Trivia question: When was DOE created and what was their original charter? 1977 under the Carter administration to lessen US dependence of foreign oil. Now with 16K employees and 100,000 contractors and a $25B budget.

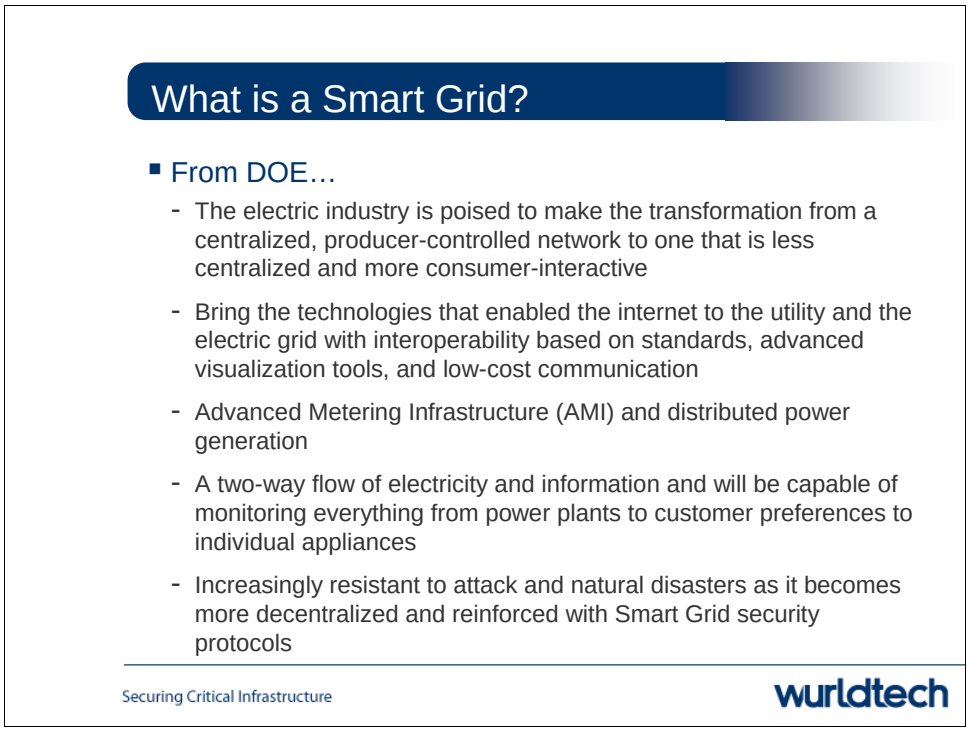
Outline

- Summary
- Aurora – Lessons Learned?
- What is a Smart Grid?
  - Smart Grid – The Business Case
  - Smart Grid Regulators
  - Smart Grid Standards
- How Secure is the Smart Grid? – A Survey
- Smart Grid Security – Current Efforts
- Smart Grid Security – Some Ideas
- Conclusion

Looking Back - Aurora

Aurora – Lessons Learned?

