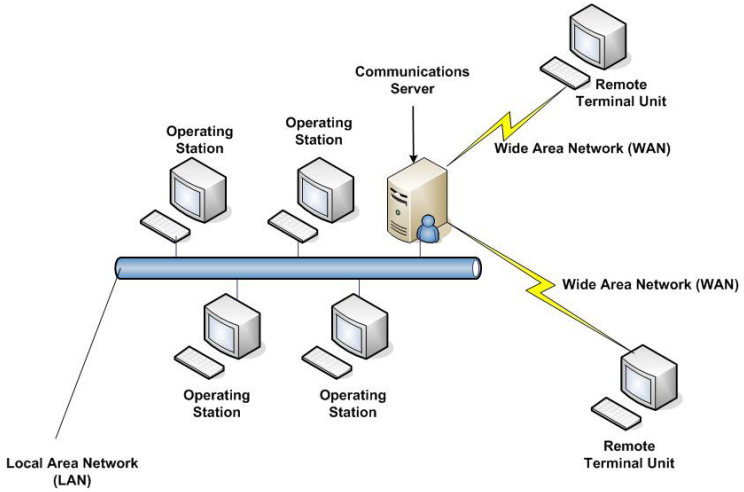
Assuming 100's of millions of devices –

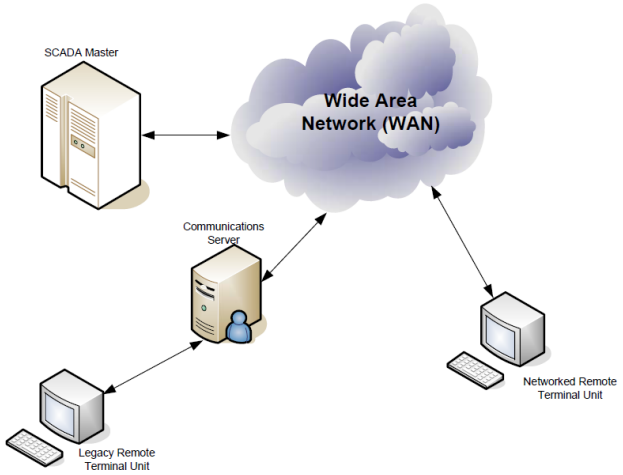
Need between 3 - 300 PetaBytes of storage for data per year

