Carnegie Mellon Electricity Industry Center

Increasing the Security & Reliability of the USA Electricity System

Lester Lave, Jay Apt, & Granger Morgan

Carnegie Mellon Electricity Industry Center

www.cmu.edu/electricity

Carnegie Mellon Electricity Industry Center

- Begun in 2001: Core funding by the Alfred P. Sloan Foundation and EPRI
- Co-Directors: Lester Lave & Granger Morgan
- Executive Director: Jay Apt
- 17 Faculty and 23 Ph.D Students
- The focus of CEIC is strategic, research on engineering-business issues
- Reshape the industry through strategic research & technology-informed policy

The Cost of Blackouts

Everything depends on electricity: computers, communication, space conditioning, …

Electronics requires power quality

Cost of having no power – August 14

Cost of protecting against blackout – backup generators, etc.

Reliable systems are expensive – & still can fail

So – eliminate blackouts!

Some Recent Large Blackouts

11/9/65	Northeast US	30 million people
7/13/77	NYC	9 million
8/24/92	Florida	1 million
7/2/96	Western US	2 million
8/10/96	Western US	7.5 million
Jan 98	Québec	2.3 million
Feb-Apr 98	Auckland	1.3 million
8/14/03	Great Lakes	50 million
8/30/03	London	½ million
9/18/03	Tidewater US	4 million
9/23/03	Denmark & Sweden	4 million
9/28/03	Italy	57 million
11/7/03	Chile	15 million

Can Blackouts be Prevented?

- The HV part of the system contains 157,000 miles, thousands of nodes.
- Natural disasters: Ice storms, hurricanes, earthquakes
  - Québec Ice Storm: 770 transmission towers
  - Hurricane Andrew: 300 towers down
  - Hurricane Isabel: 3 million without power

Common Themes from Blackout Investigations

- Monitoring of the power grid is sparse, and data are not shared among power companies. Inadequate regional and interregional monitoring of the power system.
- Inappropriate standards: vegetation trimmed every 5 years.
- Operators are not routinely trained using realistic simulations.
- Companies have very different equipment, data, and training. Some can quickly interrupt power during an emergency, while others cannot.
- 1982 unimplemented recommendations to display data in a form that makes it easy to see the extent of a problem.

Lessons from Air Traffic Control

- Companies get blamed for systems failures – “operator error”
- Poor monitoring and control systems lead to conservative operations standards that use equipment inefficiently – and still don’t prevent crashes. Comprehensive monitoring is crucial, and so is the ability to interpret the data in real time and take action.
- Individual companies do not have the incentives to fix the problems; voluntary solutions are unlikely to work – regulators must be informed, but rarely have the expertise to arrive at the best solution.
- Investigation and operations should be in separate hands.
- Many of the actions are local or regional, but a national coordination center is required to bring controllers together.

Applying these lessons

The air traffic control system moved beyond a reactions to a crash to a comprehensive plan which included R&D and facilities to handle future issues.

A national grid operations plan is needed, and it should be implemented through an organizational structure which recognizes that human beings make mistakes and that checks and balances are required.

Applying these lessons

Realistic simulator training

- recognize and act upon signs of extreme system stress which may be well outside daily operations experience. “Years of boredom punctuated by moments of stark terror.”
- expose structural deficiencies such as poor lines of authority and insufficient staffing.
- Federal standards for training, licensing, and certification of grid operators and control centers are warranted to ensure that a single weak control center does not bring down a large area

Applying these lessons

3. Operations control centers must be able to control
   - Load shedding
   - Load reduction
4. Periodic testing of all systems, including load shedding, emergency power, telemetry
5. Regional standards for maintenance (such as tree trimming)

Evolving to an ATC-like system

- If ERO is eventually passed, it will be an interesting social experiment
  - Federally-chartered industry organization enforcing with penalties standards it develops
  - Who will have a veto on the standards?
- Should be expanded
  - Certification of operators, data and control systems, control rooms, training, periodic testing

