



# Smart Grid: Benefits and Security Challenges

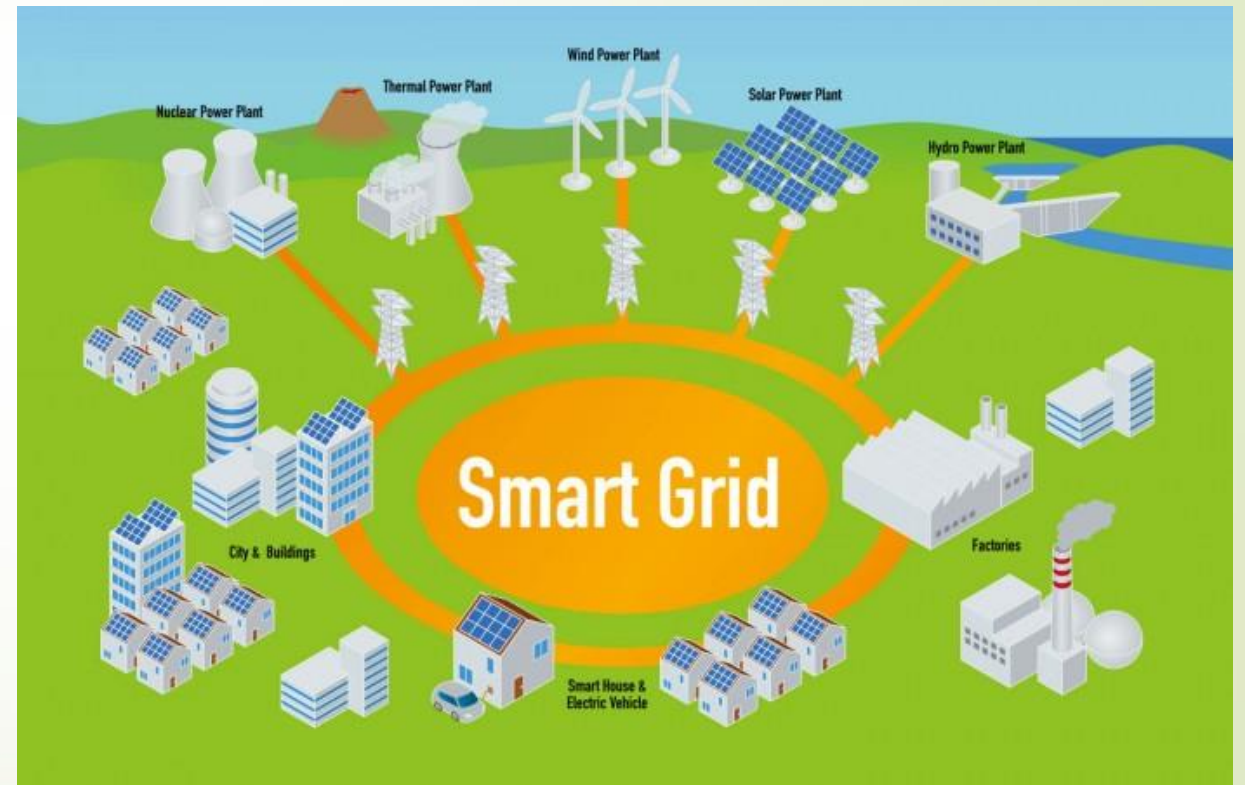
Susan Lincke PhD

Associate Professor Computer Science

University of Wisconsin-Parkside

# Smart Grid: Benefits and Challenges

- Motivation: Energy, Renewables, & Climate Change
- Intro to the Smart Grid
- Challenges: Security Issues



