Smart Grid: Robust/Energy Efficient vs. Hackable Orwellian Nightmare?

John C. Bean

Outline

How major U.S. blackouts prompted thinking about a "Smart Resilient Grid"

And how deregulation has since made the Grid even less reliable

The five elements proposed for such a robust and energy-efficient Grid:

Sensing trouble: Phasor (phase and frequency) Measurement Units (PMUs)

Isolating trouble: Local, smart, microprocessor-based sensors & circuit breakers

Logging & managing trouble: Digital Supervisory Control & Data Acquisition (SCADA)

Communicating trouble: An Intranet to linking whole Grid together

Controlling demand thereby mitigating trouble: An Advanced Metering Interface (AMI)

The latter involving power companies monitoring and/or controlling **your** IoT home appliances

Raising huge security and privacy issues (including hacker/governmental sabotage)

Versus some far less intrusive smart(ish) energy-saving tools & strategies

(Written / Revised: December 2017)

Smart Grid: Robust/Energy Efficient vs. Hackable Orwellian Nightmare?

As citizens, we've almost all heard about the "Smart Grid"

But, when push comes to shove, we're still a bit vague about what it is

Well, it turns out that the experts are a bit vague too

Indeed, many have **very different** views on what a "Smart Grid" is (or might be)

Some of which aren't really focused upon smartness

Some of which have little to do with the traditional Grid

In fact, the whole idea was originally driven more by what we wanted to **avoid**

Than by what we wanted to **achieve**

THIS was the sort of thing we **really** wanted to avoid:

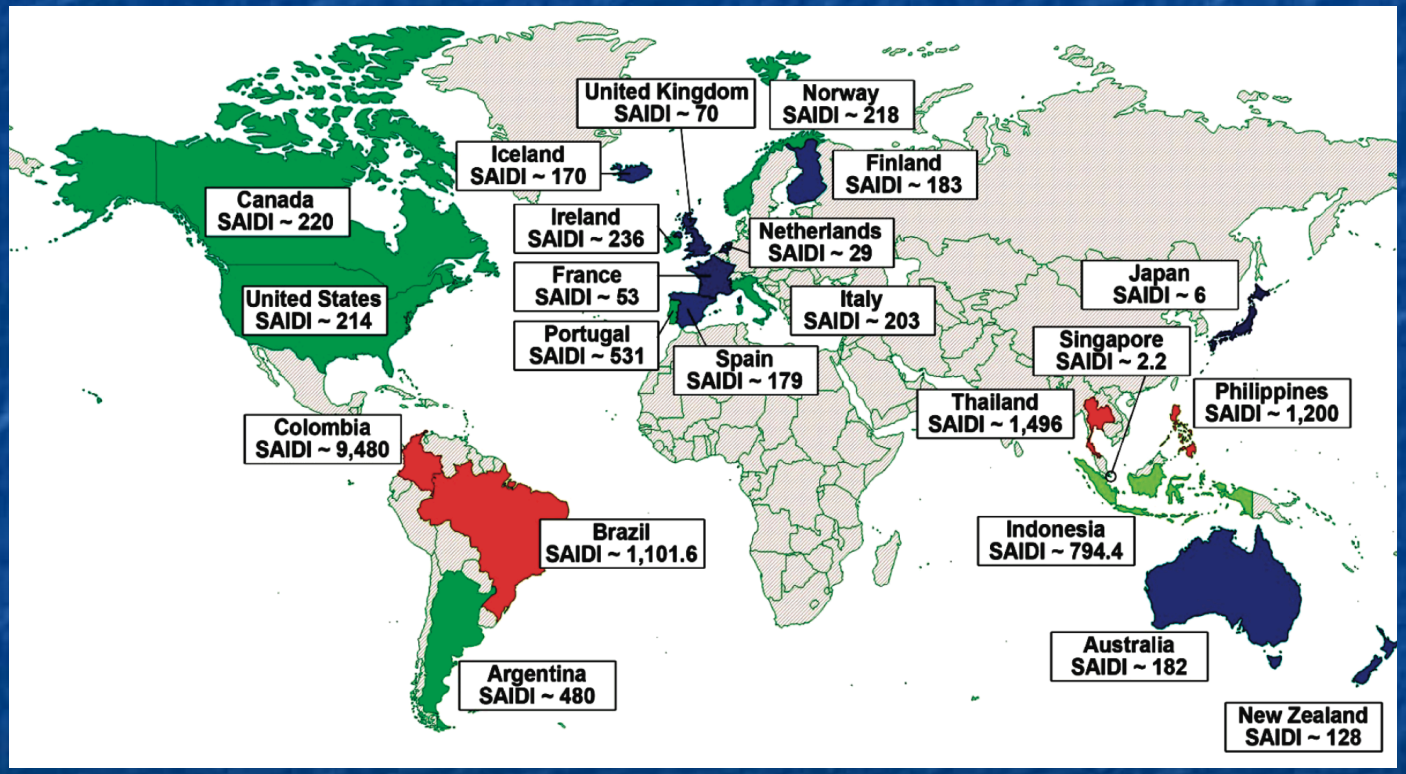
Satellite view of the U.S. on the evening of 14 August 2003:

Missing? Electrical power to 45 million people, spanning eight states!

Problems with Grid were obvious at least a decade before:

For the period 1992-2001, **excluding** outages due to storms/hurricanes:

System Average Interruption Duration Index (SAIDI) =
Average time that customers are without power during the period analyzed



SAIDI (in minutes):

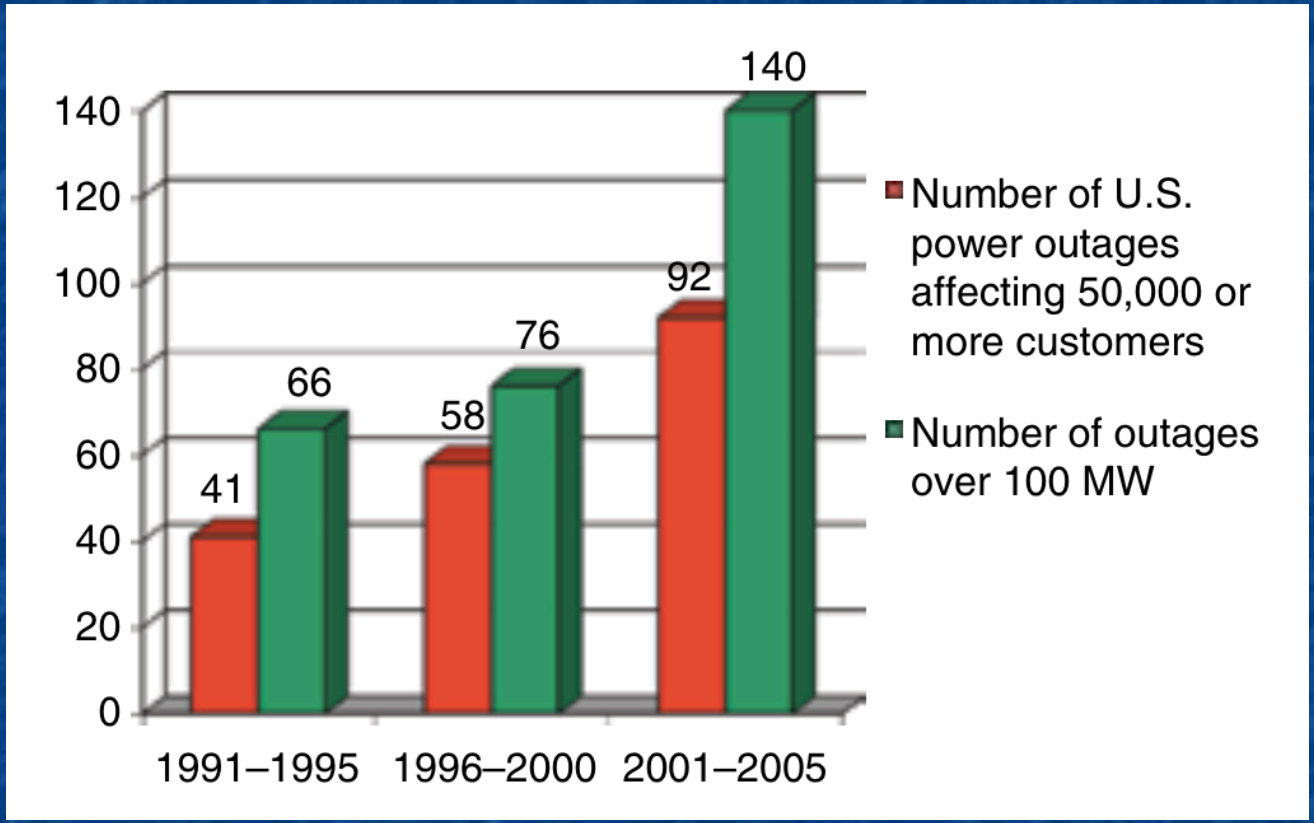
220 – Canada
214 - U.S.
203 – Italy
182 – Australia
128 – New Zealand
70 – U.K.
63 – France
29 – Netherlands
6 - Japan

U.S. power system was already one of the **least reliable** in the developed world

Terrorism and the Electric Power Delivery System, page 10, U.S. National Academies Press 2011
http://www.nap.edu/catalog/12050/terrorism-and-the-electric-power-delivery-system

How have things been going since 2001?

Not very well:



The Electric Power Grid: Today and Tomorrow, Massoud Amin and John Stringer, MRS Bulletin 33 (April 2008)
http://massoud-amin.umn.edu/publications/The_Grid_Amin_Stringer.pdf

Observations from a range of sources:

"On any given day, **500,000 customers** in the United States are without power for at least two hours" [1]

"The five-year annual average of outages doubled every five years . . . In **the first six months of 2014**, there were 130 reported grid outages - which puts that six month period as having **more outages than all but four years since 2000**" [2]

"In the past decade alone, an estimated **679 widespread power outages** occurred due to severe weather, costing the United States an annual average of between $18 billion and $33 billion.

Seven of the 10 costliest storm outages in United States history occurred between 2004 and 2012.

