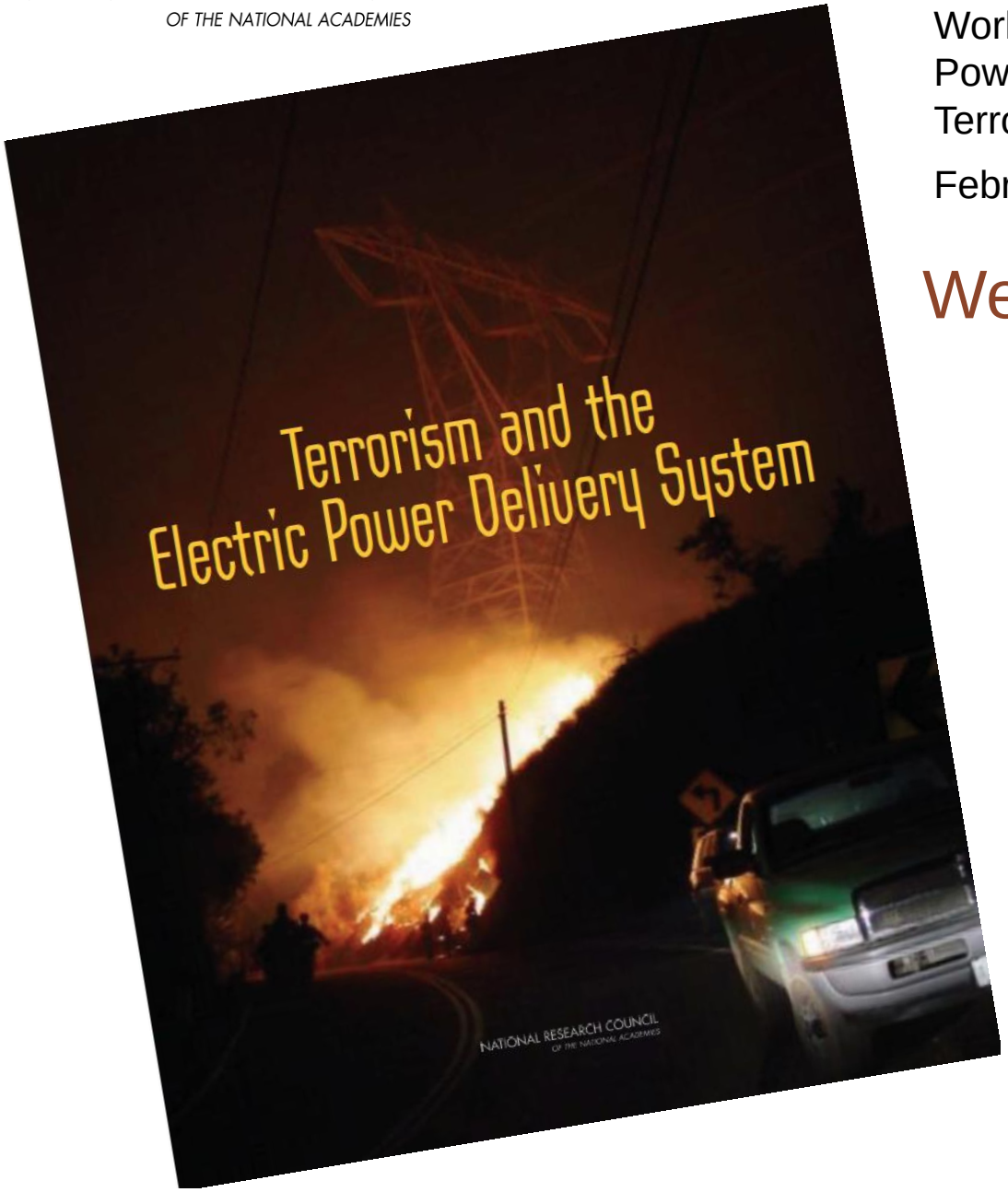
NATIONAL RESEARCH COUNCIL
OF THE NATIONAL ACADEMIES



Workshop on the Resiliency of the Electric Power Delivery System in Response to Terrorism and Natural Disasters

February 27-28, 2013

Welcome and The NRC Report

M. Granger Morgan
Committee Chair
Head, Dept. of Engineering and Public Policy
Carnegie Mellon University
Pittsburgh, PA 15213
412-268-2672
granger.morgan@andrew.cmu.edu

COMMITTEE ON ENHANCING THE ROBUSTNESS AND RESILIENCE OF FUTURE ELECTRICAL TRANSMISSION AND DISTRIBUTION IN THE UNITED STATES TO TERRORIST ATTACK

M. GRANGER MORGAN, NAS, Carnegie Mellon University, *Chair*
MASSOUD AMIN, University of Minnesota
EDWARD V. BADOLATO,* Integrated Infrastructure Analytics Inc.
WILLIAM O. BALL, Southern Company Services
ANJAN BOSE, NAE, Washington State University
CLARK W. GELLINGS, Electric Power Research Institute
MICHEHL R. GENT, North American Electric Reliability Corporation (retired)
DIANE MUNNS, Edison Electric Institute
SHARON L. NELSON, State of Washington Attorney General's Office (retired)
DAVID K. OWENS, Edison Electric Institute
LOUIS L. RANA, Consolidated Edison Company of New York
B. DON RUSSELL JR., NAE,Texas A&M University
RICHARD E. SCHULER, Cornell University
PHILIP R. SHARP, Resources for the Future
CARSON W. TAYLOR, NAE, Bonneville Power Administration (retired)
SUSAN F. TIERNEY, Analysis Group
VIJAY VITTAL, NAE, Arizona State University
PAUL C. WHITSTOCK, Marsh USA Inc.

Project Staff

Board on Energy and Environmental Systems

ALAN CRANE, Study Director
DUNCAN BROWN, Senior Program Officer (part time)
HARRISON T. PANNELLA, Senior Program Officer (until July 2007)
JAMES J. ZUCCHETTO, Director, BEES

National Academy of Engineering Program Office

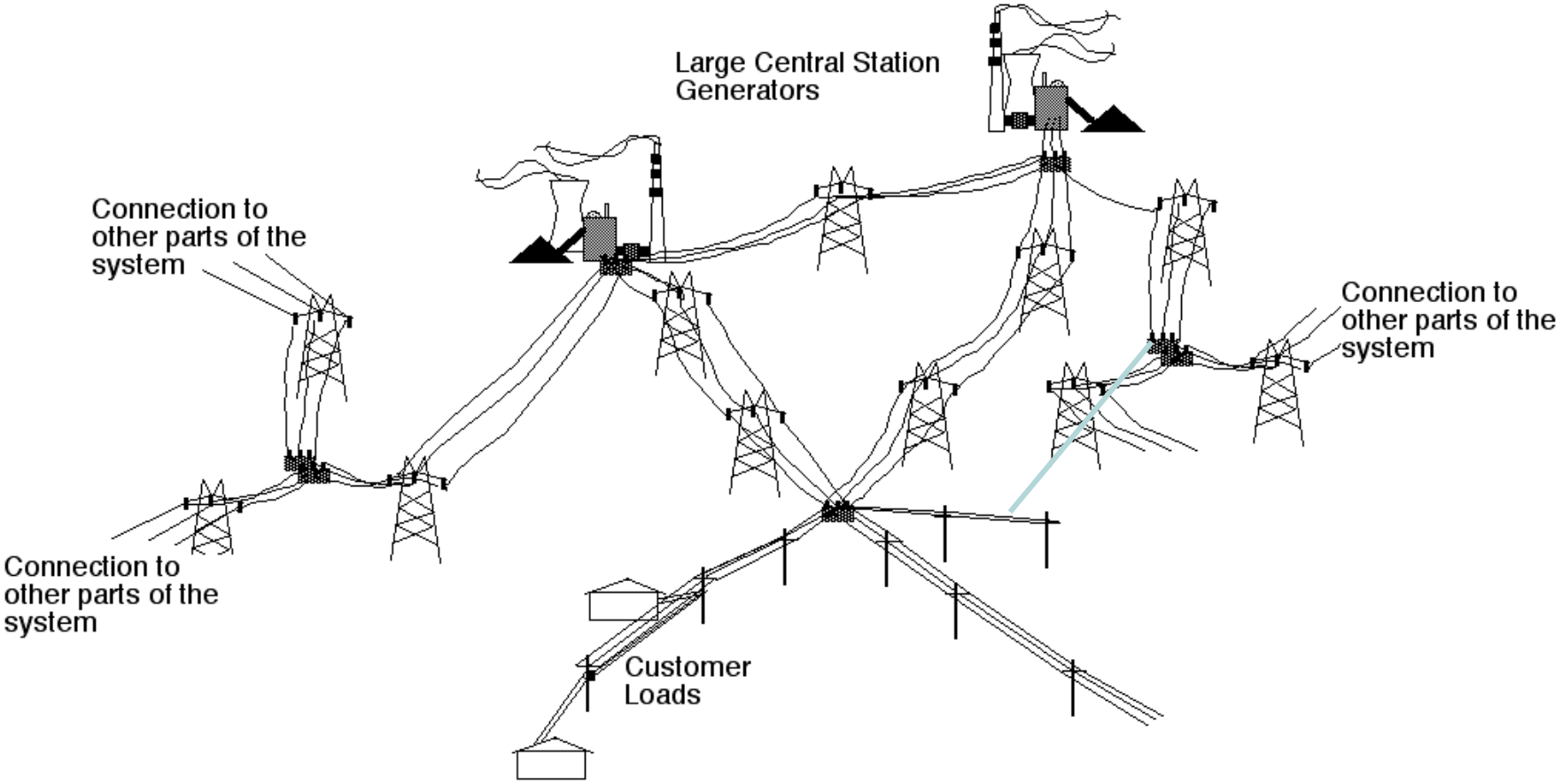
PENELOPE GIBBS, Senior Program Associate

* Died October 30, 2008.