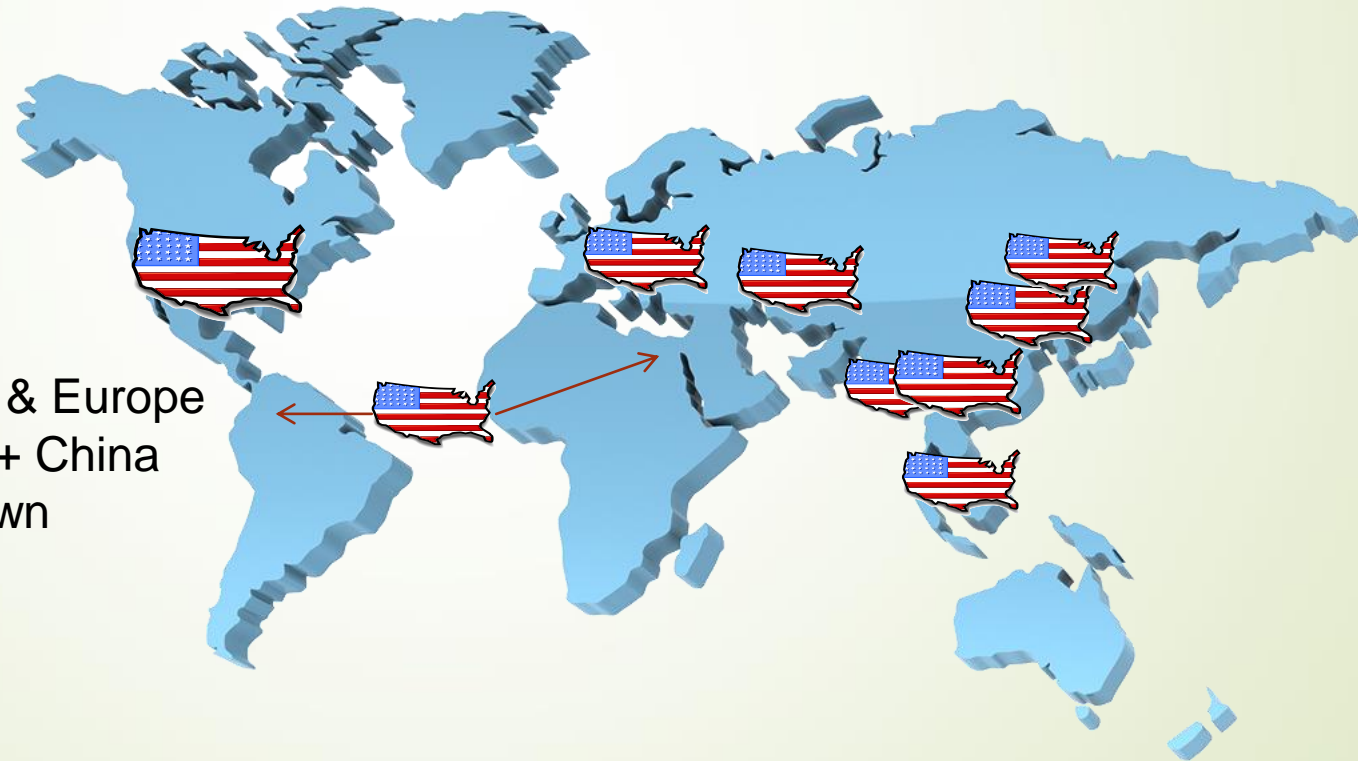
# Hot, Flat, and Crowded

Thomas L Friedman

## 5. Our Carbon Copies (or, Too Many Americans)

"I certainly don't blame the citizens of Doha or Dalian for aspiring to an American lifestyle..."

Previous: US & Europe  
Now: + India + China  
2030: As shown





# Hot, Flat, and Crowded

Thomas L Friedman

## 5. Our Carbon Copies (or, Too Many Americans)

“Does that mean we don't want people to live like us anymore? No. It means that we have to take the lead in redesigning and reinventing what living like us means – what constitutes the “American way” in energy and resource consumption terms.”

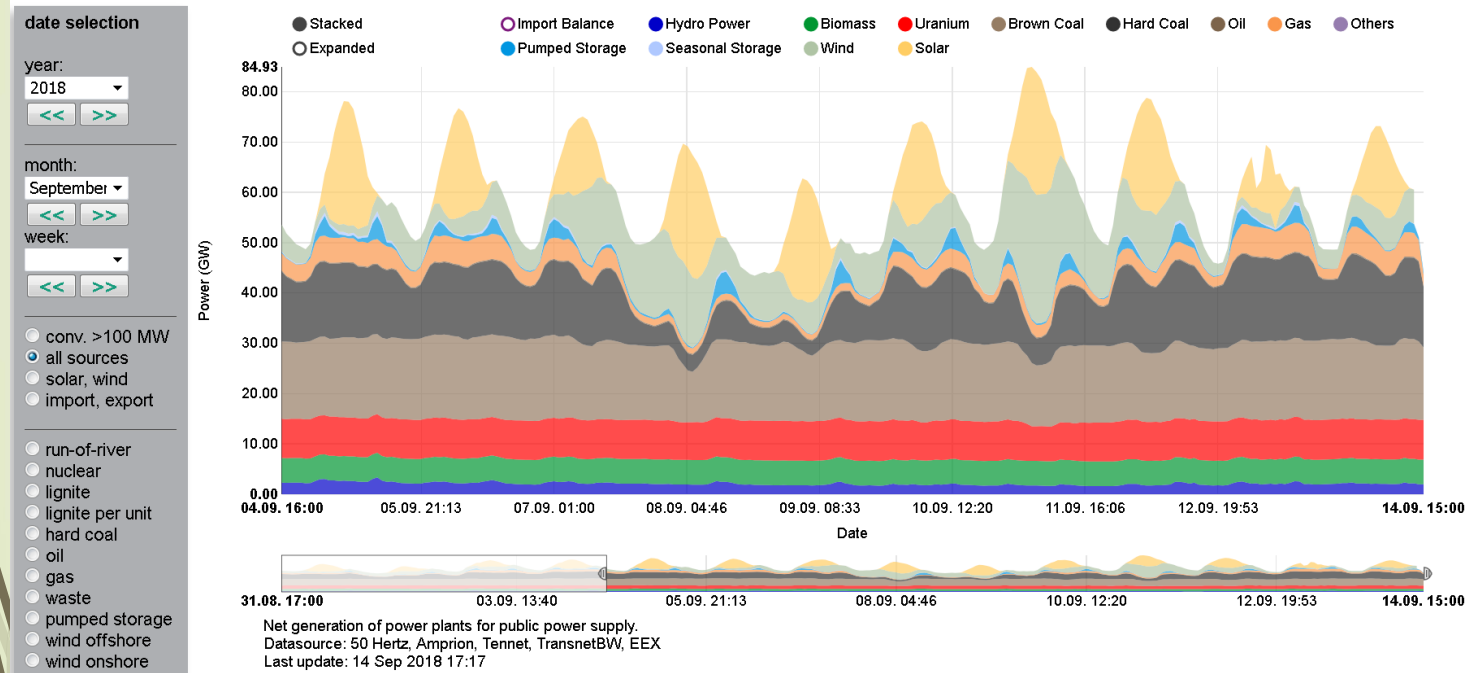
### GHG Per Capita Emission Rates (tons):