Blackouts cost the economy $112 USD per person per day, before accounting for injury, death, crime and delay, according to one analysis." [3]

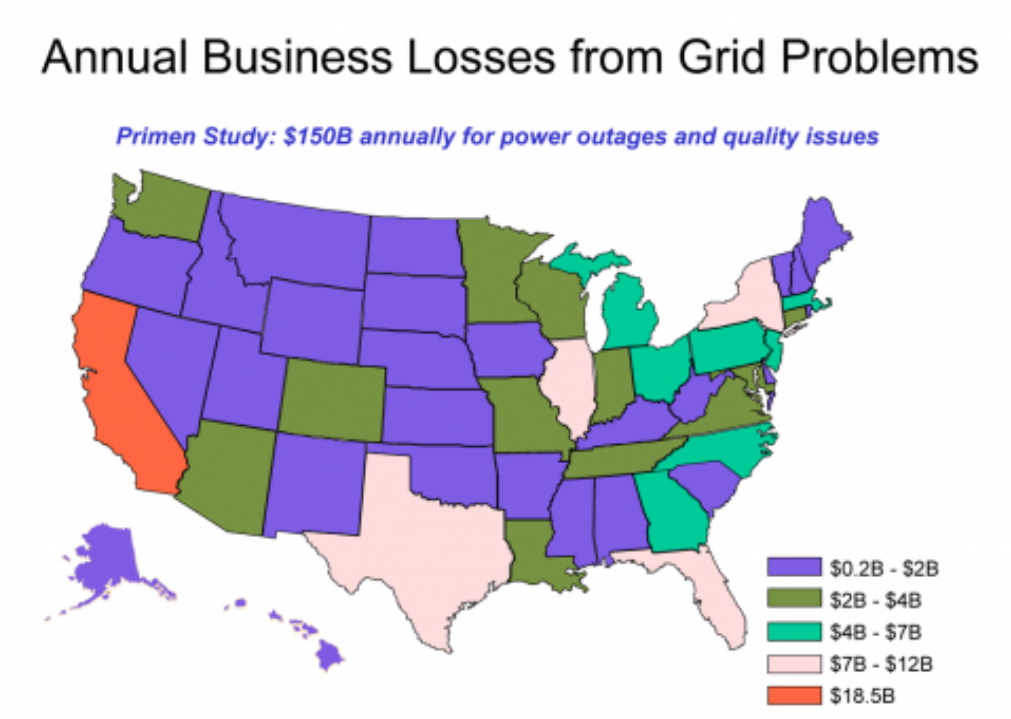
1) Securing the Grid, S. Massoud Amin: http://massoud-amin.umn.edu/publications/Securing-the-Electricity-Grid.pdf

2) http://insideenergy.org/2014/08/18/power-outages-on-the-rise-across-the-u-s/

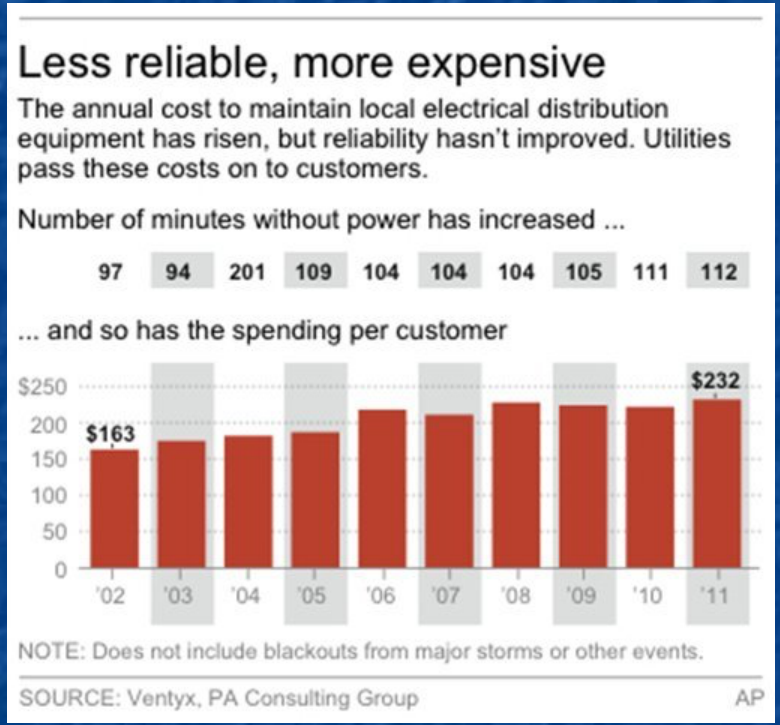
3) http://natgeotv.com.au/tv/american-blackout/american-blackout-facts.aspx

Speaking of costs:

Forbes Magazine:



The Washington Post:

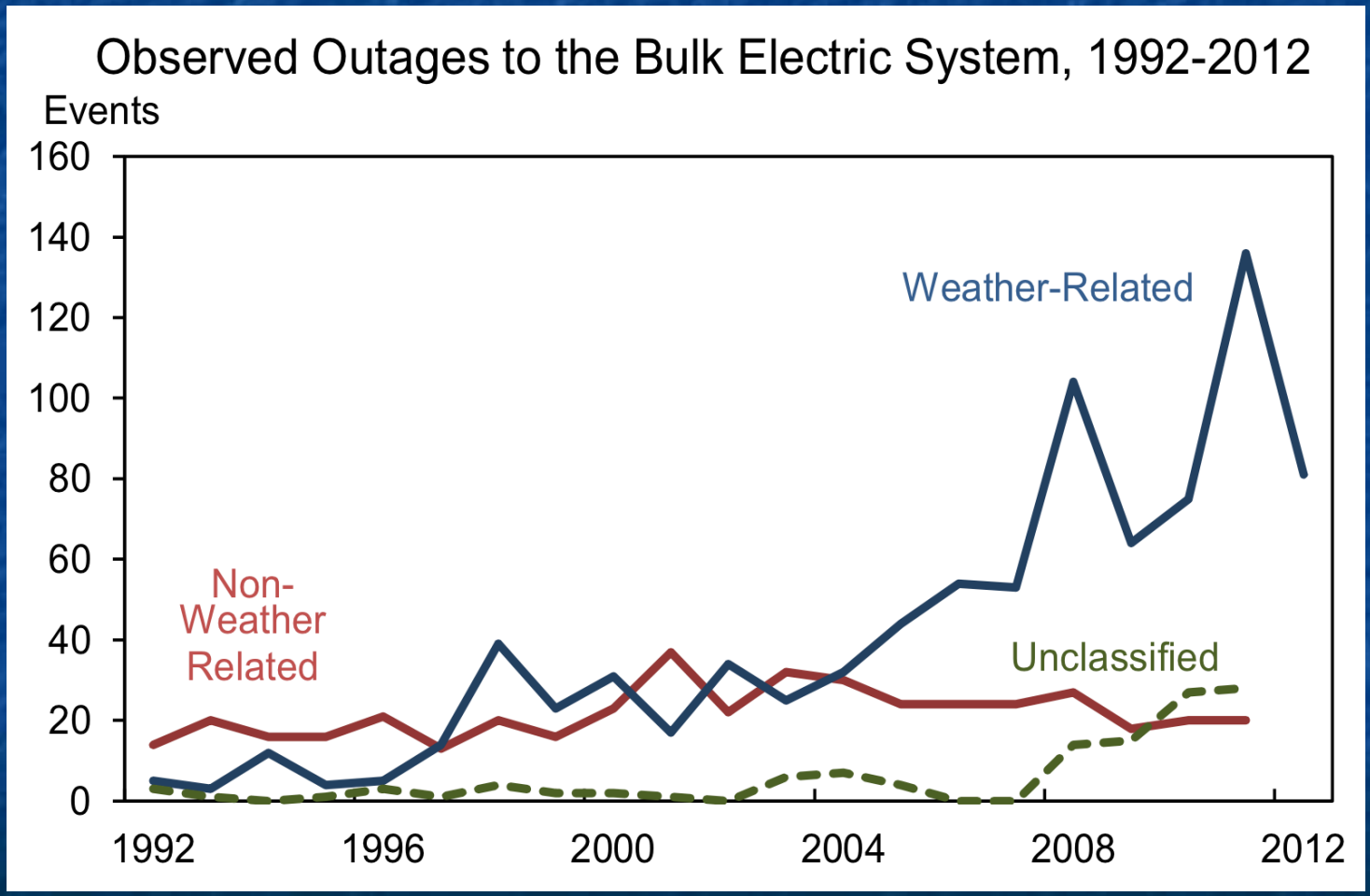


Left: Blackout Risk Tool Puts Price Tag On Power Reliability, Forbes Magazine (30 August 2013) http://www.forbes.com/sites/williampentland/2013/08/30/blackout-risk-tool-puts-price-tag-on-power-reliability/

Right: http://www.washingtonpost.com/blogs/wonkblog/wp/2013/03/08/surprise-the-u-s-power-grid-is-getting-pricier-less-reliable/

And if you include weather / possible global warming effects:

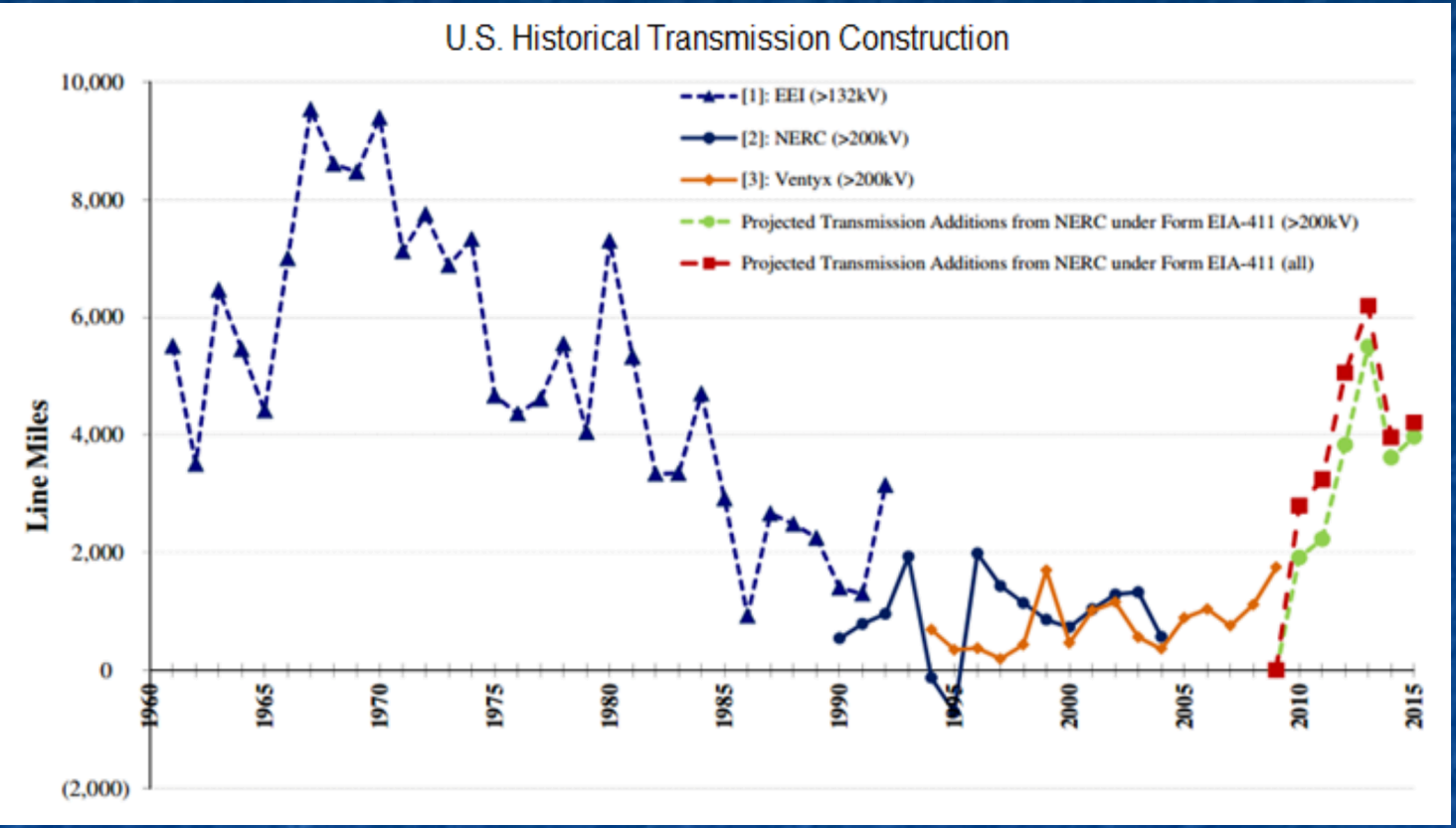
From a White House report:



p. 8, Economic Benefits of Increasing Electric Grid Resilience to Weather Outages – White House Report
http://energy.gov/sites/prod/files/2013/08/f2/Grid%20Resiliency%20Report_FINAL.pdf

What's going on?

