Improving Energy Infrastructure Security: Costs and Consequences

Alex Farrell¹, Hisham Zerriffi², Lester Lave², Granger Morgan²

¹Energy and Resources Group, UC Berkeley
²Dept. of Engineering and Public Policy, Carnegie Mellon University

26th Annual Conference of the International Association for Energy Economics
Prague, Czech Republic
June 7, 2003
Part 1: Thinking about *Stress* in the Electric Power Sector

- **Definition**
  - Deliberate attack to create panic and political pressure
  - Other socially-created conditions that are not captured by traditional ideas of ‘reliability’

- **NOT**
  - Price shocks in international oil markets
  - Routine equipment failures
  - Weather-related outages
  - “Guards, gates, and guns”
Stress

• Define
  – Conditions outside of “typical” reliability planning assumptions.

• Examples
  – Localized direct conflict damage (e.g. Columbia, or the U.S.)
  – System-wide direct conflict damage (e.g. Bosnia)
  – Inadequate investment/maintenance (e.g. India)
  – Incomplete institutional arrangements (e.g. Palestine)

• Literature
  – scarce
Reliability

- Restoration of power supply from single-point failures under well-defined conditions
- OECD power systems are extremely robust in the face of weather and equipment failures
- Great Northeast Blackout of 1965
- Southern Ontario ice storm of 1998
- 2000 North American Reliability Council (NERC) major incidents
  - 26 due to weather (mostly thunderstorms)
  - 12 operator error or maintenance error
  - 12 equipment failures
  - 2 forest fires (largest – NM, 660,000 people, <4 hours)
Stress is not Weather

• Repeated
• Threats to repair personnel
• Focused on damaging crucial infrastructure
  – Transformers
• High-hazard facilities
  – Dams and locks
  – Nuclear power plants (spent fuel)
  – Cooling towers
  – Electro-magnetic pulse
• Cyber attacks on electronic data collection and control systems (SCADA)
  – Internet-based
• Insider attacks
Institutions for reliability

- Reliability and security are both public goods – role for government
- Institutions that promote reliability
  - State-owned enterprises
  - State public utility commissions
  - Monopoly franchise – incentives for transmission investment
  - NERC
  - EPRI
  - NRC
    - 1999 review: “significant weaknesses” in 27 of 57 facilities
    - Red Team exercises: staff are briefed about timing and detailed plans
    - Nuclear industry pushing for ‘self-regulation’

- What are the institutions that will promote security?
Failure in complex, engineered systems

- Complex systems seem to have more large-scale disruptions than a normal distribution, or even a log-normal distribution, would suggest.

- Failure detection in an unbounded system (incompletely observed) may be slow and difficult.

- Suggests that the only strategy it to accept that vulnerabilities will always exist, that failures (even large ones) will always occur.

- Non-storability and system balancing in electric power systems make this even more problematic
**Survivability offers a coherent framework**

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

Source: Howard Lipson, SEI
Survivability

- Fundamental assumption: No individual component of a system is immune to all attacks, accidents, and design errors.

- Goal: The mission must survive, not any individual component, not even the system itself.

- Contrasts with the ‘fortress’ model of system security – failures can be catastrophic.

- Survivability is an emergent property of a system.

- Contrast to “fortress” model
Example – Traffic Lights

• Major problem during blackouts: traffic accidents
• Backups available
  –  LED lights, solid-state switches, batteries
• “Fortress-type” thinking:
  –  Blackouts will not occur, so don’t plan for operation during them
  –  All loads on the same circuit
  –  Blackouts lead to accidents and create gridlock for police, etc.
• Survivability thinking:
  –  Recognize: open breakers upon power failure
  –  Adapt: operate on battery power
  –  Recover: re-connect when power is restored.

• But who pays?
Restructuring

- Changes (reduces mostly) the role of many reliability institutions
- Incomplete restructuring makes incentives for investment in transmission system unclear
- May result in poor incentives for transmission investment
- Data sharing is problematic
- Key issue – WHO PAYS FOR SECURITY?
- Must be resolved before security issues can be resolved.
Part 2: Analysis of Stress

• How do different system architectures affect reliability and survivability?
  – Large central generation
  – Distributed generation

• How do sensitivities change?

• What are the costs?

• Possible advantages of DG
  – Law of large numbers in generation
  – Less reliance on electricity T&D
  – Fuel switching
  – Advantages of gas T&D
    • Underground
    • Storage
    • Operational simplicity
Method

- Stochastic reliability model using IEEE Test System
  - Modify to include DG
  - Modify to represent stress (Stress Adjustment Factor – SAF)

- Cost model to estimate the costs of energy supply, outages

- Gas T&D
- Mixed architectures
- Heterogeneity of local loads
- Power flows
## System Architectures

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Number of Units</th>
<th>Unit Sizes (MW)</th>
<th>Total Capacity (MW)</th>
<th>Capacity Reserve (percent)</th>
</tr>
</thead>
<tbody>
<tr>
<td>C (Centralized System)</td>
<td>32</td>
<td>12-400</td>
<td>3,405</td>
<td>19.5</td>
</tr>
<tr>
<td>DG0 (Minimum System)</td>
<td>5700</td>
<td>0.5</td>
<td>2,850</td>
<td>0</td>
</tr>
<tr>
<td>DG5</td>
<td>5985</td>
<td>0.5</td>
<td>2,992</td>
<td>5</td>
</tr>
<tr>
<td>DG10</td>
<td>6270</td>
<td>0.5</td>
<td>3,135</td>
<td>10</td>
</tr>
<tr>
<td>DG15</td>
<td>6555</td>
<td>0.5</td>
<td>3,277</td>
<td>15</td>
</tr>
<tr>
<td>DG20 (Match Centralized)</td>
<td>6840</td>
<td>0.5</td>
<td>3,420</td>
<td>20</td>
</tr>
</tbody>
</table>
Loss of Energy Expectation

Loss of Energy Expectation as a Function of Stress

Loss of Energy Expectation (MWh/yr) vs Stress Adjustment Factor (applied to all unit unavailabilities)
Thanks to

- UC Berkeley, Committee on Research
- Carnegie Mellon Electricity Industry Center

www.cmu.edu/electricity

References