US	20
England, Japan	10
Average	4.3
India	1

Key World Energy Statistics 2008, World Energy Outlook

# Energy Consumption

## Electricity production in Germany in September 2018



- Peak generation: Build to the busy hour.
  - Highest: Hot summer days-> lots of air conditioning
  - Lowest: Evenings and nights: less business energy consumption
- Cheapest to most expensive energy producers used in succession
- Dynamic pricing: The price of electricity changes based on demand

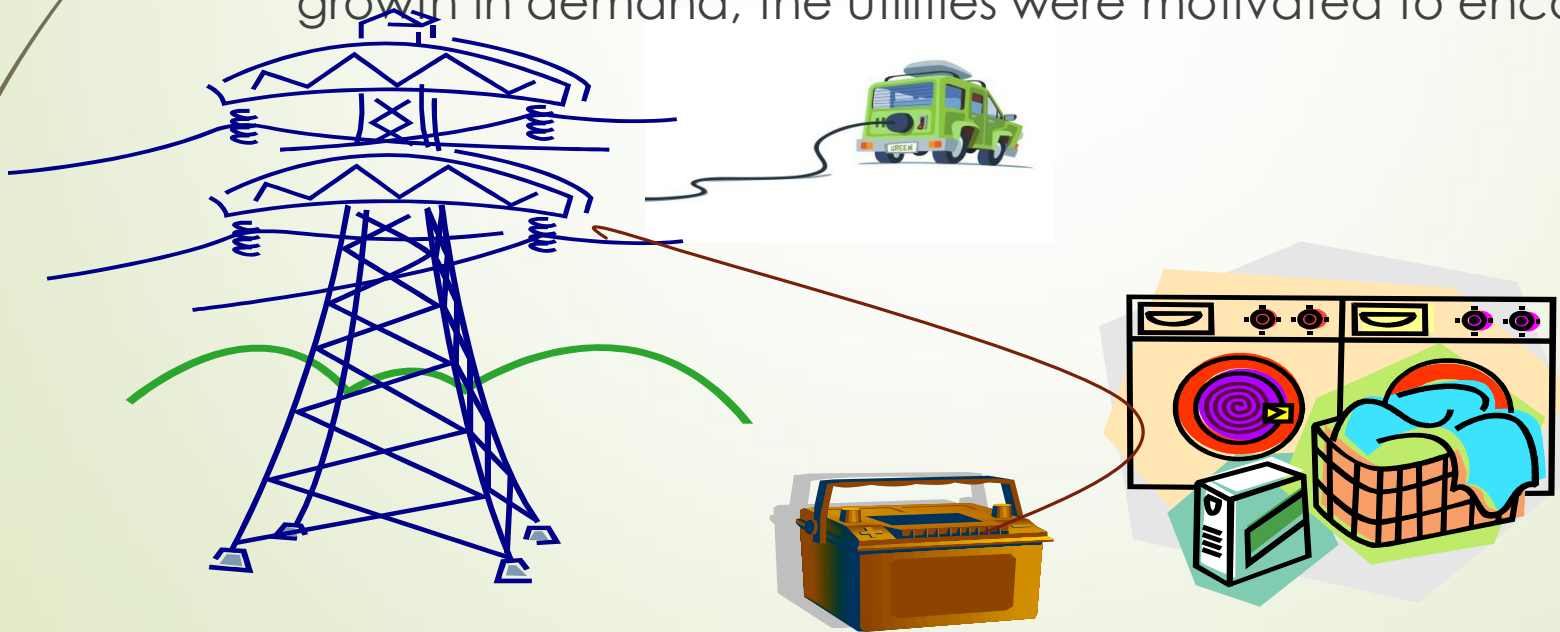
# Hot, Flat, and Crowded

Thomas L Friedman

Chapter 12. The Energy Internet: When IT meets ET

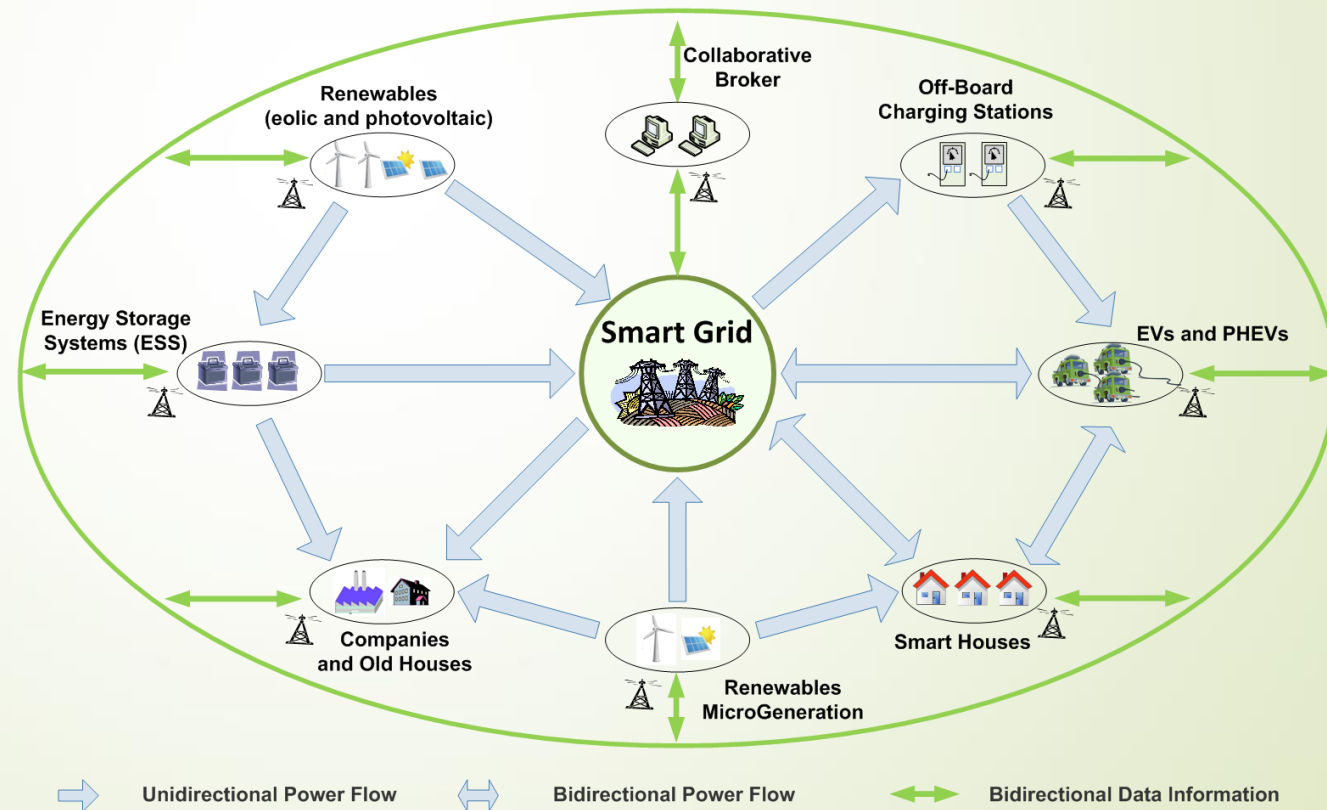
IT=Information Technology    ET=Energy Technology

