Department of Nuclear Science & Engineering

# Risk and Decision Analysis in Infrastructure Protection

**George E. Apostolakis**

**Massachusetts Institute of Technology**

**apostola@mit.edu**

**Presented at the 3rd International Workshop on Critical Information Infrastructure Security (CRITIS '08)**
**Frascati (Rome), Italy**
**October 13-15, 2008**

# Risk Analysis for Technological Systems

- **Probabilistic Risk Assessment (PRA) answers the following questions:**
  - **What can go wrong? (accident sequences or scenarios)**
  - **How likely are these scenarios?**
  - **What are their consequences?**

- **PRA supports risk management by:**
  - **Identifying accident scenarios**
  - **Ranking these scenarios according to their frequency of occurrence**
  - **Ranking systems, structures, and components according to their risk significance.**

# Observations on Infrastructures

- **Large, diffuse, inter-connected networks, as opposed to well defined systems such as nuclear power plants and the International Space Station.**

- **Difficult to analyze using top-down conventional mathematical theories, such as Probabilistic Risk Assessment.**

- **The consequences of "what can go wrong" (the PRA "end states") are multidimensional and not limited to health and safety.**

# The Needs

- **Risk managers need to identify and rank vulnerabilities in infrastructure systems**
- **The analysis must include:**
  - **The capacity of the system's elements**
  - **The influence of the Mean Time To Repair (MTTR) on the vulnerability**

# Objective

- To rank the elements of an infrastructure according to their risk value for "random" failures or their vulnerability to terrorism (dual benefit).
- In both cases, the value of the element to the Decision Maker (DM) and the relevant Stakeholders (SHs) is assessed using a value tree and disutility functions.
- For random failures, the expected disutilities are the basis for ranking the infrastructure elements. This decision rule is borrowed from Multiattribute Utility Theory (MAUT), the only normative decision-making theory.
- For malevolent acts, probabilities of attack are difficult to evaluate. The element's value is combined with its susceptibility to attack to develop a vulnerability ranking.

# The Case Studies

- **Specific Assets**
  - Six buildings on the MIT campus
  - Three infrastructures (electric power, water, natural gas)
  - Binary logic for the elements
  - Critical locations identified via minimal cut sets
- **A Town**
  - Water infrastructure of a European city
  - Network's capacity and time included.
- **Bulk Electric Power Grid**
  - Test grid: IEEE 1996 Reliability Test System (RTS-96)
  - Grid's capacity and time included
- **Small Community (MIT Campus)**
  - Identification of critical locations using importance measures
  - Multi-hazard evaluations
- **In all cases**
  - An objectives hierarchy (value tree) is developed with the DM and SHs
  - The threat is assumed to be minor.