Well, for one, we are investing far less in our Grid:



Rise at right was only a projection of reaction to U.S. economic stimulus funding (not independent private investment)!

p. 7, Economic Benefits of Increasing Electric Grid Resilience to Weather Outages – White House Report 2011
http://energy.gov/sites/prod/files/2013/08/f2/Grid%20Resiliency%20Report_FINAL.pdf

What led to this situation?

In 1978 Congress passed the **Public Utility Regulatory Policy Act (PURPA)**

Prior to this act, power companies were . . . power companies

That is, as government-regulated monopolies, they did it all

Both producing power and delivering power

But PURPA not only removed their monopoly on in-house power production,

It also compelled them to buy power from **others** when it cost less

And then distribute that power over their transmission networks

This was partially motivated by desire to open the Grid to emerging power sources

But major motivation was belief that free market might just better provide power

The same belief that led to break-up of Bell System (my former employer)

This Act and others led to:

A change in **Federal Energy Regulatory Commission (FERC)** policy:

Which, in the 1980's and 1990's, began encouraging power companies to:

Sell off their in-house power generation capabilities

Substitute bought-in market-supplied power

If they fully responded: Power companies => Transmission companies ONLY

But the responsibility for the Grid then got **really** muddy:

These power/transmission companies were still government-regulated

And were still held responsible for delivering affordable, reliable power

Despite fact that they no longer fully controlled the power system

While their free-market **power suppliers** were NOT regulated

And now add in the need for "power generation margin"

Power generation margin =

Extra power plants / transmission lines used **only** for power surges

This is a bit different from more common **dispatchable** power plants

Which are **predictably** required every evening as demand peaks

Generation margin is instead designed to meet **unpredictable** demand

As in emergencies, including (possibly) when:

2 minutes from now when something leads everyone to flick on their TV

Yes, a spike in TV viewing could cause a Grid "emergency"

Because there is essentially zero elasticity in electrical power:

Millisecond by millisecond, power **produced** must = power **consumed**

Tolerable mismatch between power production and demand:

From my **Generic Power Plant & Grid** (pptx / pdf / key) notes:

AC voltage has to be held within 5% of 115 Volts

Frequency has to be held within ~ 0.067 Hz of 60Hz

Phase must be held within 10° (i.e., 1/36th of cycle)

The latter two frequency specs correspond to 0.1% and 0.5 millisecond shifts

So timing and precision are everything, and this compels power companies to:

Not only keep spare power plants off line (on standby), but also to:

Keep some power plants spinning idly, all of the time

So that they can be put into service, within seconds

HOWEVER: This equipment may be needed less than 1% of the time!

What effect has deregulation had upon this safety margin?

Pre-deregulation power generation margins had been held at **25-30%**

After the above changes in regulatory policy, they fell to **10-15%**

(What MBA is going miss the opportunity to cut back on something used 1% of the time!)

While U.S. power demand in the 1990's rose by **35%**

Investment in new transmission lines rose by only **18%**

In this decade some predict that power demand might rise by another **20%**

But transmission capability is expected to rise only **4%**

Put another way (from the same source as numbers above[1]):

"The (U.S.) power industry spends a smaller proportion of annual sales on R&D than do the dog food, leather, insurance, or many other industries - less than 0.3%, or about $600 million per year"

1) For the Good of the Grid, Massoud Amin, U. Minnesota + Electric Power Research Institute
http://massoud-amin.umn.edu/publications/FortheGoodoftheGrid.pdf

Muddied responsibility + MBA's => Reduced margins, investment, R&D . . .

Thus demand more often exceeds reduced power production margins

= Explanation for increased power blackouts, right?

Yes and No:

YES: Local failures have been caused by unexpected demand

Or by spot failures in power production and/or transmission equipment

NO: But this does not account for the massive size of many U.S. power blackouts

As seen in some of our biggest U.S. / Canadian blackouts:

9 November 1965

Blacked out: 30 million people / 80,000 square miles

"Maintenance personnel incorrectly set a protective relay on one of the transmission lines . . . a small surge of power originating from the Robert Moses generating plant in Lewiston, New York caused the improperly set relay to trip at far below the line's rated capacity" [1]

Cause = 1 human error + 1 small surge, shutting down 1 local power line

http://en.wikipedia.org/wiki/Northeast_blackout_of_1965

14 August 2003

Blacked out: 45 million people / Eight U.S. states

"The blackout's primary cause was a software bug in the alarm system at a control room of the FirstEnergy Corporation, located in Ohio. A lack of alarm left operators unaware of the need to re-distribute power after overloaded transmission lines hit unpruned foliage" [1]

CAUSE = 1 branch hitting 1 transmission line + 1 malfunctioning alarm

Which, led to 568 generators at 265 power plants tripping off!

http://en.wikipedia.org/wiki/Northeast_blackout_of_2003

Precipitating events were almost trivial:

Amount of power initially lost was **insignificant** on scale of area ultimately affected!

So while diminished **power production margin** might have caused **local** problem

It can't be wholly blamed for hugely larger eventual blackouts

As borne out by another blackout in 1966 starting at Oregon – California border:

Blacking out 13 states and provinces => 1.5 billion dollars in damage

But for which later analysis indicated that:

"shedding (dropping) some **0.4%** of the total load on the grid for just 30 minutes would have prevented the cascading effects and prevented large-scale regional outage" [1]

So problem is more about a fundamental instability in the grid

1) http://massoud-amin.umn.edu/publications/FortheGoodoftheGrid.pdf

So why IS the Grid so unstable?

And why **didn't** they

Just cut off 0.4% of their customers to stop the blackout?

Answers:

First (as noted above): **Tolerance for anomalous power is razor thin**

Second: **Impact of anomalies spreads at almost the speed of light**

This means protective actions have to be taken in milliseconds to seconds

- Human organizations cannot make decisions at that speed

- A human being cannot even fully comprehend the problem in that time

So human beings must be removed from the (immediate) loop

AND "decisions" must be made at the ***site*** *of the problem*

The most basic action/decision? Open up a circuit breaker to isolate problem area

But a standard circuit breaker may be too slow (e.g., 100's of milliseconds!)

Further, it can only make rather simple / dumb decisions based on:

"Current is too high!" or possibly: "Voltage is too low!"

So we need ultrafast breakers capable of reacting to more complex faults

Frequency anomalies are **particularly** critical:

Frequency should be synchronized across grid to within 0.067 Hz of 60Hz

Generators can melt down if they are mismatched by just 2 Hz!

So we also need local sensors capable of detecting minute frequency shifts

=> ***"A Smart Resilient Grid"*** **-** *then shortened to just* ***"A Smart Grid"***

Which would involve these responsibilities / handled via these features: [1]

1) **Sensing Trouble**: **Phasor Measurement Units (PMUs)**

Sensors comparing local AC frequency and phase to the grid standard

GPS enabled + using satellites' hyper-accurate atomic clocks

2) **Isolating trouble**: **Local microprocessor-based sensors & circuit breakers**

Capable of analyzing and responding to complex / subtle faults

Based on **programmable logic controllers (PLCs)**

3) **Logging and managing trouble**:

Digital supervisory control & data acquisition systems (SCADA)

To make the required, almost instantaneous, protective decisions

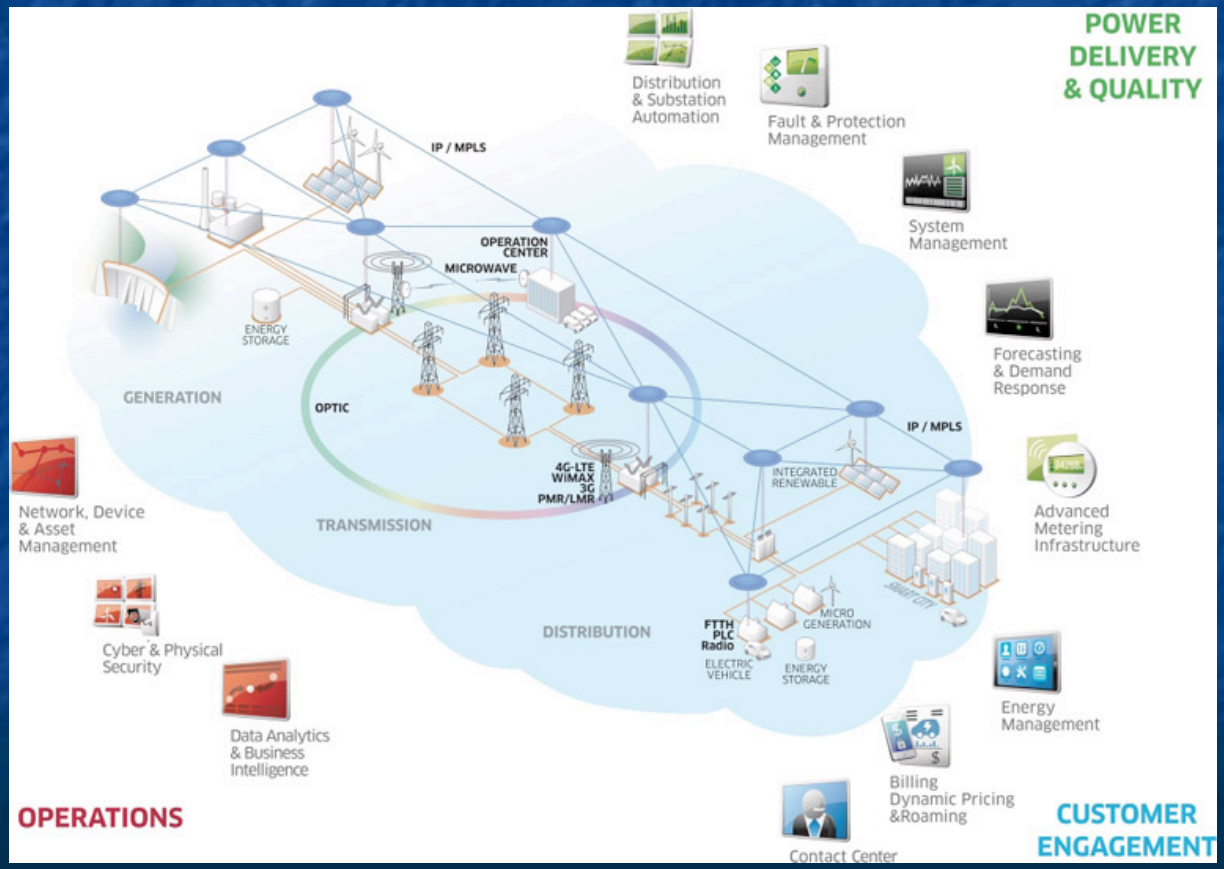
1) http://www.epri.com/abstracts/Pages/ProductAbstract.aspx?ProductId=000000000001022519