“Utilities made their money by building stuff – more power plants and more power lines that enabled them to sell more and more electrons to more and more customers – because they were rewarded by their regulators with increased rates on the basis of those capital expenditures. The more capital they deployed, the more they made. And since their new capital investments had to be justified by growth in demand, the utilities were motivated to encourage consumption...”



# Intro to the Smart Grid

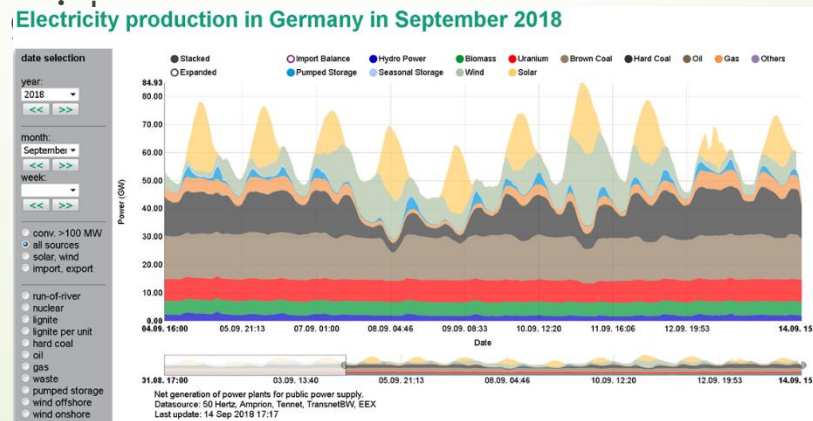
Power Flow and Information and Communication Technology (ICT) in Smart Grids





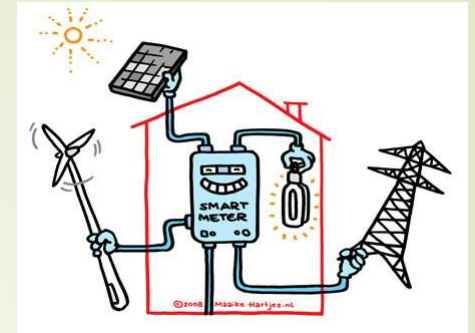
# Goal: Integrate Renewable Energy into Distributed Grid