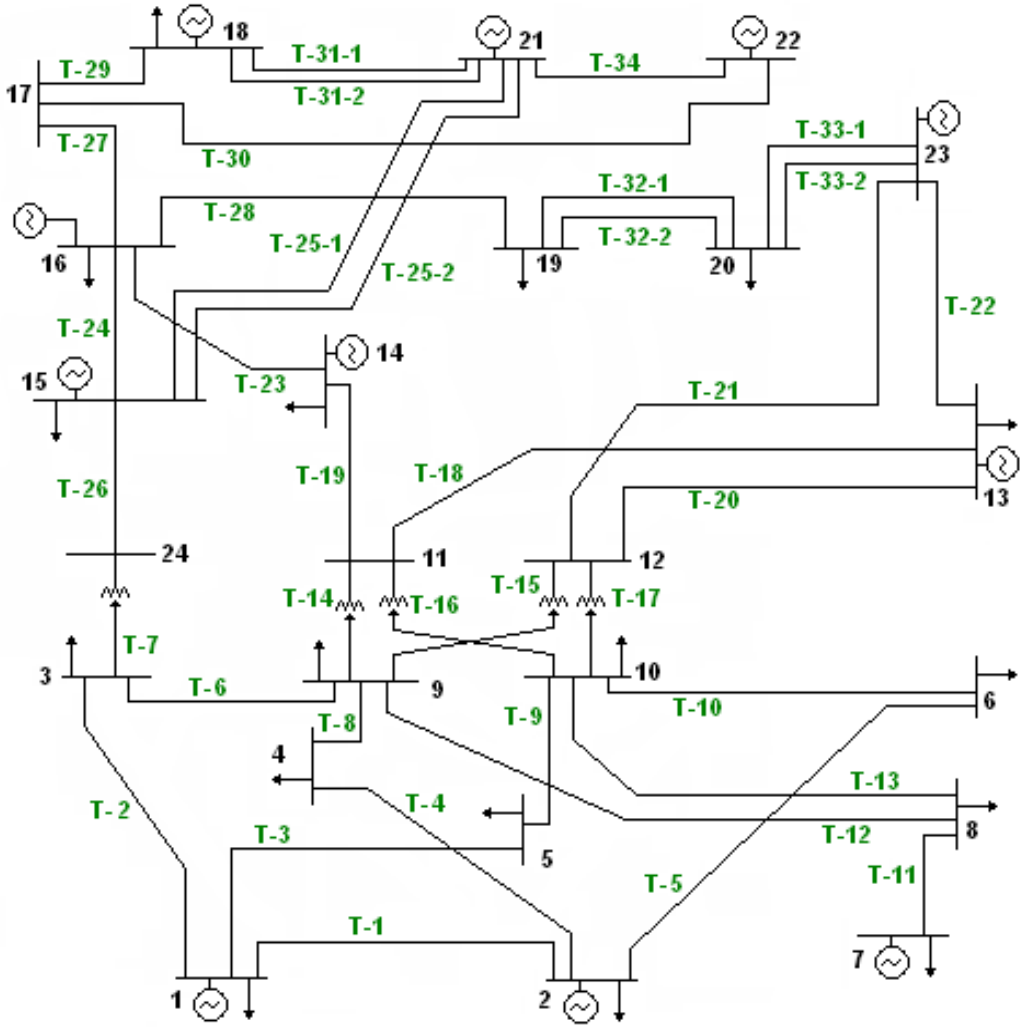
# Proposed Approach

- **Assess the value of each element of the system by combining MAUT with a "brute force" approach to evaluate the consequence of losing this element on the overall system's ability to accomplish its mission**

- **For random failures**
  - **Rank the elements according to their expected value**

- **For malevolent acts:**
  - **Assess the susceptibility of each element to the threat**
  - **Aggregate value and susceptibility to assess vulnerability**
  - **Rank the elements according to their vulnerability**