*But that control system should be both local **and** distributed:*

Local to take immediate protective actions

Distributed to instigate **grid-wide** protective measures

For example: Cueing human operators to start up reserve generators



https://www.csiac.org/journal_article/efficacy-and-challenges-scada-and-smart-grid-integration

Distributed part of SCADA => 4th Smart Grid feature: **An Intranet**

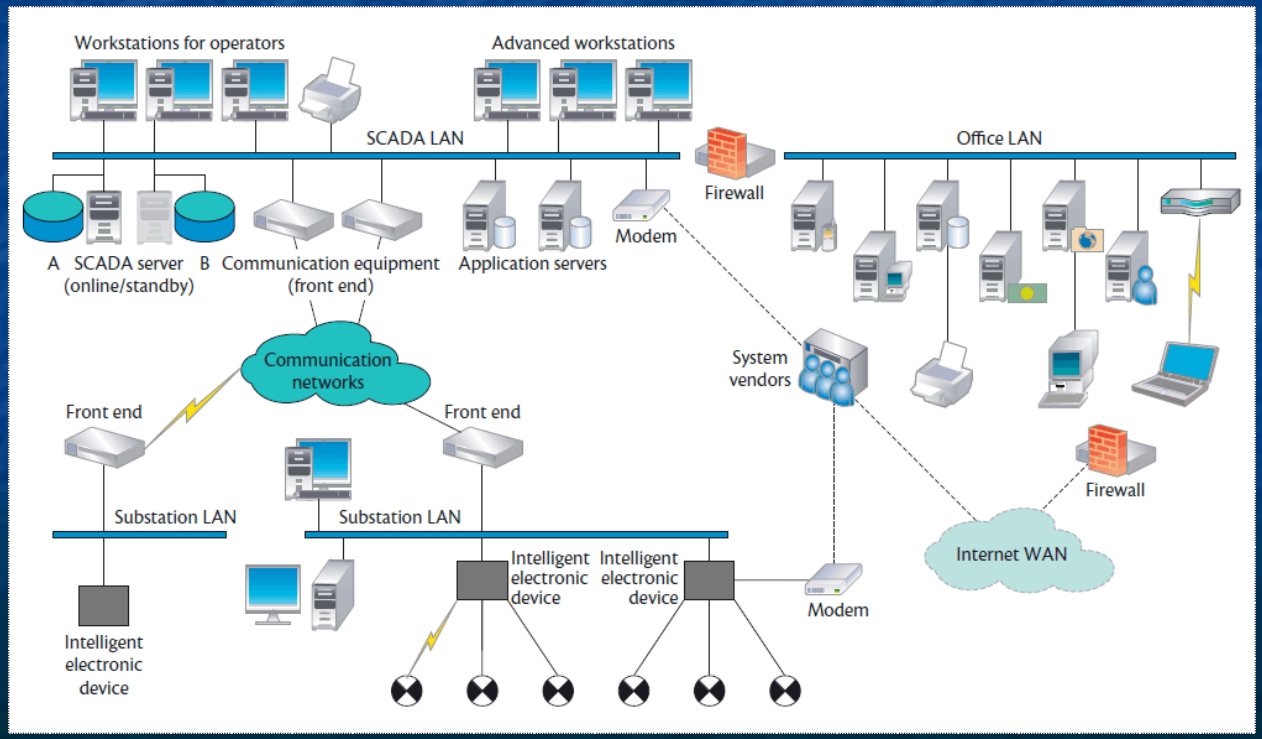
With the responsibility of communicating trouble

Essentially a very high reliability, very high speed version of the Internet

You can't just break data into packets and idly sprinkle them into a network

(Which is what we do with our data on the Internet!)

Instead, power system alarm data must get through, intact, **within milliseconds**!



http://www.computer.org/csdl/mags/sp/2012/04/msp2012040062-abs.html

And it's not just about the hardware:

We are not really sure of HOW the SOFTWARE should operate!

The Grid is HUGELY more complex than normal industrial control systems

Power system complexity & critical timing begin resemble a human brain

So Grid software models have invoked or drawn analogies with (partial list only[1]):

Optimal Control Theory	Ecology	Human Cognition
Glassy Dynamics	Information Theory	Bio-Systems
Microphysics of Clouds	Kuramoto Oscillators	Markow Processes
Random Fuse Networks	Neural Networks	

Maximum Entropy (e.g., as in Shannon communication theory) . . .

*1) For **Slightly** more detail + references see: http://en.wikipedia.org/wiki/Smart_grid*

Some Smart Grid descriptions **also** *emphasize changes in layout:*

For instance, the need for multiple power delivery routes to enhance resiliency

But this is old news, the Grid has been doing this for a century!

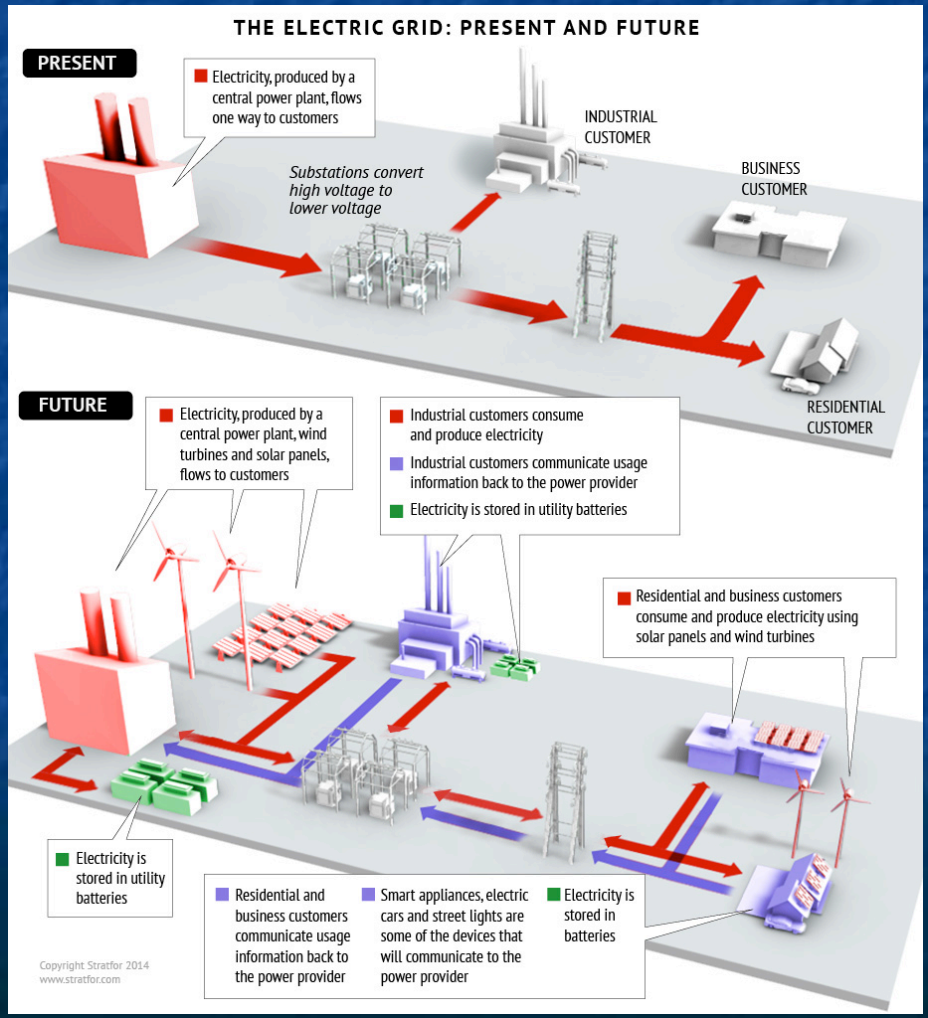
Or 2-way power transmission:

For example, to accommodate house-by-house production of solar or wind power:

But contrary to impression given at right

Change is not new 2-way wires!