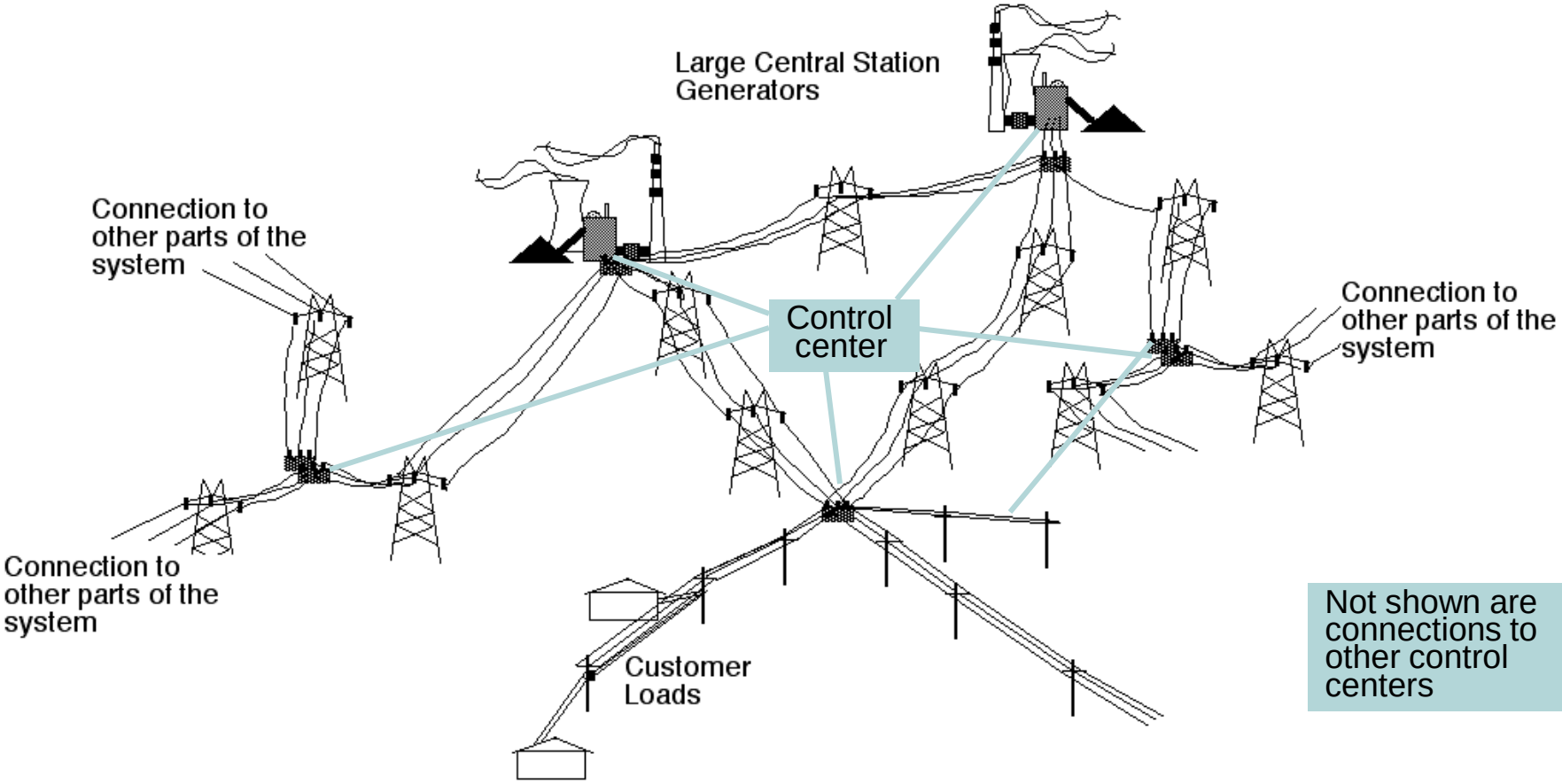
This afternoon I will:

- Begin with a very brief tutorial about the bulk power system and note some of its key vulnerabilities.
- Observe how much modern society depends on the continuous availability of electricity.
- Say a few words about:
  - The importance of being better prepared to restore the bulk power system after an outage has occurred.
  - The need to develop strategies to continue to support critical social services when the power goes out.
- Conclude with a short comment on challenge of balancing the desire to add more intelligence in the power system with the need to reduce the systems' vulnerability to cyber attack.

A brief tutorial on the structure of the power system

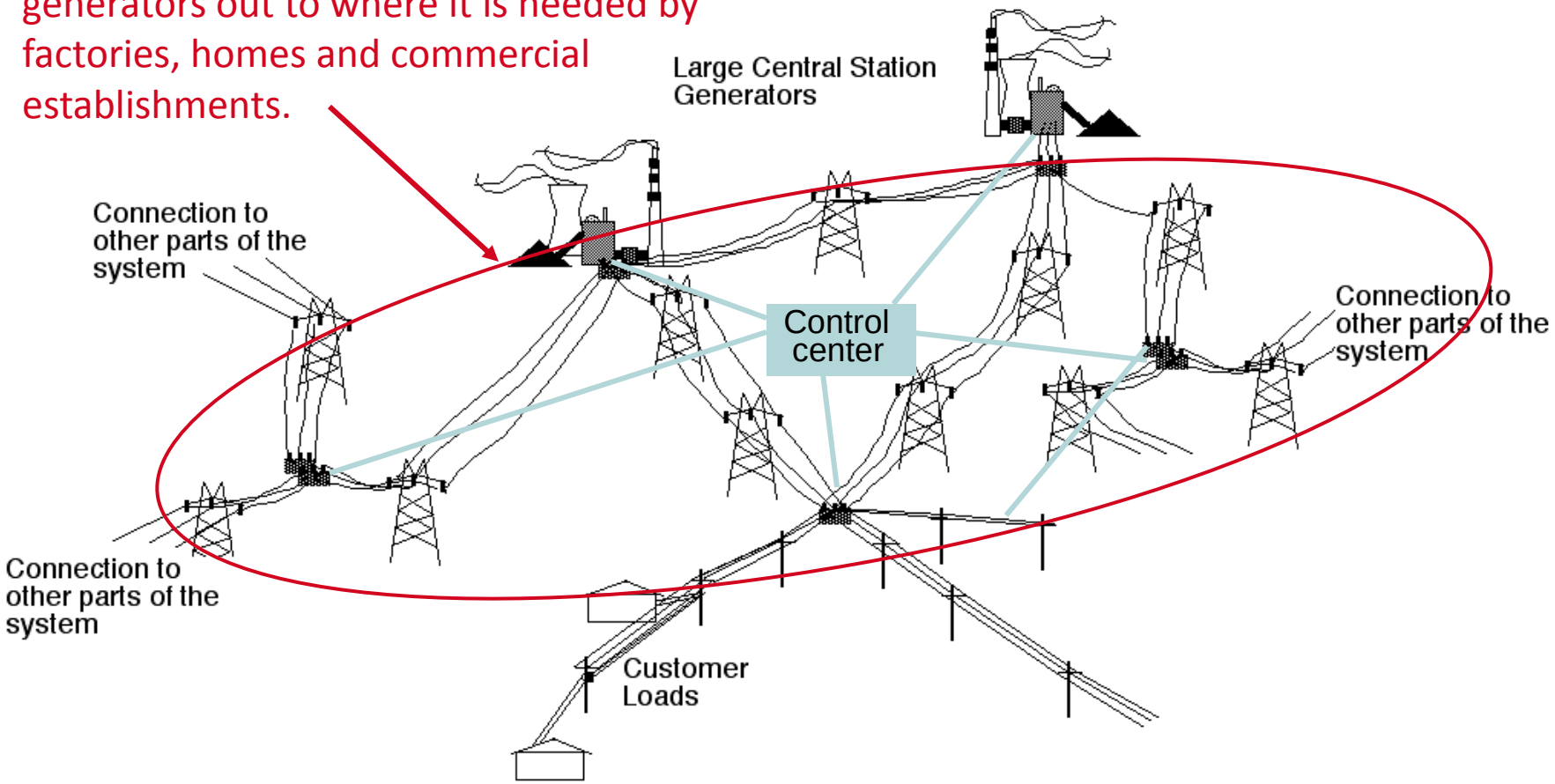


A brief tutorial…(Cont.)



