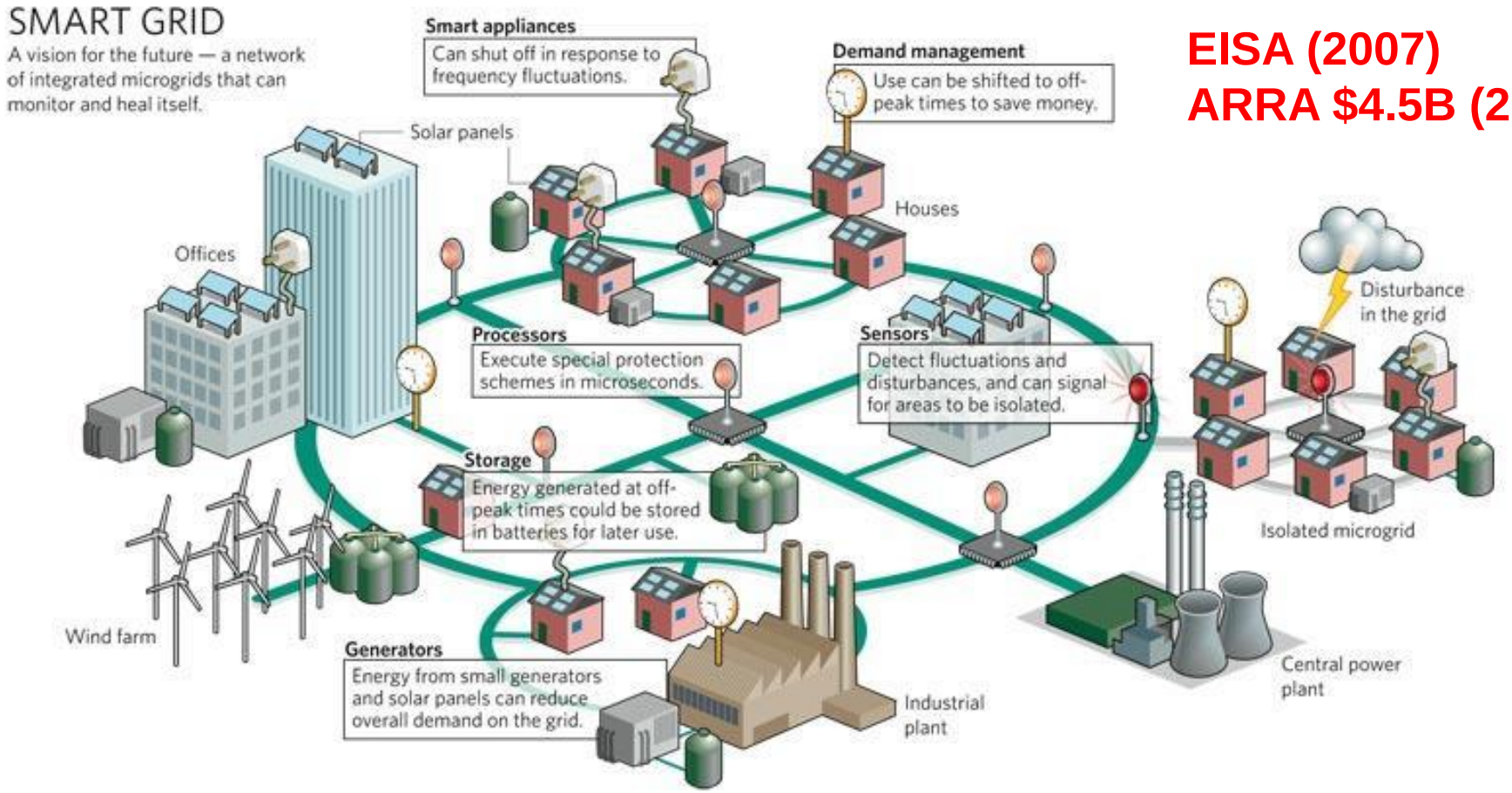
Thinking About System Reliability in the Smart Grid Era

Anu Narayanan

Electric Power Industry Conference
Swanson School of Engineering
University of Pittsburgh
November 11, 2013

http://tli.umn.edu/blog/wp-content/uploads/2010/08/electric.grid_.jpg

The "Smart Grid" includes advancements in intelligence, controls and communications.