Wires are intrinsically 2-way



https://www.stratfor.com/analysis/architecture-electricity-evolving-albeit-gradually

Change is instead at the ENDS of the wires:

In the 5th Smart Grid feature, an **Advanced Metering Interface (AMI)**

With the job of controlling demand, and thereby mitigating trouble

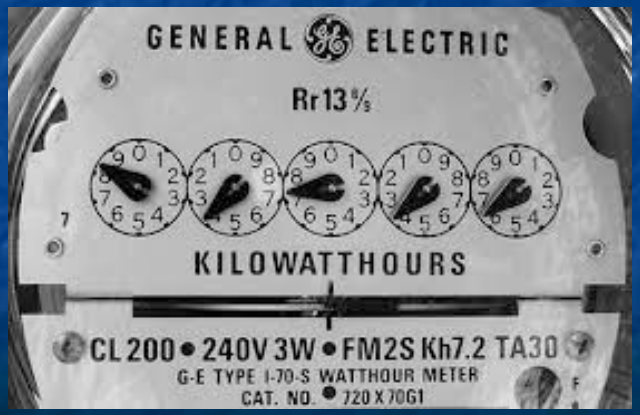
At its lowest level, this consists of a **Smart Meter**

Old power meters only recorded your **total** monthly power consumption

Smart meters instead tell the power company **what** power you consumed **when**

They also "run backward" if you produce power and send it **back into the Grid**

Old dumb meter:



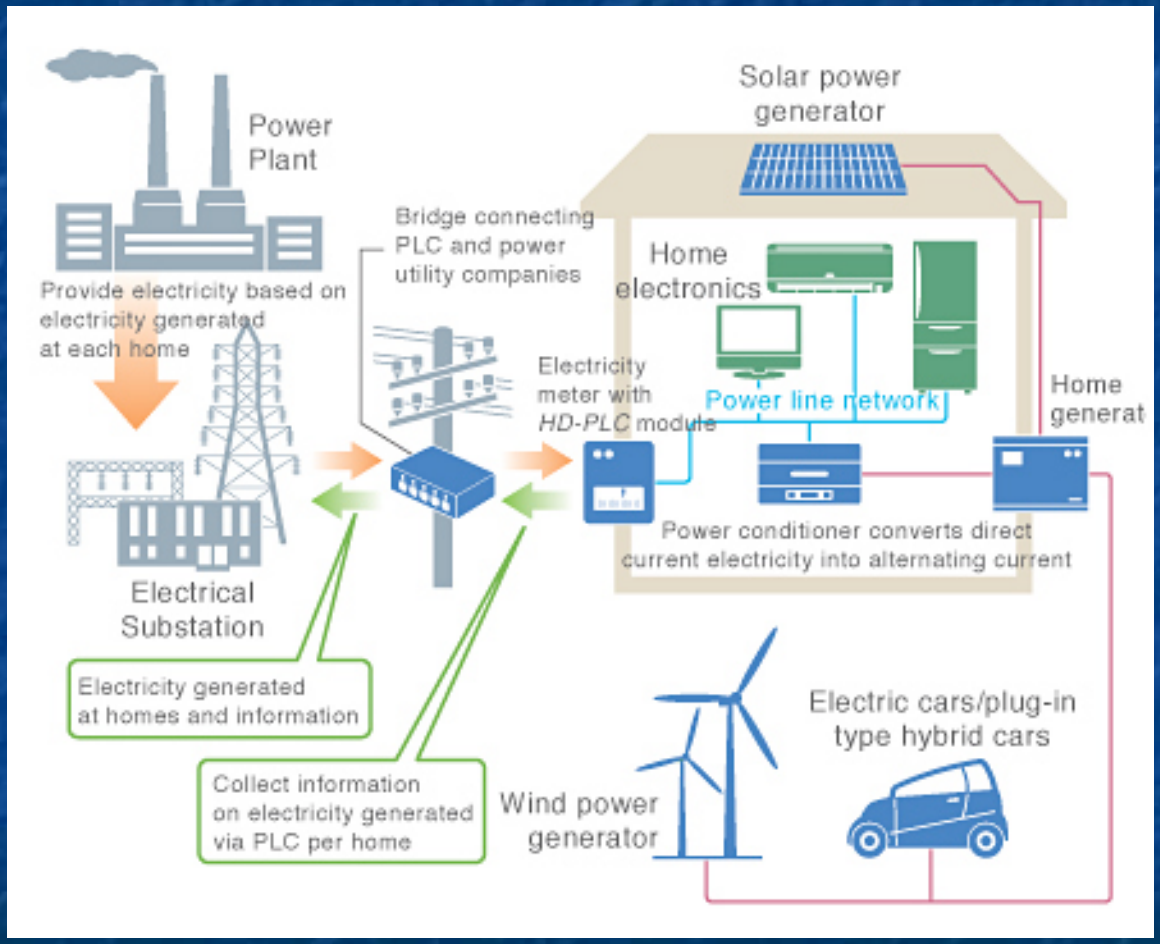
http://www.treehugger.com/clean-technology/baltimore-announces-massive-smart-grid-program-2-million-meters-to-be-installed.html

New smart meter:

http://www.wired.com/2010/03/smart-grids-done-smartly/

But full blown AMI would operate more like this:

As the interface with a whole-house power management/information system:



This, finally, sounds like the "Smart Grid" as it is known to most consumers

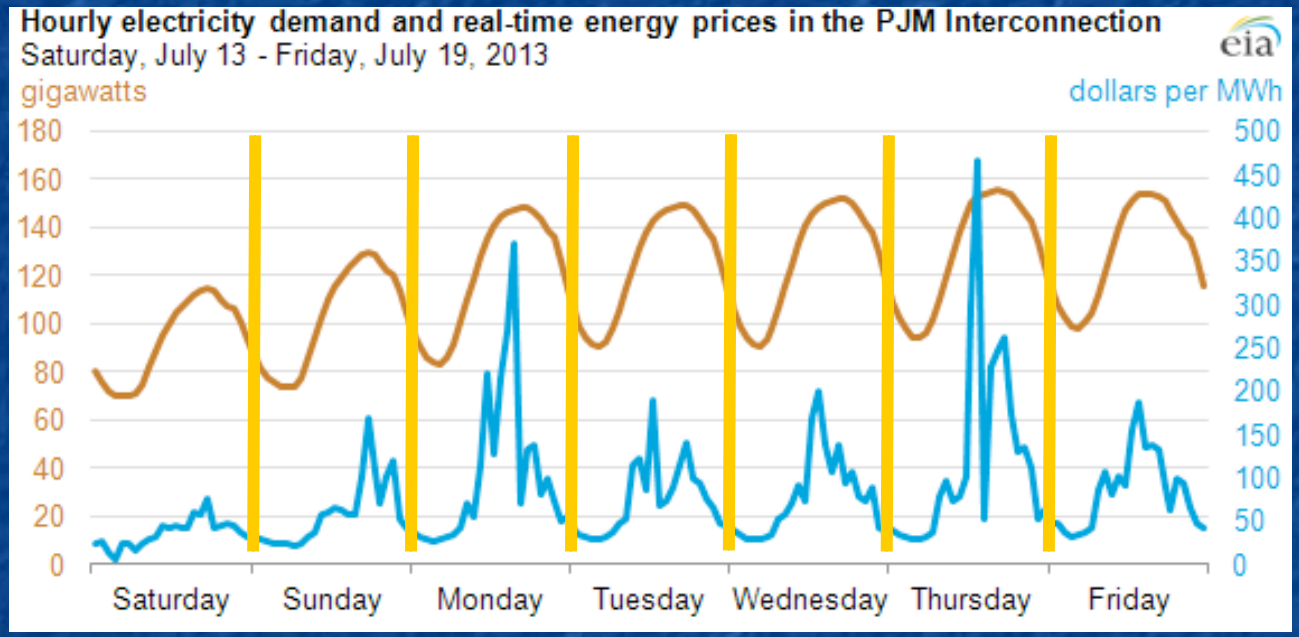
http://www.hd-plc.org/modules/feature/090619.html

Which would enable Smart Grid functions of:

a) Billing for power based on its true cost of production at that time

= The prime incentive for smarter household/business consumption of energy

From **Energy Production & Consumption** (pptx / pdf / key) notes, looking at right axis:



Midday true cost of power can be **2X** times cost in middle of the night

Evening true cost of power can be **4X** times cost in middle of the night

www.eia.gov/todayinenergy/detail.cfm?id=12711

Full AMI would ALSO allow:

b) Payment for power put back into the Grid by "customers"

= Prime incentive for **distributed** household/business power production

Which would, in turn, incentivize the possibility of:

c) Home-based Grid energy storage

Via schemes such as Vehicle to Grid [1] (V2G):

Or via new, more affordable and efficient, in-home batteries:

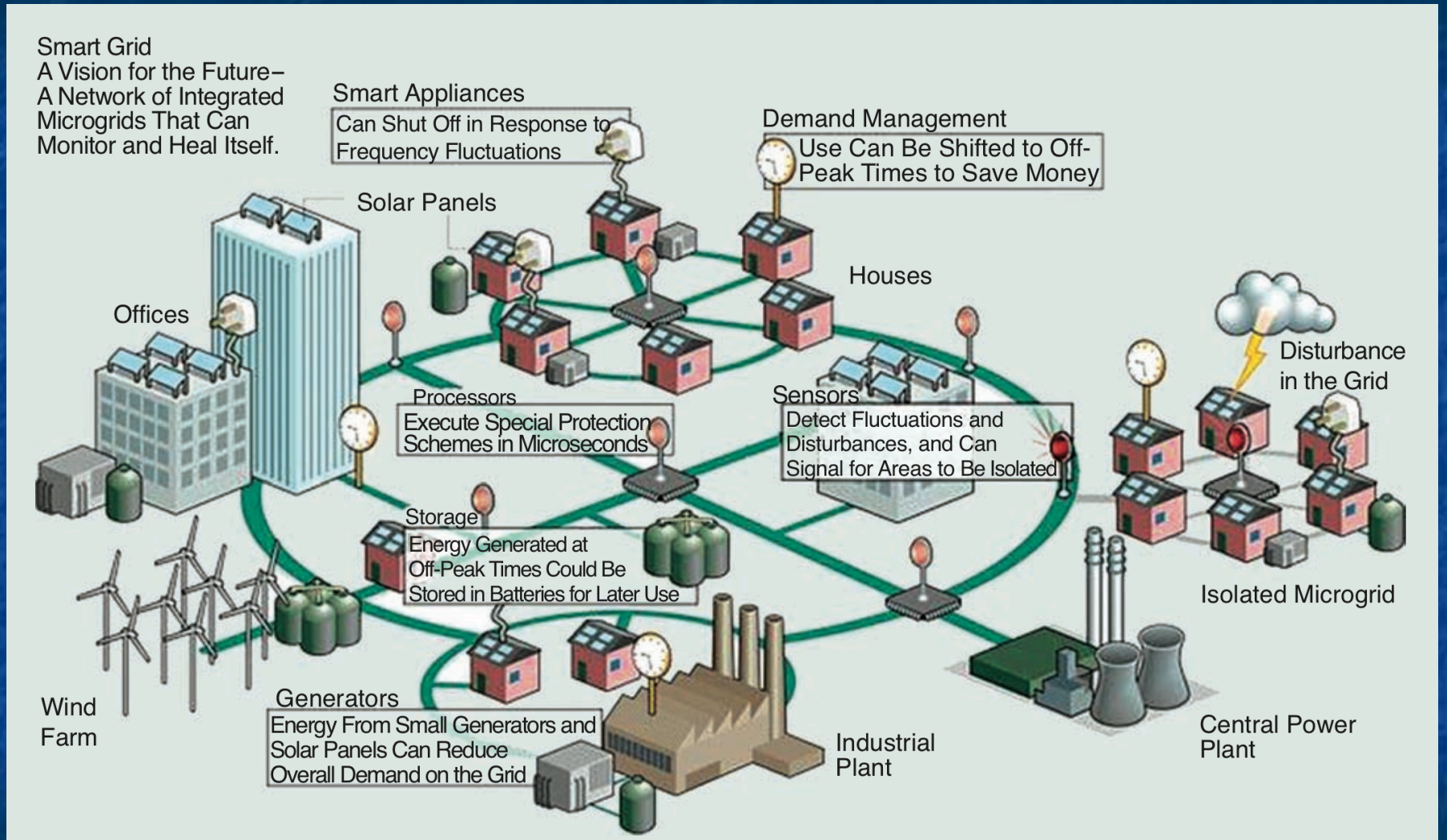
"Tesla Unveils Batteries to Power Homes" [2]