DG and Security

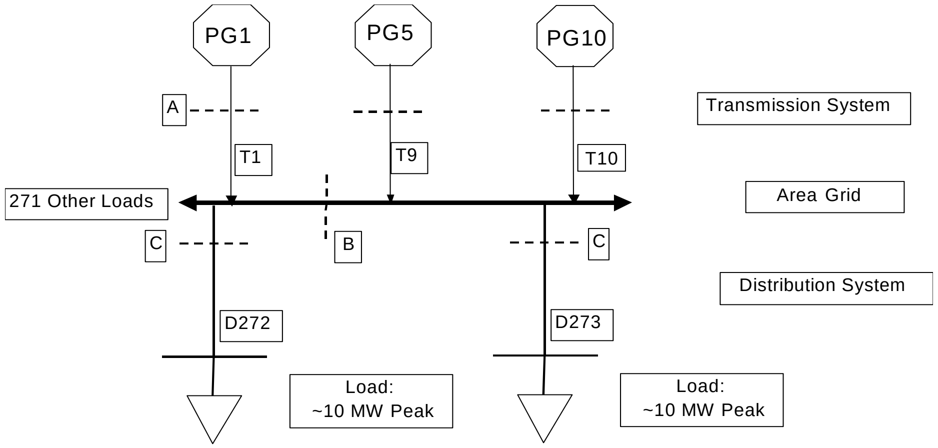
There has been lots of talk about how DG might be used to increase service reliability. Hisham Zerriffi's Ph.D. thesis is the first to analyze this claim quantitatively.

DG *together with intelligent control* can substantially increase reliability.

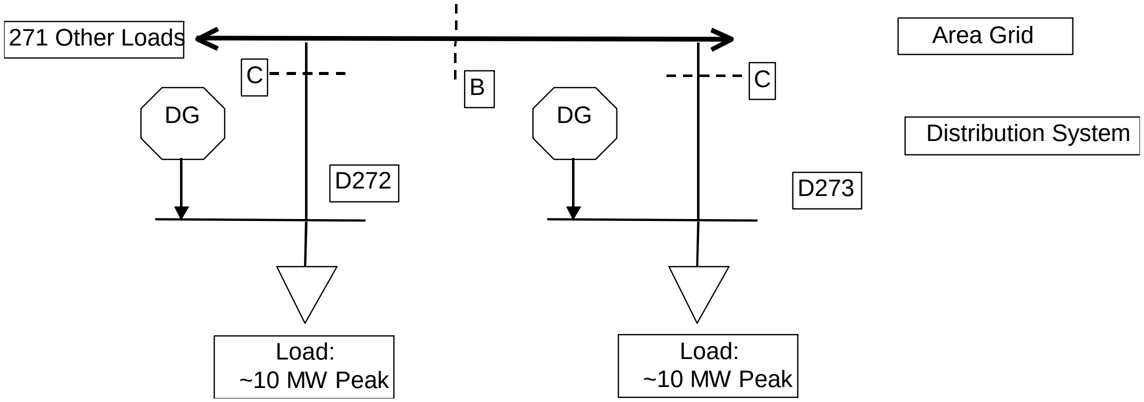
Topology of the electrical systems

A simple "typical" topology has also been modeled for the natural gas system.

Centralized:

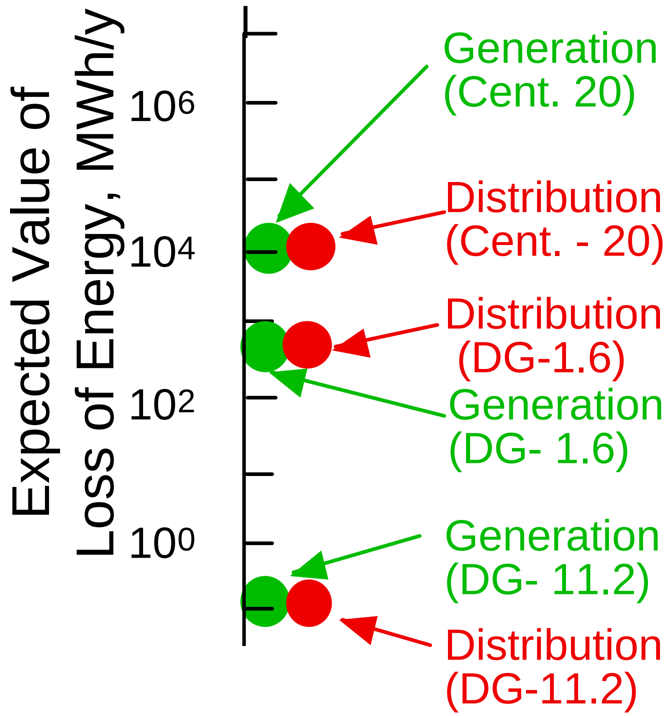


Distributed:



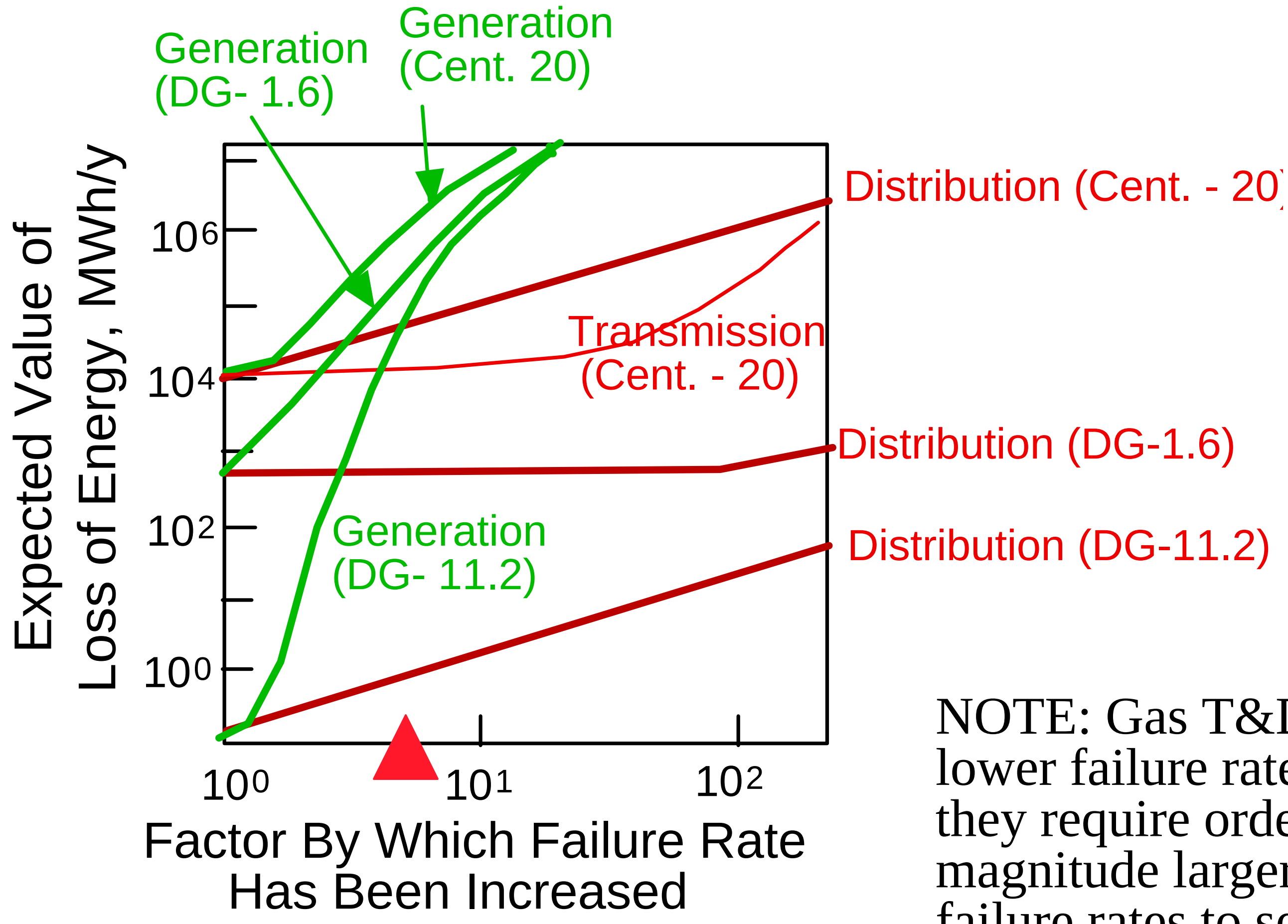
Details of the modeling assumptions can be found in Hisham Zerriffi, Hadi Dowlatabadi, and Alex Farrell, "Incorporating Stress in Electric Power System Reliability Models," *Proceedings of the IEEE*, in review for a special issue.