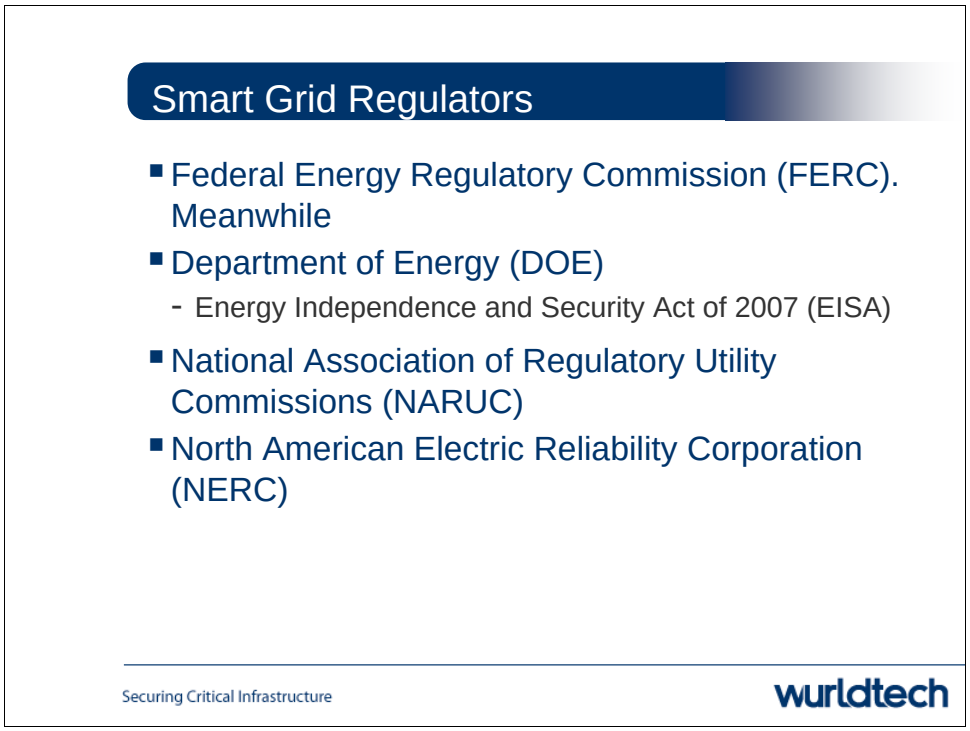
- Physical damage can result from a cyber attack
- Public-private partnerships are complicated
  - Opposing perspectives/competing needs
- Vulnerability disclosure policy was lacking
- Regulatory guidance and standards
- Not all vulnerabilities are bugs



•The electric industry is poised to make the transformation from a centralized, producer-controlled network to one that is less centralized and more consumer-interactive
•Bring the technologies that enabled the internet to the utility and the electric grid with interoperability based on standards, advanced visualization tools, and low-cost communication
•Advanced Metering Infrastructure (AMI) and distributed power generation
•A two-way flow of electricity and information and will be capable of monitoring everything from power plants to customer preferences to individual appliances

Smart Grid – The Business Case

- Reduced cost to consumers
- Electricity producers are better able to manage the peaks in demand
- Defer or avoid building additional infrastructure
- Significantly reducing greenhouse gases and pollutants
- Integrating wind or solar power into the grid at levels higher than 20%
- PNNL study - existing U.S. power plants could meet electricity needs of 73% of US light vehicles if they were plug-ins that recharged at night



National Association of Regulatory
Utility Commissions (NARUC) are exploring options for expediting Smart
Grid implementation with their federal counterpart, the Federal Energy Regulatory Commission (FERC). Meanwhile, DOE is providing leadership with
the passing into law of the Energy Independence and Security Act of 2007
(EISA),

Inherent in the ability to fully manage something is the ability to screw it up.

Smart Grid Standards

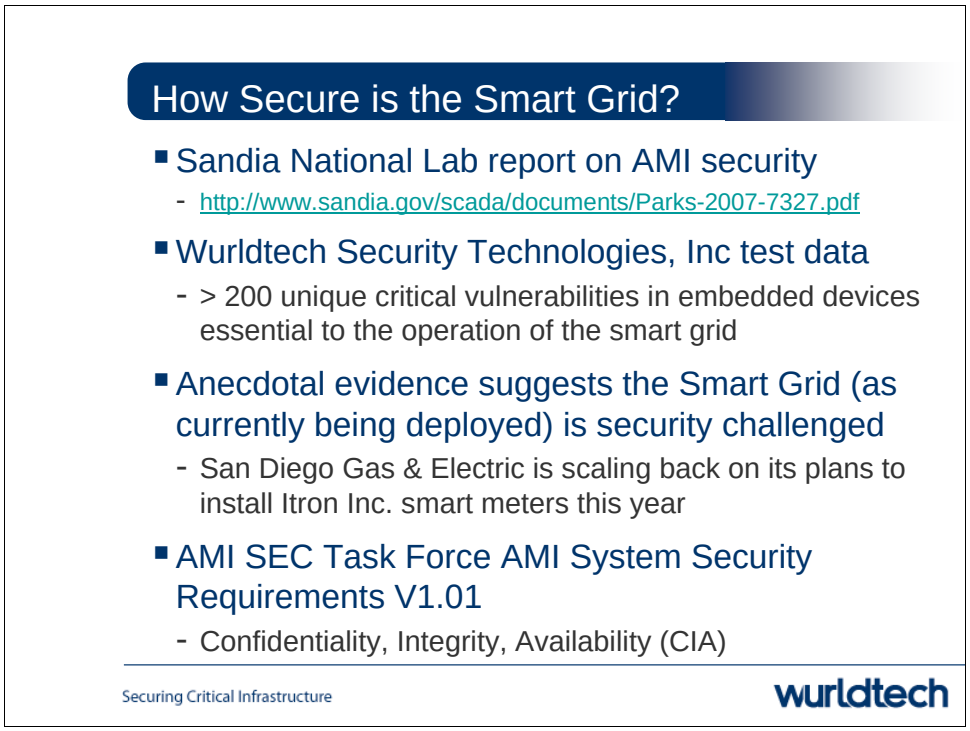
- The National Institute of Standards and Technology (NIST) under EISA
- GridWise Architecture Council
- American National Standards Institute (ANSI)
- Institute of Electrical and Electronics Engineers (IEEE)
- International Society of Automation (ISA)
- International ElectroTechnical Commission (IEC)
- Electric Power Research Institute (EPRI)
- ZigBee Alliance