- **Integrated Distributed Network:** integrate renewable energy generation facilities (i.e., wind, solar, thermal power, etc.) as part of total energy sources.
- **Bidirectional Metering:** enable customer and micro-grid energy generation requires bidirectional metering and bidirectional energy distribution networks.
- **Improved Energy Forecasting:** project expected demand, predict alternative generation capacities, and integrate distributed generation into the distribution





# Goal: Enable Smart Metering and Dynamic Pricing



- **Advanced Metering Infrastructure (AMI):** Smart meters provides customers real-time pricing of electricity
  - help utilities achieve necessary load reductions.
  - Implement residential Demand Response (DR) through dynamic pricing.
- **Infrastructure changes require:**
  - bidirectional flows of energy, two-way control capabilities, new applications including smart metering for homes and businesses.
    - two-way network between advanced meters and utility business systems to collect and send information to customers, retail suppliers or the utility.
  - computing and communication technologies to existing electricity delivery infrastructure.




# Goal: Lower Peak Energy Use

- **Distributed energy storage:** Enable new energy storage capabilities in a distributed fashion and mechanisms for feeding energy back into the energy distribution system.
  - Goal: evenly distribute the demand
  - Goal: lower the need for peak generation facilities
- **Grid monitoring and management:** Enable demand response and consumer energy efficiency through balancing the power supply and demand.
  - Goal: enable business, industrial, and residential customers to reduce energy usage, and thus costs, during peak demand.


# Goal: Support Electric Vehicles within Grid

- Enable large-scale integration of plug-in electric vehicles (PEVs) into the transportation system.
  - Support PEV charging
  - Establish charging infrastructure, including the power distribution capacity to prevent overloading of circuits and the charging facility.
  - Establish information system to manage the energy distribution, customer accounting and billing.