Size of Facebook: 100 – 300 PB

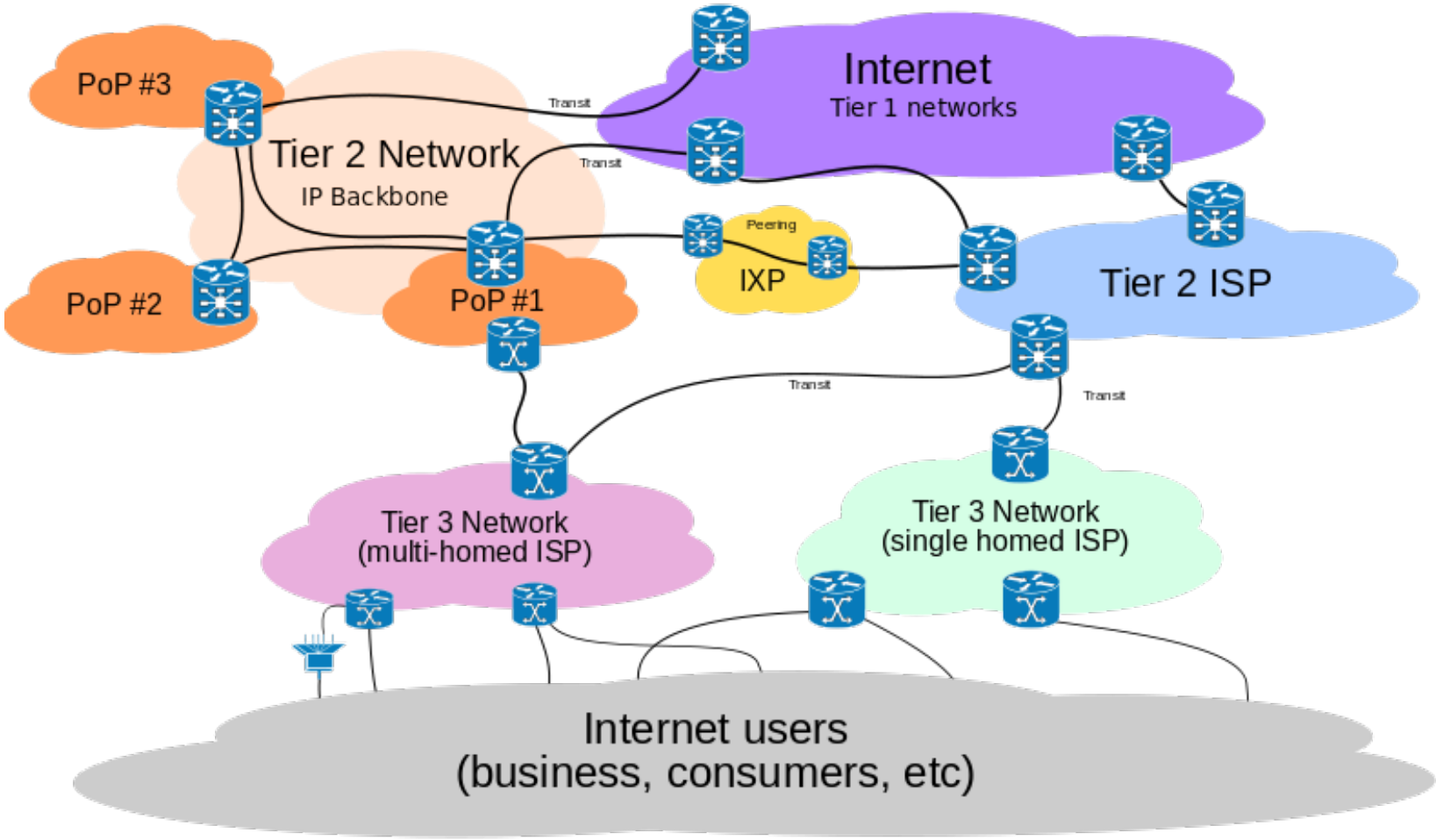
Different network architecture





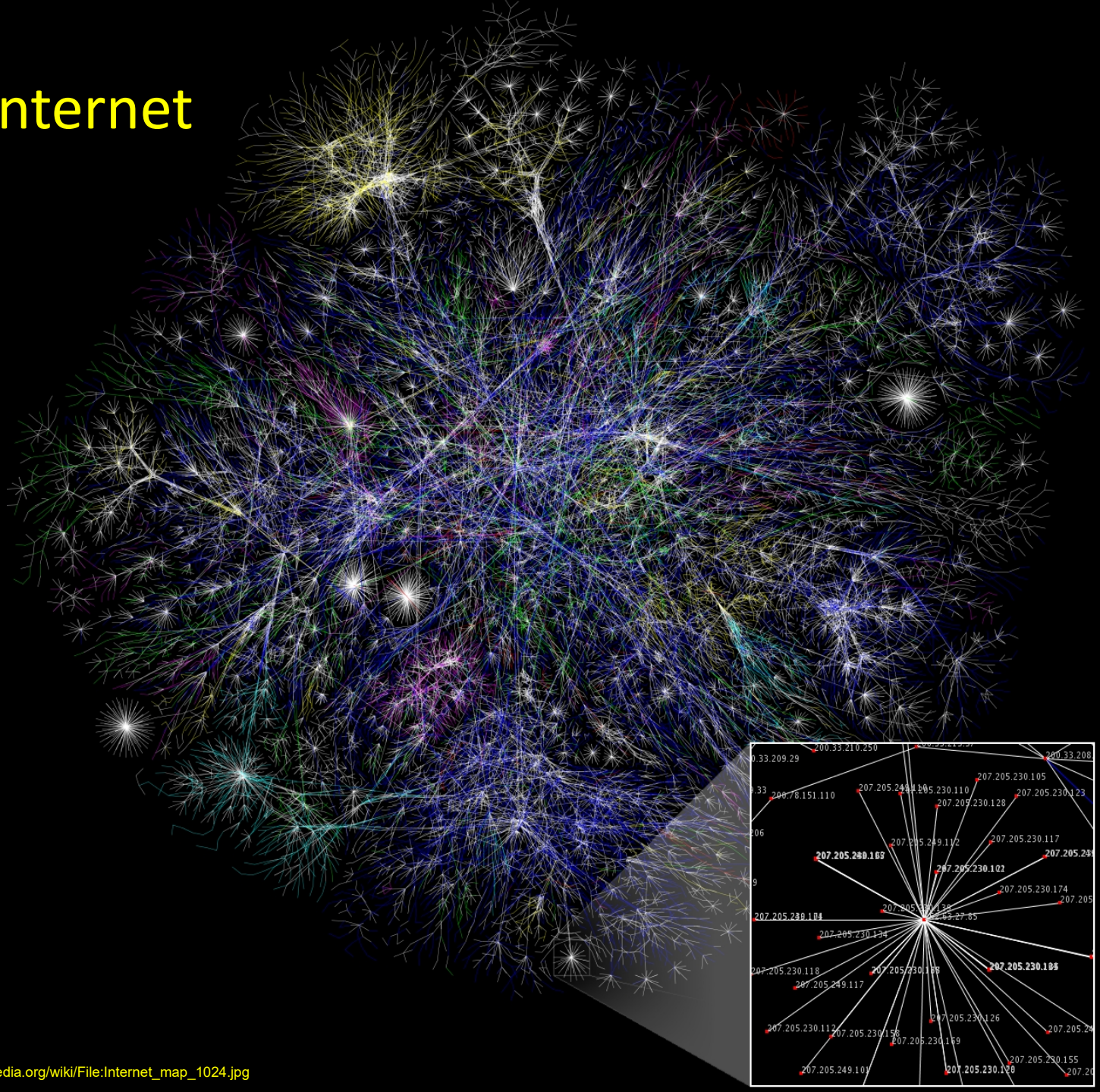


The Internet



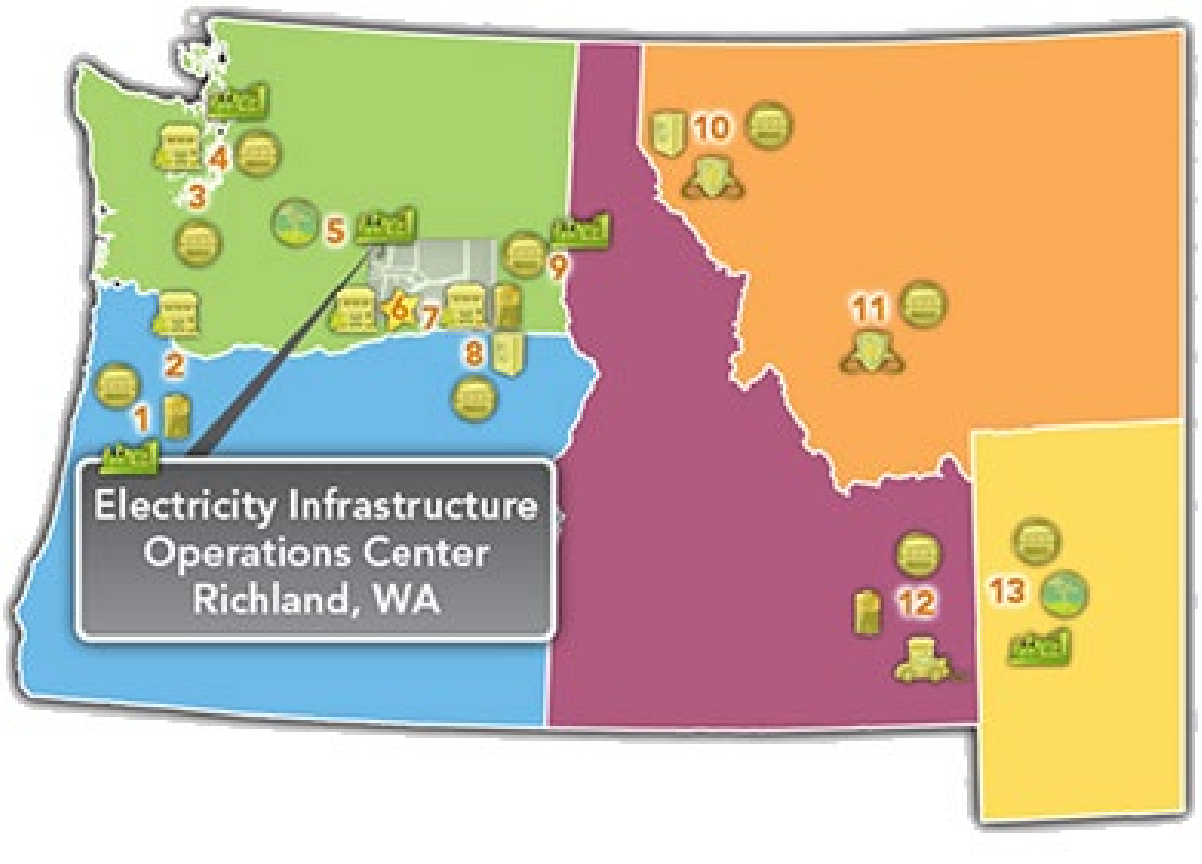
http://en.wikipedia.org/wiki/The_internet