Simulation results for the electric portion of the systems



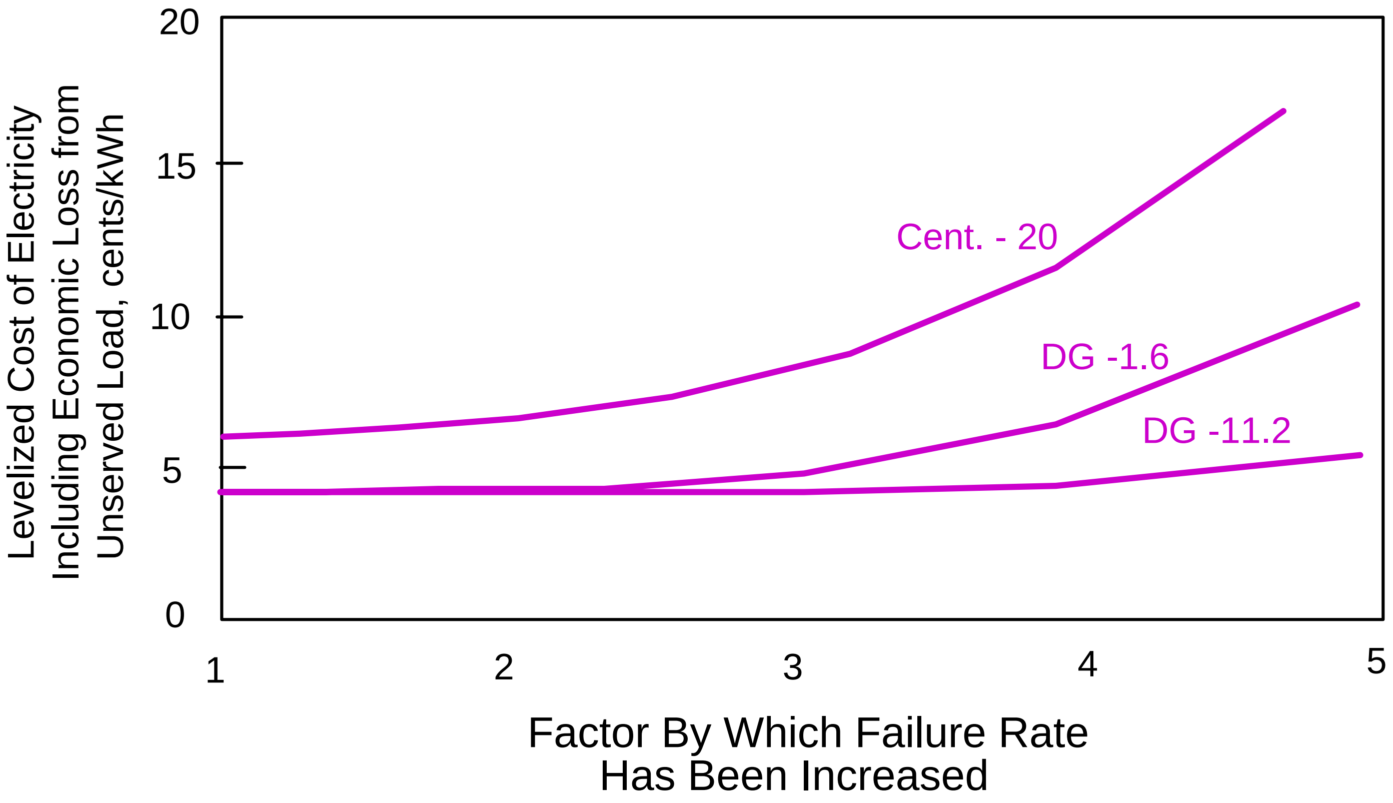
Results are for the current levels of generation and distribution system reliability.

Increased levels of stress on the system:



NOTE: Gas T&D have *much* lower failure rates, hence they require orders of magnitude larger increases in failure rates to see comparable loss of energy.