"The rechargeable lithium-ion battery unit would be built using the same batteries Tesla produces for its electric vehicles . . . The system is called Powerwall and Tesla will sell the 7kWh unit for $3,000 while the 10kWh unit will retail for $3,500"

1) For details on V2G see my "Electrification of Transportation" lecture notes

2) http://www.bbc.com/news/technology-32545081

Putting this all together = A Smart Resilient Grid:



http://massoud-amin.umn.edu/publications/FortheGoodoftheGrid.pdf

Paraphrasing those almost unreadable boxes, this Grid would:

Monitor and heal itself by:

- Detecting fluctuations and disturbances, signaling areas to be isolated
- Using processors executing special protection schemes in microseconds

Protect our homes by:

- Using smart appliances that shut off in response to frequency fluctuations

Enhance Grid efficiency by:

- Demand management shifting power use off peak, saving money
- Allowing energy generated off peak to be stored in batteries for later use
- Using small home/business generators to reduce overall demand on grid

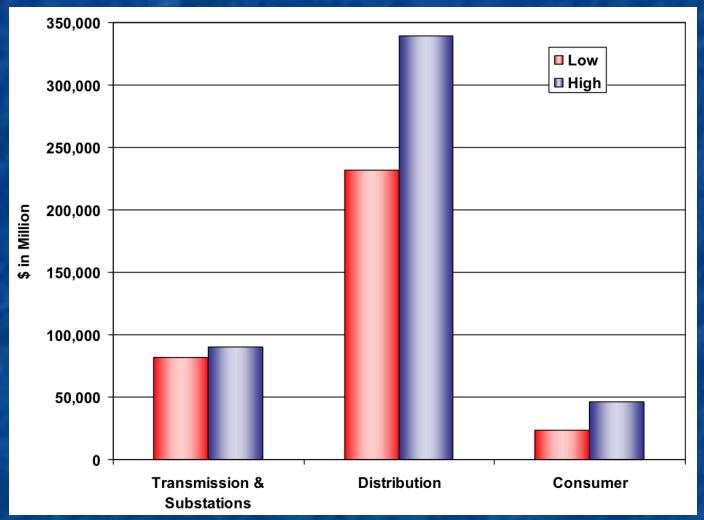
http://massoud-amin.umn.edu/publications/FortheGoodoftheGrid.pdf

OK, sounds pretty good so far, what are the issues?

First, of course, is cost: From New York Times article [1] based on an EPRI study: [2]

"Deployment of smart grid technology from U.S. utility control centers and power networks to consumers' homes could cost between **$338 billion** and **$476 billion** over the next 20 years"

WHERE would that money need to be spent? Mostly on the power distribution system: [2]



1) http://www.nytimes.com/cwire/2011/05/25/25climatewire-smart-grid-costs-are-massive-but-benefits-wi-48403.html?pagewanted=print

2) http://www.epri.com/abstracts/Pages/ProductAbstract.aspx?ProductId=000000000001022519

With very little going into the "smart" things in or near our homes

And only a minor share going into long-distance power transmission

Instead, spending => Smart circuit breakers, PLCs, PMUs, SCADA, and power intranet

Who is going to ultimately foot the bill for this? We are, of course:

From that EPRI (Electric Power Research Institute) report: [1]

Smart Grid Cost to Consumers – Allocated by Annual kWh (a)								
Class	$/Customer Total Cost (b)		$/Customer-Year, 10-Yr Amortization (c)		$/Customer-Month, 10-Yr Amortization (d)		% Increase in Monthly Bill, 10-Yr Amort (e)	
	Low	High	Low	High	Low	High	Low	High
	$/Customer	$/Customer	$/Cust/yr	$/Cust/yr	$/Cust/ Month	$/Cust/ Month		
Residential	$1,033	$1,455	$103	$145	$9	$12	**8.4%**	**11.8%**
Commercial	$7,146	$10,064	$715	$1,006	$60	$84	**9.1%**	**12.8%**
Industrial	$107,845	$151,877	$10,785	$15,188	$899	$1,266	**0.01%**	**1.6%**

(a) LOW refers to EPRI low estimate of $ total SG costs; HIGH is the other SG cost. Customer numbers by class (residential, commercial industrial) are for 2009 from EIA. SG costs are allocated to customer classes based on 2009 kWh sales (38 %residential; 37% Commercial; 25% industrial).

(b) Total SG cost divided by customers for each segment (residential +commercial+ industrial).

(c) Annual cost per customer per year for total SG cost spread out (amortized) equally over 10 years (nominal values).

(d) Annual cost per customer per month for total SG cost spread out (amortized) equally over 10 years (nominal values).

(e) Annual increase in monthly bill for based on (d).

(yellow highlight added)

1) http://www.epri.com/abstracts/Pages/ProductAbstract.aspx?ProductId=000000000001022519

What will that investment get us?

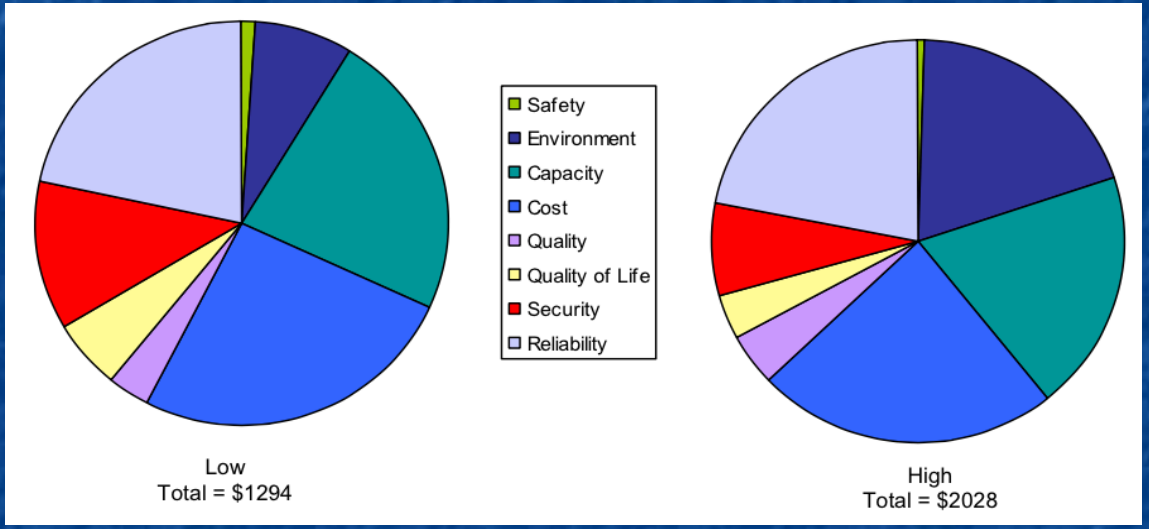
"**$1.3 trillion** to **$2 trillion** in benefits over that period."

Benefit / Cost ratio ~ 3:1 to 6:1

With savings / benefits breaking down approximately as follows:

Estimated Benefits of the Smart Grid

Attribute	Net Present Worth (2010) $B	
	Low	High
Productivity	1	1
Safety	13	13
Environment	102	390
Capacity	299	393
Cost	330	475
Quality	42	86
Quality of Life	74	74
Security	152	152
Reliability	281	444
Total	**1294**	**2028**

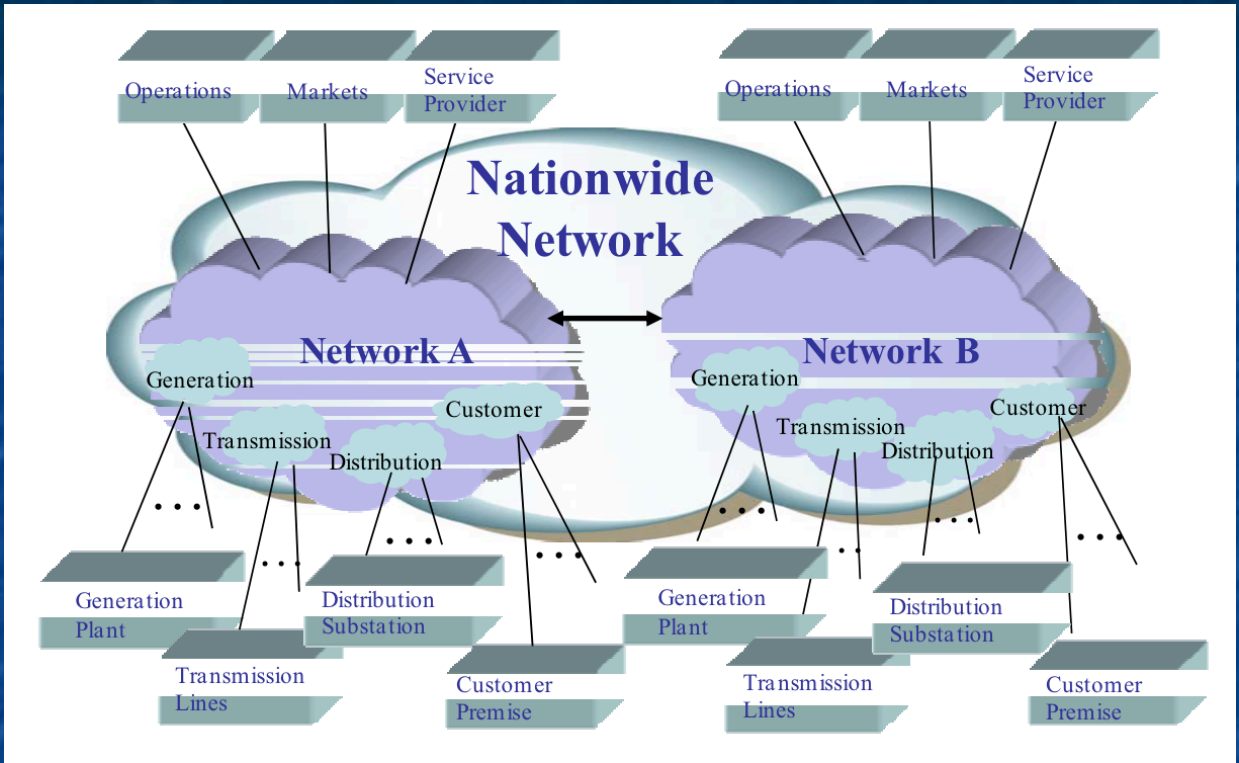


Also very important (for savings AND the environment):

"Demand response and efficiency gains enabled by smart grid technologies would reduce annual electricity growth to less than 0.7 percent . . . The growth rate in peak energy demand would be even lower."

http://www.epri.com/abstracts/Pages/ProductAbstract.aspx?ProductId=000000000001022519

*But EPRI also points out that this will require a **nationwide** effort:*



To work, 48 states and dozens (hundreds?) of power companies must fully cooperate

Meaning that the U.S. government will have to lead in BIG way

Is this likely in an era where: BIG + Government => Gridlock ?

http://www.epri.com/abstracts/Pages/ProductAbstract.aspx?ProductId=000000000001022519

The U.S. has **another** *unique cost + government issue:*

As noted above, a Smart Resilient Grid requires a high capability intranet

Providing reliable millisecond interconnection of its control system (SCADA)

And that intranet also better be damned secure!