# Case Study: IEEE RTS-96 Network

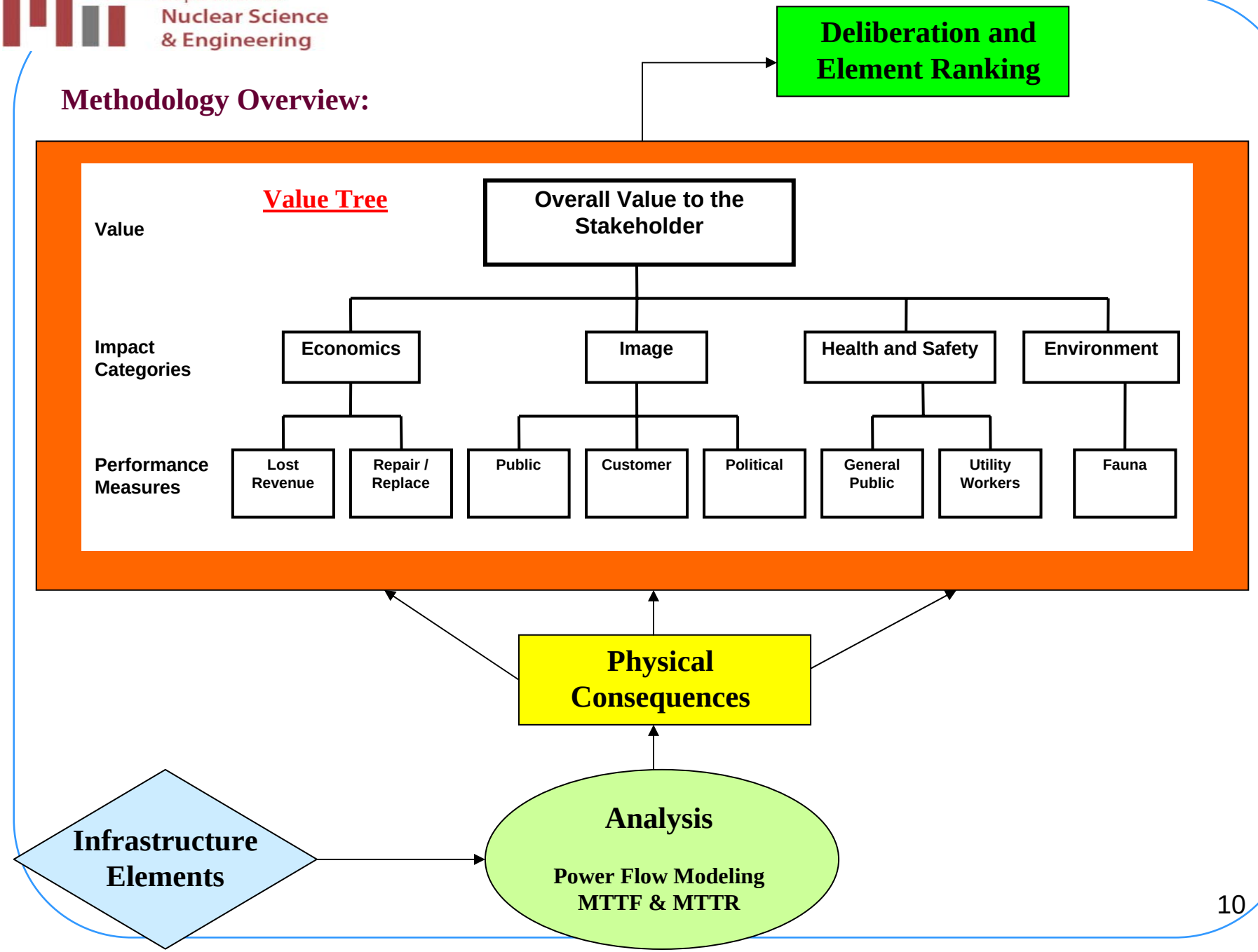



- 24 buses
- 10 Generation Sites
- 17 Load Sites
- 38 Transmission Lines
- Customer Groups
  - Residential
  - Commercial
  - Small – Medium Industrial
  - Large Industrial

# Stakeholders

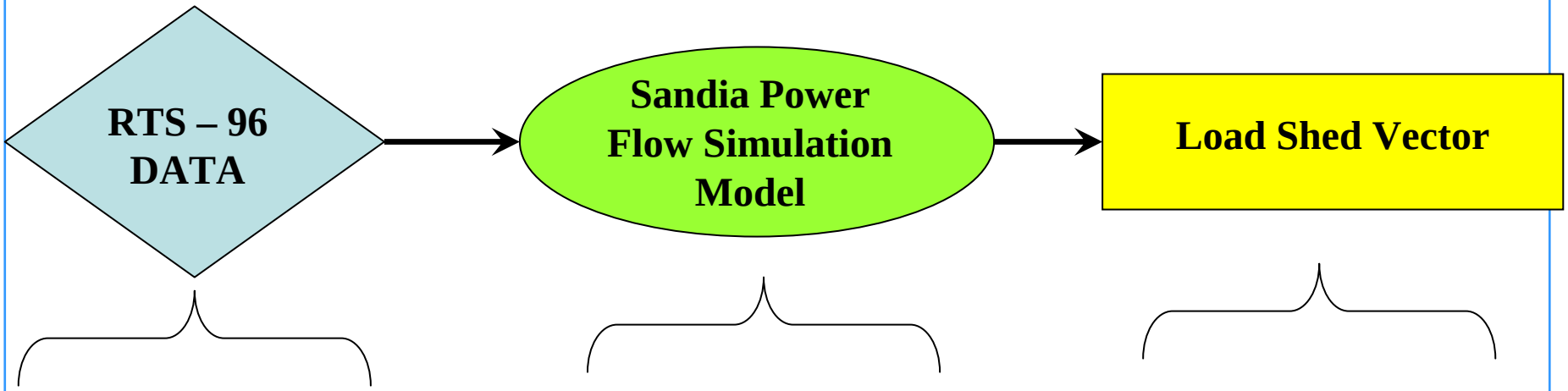
| Stakeholder | Organization |
|---|---|
| S-1 | Management Division |
| S-2 | Transmission Department |
| S-3 | Transmission Department |
| S-4 | Management Division |
| S-5 | Transmission Department |