The Internet



http://en.wikipedia.org/wiki/File:Internet_map_1024.jpg

$130 million project by PNNL



- 60,000 metered customers
- Engaging responsive electricity system assets of approximately 80 megawatts

“Transactive” Grid

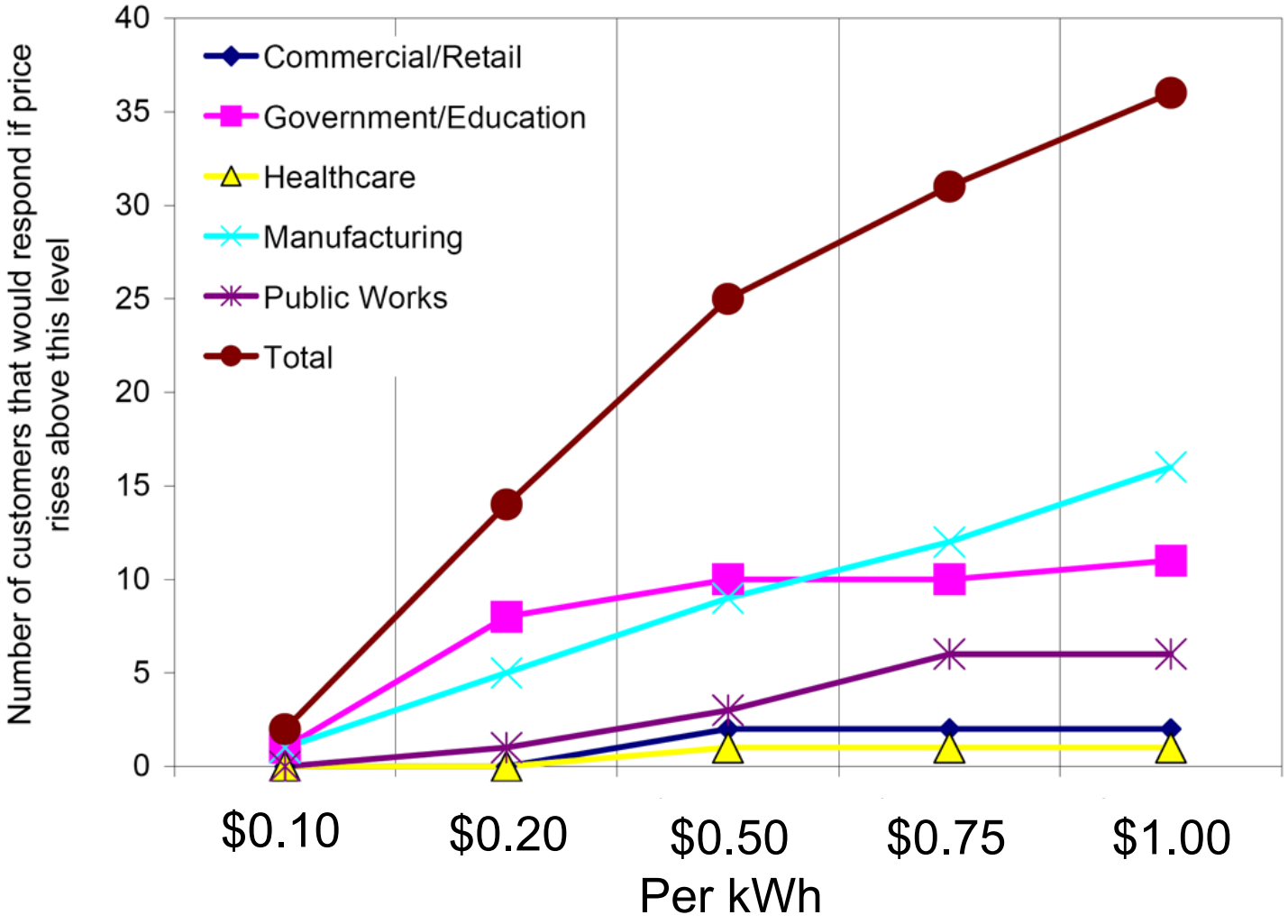
- A technique for managing the generation, consumption or flow of electric power within an electric power system through the use of economic or market based constructs while considering grid reliability constraints.

- Or a merging of

- *Energy* Management
- *Finance* Signals
- Enabled with abundant *Information*

Underlying assumption:

Is energy consumption *elastic* to price?



