Electric Power: Cyber and Electromagnetic Security Issues

George H Baker, James Madison University
Electric Power: Cyber and Electromagnetic Security Issues

Presentation to the Commonwealth of Virginia Energy & Sustainability Conference (COVES)
18 October 2007

George H. Baker
Institute for Infrastructure and Information Assurance
James Madison University
Outline

• Backdrop
• State of the Electrical Grid
• Cyber and Electromagnetic Threats
• Elements of Preparedness
Backdrop

- Electric Power is arguably the most critical infrastructure we have
  - Ubiquity
  - Immediacy of system failure effects

- Deregulation
  - Demand increasing, supply stagnant
  - R&D/innovation lagging
  - Growth in use of internet for system control

- Incomplete understanding of interdependencies

- New concerns re. large scale outages
  - Natural hazards
  - Control system hacking
  - Terrorist interest in infrastructure
  - High altitude nuclear weapon effects
Grid Capacity Margin Cut More than 50% Since 1982

→ System crashes more easily and frequently during
  - Demand surges
  - Supply failures induced by natural hazards or intentional damage
Power Outages on the Increase

Increasing frequency and size of US power outages 100 MW or more (1991-1995 versus 1996-2000), affecting 50,000 or more consumers per event.

Data courtesy of NERC’s Disturbance Analysis Working Group database

Source: Massoud Amin, University of Minnesota
Industry R&D Expenditures


Electric, Gas and Sanitation Services

*R&D expenditures as % of net sales

Source: Massoud Amin, University of Minnesota
Capital Invested in Grid as % of Revenues

Sources: Electric Utility Industry Statistics; Financial Review, Edison Electric Institute
University of Minnesota Institute of Technology
### U.S. Transmission Line Investment Lagging

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>New Zealand</td>
<td>22.0</td>
<td>1</td>
</tr>
<tr>
<td>England &amp; Wales (NGT)</td>
<td>16.5</td>
<td>1</td>
</tr>
<tr>
<td>Denmark</td>
<td>12.5</td>
<td>2</td>
</tr>
<tr>
<td>Spain</td>
<td>12.3</td>
<td>1</td>
</tr>
<tr>
<td>The Netherlands</td>
<td>12.0</td>
<td>1</td>
</tr>
<tr>
<td>Norway</td>
<td>9.2</td>
<td>1</td>
</tr>
<tr>
<td>Poland</td>
<td>8.6</td>
<td>1</td>
</tr>
<tr>
<td>Finland</td>
<td>7.2</td>
<td>1</td>
</tr>
<tr>
<td>United States</td>
<td>4.6</td>
<td>450</td>
</tr>
</tbody>
</table>

Source: IEEE PES, 2006
Perceived Cyber Threats to Power System Controls

Source: Massoud Amin, University of Minnesota
Cyber Attacks May Be Used to Cause Physical Damage

2007 Idaho National Laboratory Experiments

- Remote cyber attack on generator control system
- Caused damage to generator that would take months to repair
- Large scale outage conceivable
- Utilities asked to ensure that power control systems cannot be accessed by unauthorized computer operators
- DHS official: A lot of risk has been "taken off the table" since experiment

Large Scale Outage from EMP


- WASHINGTON, D.C. – Congressman Roscoe Bartlett (R-6-MD) participated in a Washington, DC news conference today to release a study that projected the economy in the Baltimore-Washington, DC-Richmond corridor would suffer a blow of between $34 to $770 billion from an electromagnetic pulse (EMP) attack, not including the cost of any infrastructure repairs.

  “EMP is a low risk, but asymmetrical form of devastating attack that would dwarf the scale of the damage from the 9/11 terrorist attack,” said Congressman Bartlett.

- Also participating in the news conference were Chuck Manto, President of Instant Access Networks (IAN), a Frostburg, MD company that commissioned the study…

- Loss estimates based on widespread electric power outage - costs likely higher
  - Estimates of lost revenues – do not include cost to repair grid
  - Affected area can be much larger
Nature and Magnitude of EMP Threats

- EMP is one of a small number of threats that may
  - Hold at risk the continued existence of today’s US civil society
  - Disrupt our military forces and our ability to project military power
- The number of US adversaries capable of EMP attack is greater than during the Cold War
- Potential adversaries are aware of the EMP strategic attack option
- The likelihood of attack depends on the actions we take to be prepared

EMP Coverage for Bursts of Various Heights
- HOB = 500 km
- HOB = 300 km
- HOB = 100 km

- Wide area coverage
  - A million square miles
- Intensity depends on:
  - Weapon design
  - Height of burst
  - Location of burst
- Broad frequency range
- Threat to all exposed electronics
EMP Vulnerability of US Electric Power Infrastructure

- EMP induced functional collapse of the electrical power grid risks the continued existence of US civil society
  - Immediate EM transients likely to exceed capabilities of protective safety relays
  - Late time EMP could induce currents that create significant damage throughout the grid
- National electrical grid not designed to withstand near simultaneous functional collapse
- Procedures do not exist to perform “black start”
  - Restart would depend on telecom and energy transport which depend on power
- Restoration of the National power grid could take months to years
  - Typical 500kV transformer is custom tailored to application
  - Spares are seldom available
  - Manufacturing performed offshore
  - Normal delivery time months to more than a year

Electric power is key to a functioning society and military. EMP induced destruction of power grid components could substantially delay recovery.
Strategy and Recommendations

• Pursue intelligence, interdiction and deterrence to discourage attacks
  – Highest priority is to prevent attacks
  – Make it difficult and dangerous to try
  – Reduce incentive by increasing system protection/resiliency
• Protect critical components of power grid
  – Especially “long lead” replacement components
• Maintain ability to monitor/evaluate condition of system
  – Absence of information can make things worse through inaction
  – Or inappropriate action re. August 13, 2003 Blackout
• Be able to recognize cyber and EMP attacks
  – Alert operators to likely effects
  – How they differ from other disruptions
• Plan to carry out systematic recovery of the power grid and affected infrastructures
  – Demonstrate the will and capacity to recover from any attack

http://empcreport.ida.org
Summary

• Electric power is essential to the functioning of US society
• The system increasingly operates at or near its reliability limits
• The geographic scale of tightly coupled networks makes the system highly susceptible to large scale outages
• More frequent natural and accidental failures portend the possible catastrophes from intentional disruption.
  – A widespread blackout involving physical damage to multiple components may produce a long term outage far exceeding historical experience.
  – Cyber attacks and EMP are high leverage means
• Techniques to prevent attacks and reduce vulnerabilities are available and affordable
• Recovery from large scale outages must be part of the national planning/exercise process