## Methodology Overview:



Department of Nuclear Science & Engineering

# Infrastructure Analysis




**Load Data**
**Generation Data**
**Line Data**
**Repair Times**
**Failure Rates**

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

**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.**

Department of Nuclear Science & Engineering

# Example load shed vector (Transmission line T-4)

| Bus | Load Shed Vector | Residential | Commercial | S – M Industrial | Large Industrial |
|---|---|---|---|---|---|
| 2 | 0.10 | 3,580 | 569 | 26 | 0 |
| 3 | 0.10 | 8,320 | 680 | 94 | 0 |
| 4 | 0.10 | 1,392 | 600 | 35 | 0 |
| 6 | 0.10 | 6,093 | 558 | 69 | 0 |
| 7 | 0.10 | 48,470 | 6850 | 395 | 0 |
| Total | | 67,855 | 9,257 | 619 | 0 |

- The duration of transmission line T-4 being out of service is assumed to be 10 hours.

Department of Nuclear Science & Engineering

# Stakeholder S-1 Input (Analytic Hierarchy Process)

**Instructions:**
1. Compare the two items listed; circle the item that you feel is the most important.
2. Indicate how much more important the circled item is using the scale provided:
   1 – equally  3 – weakly  5 – moderately  7 – strongly  9 – extremely
   Use even numbers to indicate importance between these increments.

## Impact Categories

1. Economic vs. Image — 4
2. Economic vs. Health & Safety — 2
3. Image vs. Health & Safety — 2
4. Environment vs. Economic — 4
5. Environment vs. Health & Safety — 2
6. Environment vs. Image — 4

## Economics:

1. Lost Revenue vs. Repairs — 6

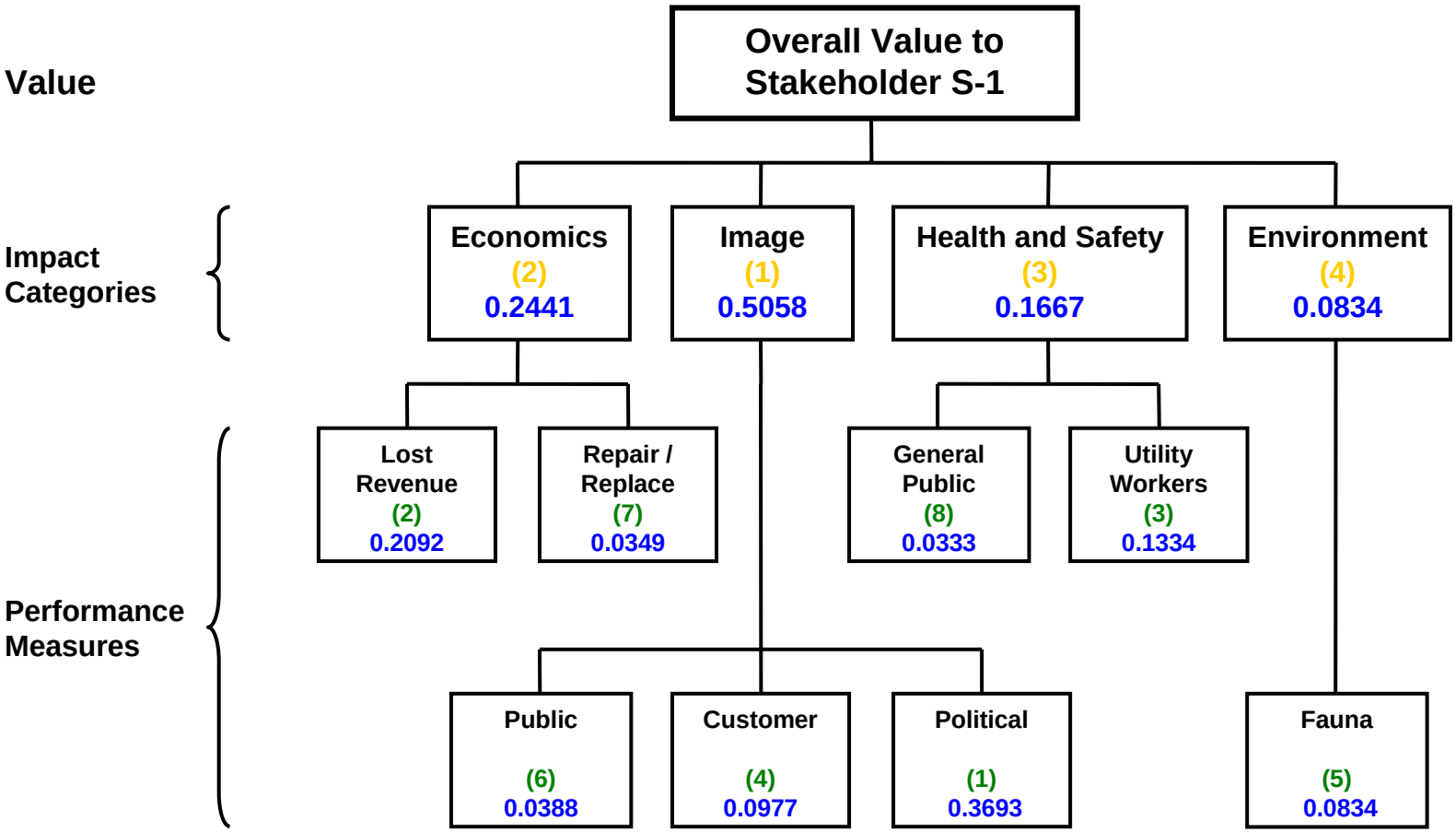
## Image:

1. Public vs. Customer — 4
2. Public vs. Political — 6
3. Customers vs. Political — 6

## Health & Safety:

1. General Public vs. Utility Worker — 4

# Value Tree with Weights (Stakeholder S-1)



# Stakeholder Weights and Rankings

| Stakeholder | Economics | Image | Heath & Safety | Environment |
|---|---|---|---|---|
| S-1 | 0.2441 (2) | 0.5058 (1) | 0.1667 (3) | 0.0834 (4) |
| S-2 | 0.2849 (2) | 0.4935 (1) | 0.1645 (3) | 0.0570 (4) |
| S-5 | 0.1991 (2) | 0.0427 (4) | 0.6504 (1) | 0.1078 (3) |
| S-4 | 0.1088 (3) | 0.0405 (4) | 0.5139 (1) | 0.3368 (2) |
| S-3 | 0.0614 (4) | 0.1487 (3) | 0.4954 (1) | 0.2946 (2) |

# Constructed Scale for *Public Image*

| Level | Constructed Scale | Disutility | Weighted Disutility |
|---|---|---|---|
| 4 | International media interest | 1.0000 | 0.0388 |
| 3 | Repeated publications in national media | 0.4862 | 0.0189 |
| 2 | Repeated publications in local media, appearance in national media | 0.1873 | 0.0073 |
| 1 | Single appearance in local media | 0.0501 | 0.0019 |
| 0 | No Impact | 0.0000 | 0.0000 |

# *Public Image* PM

| Level | Description | Residential | | |
|---|---|---|---|---|
| | | *10 hours* | *1 day* | *1 week* |
| 4 | International media interest | 1,000,000 | 1,000,000 | 500,000 |
| 3 | Repeated publications in national media | 500,000 | 500,000 | 100,000 |
| 2 | Repeated publications in local media, appearance in national media | 10,000 | 10,000 | 500 |
| 1 | Single appearance in local media | 500 | 500 | 100 |
| 0 | No Impact | 0 | 0 | 0 |

**67,855 Residential Customers for 10 hours.**

Department of Nuclear Science & Engineering

# PM Impacts
# (S-1 and Transmission Line T-4)

| PM | Level | Disutility | Weighted Disutility |
|---|---|---|---|
| Lost Revenue | 3 | 0.1761 | 0.0368 |
| Repair / Replace | 2 | 0.0687 | 0.0024 |
| Public Image | 2 | 0.1873 | 0.0073 |
| Political Image | 0 | 0.0000 | 0.0000 |
| Customer Image | 3 | 0.3317 | 0.0324 |
| General Public | 0 | 0.0000 | 0.0000 |
| Utility Workers | 1 | 0.0707 | 0.0094 |
| Fauna | 0 | 0.0000 | 0.0000 |

