Bulk Power Risk Analysis: Ranking Infrastructure Elements According to their Risk Significance

George E. Apostolakis
Massachusetts Institute of Technology
apostola@mit.edu

Presented at PSAM 9
Hong Kong
May 19, 2008
Methodology Overview:

Infrastructure Elements Analysis

Power Flow Modeling
MTTF & MTTR

Element Ranking

Value Tree

Overall Value to the Stakeholder

Impact Categories

Economics
Image
Health and Safety
Environment

Performance Measures

Lost Revenue
Repair / Replace
Public
Customer
Political
General Public
Utility Workers
Fauna

Physical Consequences

Analysis
Power Flow Modeling
MTTF & MTTR

Value

Impact Categories

Performance Measures

Overall Value to the Stakeholder

Element Ranking

Infrastructure Elements
IEEE RTS-96 Network

- 24 buses
- 10 Generation Sites
- 17 Load Sites
- 38 Transmission Lines

Customer Groups
- Residential
- Commercial
- Small – Medium Industrial
- Large Industrial
Infrastructure Analysis

RTS – 96 DATA

Load Data
Generation Data
Line Data
Repair Times
Failure Rates

Sandia Power Flow Simulation Model

AC load flow model determines the effects a failed component has on the system.

Load Shed Vector

Used to determine the physical consequences that serve as input into the risk assessment methodology.

- The physical consequence of a scenario is the combination of outage duration along with the number of customers affected in each customer group.
## Stakeholders

<table>
<thead>
<tr>
<th>Stakeholder</th>
<th>Organization</th>
</tr>
</thead>
<tbody>
<tr>
<td>S-1</td>
<td>Management Division</td>
</tr>
<tr>
<td>S-2</td>
<td>Transmission Department</td>
</tr>
<tr>
<td>S-3</td>
<td>Transmission Department</td>
</tr>
<tr>
<td>S-4</td>
<td>Management Division</td>
</tr>
<tr>
<td>S-5</td>
<td>Transmission Department</td>
</tr>
</tbody>
</table>
Value Tree with Weights
(Stakeholder S-1)

Value

Impact Categories

Performance Measures

Overall Value to the Stakeholder

Economics
(2)
0.2441

Image
(1)
0.5058

Health and Safety
(3)
0.1667

Environment
(4)
0.0834

Lost Revenue
(2)
0.2092

Repair / Replace
(7)
0.0349

General Public
(8)
0.0333

Utility Workers
(3)
0.1334

Public
(6)
0.0388

Customer
(4)
0.0977

Political
(1)
0.3693

Fauna
(5)
0.0834
Prioritization Methodology

• Performance Index (expected disutility)

\[
\overline{PI}_j = \sum_{i}^{K_{pm}} w_i \overline{d}_{ij}
\]

- $\overline{PI}_j$: expected performance index for vulnerability $j$
- $w_i$: weight of the performance measure $I$
- $\overline{d}_{ij}$: expected disutility of performance measure $i$ for vulnerability $j$
- $K_{pm}$: number of performance measures

- For random failures, expected values will be calculated.
- For malevolent acts, they will not.
Results (S-1)
(random failures)
## Vulnerability / Risk Categories

<table>
<thead>
<tr>
<th>Category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>I (Red)</td>
<td>This category represents a severe vulnerability in the infrastructure. It is reserved for the most critical locations that are highly susceptible to attack. Red vulnerabilities may require the most immediate attention.</td>
</tr>
<tr>
<td>II (Orange)</td>
<td>This category represents the second priority for counter-terrorism efforts. These locations are generally moderately to extremely valuable and moderately to extremely susceptible.</td>
</tr>
<tr>
<td>III (Yellow)</td>
<td>This category represents the third priority for counter terrorism efforts. These locations are normally less vulnerable because they are either less susceptible or less valuable than the terrorist desires.</td>
</tr>
<tr>
<td>IV (Blue)</td>
<td>This category represents the fourth priority for counter terrorism efforts.</td>
</tr>
<tr>
<td>V (Green)</td>
<td>This is the final category for action. It gathers all locations not included in the more severe cases, typically those that are low (and below) on the susceptibility scale and low (and below) on the value scale. It is recognized that constrained fiscal resources are likely to limit efforts in this category, but it should not be ignored.</td>
</tr>
</tbody>
</table>
Results (S-1)  
(malevolent acts)
Insights (S-1)

• Transmission lines appear as the top ranked components with respect to both random failures and malevolent acts. This is due to the usually more wide-spread consequences resulting from failures of transmission lines. Their high level of susceptibility is also a key factor.

• Due to their lower Forced Outage Rates and low susceptibility levels, generators are not present in the higher levels of the expected disutility and vulnerability rankings. They are all placed within the Blue or Yellow vulnerability categories.

• Buses do not appear in the upper rankings of random failures because of their very low failure frequencies.

• Buses appear in the vulnerability rankings as Orange vulnerabilities and below because of their large consequences and moderate susceptibility.
Conclusions

• All stakeholders share T-7, T-16, and T-17 within their top five components for vulnerability rankings. All but S-2 complete their top five vulnerabilities with B-17 and B-20.

• *Lost Revenue* and *Customer Image* remain the dominant factors determining a failure scenario’s value even for the stakeholders that ranked Health & Safety as the #1 impact.

• All stakeholders share the top 10 components for random failure events with very few differences in the component ordering. This is due to transmission lines having both relatively short durations and higher failure frequencies.