EISA (2007)
ARRA $4.5B (2009)

Image source: Smart Grid 2030 Associates
http://www.smartgrid2030.com/?page_id=445

Elements of the smart grid can change how we think about system reliability…

- **Reliability refers to the ability of a system to perform as expected.**
- **Added intelligence in the form of added sensors, better stability control and advanced predictive capabilities can boost reliability *directly*.**
- **Distribution system controls and automation coupled with distributed generation sources can *indirectly* boost reliability if used to keep critical services operational during grid failures.**

…But more intelligence, automation, and control can mean increased security risks.

- **Increased intelligence and progressively decentralized control → potentially increased number of entry points for a cyber attack**

What are the net implications for reliability resulting from the addition of intelligence and controls to the electric power distribution system?

The electric grid is far from failsafe.

Despite the best efforts of power engineers and system operators, sometimes the electric grid goes down, causing extended and widespread outages.

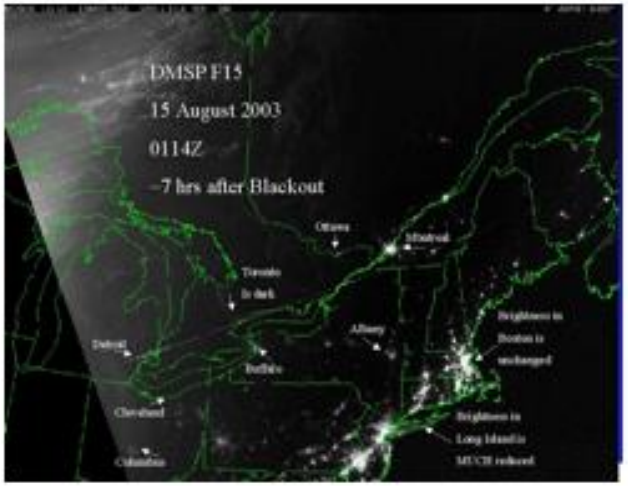


Image sources: Defense Meteorological Satellite Program, Environment Canada, stitoday.com, video_demos.colostate.edu

Power outages are costly.

- **Economic cost of 2003 North East blackout estimated to be ~$4 billion - $6 billion**
  - **50 million people without power**

- **Economic cost of 1998 ice storm in Quebec estimated to be ~$1.6 billion**
  - **1.7 million people without power**
  - **$1 billion in repair costs**
  - **28 deaths in Canada and 17 in the U.S – Many associated with lack of power**

We can do several things to protect the electric grid.

Central plants: **Physical security, personnel security**

Transmission system: **More use of self-supporting tower structures that can prevent domino collapse**

Substations: **Protective barriers, walls and roofs, personnel security, stockpiled equipment, emergency replacement transformers**

Control and communication systems: **Improved/advanced monitoring and control systems, redundancy, advanced simulator training, personnel security**

Distribution system: **Ability to selectively serve only the most critical loads, distributed generation, intelligent distribution automation.**

But unlike food or water, we do not consume electricity! We rely on essential services that electricity enables.

Source: NRC Report, "Terrorism and the Electric Power Delivery System", 2012

We should devise ways to protect essential services when the power goes out.