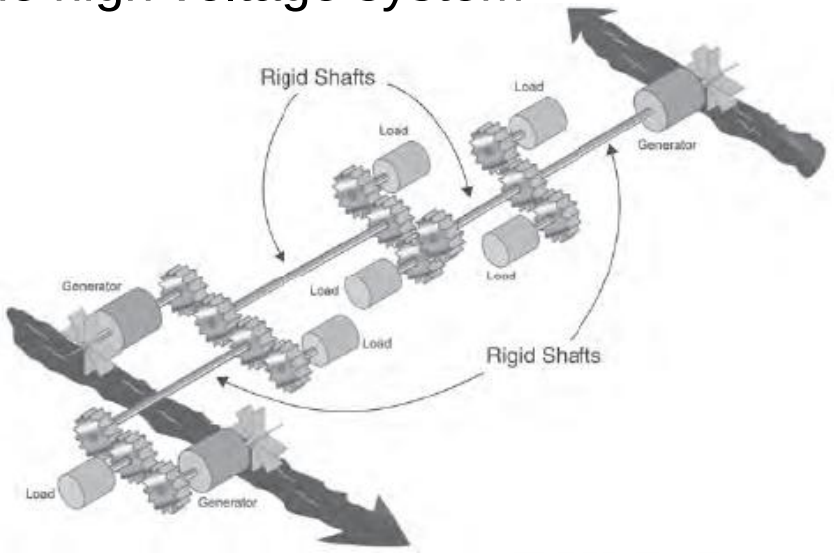
A brief tutorial…(Cont.)

The *high voltage transmission system* moves power from central generators out to where it is needed by factories, homes and commercial establishments.



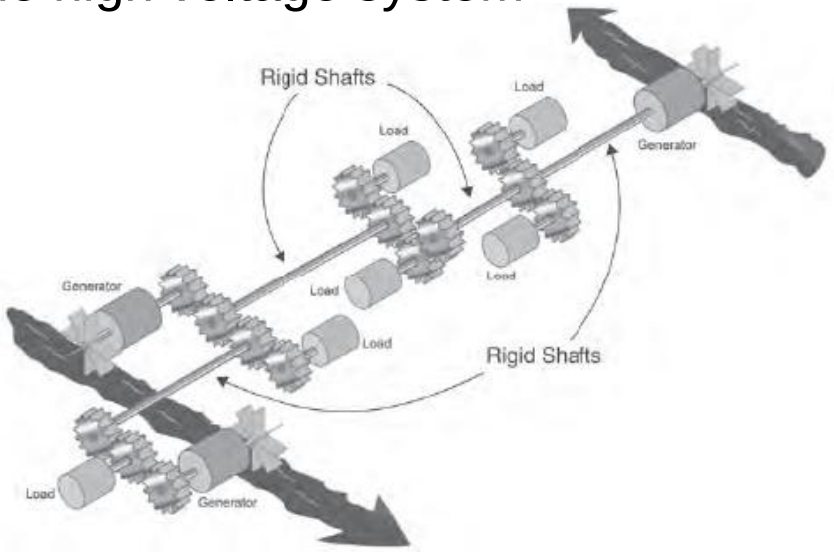
A brief tutorial…(Cont.)

While it is tempting to think of the high voltage system as working like this:

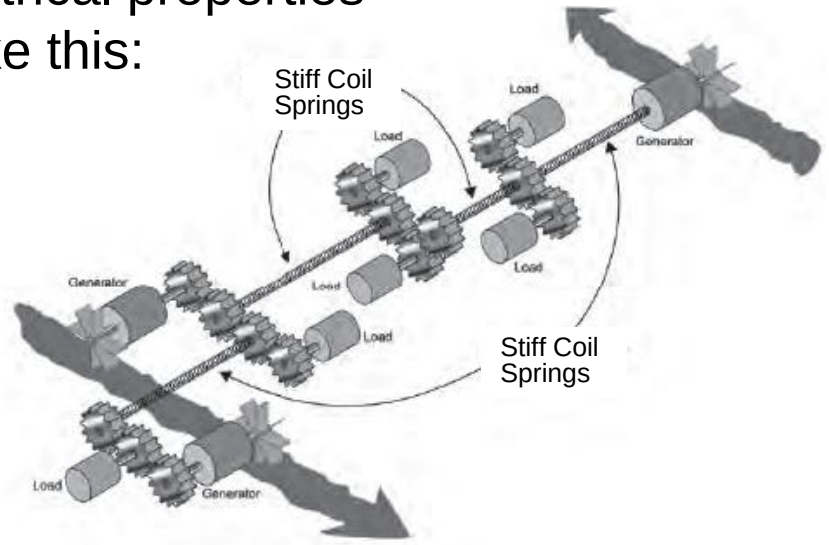


A quick tutorial…(Cont.)

While it is tempting to think of the high voltage system as working like this:

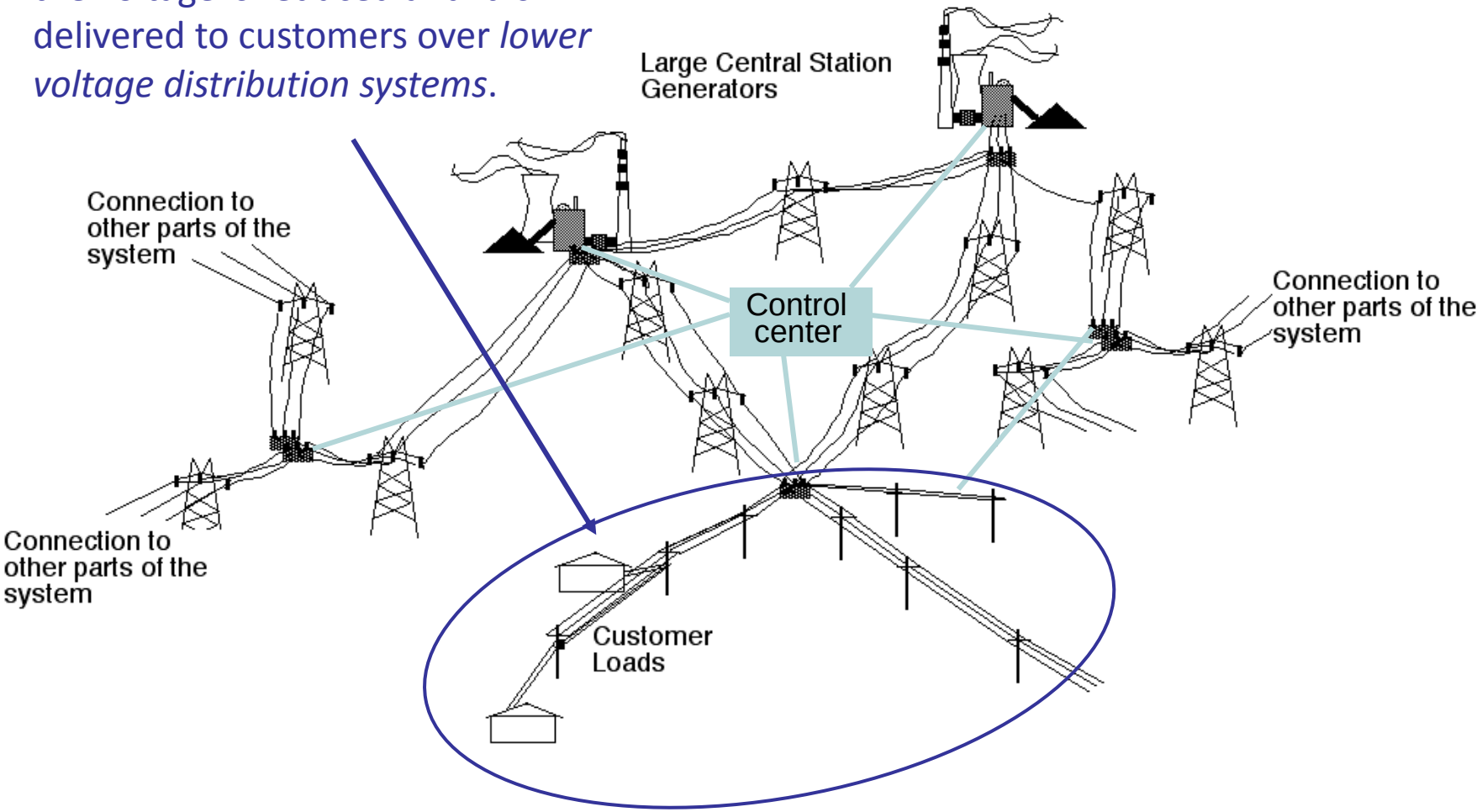


Because of its dynamic AC electrical properties a more accurate model looks like this:

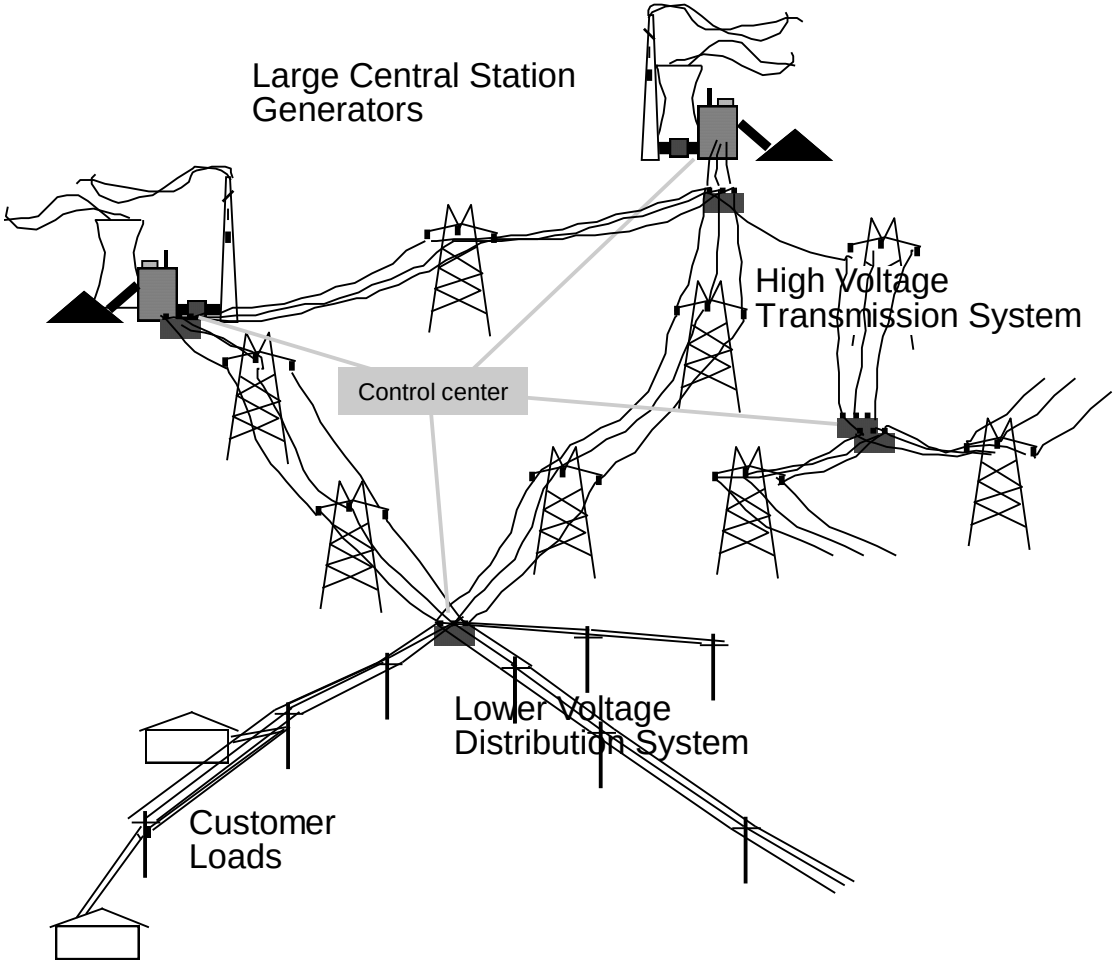


A brief tutorial…(Cont.)

Once the power has been delivered to the region where it will be used, the voltage is reduced and it is delivered to customers over *lower voltage distribution systems*.



Potential points of vulnerability



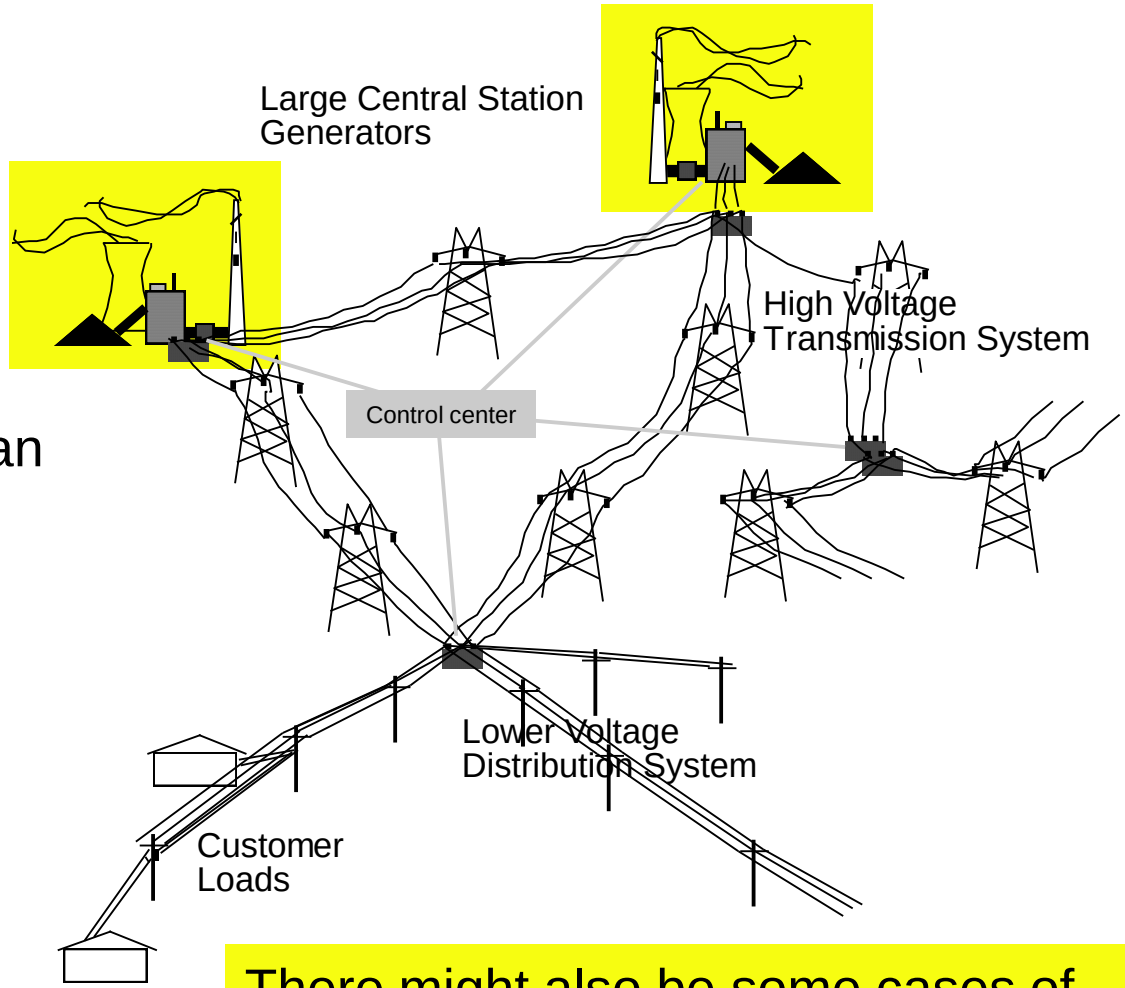
Potential points of vulnerability

1. Real or feigned attacks on (or failures at) central generation stations.

   Most power plants are rather secure against all but very large terrorist attacks.

   Large natural disasters can of course disrupt them.

Photo from www.rsc.org

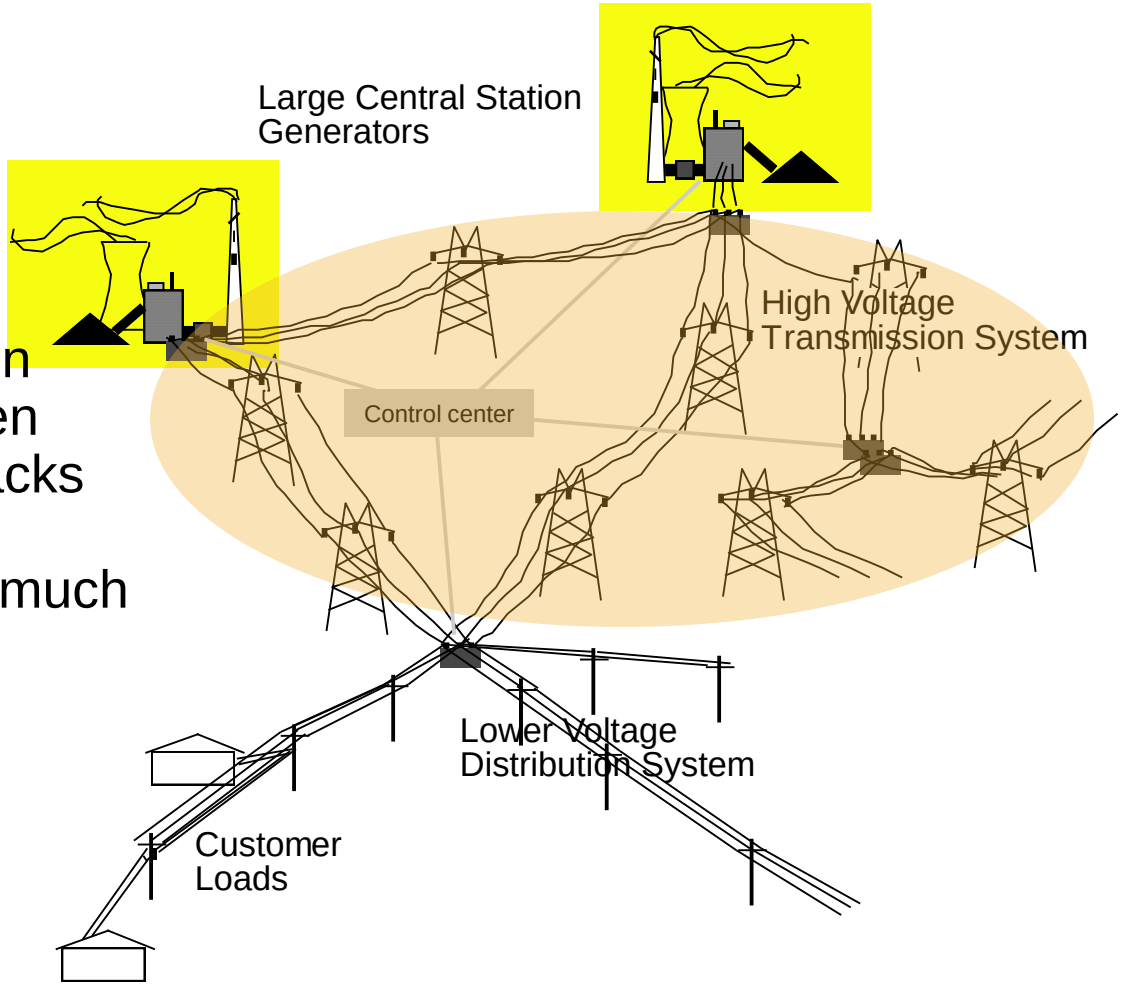


There might also be some cases of fuel supply vulnerabilities (e.g. gas)