Price Elasticity of Demand for Electricity: A Primer and Synthesis EPRI 2008

Creating a Demand Curve

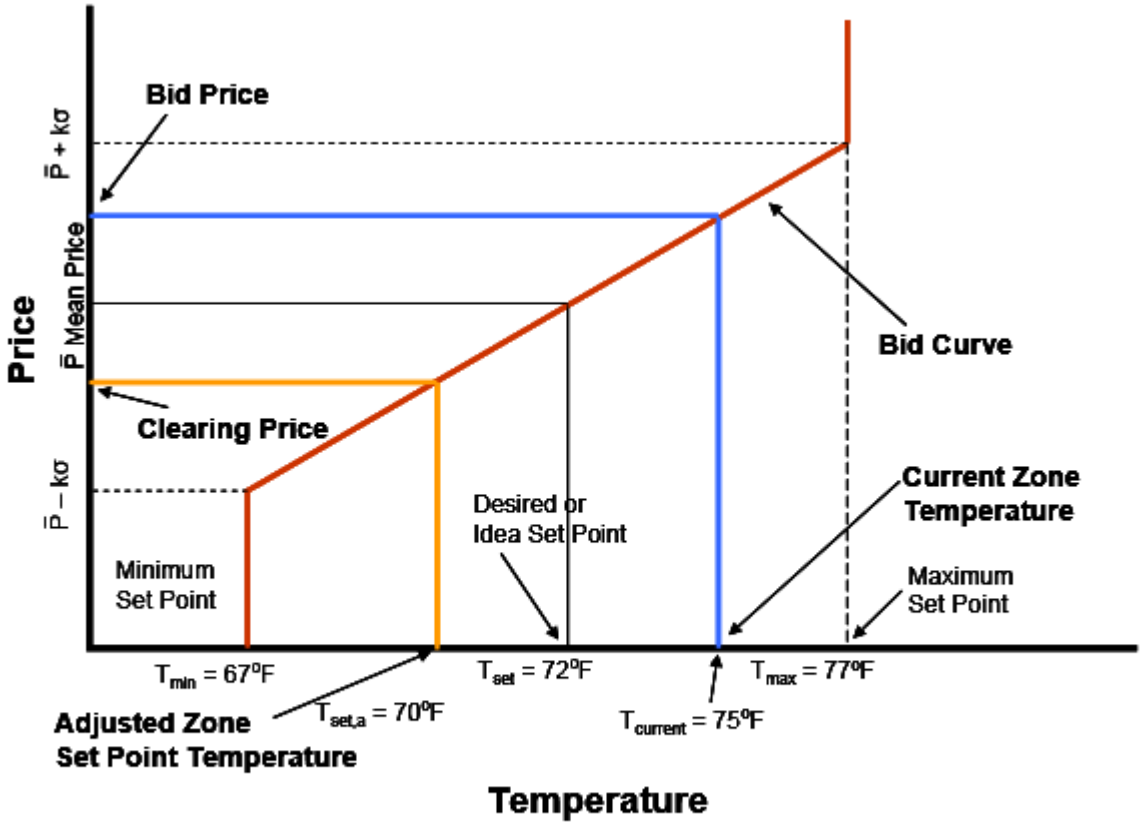


Figure 2 – Illustration of the Bid and the Response Strategy for Thermostatically Controlled HVAC Systems: Cooling Mode

Prices to devices – creating a demand curve

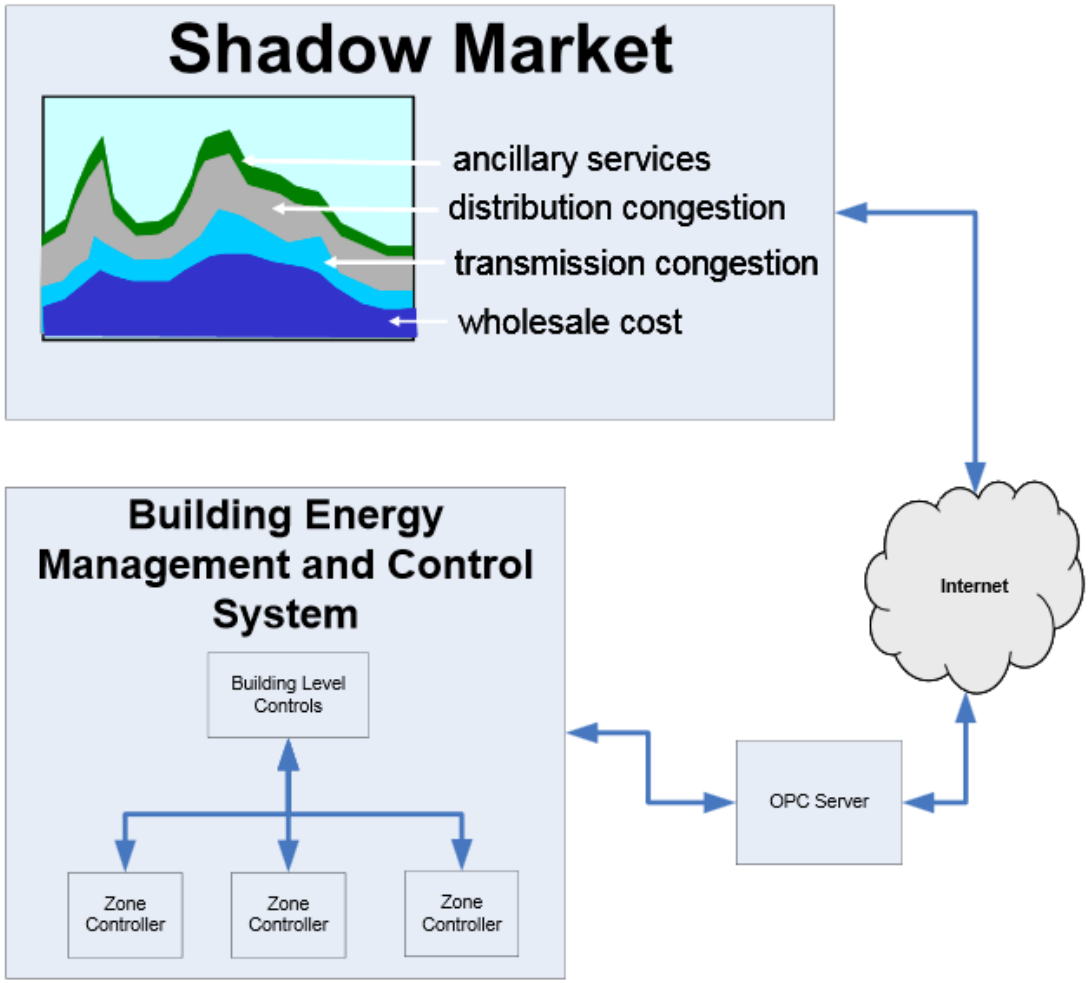


Figure 3 – Schematic of Transactive Controls Implementation in a Commercial Building

Problem is control

Utility control via a price signal?

End-User control via preferences?