Further if, as is likely, it handles both Grid control AND customer transactions:

Firewall between those functions had better be exceptionally strong

All of this makes it likely that Grid intranet will be very expensive

Which makes it VERY tempting to look for other ways of making it pay

Power companies are thus talking about becoming digital service providers (DSPs)

Driving **our existing** DSP's / Cable / Satellite companies up the walls!

Thus Smart Grid projects sometimes move **faster/farther** in countries where **governments** provide (or heavily regulate) BOTH power and DSP services!

Further, I glossed over a potential land mine:

Smart meters will allow power companies to **charge you more** for peak power

Or **pay you more** for home power generation during peaks

But full industry Smart Grid proposals [1] call for much more:

Smart Grid intranet would talk to your individual appliances:

Through a new **Home Area Network (HAN)**

Also sometimes nicknamed **The Internet of Things (IoT)**

The **HAN** could use its 2-way appliance communication to do things like:

Changing temperature settings on heat, AC, refrigerators . . .

Even turning off certain appliances during peak demand

1) http://www.epri.com/abstracts/Pages/ProductAbstract.aspx?ProductId=000000000001022519

Do we really want to give power companies control over our appliances?

And implicit in that control:

Do we want the power company to **know** every time we push an "on" button?

Do we trust them with minute-by-minute information about our lives?

How long will it take an MBA to realize he/she can sell that information,

leading to this (eminently / imminently) possible scenario:

You open the door to your microwave oven

and **instantaneously** an advertisement for microwave popcorn

appears on the screen of your TV / iPhone / iPad / laptop / etc. . . . ?

Even if suitable privacy laws could be enacted (with gaping loopholes for the NSA?):

Are power companies **capable** of designing and implementing a

hacker-proof network stopping **others** from exploiting such information?

*"Smart" home appliances are **already** being hacked (massively!)*

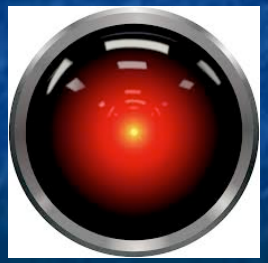
Prime example: The Google-Nest Learning Thermostat

At the August 2014 "Black Hat USA" computer security conference [1]

Hackers needed **15 seconds** to get thermostat to display this message: [2,3,4]

"Hello Dave"

"I know that you and Frank were planning to disconnect me, and I am afraid that is something I cannot allow to happen."



1) https://www.blackhat.com/us-14/
2) http://venturebeat.com/2014/08/10/hello-dave-i-control-your-thermostat-googles-nest-gets-hacked/
3) http://www.computerworld.com/article/2476599/cybercrime-hacking/black-hat-nest-thermostat-turned-into-a-smart-spy-in-15-seconds.html
4) http://www.theinquirer.net/inquirer/news/2359748/hackers-root-googles-nest-thermostat-in-15-seconds

A Nest expert was interviewed about this

And he correctly pointed out that: [1]

> "All hardware devices - from laptops to smartphones - are susceptible to jailbreaking; this is not a unique problem. This is a physical jailbreak **requiring physical access**

But he then went on to recommend that:

> "One of your best defenses is to buy a Dropcam Pro
> so you can monitor your home when you're not there"

Dropcam is **another** Google-Nest company, which led to the article's headline:

"Hackers root Google's Nest thermostat in 15 seconds

Firm advises buying one of its security cameras"

(Psst! Google Guys: Might **adding** a web-accessible camera just compound the problem?)

1) http://www.theinquirer.net/inquirer/news/2359748/hackers-root-googles-nest-thermostat-in-15-seconds

Sample of now almost weekly reports on "Internet of Things" insecurity:

From a variety of computer security experts interviewed by CBS News: [1]

"future and current technologists will have to design
devices that are resilient on their own,
rather than assuming that the home network is already secure"

"Hackers who could get access to something as simple
as your historical thermostat records
could predict when you are in [or] out of the house (giving clues when to rob it)"

From "Spies in our Living Room" about a HP computer security report: [2]

"**70% of smart appliances have serious security weaknesses**,
running the gamut from lack of encryption
to insecure firmware to easily guessed passwords"

1) http://www.cbsnews.com/news/keeping-smart-homes-safe-from-hackers/
2) http://www.geek.com/apps/the-spies-in-your-living-room-70-of-smart-appliances-vulnerable-to-cyber-attack-1600725/

And then there are the infamous refrigerator and Barbie Doll hacks:

From articles about a report from computer security firm Proofpoint:

"For the first time, hackers used a refrigerator to attack businesses:

hackers broke into more than 100,000 everyday consumer gadgets, such as home-networking routers, connected multi-media centers, televisions, and at least one refrigerator, Proofpoint says. They then used those objects to send more than 750,000 malicious emails to enterprises and individuals worldwide." [1]

From Christmas 2015 articles in the Guardian [2] (and elsewhere):

"Mattel's latest Wi-Fi enabled Barbie doll can easily be hacked to turn it into a surveillance device for spying on children and listening into conversations without the owner's knowledge."

"It connects to the internet via Wi-Fi and has a microphone to record children and send that information off to third-parties for processing before responding with natural language responses.

1) http://www.cbsnews.com/news/keeping-smart-homes-safe-from-hackers/
2) http://www.geek.com/apps/the-spies-in-your-living-room-70-of-smart-appliances-vulnerable-to-cyber-attack-1600725/

BREAKING NEWS:

As reported in the December 2107 article in the New York Times entitled

A Cute Toy Just Brought a Hacker Into Your Home [1]

Even the **FBI** has issued a warning about "smart" IoT children's toys, which begins: [2]

Public Service Announcement

FEDERAL BUREAU OF INVESTIGATION

July 17, 2017

Alert Number
I-071717(Revised)-PSA

Questions regarding this PSA should be directed to your local **FBI Field Office**.

Local Field Office Locations:
www.fbi.gov/contact-us/field

CONSUMER NOTICE: INTERNET-CONNECTED TOYS COULD PRESENT PRIVACY AND CONTACT CONCERNS FOR CHILDREN

The FBI encourages consumers to consider cyber security prior to introducing smart, interactive, internet-connected toys into their homes or trusted environments. Smart toys and entertainment devices for children are increasingly incorporating technologies that learn and tailor their behaviors based on user interactions. These toys typically contain sensors, microphones, cameras, data storage components, and other multimedia capabilities – including speech recognition and GPS options. These features could put the privacy and safety of children at risk due to the large amount of personal information that may be unwittingly disclosed.

1) https://www.nytimes.com/2017/12/21/technology/connected-toys-hacking.html?smprod=nytcore-ipad&smid=nytcore-ipad-share
2) https://www.ic3.gov/media/2017/170717.aspx

Root Causes?

1) Security is just not built into or monitored in most IoT devices

From articles about the same Proofpoint report:

"IoT devices are typically not protected by the anti-spam and anti-virus infrastructures available to organizations and individual consumers, nor are they routinely monitored by dedicated IT teams or alerting software to receive patches to address new security issues as they arise." [1]

2) Attitude that IoT device manufacturer owns data it collects (not you)

Implications for the "Smart" (home appliance accessing/controlling) Grid?

Nest is a Google company

Comments are from Internet's top security experts

What are the odds power companies will create a more secure network?

1) http://www.marketwatch.com/story/proofpoint-uncovers-internet-of-things-iot-cyberattack-2014-01-16?reflink=MW_news_stmp

BREAKING NEWS:

Enter then head of the National Security Agency, Admiral James Clapper:

Who testified to the U.S. Senate about the IoT in February 2016

But his testimony was not to warn us about the risk of the IoT,

he instead pointed out **opportunities** it provided to the NSA:

> "In the future, intelligence services might use the [internet of things] for identification, surveillance, monitoring, location tracking, and targeting for recruitment, or to gain access to networks or user credentials"

In the same Guardian News article,[1] security expert Lee Tien noted that:

> "One of my technologists has a phrase: 'internet of other people's things.' Even if you bought it, it's not necessarily truly yours – it may need to talk to the vendor's machines to work, handing over data about you or those around you (if it has sensors); it may have features you don't know about or don't know how to control or can't control."

1) http://www.theguardian.com/world/2016/feb/10/internet-of-things-surveillance-smart-tv-cars-toys

And what if government monitoring becomes government **cyber warfare***?*

In 2010, Iran's nuclear program was sabotaged by the **Stuxnet virus**: [1]

From the **Nuclear Power - But they Blow Up!** (pptx / pdf / key) note set:

^{235}U's natural abundance is ~ 0.7%

^{238}U's natural abundance is ~ 97.3%

Nuclear fission bombs require uranium "enriched" to ~ 80% ^{235}U

Uranium is often "enriched" by spinning UF_6 gas in ~ 90,000 RPM centrifuges [2]

=> $^{238}UF_6$ goes to the outside, but lighter $^{235}UF_6$ stays near the center

But these incredible speeds require vacuum plus magnetic levitation bearings

If centrifuge's power is interrupted, it can tear itself to shreds

Stuxnet cut power to Iran's centrifuges, reportedly destroying one fifth of them

(Leading suspects? Israel's Mossad collaborating with the U.S. CIA)

1) http://en.wikipedia.org/wiki/Stuxnet
2) https://en.wikipedia.org/wiki/Zippe-type_centrifuge

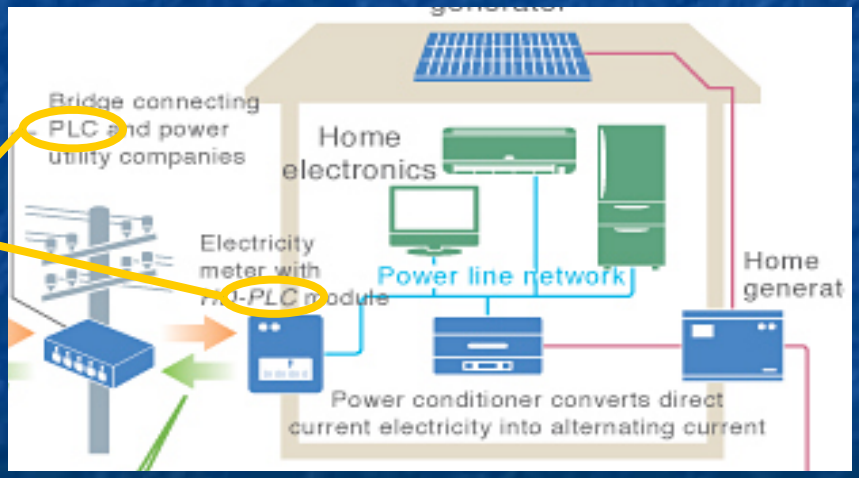
But how is Stuxnet relevant to the Smart Grid?