Potential points of vulnerability

2. Attacks on (or failures in) transmission lines.

In other parts of the world, terrorists and insurgents have attacked transmission lines. There have also been occasional "loan wolf" attacks in the U.S. Ice storms and hurricanes probably pose much greater risks in the U.S.



Images: environment Canada; glassian.org

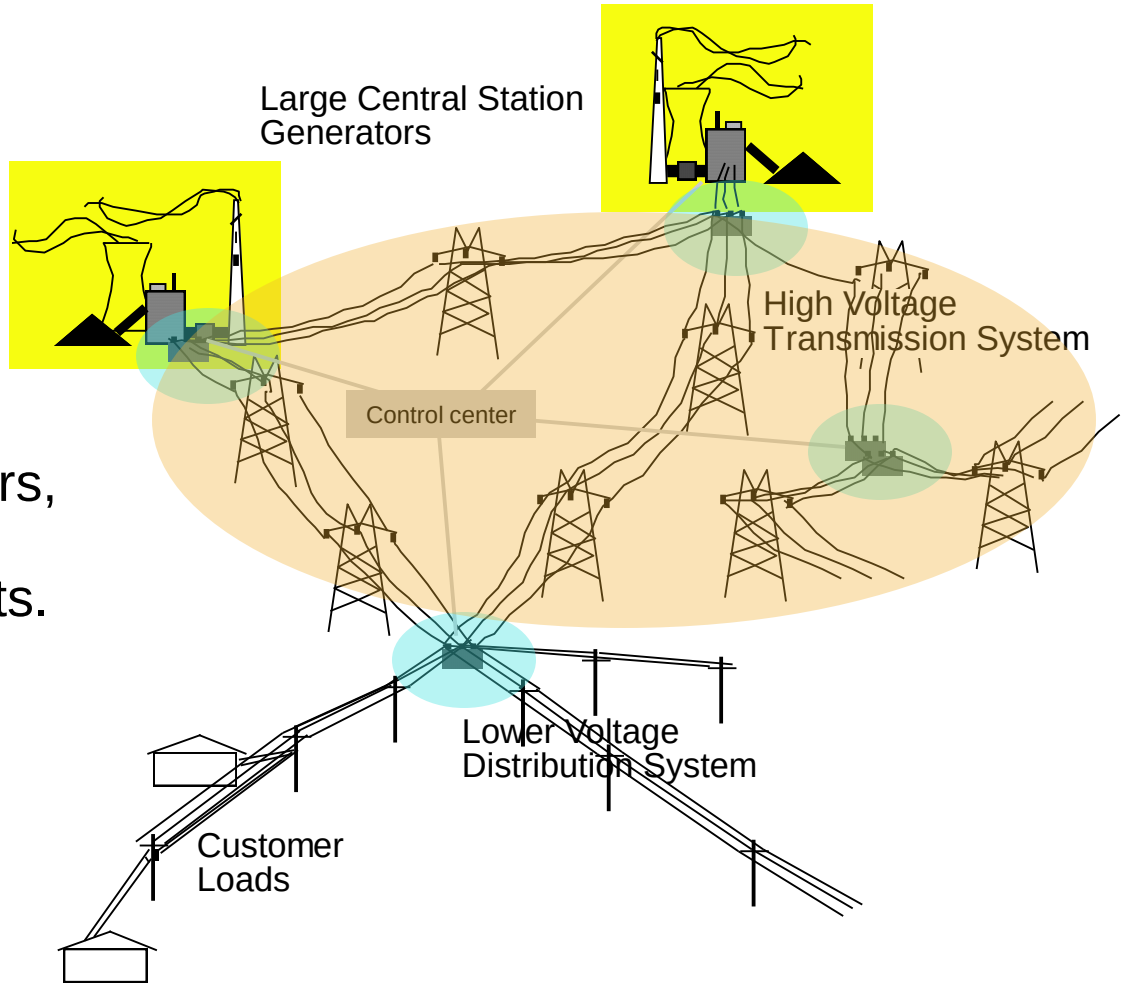
Potential points of vulnerability

3. Attacks on (or failures at) substations.

   A coordinated attack on a number of high voltage transformers is probably the greatest terrorist risk.

   Of course, in small numbers, substations are also vulnerable to natural events.

Photo: firedirect.org



Potential points of vulnerability

4. Physical and cyber attacks and failures in communication and control systems.

It is very difficult to develop a solid assessment of the risk, but it is clearly growing.

Unlike a physical attack on multiple high voltage transformers, a cyber attack is unlikely to bring power down for many weeks or months.

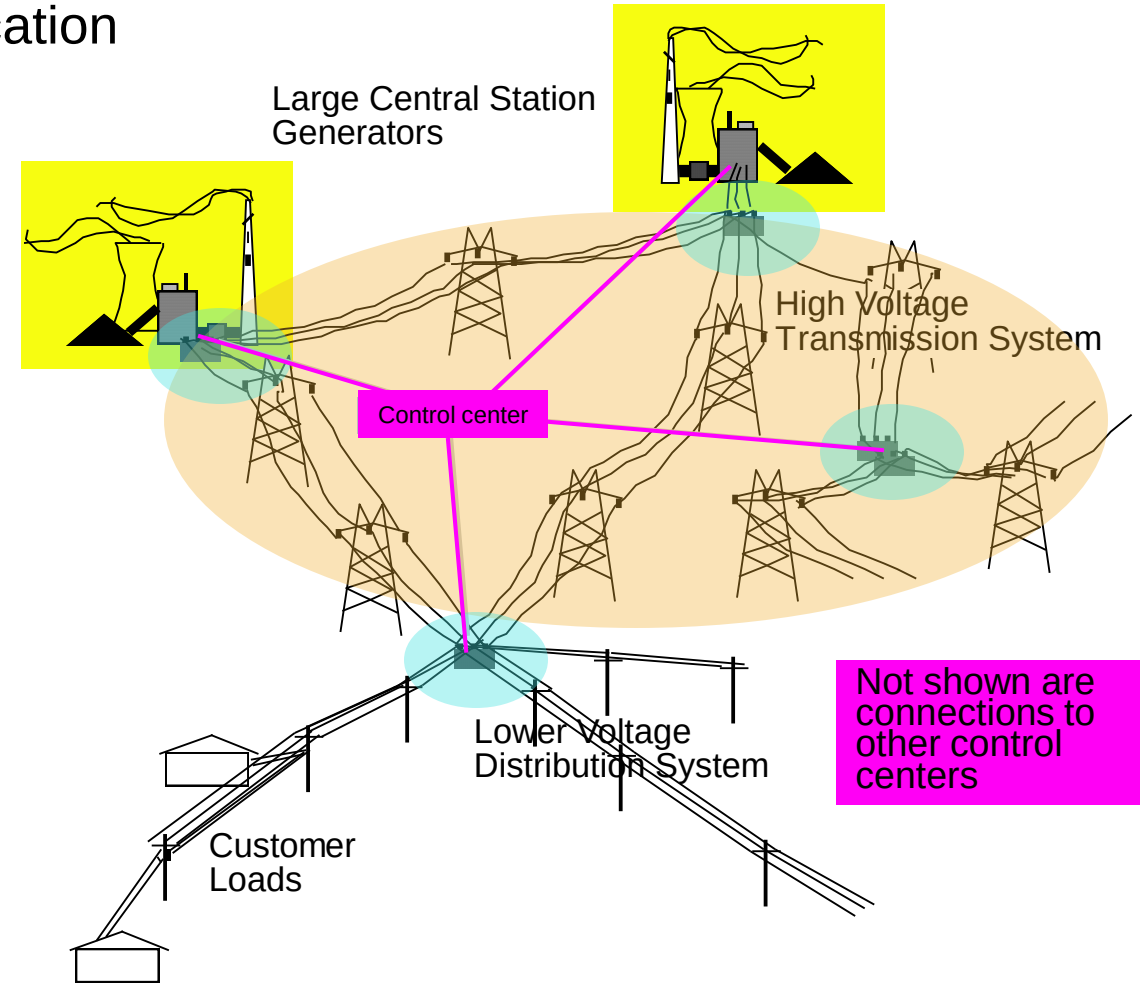


Image source: defensetech.org

Protection strategies

Central plants: Physical security, guards, guns and dog, etc., personnel security. Move spent nuclear fuel to long-term storage.

