Physical Grid Vulnerabilities

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

February 27, 2013

Dr. John G. Kassakian

The Massachusetts Institute of Technology

Geographic Reach

- Localized attacks similar to common contingencies.
  - Unplanned line/generator outage
  - N-1, N-2 reserve protocols
  - Restoration procedures well documented
- Wide-area assaults more difficult to anticipate/remediate
  - Katrina
  - 1965/2003 blackouts

Restoration/Repair Challenges

- Limited scope
  - Restoration rapid.
  - Time available for repair.
  - Exception may be under-street metropolitan cables.
- Wide-area affected
  - 1965/2003 need was restoration, not repair.
  - Katrina required repair.
    - Restoration on order of weeks/months
    - Repair on order of years

The Transformer Problem

- Large transformers no longer manufactured in U.S.
- Lead times on order of years.
- Spares and suitability are limited.
- Transport requires unique equipment, detailed routing, and is slow.

Unit Transformer on a Schnabel Car

Source: Consumers Power

Another Schnabel Car Example

Source: Raimond Spekking

Stator Being Loaded on Schnabel Car

Source: Carl Youman

Operational Intrusion

- System collapse
  - Scope can be limited.
    - New technology (e.g., synchrophasor network).
    - New system topology (e.g., islands with dc interties).
- Physical damage
  - Due to misoperation of relays/generators/SCADA systems.
- Prevention responsive to cybersecurity measures.

Physical Intrusion

- NERC audits.
- Can be uncoordinated and limited.
  - Most likely in dispersed parts of system
    - Lines, substations.
  - Treated as single contingency.
  - Propagation circumscribed.

Physical Intrusion (cont'd)

- Can be coordinated and widespread
  - Communication and action protocols critical.
  - Rapid identification of event.
  - Creates human and equipment resource problem.
  - Extensive and prolonged social disruption.
  - Most debilitating if transformers involved.
  - Greatest vulnerability is multiple substations.

50 kV/10 kV Substation
(Innsbruck)