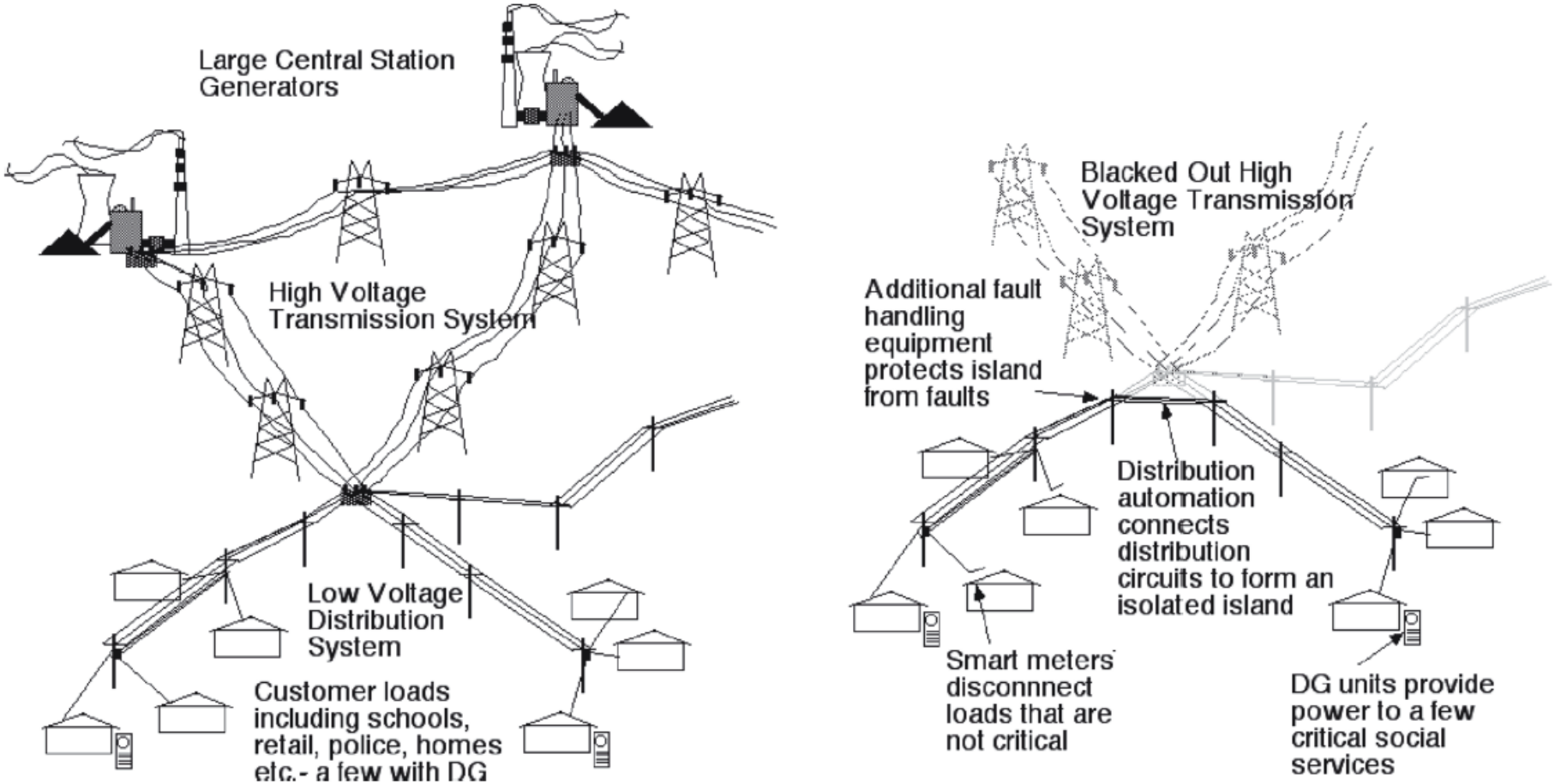


Figure source: Narayanan and Morgan, "Sustaining Critical Social Services During Extended Regional Power Blackouts," *Risk Analysis*, *32*, 1183-1193, 2012.