Transmission system: More use of 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, improved system estimation and response, high quality physical and cyber security, redundancy, advanced simulator training, personnel security.

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

Bottom line: even with the best protection the system will remain very vulnerable.

This afternoon I will:

- Offer a very brief tutorial about the bulk power system and note some of its key vulnerabilities.
- Observe how much modern society depends on the continuous availability of electricity.
- Say a few words about:
  - The importance of being better prepared to restore the bulk power system after an outage has occurred.
  - The need to develop strategies to continue to support critical social services when the power goes out.
- Conclude with a short comment on challenge of balancing the desire to add more intelligence in the power system with the need to reduce the systems' vulnerability to cyber attack.

A secure and reliable supply of electricity is *very* important

Annual U.S. sales of electricity in 2011 totaled $371 billion, and, of course, that does not begin to convey its value.

Nearly every aspect of productive activity and daily life in a modern economy depends on electricity for which there is, in many cases, no close substitute.

OTA

In 1990, in a report titled *Physical Vulnerability of the Electric System to Natural Disasters and Sabotage,* the Office of Technology Assessment concluded that:

> Some terrorist groups hostile to the United States clearly have the capability of causing massive damage-the loss of so many generating or transmission facilities that major metropolitan areas or even multi-state regions suffer severe, long-term, power shortages. The absence of such attacks has as much to do with how terrorists view their opportunities as with their ability. U.S. electric power systems are only one target out of many ways of striking at America, and not necessarily the most attractive.

Office of Technology Assessment, *Physical Vulnerability of Electric System to Natural Disasters and Sabotage, OTA-E-453*, U.S. Government Printing Office, 63pp., June 1990.

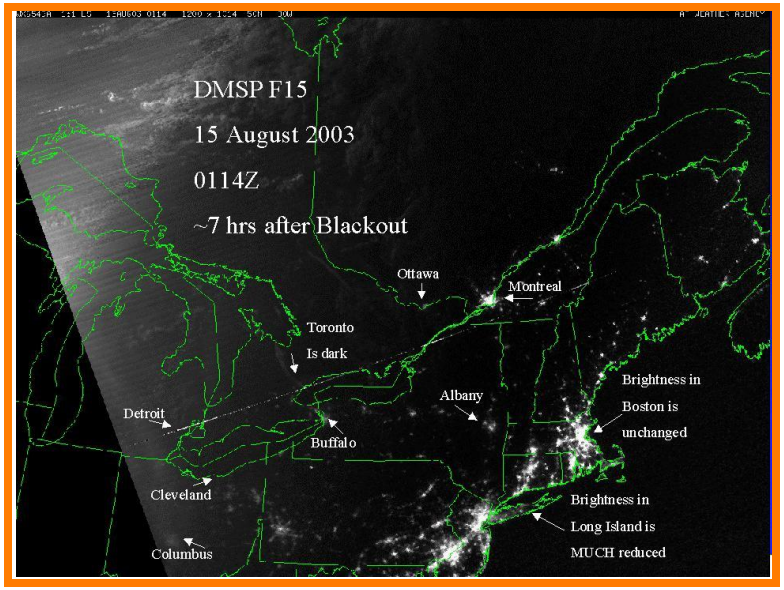
NRC

In 2002, the NRC report *Making the Nation Safer* noted:

> Analysis of possible targets, weapons, and delivery systems and of direct and indirect consequences reveals several very dangerous scenarios. The scenarios of greatest concern involve the electrical system. When service is lost, there are immediate consequences to every person, home, and business. An extended outage of electricity would have profound consequences…
>
> …The impact of a prolonged interruption in the electric power supply to any region of the country would be much larger than the economic loss to the energy sector alone…The nation's electric power systems must clearly be made more resilient to terrorist attack.

NRC Committee on Science and Technology for Countering Terrorism, *Making the Nation Safer: The role of science and technology in countering terrorism*, National Research Council, 415pp., 2002.

High value of electricity



Source: Defense Meteorological Satellite Program

The economic cost of the North East blackout in 2003 came to approximately $5 per foregone kWh, a figure that was roughly 50 times greater than the average retail cost of a kWh at that time.

Note: for outages of days rather than weeks there is the issue of deferred output. See pg. 16 of the NRC report for other estimates of blackout costs.

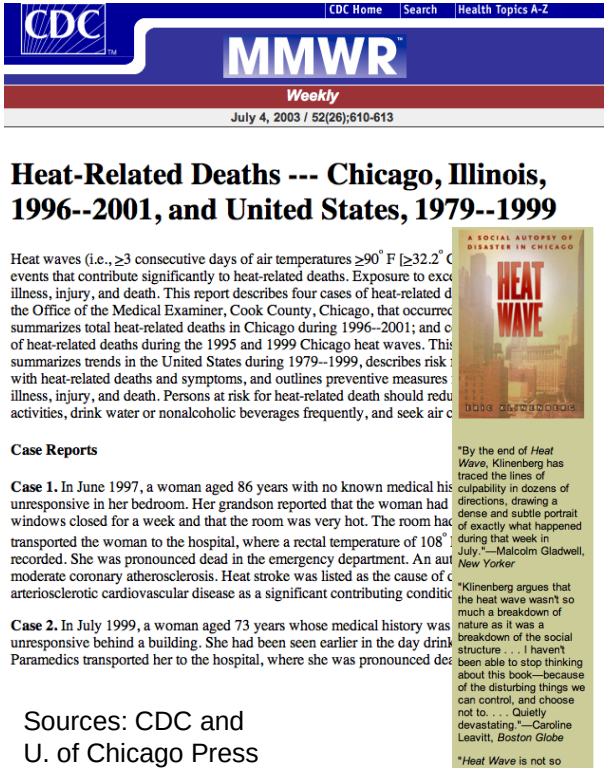
To operate portable electronic devices, consumers routinely pay $1.85 for a D-cell alkaline battery that can produce 0.017 kWh, yielding an equivalent price of $108/kWh!

Source: energizerbatteryfinder.com

A widespread outage that…

….went on for weeks or months rather than a few days could be devastating to the U.S. economy…to say nothing of the enormous inconvenience it would produce.

If it occurred during a heat wave or a particularly cold spell, it could also be life-threatening for more vulnerable segments of the population.



CDC | CDC Home | Search | Health Topics A-Z

MMWR Weekly

July 4, 2003 / 52(26);610-613

Heat-Related Deaths --- Chicago, Illinois, 1996--2001, and United States, 1979--1999

Heat waves (i.e., ≥3 consecutive days of air temperatures ≥90° F [≥32.2° C
events that contribute significantly to heat-related deaths. Exposure to exce
illness, injury, and death. This report describes four cases of heat-related d
the Office of the Medical Examiner, Cook County, Chicago, that occurred
summarizes total heat-related deaths in Chicago during 1996--2001; and c
of heat-related deaths during the 1995 and 1999 Chicago heat waves. This
summarizes trends in the United States during 1979--1999, describes risk
with heat-related deaths and symptoms, and outlines preventive measures
illness, injury, and death. Persons at risk for heat-related death should redu
activities, drink water or nonalcoholic beverages frequently, and seek air c

Case Reports

Case 1. In June 1997, a woman aged 86 years with no known medical his
unresponsive in her bedroom. Her grandson reported that the woman had
windows closed for a week and that the room was very hot. The room had
transported the woman to the hospital, where a rectal temperature of 108°
recorded. She was pronounced dead in the emergency department. An aut
moderate coronary atherosclerosis. Heat stroke was listed as the cause of
arteriosclerotic cardiovascular disease as a significant contributing conditio

Case 2. In July 1999, a woman aged 73 years whose medical history was
unresponsive behind a building. She had been seen earlier in the day drink
Paramedics transported her to the hospital, where she was pronounced dea

"By the end of *Heat Wave*, Klinenberg has traced the lines of culpability in dozens of directions, drawing a dense and subtle portrait of exactly what happened during that week in July."—Malcolm Gladwell, *New Yorker*

"Klinenberg argues that the heat wave wasn't so much a breakdown of nature as it was a breakdown of the social structure . . . I haven't been able to stop thinking about this book—because of the disturbing things we can control, and choose not to. . . . Quietly devastating."—Caroline Leavitt, *Boston Globe*

"*Heat Wave* is not so

Dying Alone

An interview with Eric Klinenberg
author of *Heat Wave: A Social Autopsy of Disaster in Chicago*

Question: Take us back to July 1995 in the city of Chicago. How hot was it? What were the city and its residents going through?

Klinenberg: Chicago felt tropical, like Fiji or Guam but with an added layer of polluted city air trapping the heat. On the first day of the heat wave, Thursday, July 13, the temperature hit 106 degrees, and the heat index—a combination of heat and humidity that measures the temperature a typical person would feel—rose above 120. For a week, the heat persisted, running between the 90s and low 100s. The night temperatures, in the low to mid-80s, were unusually high and didn't provide much relief. Chicago's houses and apartment buildings baked like ovens. Air-conditioning helped, of course, if you were fortunate enough to have it. But many people only had fans and open windows, which just recirculated the hot air.