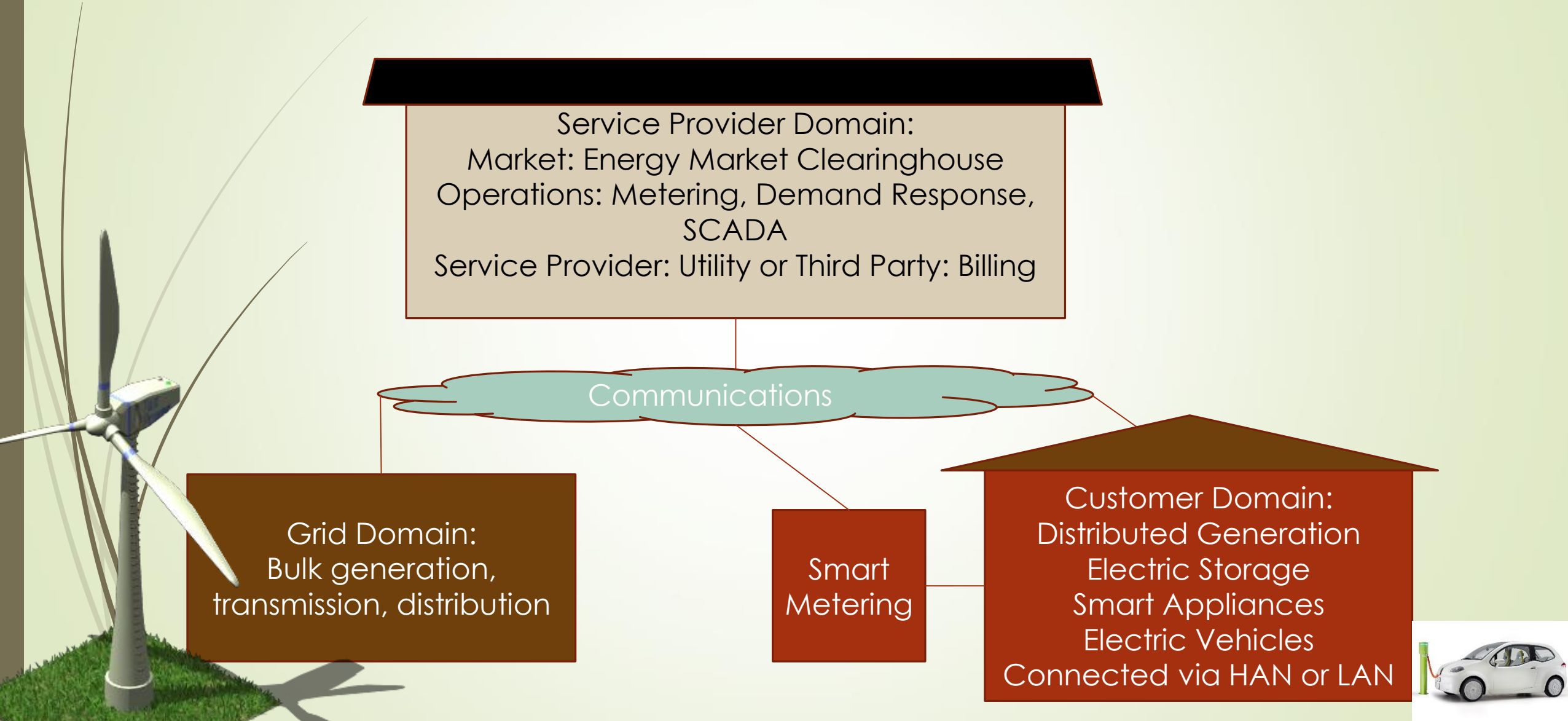




# Goal: Provide a Secure, Robust and Efficient Grid Infrastructure.

- **Intelligent grid control and management:** implement energy intelligence and QoS-aware control and data planes to provide sufficient but minimum energy.
  - **Distributed & Secured Grid:** integrate diverse networks from information technology, telecommunications, and energy sectors.
    - Implement security to ensure that a compromise in one network does not compromise security in other interconnected systems.
  - **Energy distribution management:** Make the energy distribution system more intelligent, reliable, self-repairing and self-optimizing.
  - **Connected electrical grid/communication networks:** Integrate the grid with an advanced communication network to enable intelligent control and distribution of energy.
- 

# Grid Architecture



# Home Functions

## Smart Metering Functions

- Meter control, maintenance
- Meter reading and data management
- Fault monitoring and protection



## Home User Management

- End-user functions
- Local generation and storage
- Plug-in Electric Vehicle (PEV) charging
- Demand Response (DR)
- In building/ home energy management automation



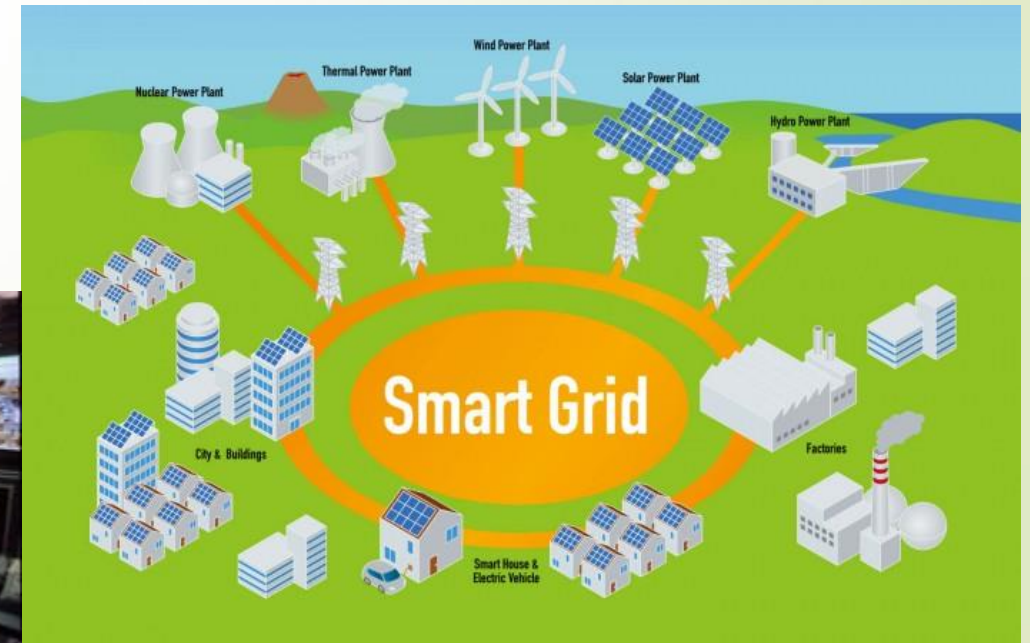


# Development of Smart Grid Standards

- The U.S. Congress recognized having interoperable standards is a major issue for the development of smart grid.
  - Energy Independence and Security Act (EISA) of 2007 assigned National Institute of Science and Technology (NIST)
  - NIST Framework and Roadmap for Smart Grid Interoperability Standards
- Develop a set of consistent, compatible standards for interoperability within the Smart Grid:
  - U.S.: NIST established the Smart Grid Interoperability Panel (SGIP) to coordinate with all SDOs
  - European Commission issued a smart grid mandate M/490 for the European SDOs
  - ITU-T FG-Smart: Key Areas for Smart Grid Standards



# Smart Grid Challenges: Security





# Information Warfare

- Next wars will be computer attacks to power, water, financial systems, military systems, etc
  - Cyberweapons are MUCH cheaper than military
  - Cause as much damage
  - High priority: Protecting utilities, infrastructure
- Black market in 0-day attacks.
  - Governments pay more > \$150,000/bug
  - Govts. include Israel, Britain, India, Russia, Brazil, North Korea, Middle Eastern countries, U.S.
  - New hacking firms openly publicize products

# Price of Military Hardware

EA-18G Growler: \$102 M



E-2D Advanced  
Hawkeye: \$232 M



How many programmers could you buy for this?





# Interesting Quotes

Independent groups of hacktivists have been able to break into sites controlled by the FBI, CIA, the U.S. Senate, the Pentagon, the International Monetary Fund, the official website of the Vatican, Interpol, 10 Downing Street in London, the British Ministry of Justice, and NASA (even breaking into the software of the space station while it was orbiting the Earth).