How Secure is the Smart Grid?

More Secure

Same Security

Less Secure



* Reputational Loss - Attacks or accidents that destroy trust in Smart Grid services, including their technical and economic integrity
* Business Attack - Theft of money or services or falsifying business records
* Gaming the system - Ability to collect, delay, modify, or delete information to gain an unfair competitive advantage (e.g., in energy markets)
* Safety - Attack on safety of the grid, its personnel or users
* Assets - Damaging physical assets of the grid or assets of its users
* Short-term Denial or Disruption of Service
* Long-term Denial or Disruption of Service (including significant physical damage to the grid)
* Privacy violations
* Hijacking control of neighbor's equipment
* Physical and logical tampering
* Subverting situational awareness so that operators take fatal actions that disrupt the system
* Cause automated system to waste resources on false alarms.
* Hijacking services
* Using Smart Grid services or the supported communication mechanisms to attack end users residential or industrial networks (e.g., allowing end-users to compromise other end-users' networked systems.)

Smart Grid Security – Current Efforts

- NIST has created 5 domain Expert Working Groups
- IEEE working group developed update to NERC CIP due summer 2009
- About 80 groups are working on various Smart Grid standard
- Many technology demonstration projects jointly sponsored between public and private
- The technology is moving fast and security needs to pick-up the pace

Smart Grid Security – Some Ideas

- Risk management – not more regulation
  - Requires more/better information (R=T*V*C) ~ David Walcott, Country Energy
- Build security in during the design phase
  - Earlier in the cycle is always cheaper ~ Ivano Labricciosa, Toronto Hydro
- No nothing (not practical when scaled to millions)
  - Advanced analytics to detect and respond ~ Eric White, IBM
- You must secure the entire grid not just AMI
  - In an “everything is connected” world, everything must be looked with security in mind ~ Joe Weiss, ACS

Smart Grid Security – Some Ideas (cont.)

- Integrate security and safety
  - Safety and security are related so adopt some of the thinking from the safety industry ~ Ron Southworth
- Formal Threat Modeling
  - Better intelligence can help manage risk ~ John Camilleri, AREVA
- Security certification at the device level
  - No cost for O/O and ROI for vendors ~ Dr. Nate Kube, Wurldtech

Conclusion

- Critical infrastructure is “critical” for a reason
- Protecting the critical infrastructure is not just a good idea – lives depend on it
- Increase funding to develop an empirical basis for measuring security
- Build security into the infrastructure instead of bolting it on later
- Expand partnerships between Government, industry, and academia
- Security does not cost, security pays!

Thank You For Your Attention

Perry A Pederson, MSc
ppederson@wurldtech.com
+1 (703) 801-9737 Cell

Questions?

For More Information Please
Visit Our Website: www.wurldtech.com