The city set new records for energy use, which then led to the failure of some power grids—at one point, 49,000 households had no electricity. Many Chicagoans swarmed the city's beaches, but others took to the fire hydrants. More than 3,000 hydrants around Chicago were opened, causing some neighborhoods to lose water pressure on top of losing electricity. When emergency crews came to seal the hydrants, some people threw bricks and rocks to keep them away.

Sources: CDC and
U. of Chicago Press

This afternoon I will:

- Offer a very brief tutorial about the bulk power system and note some of its key vulnerabilities.
- Observe how much modern society depends on the continuous availability of electricity.
- Say a few words about:
  - The importance of being better prepared to restore the bulk power system after an outage has occurred.
  - The need to develop strategies to continue to support critical social services when the power goes out.
- Conclude with a short comment on challenge of balancing the desire to add more intelligence in the power system with the need to reduce the systems' vulnerability to cyber attack.

This afternoon I will:

- Offer a very brief tutorial about the bulk power system and note some of its key vulnerabilities.
- Observe how much modern society depends on the continuous availability of electricity.
- Say a few words about:
  - The importance of being better prepared to restore the bulk power system after an outage has occurred.
  - The need to develop strategies to continue to support critical social services when the power goes out.
- Conclude with a short comment on challenge of balancing the desire to add more intelligence in the power system with the need to reduce the systems' vulnerability to cyber attack.

Chapters 6 and 7

Recommendations Chapter 6

- **Reexamine substation vulnerability.**
- **More attention to outages from multiple failures.**
- **Develop best practice for system-wide measurement and assessment.**
- **Plans for provision of service to critical customers.**

Recommendations

Recommendation 6.1 The electric reliability organization (ERO) should require power companies to reexamine their critical substations to identify serious vulnerabilities to terrorist attack. Where such vulnerabilities are discovered, physical and cyber protection should be applied. In addition, the design of these substations should be modified with the goal of making them more flexible to allow for efficient reconfiguration in the event of a malicious attack on the power system. The bus configurations in these substations could have a significant impact on maintaining reliability in the event of a malicious attack on the power system. Bus layout or configuration could be a significant factor if a transformer, circuit breaker, instrument transformer, or bus work is blown up, possibly damaging nearby equipment.

Recommendation 6.2 The ERO and FERC should direct greater attention to vulnerability to multiple outages (e.g., *N*–2) planned by an intelligent adversary. In cases where major, long-term outages are possible, reinforcements should be considered as long as costs are commensurate with the reduction of vulnerability and other possible benefits.

Recommendation 6.3 The ERO and FERC should develop best practices and standards in improving system-wide instrumentation and the ability of near-real-time state estimation and security assessments, since otherwise operators are at a disadvantage trying to understand and manage system disruptions as they unfold. System operators should be able to observe what is going on well beyond their own borders whenever necessary. Reliability coordinators can oversee larger areas, maybe comprising several balancing authorities, but new entities should be established to oversee the whole Western and Eastern interconnection.

Recommendation 6.4 Local load-serving entities should work with local private and public sector groups to identify critical customers and plan a series of technical and organizational arrangements that can facilitate restricted service to critical customers during times of system stress. DHS could accelerate this process by initiating and partially funding a few local and regional demonstrations that could provide examples of best practice for other regions across the country.

Recommendations Chapter 7

- **Fund compact restoration transformers.**
- **MOUs among key players on emergency response.**
- **Utilities with standing and emergency regulatory exemptions.**

Recommendations

Recommendation 7.1 The Department of Energy and the Department of Homeland Security should fund the research, development, manufacture, and deployment of stocks of compact, easily transported, high-voltage restoration transformers for use in temporary recovery following the loss of several to many regular transformers.

Recommendation 7.2 Utilities and federal, state, and local governments, and law enforcement agencies should develop official memoranda of understanding (MOUs). These MOUs should spell out each party's responsibilities before, during, and immediately following a deliberate destruction of utility equipment that leads to a disruption of electric service; provide a clear understanding of who is in charge; and explain how decisions will be reached in dealing with potential tensions between crime scene investigation and timely service restoration as well as unanticipated contingencies. The MOUs should also help to ensure the appropriate allocation of resources, and address concerns about potential government seizure of utility supplies and equipment during catastrophic events,[9] which can seriously hinder prompt utility restoration of electric service.

Recommendation 7.3 State and federal law or regulations should be modified to:

- Recognize utilities as essential service providers so that relevant utility employees can be trained and legally designated as first responders to deal with attacks on the power system.
- Provide utilities, when needed, with temporary exemptions from laws that restrict their use of equipment, access to roads, materials, supplies, and other critical elements for restoration of electric service to essential loads, including those that have an impact on public health and safety.
- Ensure that state regulatory agencies support prudent efforts by utilities to commit and acquire the necessary resources for service restoration and provide reasonable assurance for recovery of these costs.

Ch 7… Cont.

Recommendation 7.4 The Department of Homeland Security and the Edison Electric Institute should jointly develop programs and offer training for key utility personnel to respond to both conventional security threats and potential chemical/biological attacks on the electric infrastructure. The training should provide increased awareness of the possible threats, through risk assessments, and provide specific training for the use of protection equipment, detection and sensor equipment, and emergency decontamination procedures. Existing drills and restoration procedures must be expanded to address the potential for biological or chemical attacks that would disrupt electric operations and infrastructures.

Recommendation 7.5 The Department of Homeland Security with the Department of Energy and the electric reliability organization should work with utilities that have not yet done so to:

- Establish a team reporting to top management that coordinates physical, cyber, and operations security through comprehensive plans that clearly define what is expected of security personnel before, during, and after a deliberate destructive act; identifies the technologies and strategies to be used to continuously monitor critical company facilities; and establishes an Incident Command System and designates an incident commander to work with outside agencies.
- Examine their internal radio communications systems to determine that battery backup systems and portable generators are in place to ensure that all communication devices will remain operational during a crisis. Because traditional communication systems may become unavailable during a destructive attack on the electric system, options such as satellite communications should be evaluated (and periodically tested) for potential use as backup communication. In addition, the ERO could help ensure that neighboring utilities and operators have compatible communications systems.
- Assess black-start capabilities in their systems under the assumption that major physical disruption of the transmission system can occur, develop appropriate contingency plans, and test both the plans and the equipment on a regular basis.
- Assess the potential for the cascading collapse of long stretches of transmission line, and, where appropriate, include offsetting towers at various intervals or reinforcing or upgrading towers at more frequent intervals along the line.

Recommendation 7.6 State legislatures should change utility law to explicitly allow micro-grids with distributed generation. IEEE should revise its standards to include the appropriate use of islanded distributed generation and micro-grid resources for local islanding in emergency recovery operations. Utilities should reexamine and, if necessary, revise their distribution automation plans and capabilities in light of the possible need to selectively serve critical loads during extended restoration efforts. Public utility commissions should consider the potential emergency restoration benefits of distribution automation when they review utility applications involving such investments.

- **Training for key personnel.**
- **Assess organizational & technical preparedness.**
- **Allow private micro-grids with DG.**

This afternoon I will:

- Begin with a very brief tutorial about the bulk power system and note some of its key vulnerabilities.
- Observe how much modern society depends on the continuous availability of electricity.
- Say a few words about:
  - The importance of being better prepared to restore the bulk power system after an outage has occurred.
  - The need to develop strategies to continue to support critical social services when the power goes out.
- Conclude with a short comment on challenge of balancing the desire to add more intelligence in the power system with the need to reduce the systems' vulnerability to cyber attack.

While the grid can and should be made more secure…

…and strategies can be developed to speed restoration, prudence suggests that at the same time we should place greater emphasis on finding ways to sustain vital social services, and minimize public and private costs, when the power goes out.

In 2004, Jay Apt, Marija Ilic and I looked at this issue in an undergraduate student project course at Carnegie Mellon using Pittsburgh as a test bed. Students examined how robust the city would be in the event of outages of varying duration.

Chapter 8 of the NRC report built on this and similar previous work.