Al Gore, *The Future*, p. 73

If we went in with a drone and knocked out a thousand centrifuges, that's an act of war. But if we go in with Stuxnet and knock out a thousand centrifuges, what's that?

Richard Clarke, counterterrorism czar for 3 U.S. presidents.

# Risk Scenario 1: Cyber-Warfare



- The Ukraine power grid lost power in December 2015 and 2016 by Russian attackers. Both attacks resulted in blackouts affecting much of or the entire country.
- Russian cyber-warfare also brought down phone service and web: media, finance, transportation, military, politics and energy service for much of Ukraine repeatedly and continually.

What they did:

- Attacks included deleting data, destroying computers, compromising VPNs, overwriting firmware, bombarding with fake phone calls and a disinformation campaign.
- Phishes containing the Trojan BlackEnergy and SandWorm command and control software locked operators out of command interfaces, cleared disks via KillDisk (including master boot records), turned off power circuits and ruined battery backups.
- CrashOverride malware designed specifically for electric utilities to independently give orders to older grid equipment and to override kill-switches, which prevent surges on electrical lines and transformers.

USA Next?

- Some believe Russia used Ukraine as a testing lab for similar attacks on the U.S.
- Possible retaliatory measure if the U.S. interferes with Russian goals, e.g., Russian neighbors.
- BlackEnergy has been found on U.S. electrical grids. Recently a Vermont electrical grid computer (not on the grid) had malware used by Russian attacks.

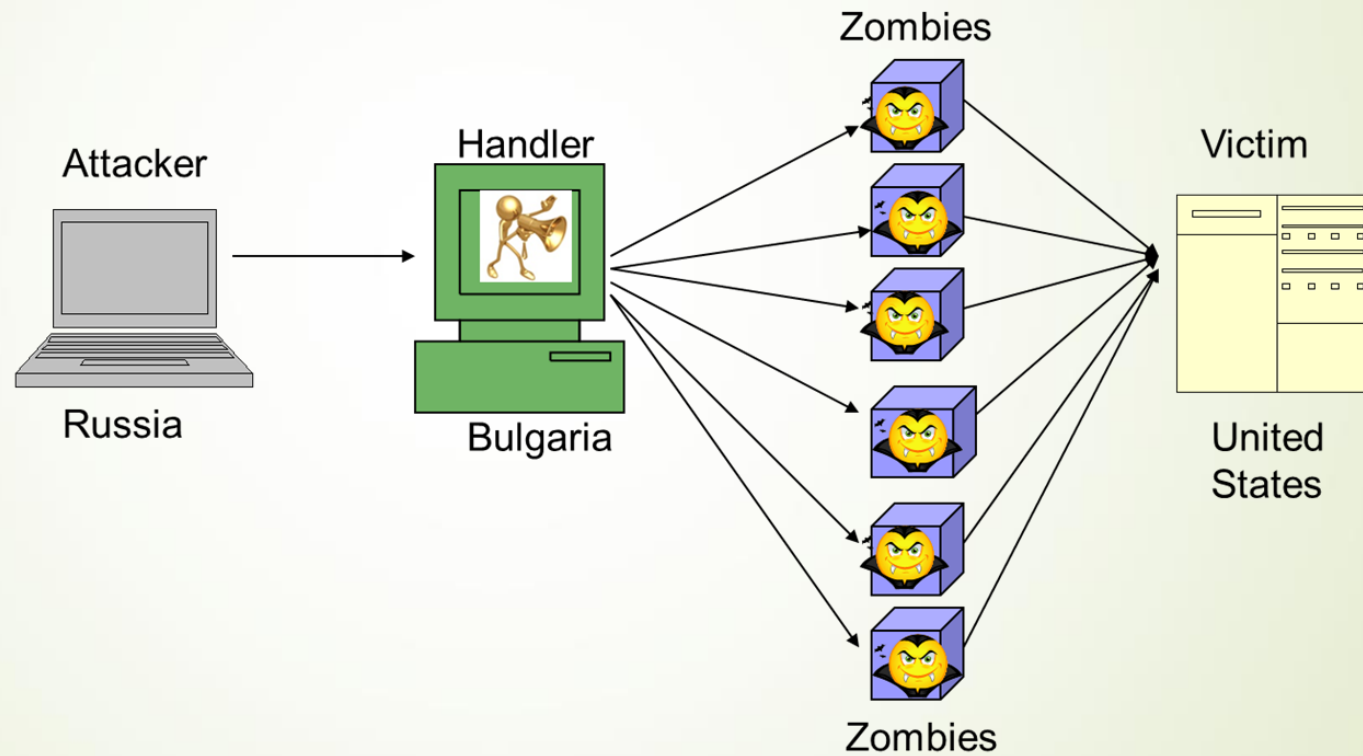




# A Risk Scenario 2: Ransomware

- Ransomware: Encrypts disks, makes servers unusable
- Recently ransomware has shut down governments, police, hospitals, banks
- The Chernobyl nuclear power plant forced to manually monitor radiation levels [18].
- More important systems are charged higher prices.
  - Atlanta was charged \$51,000 [18].
  - Electric utilities could have their control centers and controllers disabled.
- Cybercriminals can be independent or affiliated with nation-states
- North Korea uses both cyber-criminal and cyber-warfare activities, for espionage, sabotage and money-making ventures.