Economic loss from unserved load



NOTE: Loss computed as levelized cost of energy generation and transmission plus $3.83/kWh-unserved.

A More Solvable Problem

Survivability is the ability of a system to fulfill its missions, in a timely manner, in the presence of attacks, failures, or accidents.

H.F. Lipson and D. A. Fisher, *Survivability — A New Technical and Business Perspective on Security,* Proceedings of the 1999 New Security Paradigms Workshop, Caledon Hills, Ontario, Sept. 21–24, 1999, Association for Computing Machinery, New York, NY, available at http://www.cert.org/research/.

Survivable Missions

(supported by Pennsylvania's DEP)

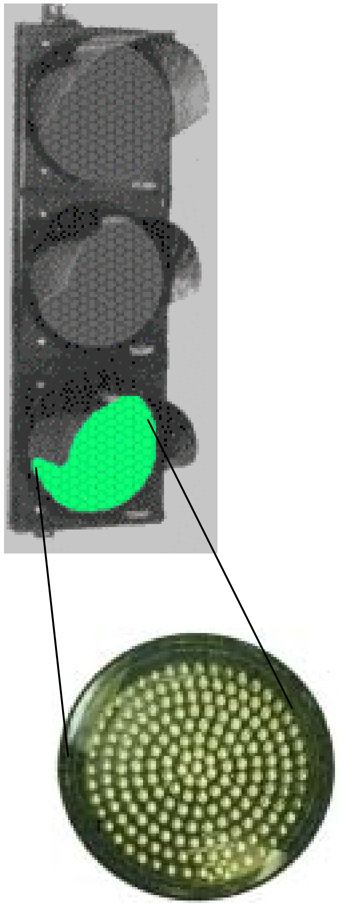
We need to make vital social services or "missions" robust in the face of power outages.

When the power went out in August 2003, traffic lights stopped working and traffic snarled in all the major cities; water and sewer lines stopped working in cities like Cleveland; people got stranded in the dark in elevators and subway systems.

There is no excuse for any of this to happen.

While we can do things to reduce the probability of cascading blackouts…we cannot eliminate them.

A simple example



When the power goes out, traffic snarls in urban cores, making it impossible for emergency vehicles to get through.

In a “normal” blackout, this is a problem. If a blackout were part of a terrorist attack, it could be very serious.

While old style traffic lights required something like 150 watts, modern traffic lights that use light emitting diodes (LEDs) use less than 15 watts.

LED traffic lights can be kept running for several days on battery back-up.

System interactions

The importance of thinking in terms of making vital missions robust *at a system level* is provided by the August 2003 blackout.

When the power went out Newark and Kennedy airports were able to quickly restore power for passenger screening and other boarding functions. On the other hand, LaGuardia could not.

Because all three are part of a closely coupled system, air traffic became snarled throughout the east.

A Solvable Problem

- Recognize that blackouts will happen.
- Reduce the social and economic costs by assuring that critical missions continue.
  - Traffic lights
  - Water and sewer pumps
  - Natural gas pressure
  - Emergency service systems
  - Exit from subways and elevators
  - Crucial economic functions

Steps

1. Define the missions which must survive.
2. Determine a set of design reference events (extent and duration).
3. Prioritize missions (12 hours vs. 2 weeks).
4. Which missions are protected already?
5. Which missions require new hardware or procedure changes?
6. Identify cost-effective technologies (for both private and public goods).
7. Allocate competing resources.

Protecting Against Terrorism

Terrorism poses the same threats as natural hazards: Taking out transmission towers, generators, etc.

It also poses different threats: Cyber attack, physical attack on nuclear sites, gas pipelines …

But: 1. A more reliable system would sustain less damage from any particular physical attack

2. Greater reliability requires an improved SCADA that should be less vulnerable to attack

3. The social cost of a damaged electricity system is lower if we have DG & survivability

4. The costs of improving reliability & security are lower if the two are done together

Hypothesis: Perhaps 90% of Protecting the Electricity System Against Terrorism is Gotten from Steps to Improve Reliability

We don’t know if terrorism will ever threaten the US electricity system

We do know that reliability is a major social cost

Our first major challenge is increasing reliability