Costs are reasonable, but there are barriers to implementation.

- **We found that the incremental costs of implementing such a strategy are modest -- < 3% of average monthly electric bill, and < 1% of median household income.**

- **Impediments to implementation include:**
  - **Legislative barriers – e.g., microgrids are illegal in most states with exclusive service territory rights preventing proliferation**
  - **Little incentive for profit maximizing utilities to invest**
  - **Limiting standards – e.g., regarding islanding and DG integration**

Recommendations

- **DoE or DHS should fund a few demonstration projects.**
  - **Can mobilize legislative, regulatory and standards changes**
    - **In turn, can promote utility participation**

- **Open research areas:**
  - **Technology (hardware, controls)**
  - **Analysis (modeling infrastructure interdependencies, articulating the value of protecting essential services)**
  - **Policy/Regulation (creating incentives for investment)**

On the flip side…

…as technologies continue to be deployed at all levels of the system, they could potentially increase the vulnerability of the system to cyber attack.

- **Potential attacks include:**
  - **On / using smart meters**
  - **Control systems**
  - **Communication systems**

- **Could result in a range of consequences from minor annoyances to implications for the bulk power grid**

What are the net implications for reliability resulting from the addition of intelligence and controls to the power delivery system?

We took a first look at the potential implications of a smart meter based attack.

- **There are ~ 20 million installed smart meters in the U.S.**

- **Tens of millions of meters are projected to be deployed in the coming years.**

- **There have been several demonstrations of smart meter hacking but little work on assessing the potential implications of such hacking for the bulk grid.**

Denial of Service

Energy Fraud

Could the cycling of a large number of system loads lead to unstable operating conditions for the bulk bulk power grid?

Targeted Disconnect

It is unlikely that a smart meter based attack could disrupt bulk power system operations.

- **The fraction of system load that would need to be cycled on and off to induce stability issues is likely to be unrealistically large.**

- **Key contribution is the provision of a quantitative framework for *further analysis*, NOT ‘proving’ that smart meters can do no harm!**

- **Significant quantitative assessment of the cyber risk is needed at all levels of the power delivery system.**

Challenges to assessing and mitigating the cyber risk include:

- **Lack of access to (often proprietary) data**
- **Lagging dynamic simulation tools for distribution system analysis**
  - **NERC's upcoming war-game is interesting!**
- **Lack of clear oversight**
  - **NIST cybersecurity standards are not mandatory**
  - **FERC does not have legal authority to mandate**
- **Distracting hype!**

In conclusion…

- **We have a long way to go in terms of knowing the "right" level of intelligence to embed in the system → further, what is optimal varies across players.**

- **In the meantime, we can use what is available wisely provided there is research $$, legislative and regulatory support!**

- **DHS / DoE funding for the following can help greatly:**
  - **Demonstration projects showcasing microgrid utility**
  - **Projects that seek to assess cyber threat, vulnerability, or impact**
  - **Analysis of infrastructure interdependencies → can motivate innovative use of smart grid elements**

Thank you!

For further questions please contact me at anarayan@rand.org

This work was supported by grants from the Gordon and Betty Moore Foundation, the MacArthur Foundation, and by Carnegie Mellon University. Thanks to my collaborators Paul Hines, Gabriela Hug, Eduardo Cotilla-Sanchez, Howard Lipson, and special thanks to my PhD committee chair Granger Morgan, some of whose slides were used in modified form in this presentation.

Backups

Conclusions

- **Even when the system is operating very close to its steady state stability margin (e.g. μ = 0.96), 19% of system load needs to be oscillated to induce instability.**

- **Assuming one smart meter controls 2 kW – 10 kW, translates to 130,000 – 660,000 meters.**

- **For more reasonable μ = 0.5, 300,000 – 1.5 million loads need to be cycled to induce instability.**

- **IMPLICATIONS: Provides quantitative framework; Helps prioritize smart grid security efforts**

18