Some examples of "critical social services"

Emergency Services
- 911, emergency operations centers, and other dispatch
- Police services
- Fire protection services
- EMS

Medical Services
- Transport ambulance services
- Life-critical in-hospital care (life support systems, operating rooms, etc.)
- Non-critical in-hospital care (refrigeration, heating and cooling, sanitation, etc.
- Clinics and refrigerated pharmacies
- Nursing homes and other non-hospital care

Non-electric Public Utilities
- Water
- Sewer
- Natural gas

Lighting
- Building evacuation and stairwell lighting
- Domestic lighting
- Lighting in commercial establishments
- Security lighting
- Street lighting

Food
- Cash registers
- Lighting
- Refrigeration
- Restock operations

Financial
- Cash machines
- Banking services
- Credit card systems

Fuel Infrastructure
- Pump operations
- Pipeline systems
- Local fuel storage capacity
- Transport and distribution capacity and operations (including river locks)
- Whole sale and retail operations

Communication and cyber services
- Radio transmission and reception
- Television transmission and reception
- Wire-line telephone
- Cable systems
- Wireless telephone
- Wired data services
- Wireless data services
- Computer services on customer's premises
- Computer services off customer's premises

Non-emergency government services
- Government information and service offices
- Prisons

Transportation and mobility
- Building elevators
- Traffic signals
- Tunnels
- Light rail systems and subways
- Conventional rail systems including railroad crossings
- Air traffic control
- Airport operations including landing and related lighting
- River lock and dam operations
- Drawbridge operations

Chapter 8

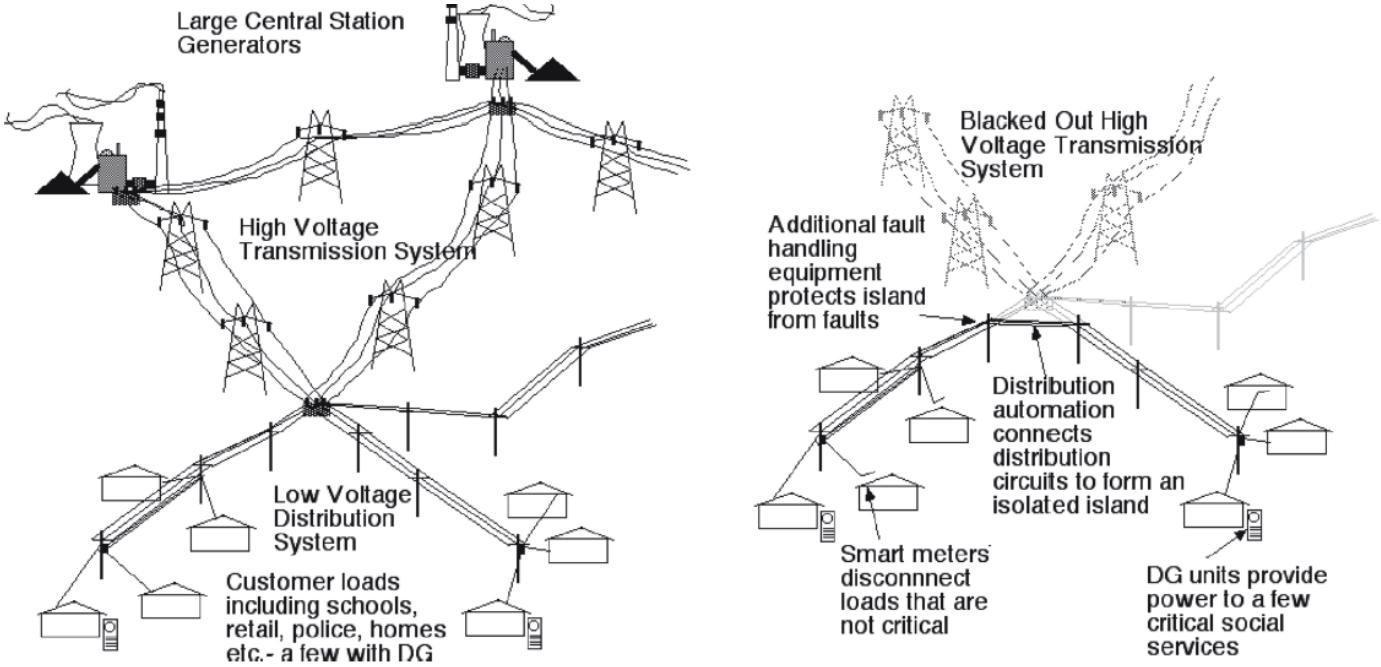


Figure source: Narayanan and Morgan, "Sustaining Critical Social Services During Extended Regional Power Blackouts," *Risk Analysis*, *32*, 1183-1193, 2012.

Chapters 9 and 10

This afternoon I will:

- Begin with a very brief tutorial about the bulk power system and note some of its key vulnerabilities.
- Observe how much modern society depends on the continuous availability of electricity.
- Say a few words about:
  - The importance of being better prepared to restore the bulk power system after an outage has occurred.
  - The need to develop strategies to continue to support critical social services when the power goes out.
- Conclude with a short comment on challenge of balancing the desire to add more intelligence in the power system with the need to reduce the systems' vulnerability to cyber attack.

There are good reasons to add more intelligence and control to the bulk power system

- Greater capacity through existing lines.
- Better stability control.
- Ability to make power flow where economics dictate
- Etc.

Extensive use of phasor measurements.

Enhanced communication.

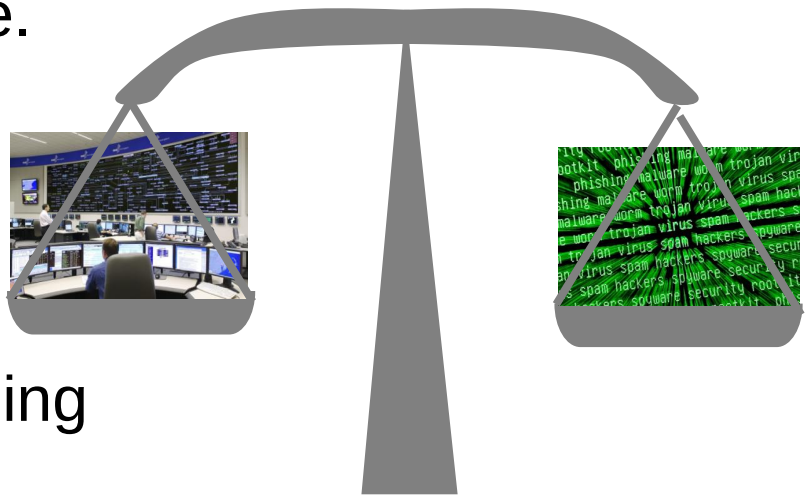
Better supervisory control and modeling of operations.

Flexible AC transmission systems.

Photo sources: LBL, ABB, news.cnet.com

BUT, more intelligence, communication and automated control…

…mean more potential points of entry for cyber attack. One key issue our committee did not address is how to strike the appropriate balance.



Indeed, doing such an analysis will be very challenging because of:

- Obvious security concerns and limits on data access;
- The inherent difficulty of assessing the risks;
- The motivation of some to hype the cyber risks.

Image sources: news.cnet.com; defensetech.org

For the balance of the meeting

1:20 PM Current and Future Needs for the Electric Power Delivery System
Panel Discussion
David Owens, Edison Electric Institute (physical infrastructure needs)
Massoud Amin, University of Minnesota (cyber security needs)
Jay Apt, Carnegie Mellon University (mitigation and response)
Sue Tierney, Analysis Group (resilience and critical services)

1:40 PM The Department of Energy Project Plan
Patricia Hoffman, Department of Energy

2:10 PM Infrastructure vulnerabilities and security
Bill Anderson, The Infrastructure Security Partnership

2:40 PM What is industry's role moving forward?
Fred Hintermeister, North American Electric Reliability Corporation

3:10 PM Break

Cyber Security Needs

3:25 PM Understanding critical cyber vulnerabilities
Panel Discussion
Galen Rasche, Electric Power Research Institute
Paul Nielsen, Software Engineering Institute
Terry Boston, PJM Interconnection

4:15 PM Open discussion on cyber security of the grid
Moderated by **Massoud Amin,** University of Minnesota

5:15 PM Adjourn public session

Balance of the meeting…(Cont.)

THURSDAY, FEBRUARY 28, 2013

8:00 AM Welcome and introduction
Granger Morgan, Carnegie Mellon University (NRC Panel Chair)

Physical Vulnerability

8:10 PM The future of the electric grid
John Kassakian, Massachusetts Institute of Technology

8:35 PM The DHS transformer program
Sarah Mahmood, Department of Homeland Security

9:00 PM Open discussion on the physical vulnerability of the grid
Moderated by David Owens, Edison Electric Institute

9:30 AM Break

Mitigation and Restoration

9:45 AM Power disruptions in the United States and improving restoration of service
Panel Discussion
Daniel Bienstock, Columbia University
Steve Whitley, NYISO
Mike Adibi, IRD Corp.

10:30 AM Open discussion on mitigation and response
Moderated by **Jay Apt,** Carnegie Mellon University

Balance of the meeting…(Cont.)

Resilience and Critical Services

11:00 AM Reducing risk and increasing national resilience
Panel Discussion
Gerry Galloway, University of Maryland (NRC Committee on Disaster Resilience)
David Kaufman, DHS/Federal Emergency Management Agency

11:45 AM Open discussion on resilience
Moderated by **Sue Tierney,** Analysis Group

12:15 PM Lunch

What can we do to move forward?
(Q&A following each speaker)

1:00 PM The regulatory environment
Joseph McClelland, Federal Energy Regulatory Commission

1:30 PM How policy will shape utilities moving forward
Miles Keogh, National Association of Regulatory Utility Commissioners

2:00 PM Building a smarter grid
Dan Reicher, Stanford University

2:30 PM Trade-offs between security, resilience, and flexibility
Sue Tierney, Analysis Group

3:00 PM Open discussion on policy options
Moderated by **Granger Morgan,** Carnegie Mellon University (NRC Panel Chair)

3:15 PM Closing remarks
Granger Morgan, Carnegie Mellon University, NRC Panel Chair

3:30 PM Adjourn public session

End