"Stuxnet's design and architecture are not domain-specific and it could be tailored as a platform for attacking modern **SCADA** and **PLC** systems (e.g., in automobile or power plants) . . . Stuxnet reportedly ruined almost one-fifth of Iran's nuclear centrifuges" – Wikipedia

SCADA, sound familiar? ("supervisory control and data acquisition" systems)

And look closely at this earlier figure on Smart Grid's interface to our homes:

PLCs (programmable logic controllers)



So the Stuxnet virus might be EASILY adapted to attack the Smart Grid

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

Prompting this U.S. Academies of Science and Engineering Report:

Terrorism and the Electric Power Delivery System (2010): [1]

> "Electric systems are not designed to withstand or quickly recover from damage inflicted simultaneously on multiple components. Such an attack could be carried out by knowledgeable attackers with little risk of detection or interdiction. Further, well-planned and coordinated attacks by terrorists could leave the electric power system in a large region of the country at least partially disabled for a very long time. Although there are many examples of terrorist and military attacks on power systems elsewhere in the world, to date international terrorists have shown limited interest in attacking the U.S. power grid" (p.1)

This report focuses almost entirely on threats to the Grid, and not to "Smart Homes"

But while Grid **will** be defended by sophisticated systems and legions of IT experts

Preceding stories show that **IoT** systems are now woefully under-protected

Which, linked to the grid, will make them particularly attractive targets

Terrorism and the Electric Power Delivery System, page 10, U.S. National Academies Press 2011
http://www.nap.edu/catalog/12050/terrorism-and-the-electric-power-delivery-system

*Leading some consumers to **rebel** against Smart Grid trials*

So is there another way of getting MANY of the benefits of a Smart Grid

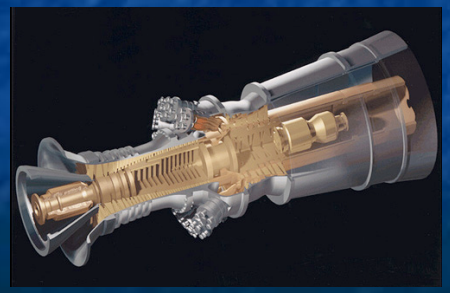
without dealing power companies

(or hackers) right into our home lives?

There might be! And it goes right back to the operation of AC generators:

Which I've depicted as:

With the key relevant element now being the actual turbines:



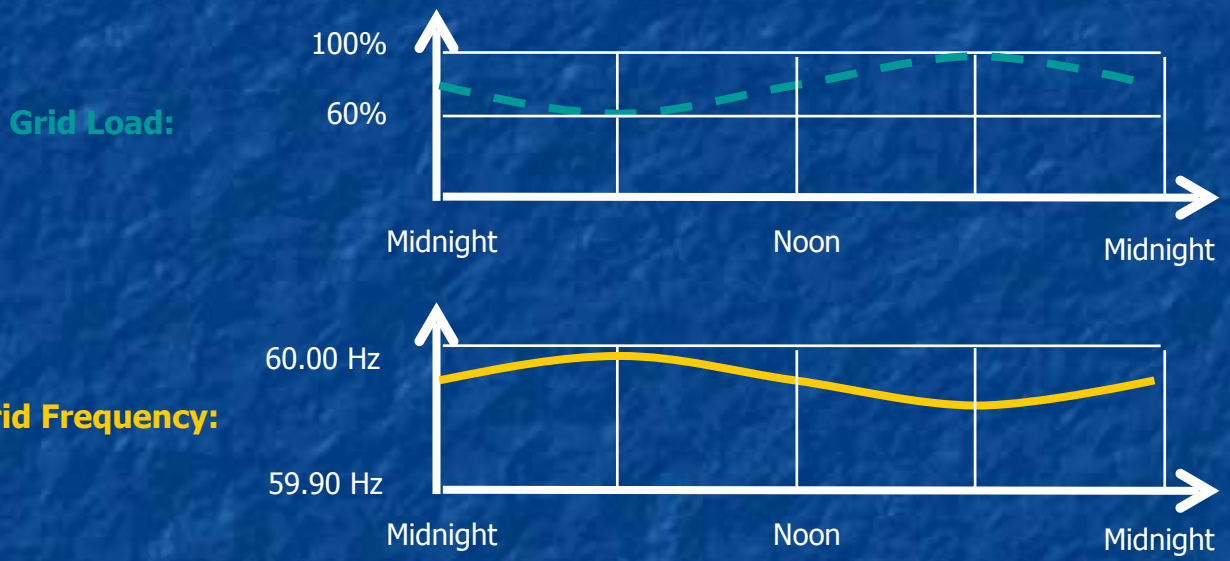
As the load on such a turbine generator increases, it slows down:

Not by a whole lot - To stay within power system specs:

Frequency has to be held within ~ 0.067 Hz of 60Hz

But a fall of 0.067 Hz in frequency CAN be easily sensed!

Due to variable load during the day, Grid frequency thus does something like this:



Then: 60.00 Hz = Grid is at minimum load (and power is at minimum cost)

59.985 Hz = Grid is at moderate load (power is at middle cost)

59.97 Hz = Grid is at heavy load (power is at maximum cost)

So instead of appliance-by-appliance intranet connections to Grid:

Install simple frequency sensor / control into particular appliances

Which is possible via a single simple integrated circuit likely costing less than $5

(versus IoT features adding $100's to appliance costs)

Power company would then no longer control or even monitor our appliances

They are back to monitoring only the whole house's **total** power consumption

But appliance "knows" the Grid's load at this moment (i.e., it can infer it).

In fact: Tell the appliance the average local power cost and it could generate a pretty accurate guesstimate of power cost at this exact moment!

And it could guess a **relative** power cost even **without** that information

That is: "It's now about twice the daily average cost"

Which appliances could make energy / $ saving use of that info?

From my **Energy Consumption in Housing** (pptx / pdf / key) note set:

Water heaters account for 17% of our home power consumption

Water heater could make sure it does not fire up during peak evening load

Dishwashers and **clothes washers** could then help out even further:

They could beep you a warning if turned on during peak evening load

And offer to automatically start wash **later** when off peak (i.e., overnight)

THAT would also push major water heating load of the washers into overnight

Compounding your electrical power savings!

Power hog **dryer** could also offer "**Wait for cheaper power?**" start up mode

Appliances with thermostats could also use that info:

Refrigerators are normally set to operate at ~ 38° F (3.3 ° C)

Sensing peak power demand, refrigerator could up this to 40° F

Control circuit could limit this reset to no more than two hours

This might cut refrigerator power to almost zero (if door not opened too much)

As refrigerator coasted slowly up to 40° F over those two hours

Result: +2° F (+1° C) for two hours => Trivial impact on food preservation

But with power costing ~ 4X more during those hours you could save $$

Furnaces could also turn down during (dinnertime) peak when we're more active

Turning temperature back up later as we slip into couch potato mode

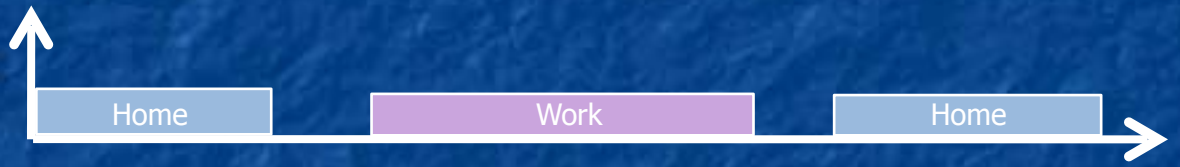
And as noted in my ***Green(er) Cars & Trucks*** *(pptx / pdf / key) note set:*

Grid load sensing (=> inferred price of power) is key to things like Vehicle to Grid:

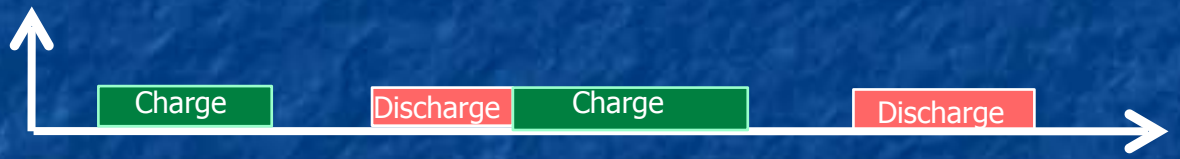
1) Power Demand:

2) Power Production:

3) Location of PHEVs:



4) PHEV ⇔ Grid:



5) Onboard energy:

BREAKING NEWS:

COMPREHENSIVE home energy monitoring WITHOUT Big Brother?

New "Sense" monitor clips onto home's incoming power lines

There it "listens" for tiny variations in power consumption

which differ for every single type of appliance

They even change when some appliances misbehave!

But it must "catalog" all these different energy consumption **fingerprints**

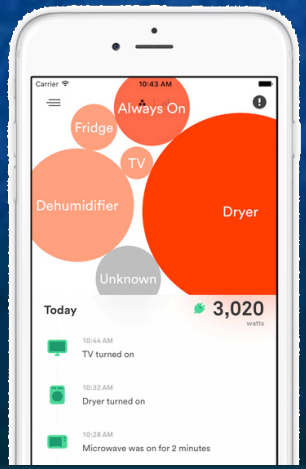
Which, for now, is done via connection back to an Internet Webserver

Which then sends ITS analysis back to your iPad

But once the library of appliance fingerprints is mature,

your iPad alone might be able to do the full analysis,

eliminating the link to a privacy-invading webserver



*Ten minute long description on PBS's **This Old House**:*

Cached copy on this note set's Resources Webpage

Original YouTube video (link)

Credits / Acknowledgements

Some materials used in this class were developed under a National Science Foundation "Research Initiation Grant in Engineering Education" (RIGEE).

Other materials, including the WeCanFigureThisOut.org "Virtual Lab" science education website, were developed under even earlier NSF "Course, Curriculum and Laboratory Improvement" (CCLI) and "Nanoscience Undergraduate Education" (NUE) awards.

This set of notes was authored by John C. Bean who also created all figures not explicitly credited above.