Source: www.e-architect.co.uk

Substation/Switchyard

Source: www.rtcmagazine.com

Switchyard

Source: www.firstelectricnewspaper.com

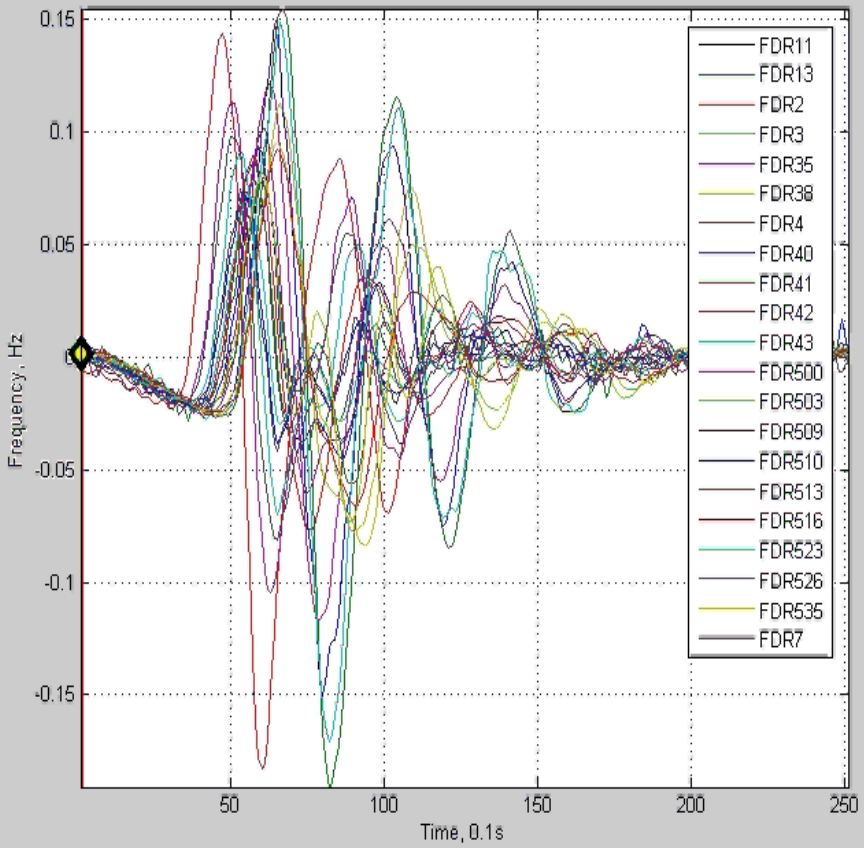
Terrorism by Electromagnetic Pulse

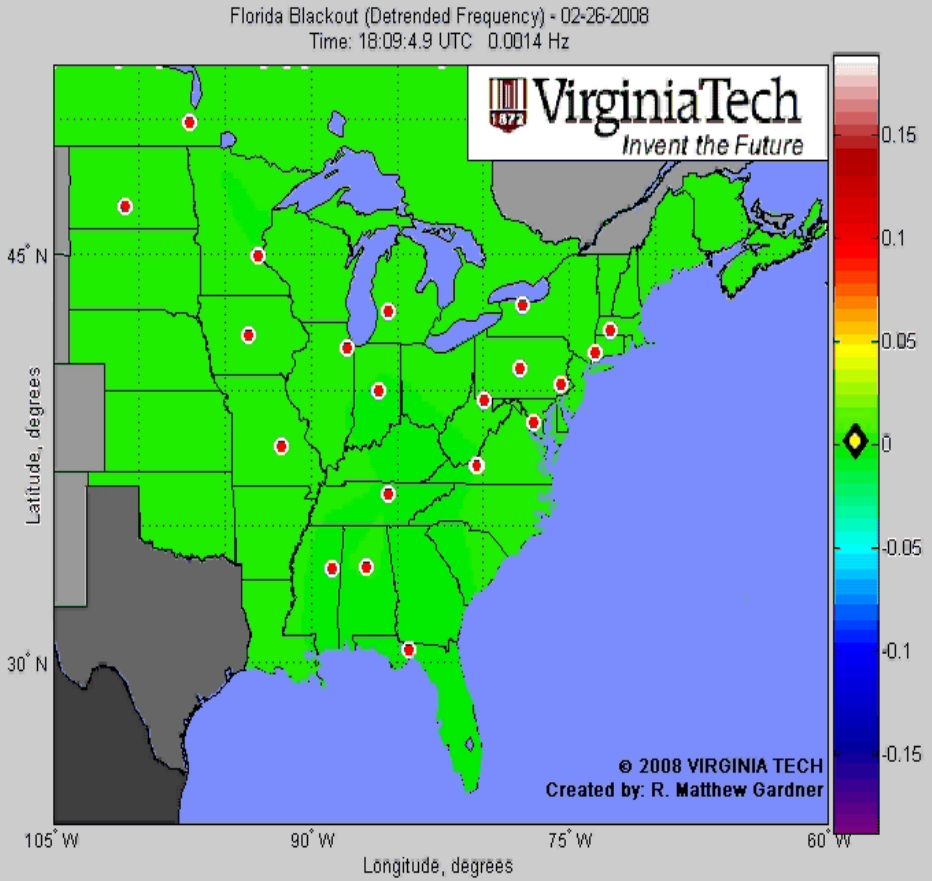
- EMP has potential for massive disruption.
  - Electronics vector of high vulnerability.
    - Loss of sensing, data exchange, control, SCADA.
    - Loss of infrastructure, e.g., transport, fuel.
  - Large quasi-dc fields can cause extensive heavy equipment damage.
- Potential demonstrated by geomagnetic storms.
  - Solar flares.
  - Causal but limited damage.

Sequence of 1989 HQ GMD Event

- 02:44:17 Tripping of static VAR compensator CLC 12 at Chibougamau.
- 02:44:19 Tripping of static VAR compensator CLC 11 at Chibougamau.
- 02:44:33 to 02:44:46 Shutdown of the four SVCs at the Albanel and Nemiscau substations.
- 02:45:16 Tripping of static VAR compensator CLC 2 at La Verendrye.
- 02:45:24.682 Tripping of line 7025 at the Jacques Cartier substation.
- 02:45:24.936 Tripping of line 7044 at the La Verendrye substation.
- 02:45:24.948 Tripping of line 7016 at the La Verendrye substation.
- 02:45:24.951 Tripping of line 7026 at Chamouchouane substation.
- 02:45:24.978 Tripping of line 7045 at the Grand-Brule and La Verendrye substations.
- 02:46:00 HQ system down.

The 2008 Florida Blackout





Mitigation Approaches

- Reserve capacity
- Spares
- Hardening of electronics
- Perimeter security
- Islanding thru dc interconnects

Conclusions

- Geographically limited intrusion:
  - manageable.
- Wide-area operational intrusion:
  - responsive to cybersecurity measures.
- Wide-area physical intrusion:
  - Approach is response vs. prevention.
  - Standard communication network and protocols essential.
  - Situational awareness and response through synchrophasor network could mitigate damage.

Loaded Stator

Source: Carl Youman