It is happening around you

http://en.wikipedia.org/wiki/Electric_vehicle

http://pinterest.com/pin/131589620332550137/

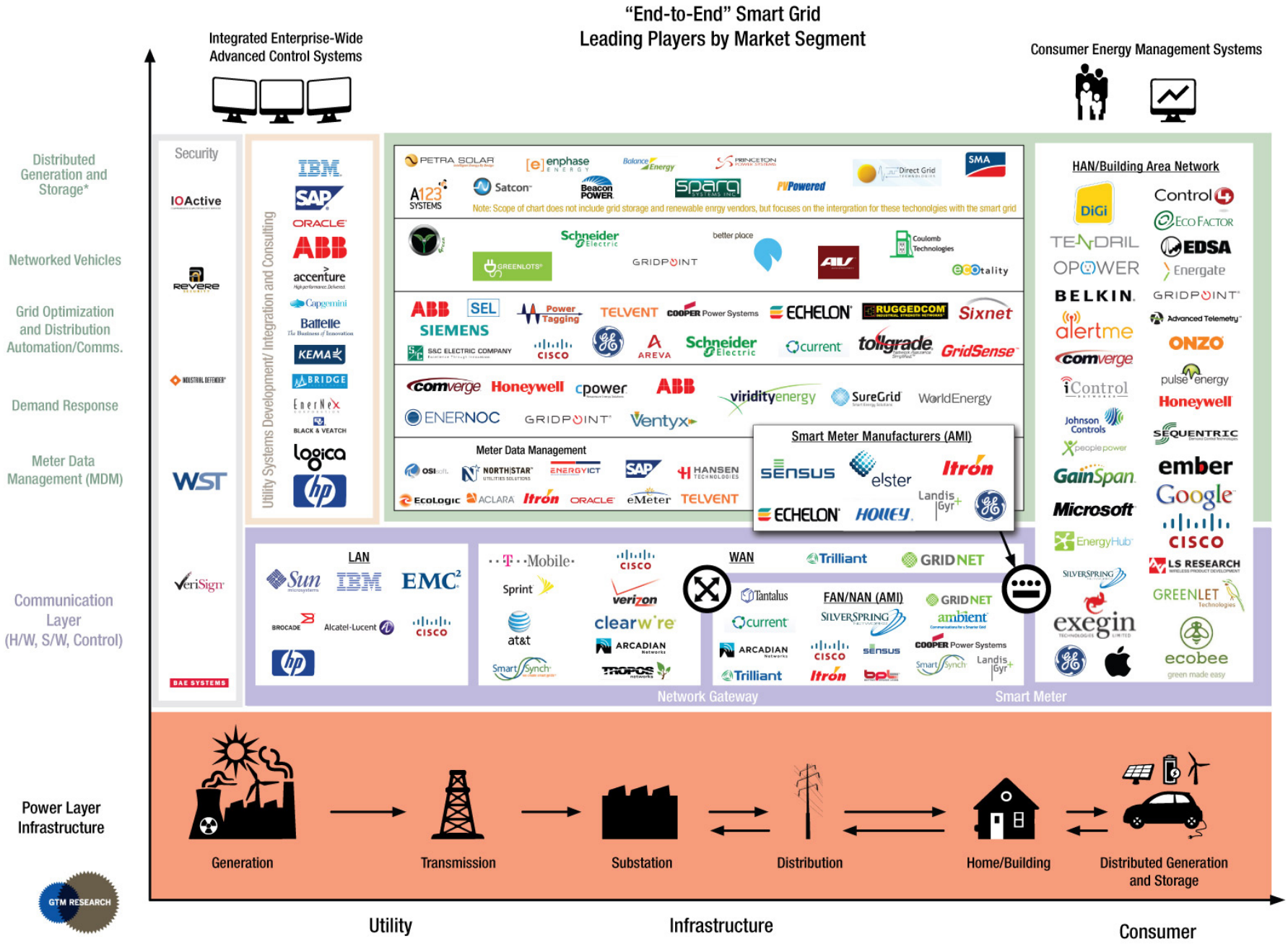
http://commons.wikimedia.org/wiki/File:MRCoffee.jpg

http://en.wikipedia.org/wiki/Microwave_oven

http://www.aeintegration.com/lighting/?postTabs=2

http://www.yankodesign.com/2010/05/28/smart-fridge-is-your-new-recipe-card/

$9.6 billion market size by 2015



Should the internet be a regulated monopoly?

- UTILITY - A tiny subset of companies that "operate with government approval as monopolies and supply a service which is *indispensable to modern life*." [Public Utility Economics, 1964]

NO:

- Twenty four states specifically prohibits its Public Utilities Commission from imposing new regulations on VoIP and other Internet services without explicit authority from the state legislature [Forbes 9/10/2012].

YES:

- The FCC … "have authority to oversee Internet service in ways that encourages competition" Tom Wheeler [FCC Chair] … Looking closely at overruling state laws that restrict the ability for cities and towns to offer broadband service to residents.

How does net neutrality affect smart grid?

FCC Rule 15-24A1

- *A person engaged in the provision of broadband Internet access service, insofar as such person is so engaged, shall not engage in paid prioritization.*

- AKA, no tolls allowed. What happens when tolls on a congested resource are banned?

LUNCH

Cyber-physical Security

Cyber-Physical Attacks

http://www.youtube.com/watch?v=fJyWngDco3g

A highly staged demonstration project in a national laboratory.

Opening and closing a circuit breaker – at resonance frequency with the AC cycle.