# Risk Scenario 3: Distributed Denial of Service Attack





# Risk Scenario 3: DDoS Attack

- Distributed Denial of Service (DDOS) used by both cyber-warfare and cyber-criminals.
- If the Internet was the base network for the grid, communications to operate, monitor and control the grid could be totally disabled, leaving the grid to be uncontrolled.
- In the smart grid, power usage and rates will be communicated between homes and the grid
- Concern: ability to provide power even when home-grid communication is disabled.
  - March 2018 DDoS attack generated 1.35 Terabits per second on Github [34]
  - Cyber-criminals charge a ransom to stop.
  - Security companies can thwart attacks at \$2000-\$15,000 per month per large company [20].

# Risk Analysis: Electrical Grid Threats

	Single loss expectancy	Annualized rate of occurrence	Annual loss Expectancy
<b>Effects on Utility</b>			
<b>Power loss (no warfare)</b>	\$822/day	500,000 persons/day	\$150 B
<b>Power Loss (warfare)</b>	\$822/day	25 M persons/day <sup>b</sup>	\$20.55 Trillion
<b>Iran Stuxnet</b>		Affected 81 million people	
<b>Rebuilding 1000 centrifuges</b>	1000@ \$20,000/ centrifuge Total: \$20 M	0.05 (20 years <sup>b</sup> )	\$1 M
<b>Rebuilding 200,000 computers</b>	200,000 @\$100/ computer Total: \$20 M	0.1 (10 years <sup>b</sup> )	\$10 M
<b>Four deaths</b>	\$1.5-20 M Death	0.1 (10 years <sup>b</sup> )	\$600,000 -\$80 M
<b>Forensic help</b>	\$100,000	0.5 (2 years <sup>b</sup> )	\$50,000

# Risk Analysis: Electrical Grid Threats (cont'd)

<b>Puerto Rico Hurricane</b>		<b>Affected 3.4 million people</b>	
<b>Replace critical infrastructure</b>	\$30 B	0.1 (10 years <sup>b</sup> )	\$3B
<b>Loss of life (low, high figures)</b>	1052 people @\$1.5 M 1052 people @ \$20 M	0.1 (10 years <sup>b</sup> )	\$1.578 B (@\$1.5M) \$21 B (@\$20M)
<b>Atlanta Ransomware</b>		8000 workers (& public)	
<b>Ransomware fee</b>	\$50,000 or more	1 (1 year <sup>b</sup> )	\$50,000
<b>DDOS attack (ransom or cyber-warfare)</b>		One large company	
<b>DDOS handling fee</b>	\$2,000-15,000/month	0.5 (2 years <sup>b</sup> )	\$1,000-7,500



# Smart Grid Security Threat

NIST IR 7628, the Guidelines for Smart Grid Cyber Security drives future system standards. A section quotes [p. 48]:

“The reality is that many elements of the Smart Grid might already or will in future make use of public networks. The cyber security risks that this introduces need to be addressed by a risk management framework and model that takes this reality into account. It should be clear that if critical real-time command and control functions are carried over public networks such as the Internet (even if technically possible), such a scheme carries significantly more risk of intrusion, disruption, tampering, and general reliability regardless of the countermeasures in place. This is true because of the sheer accessibility of the system by anyone in the world regardless of location and the fact that countermeasures are routinely defeated because of errors in configuration, implementation, and sometimes design. These should be self-evident facts in a risk metric that a model would produce.”





# Security Functions

**Security functions:** This function group interacts with all other function groups in terms of physical security, system security, and operation security. Security aspects include:

- **Identification and authentication function:** Verifies the identity of a user, process, or device as a prerequisite for granting access to resources in a smart grid system.
- **Audit and accountability function:** Establishes and examines the adequacy of security requirements and compliance with the established security policy and procedures.
- **Access control function:** Only authorized personnel or users have access to various utilities and services in the grid system.
- **Data integrity function:** Data is correct within smart grid through cryptography and integrity validation mechanisms.
- **Privacy preserving function:** Provides privacy considerations with respect to the smart grid.



# References



- **Hot, Flat, and Crowded**, Thomas L Friedman
- **Standardization of Smart Grid in ITU-T**, Gyu Myoung Lee, David H. Su, IEEE Communications Magazine • January 2013
- NIST. NISTIR 7628 Guidelines for Smart Grid Cyber Security v1.0 – Aug 2010, from [www.smartgrid.gov/files/NISTIR\\_7628\\_Guidelines\\_for\\_Smart\\_Grid\\_Cyber\\_Security\\_Vol\\_3\\_201001.pdf](http://www.smartgrid.gov/files/NISTIR_7628_Guidelines_for_Smart_Grid_Cyber_Security_Vol_3_201001.pdf).
- Greenberg, A. How An Entire Nation Became Russia's Test Lab for Cyberwar, WIRED, 20 June, 2017, from: [www.wired.com/story/russian-hackers-attack-ukraine](http://www.wired.com/story/russian-hackers-attack-ukraine).