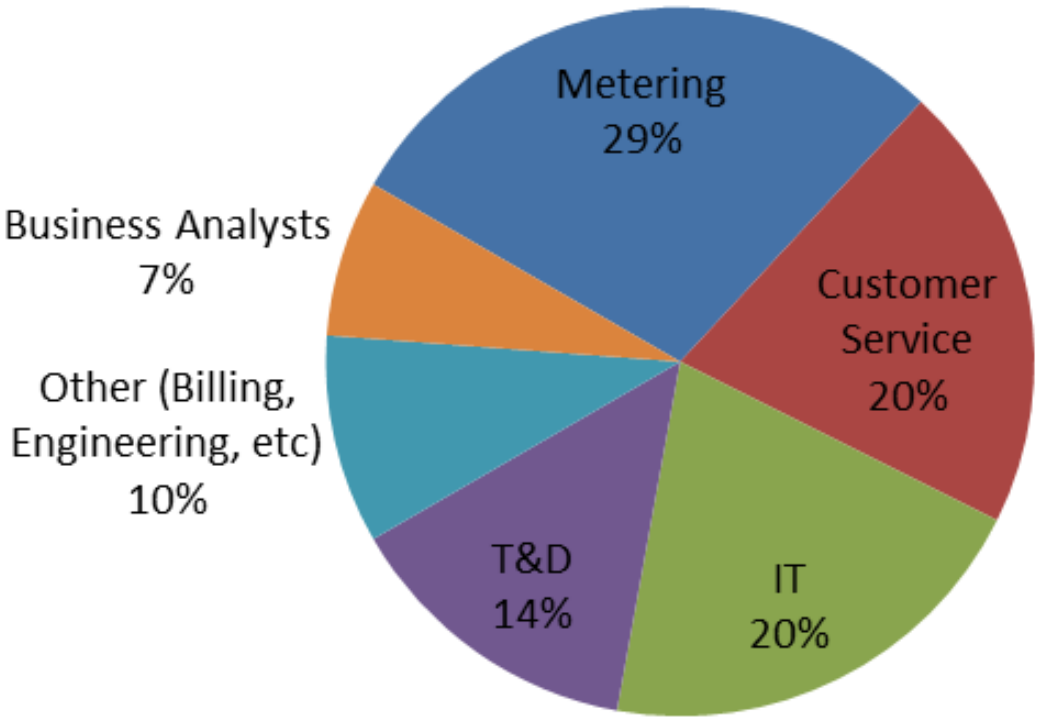
Physical AND cyber attacks

2003 NY Blackout:

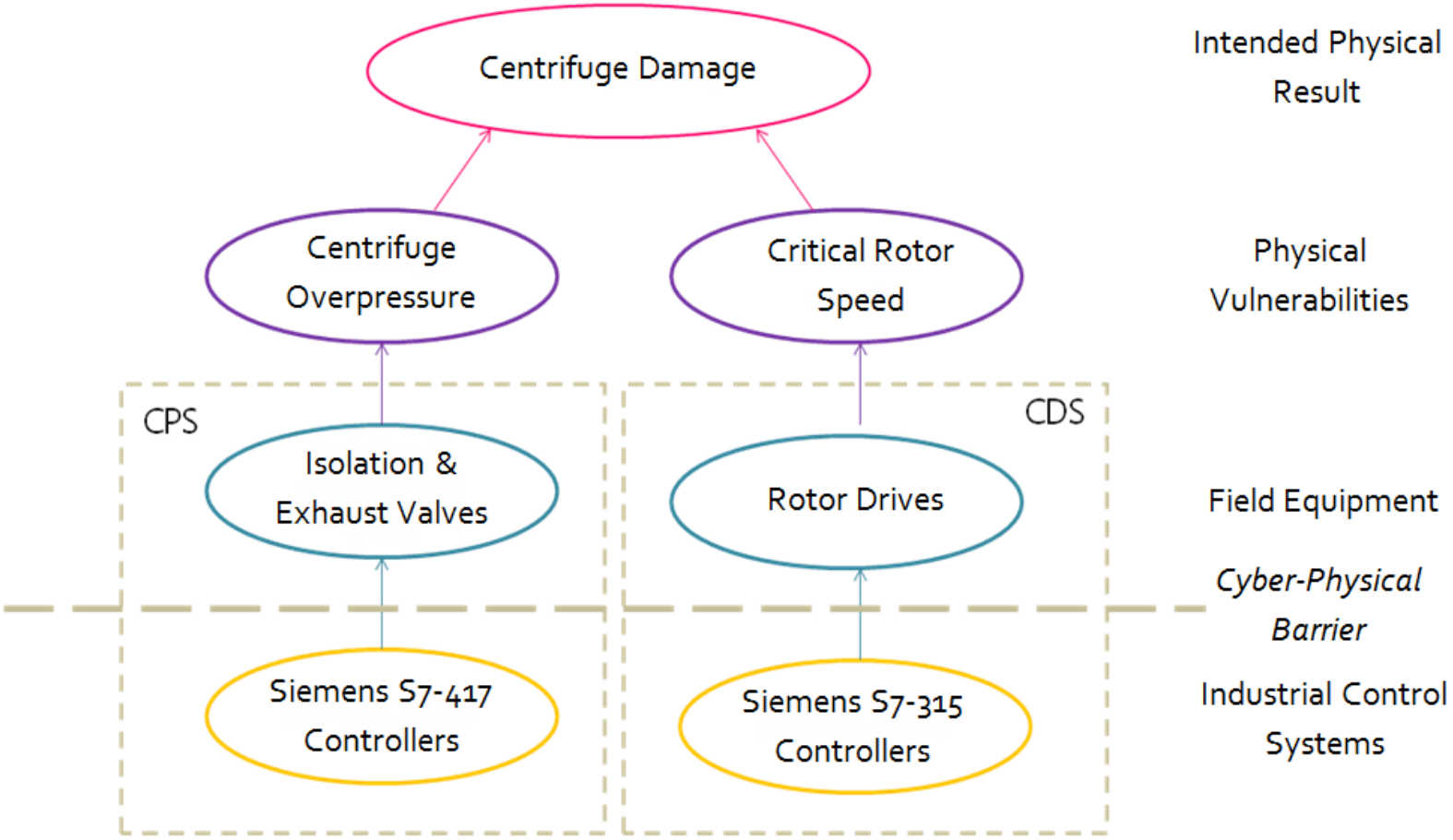
- 2:02 Tree falls onto wire
- 3:32 First failure of a line
- 4:46 Fifth line failure
- 5:13 256 power plants offline; blackout.

Aug 16, 2012 – Shamoon – 30,000 Saudi Aramco workstations

Survey results of presumed data ownership in a utility



Stuxnet



Langner, Ralph. *To Kill a Centrifuge: A technical analysis of what Stuxnet's creators tried to achieve*. Nov 2013

Ways to classify the threat

Threat Agents

Access

Misuse

Disclosure

Modify

Deny Access

Threat Communities

Employees

Contractors

Bored Teenagers

Cyber-criminals

Spies

Activists

Nation-States

Threat Consequence

Disclosure

Deception

Disruption

Ursurpation

Model-Based Approach

Attacker-centric

- Designed around the threat

Software-centric

- Based on the subsystem of code

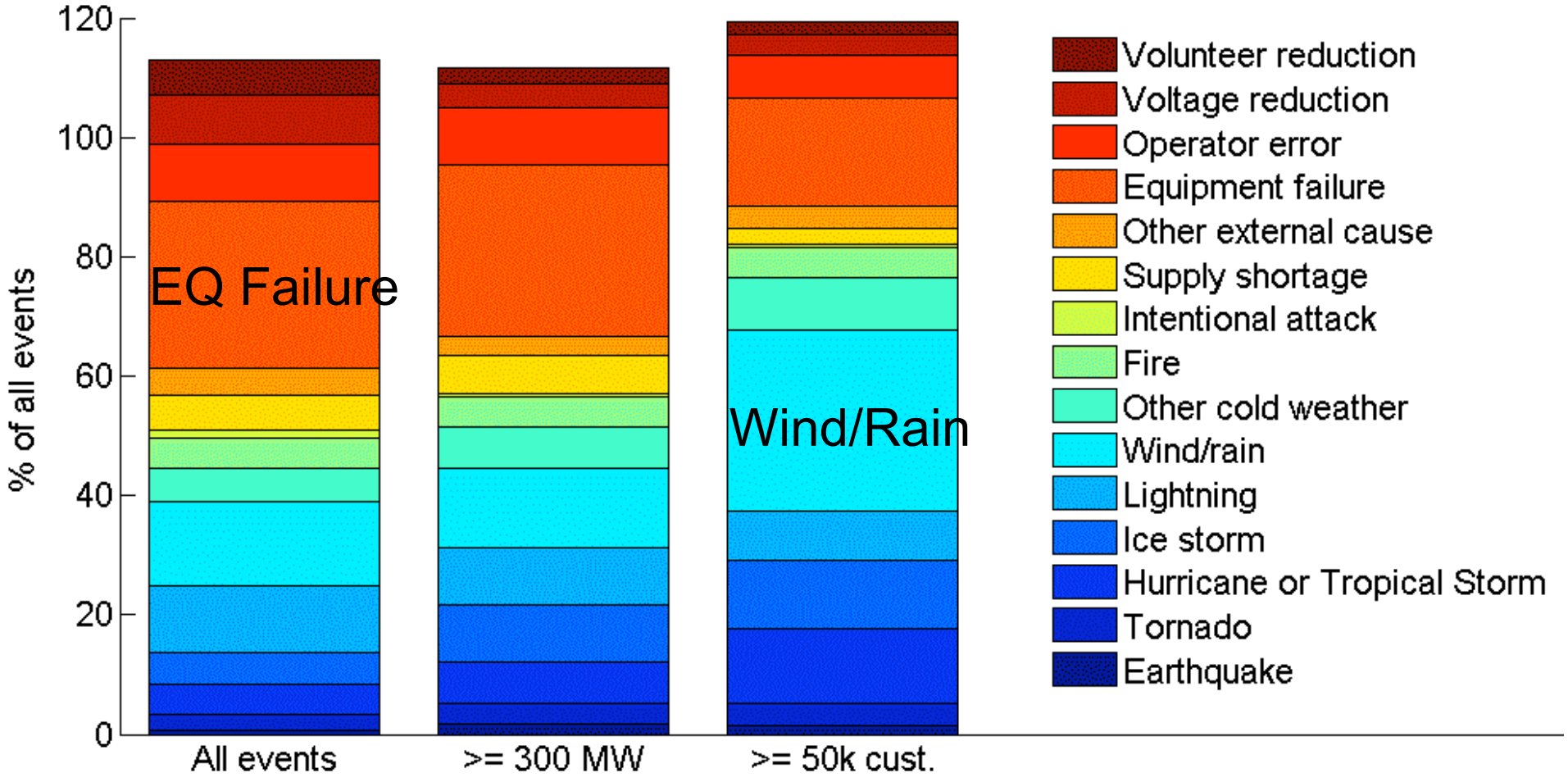
Asset-centric

- Designed around the assets being protected

Threat Vectors

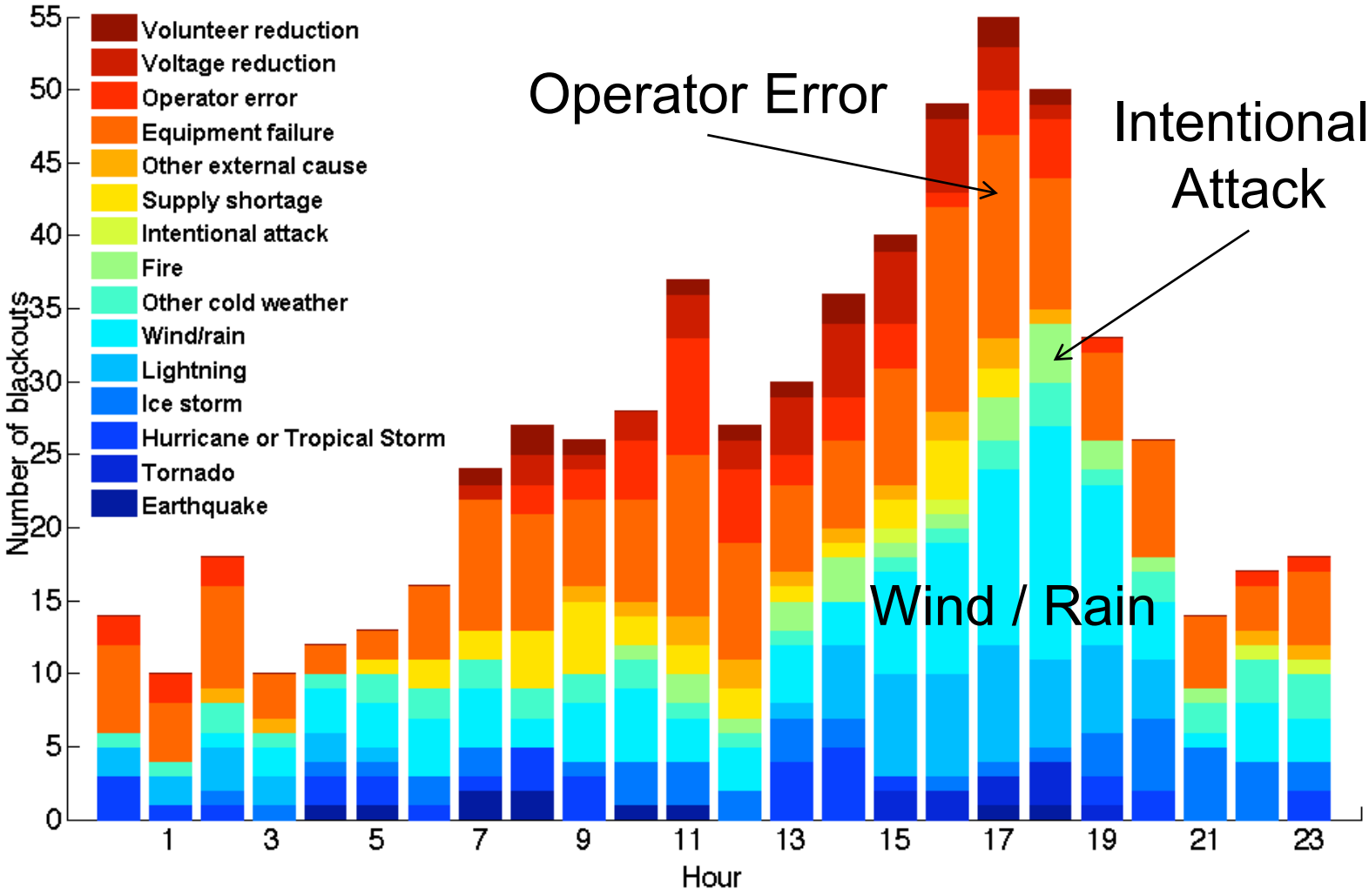
- Phishing Attack
- Unsecure Wireless Network
- Removable Media
- Mobile Devices
- Malicious Web Components
- Viruses and Malware
- Ransomware

NERC-DAWG (Disturbance Analysis Working Group)



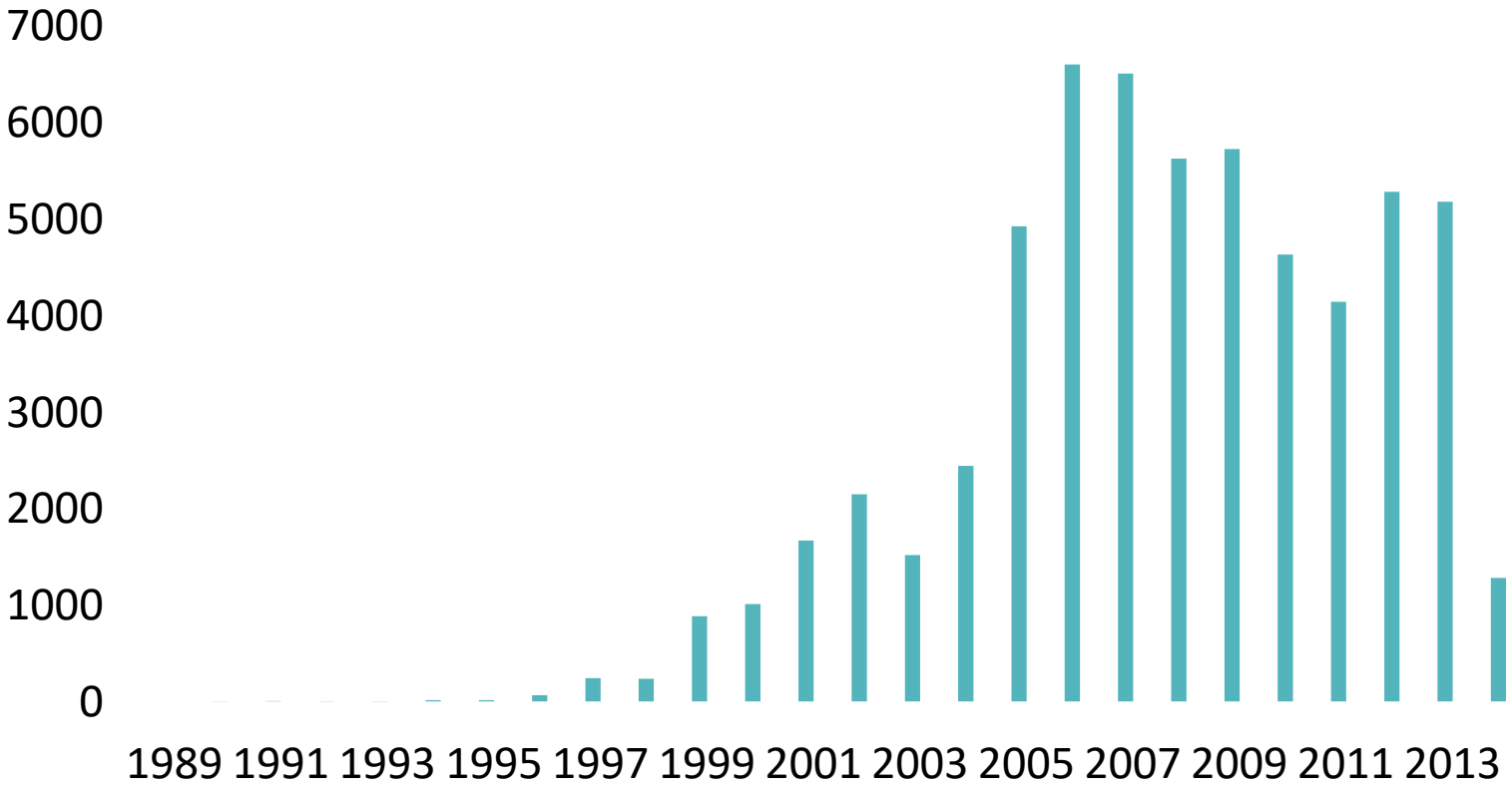
Paul Hines et. al., *Trends in the History of Large Blackouts in the United States. Energy Policy, V 37 2009*

Outage by Hour of the Day



What threats should a utility prepare against?

Number of Vulnerabilities Reported in Software



How should utilities embrace software?

Rapid adoption or slow and steady?

Generic Threat Matrix

Threat Level	THREAT PROFILE						
	Commitment			Resources			
					Knowledge		
	Intensity	Stealth	Time	Technical personnel	Cyber	Kinetic	Access
1	H	H	Years to decades	Hundreds	H	H	H
2	H	H	Years to decades	Tens of tens	M	H	M
3	H	H	Months to years	Tens of tens	H	M	M
4	M	H	Weeks to months	Tens	H	M	M
5	H	M	Weeks to months	Tens	M	M	M
6	M	M	Weeks to months	Ones	M	M	L
7	M	M	Months to years	Tens	L	L	L
8	L	L	Days to weeks	Ones	L	L	L

Reproduced from Duggan et al. [8].

Cyber-best practices

- Keep software up-to-date
- Use common software from large companies
- Use 2-factor authentication & strong passwords
- Scan all attachments
- Follow links after checking the sender

Who should defend our cyberphysical infrastructure?

Who should be responsible for the cyberphysical security of the electric grid?

- Government? (1 Fed, 50 States, 1000's cities)
- Private Industry? (180 IOUs)
- Public Industry? (1000's Coops and Munis)

What is the boundary of a *Critical Infrastructure*?

How much should we spend to defend it?

What’s the best management practice to keep it running?