# 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.**

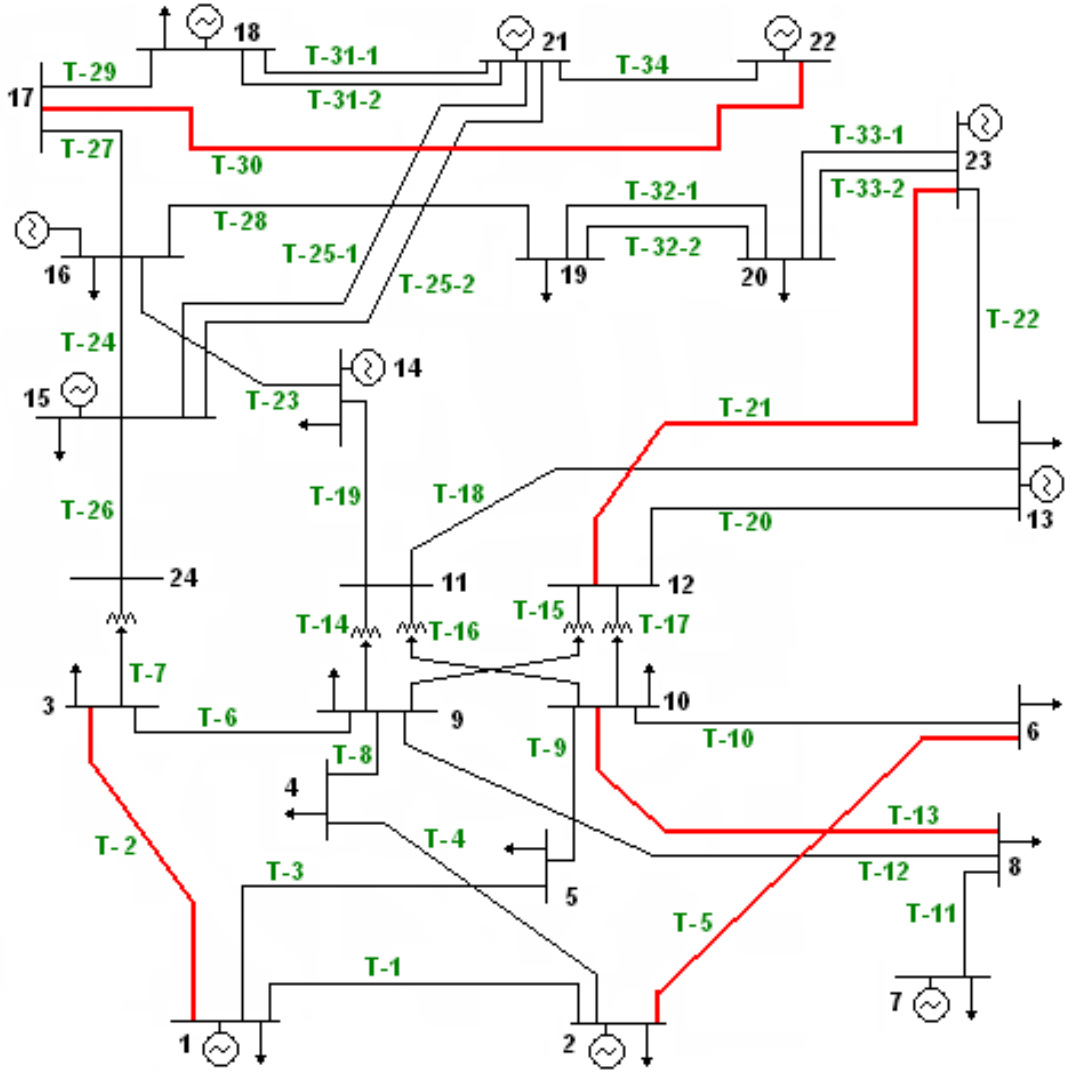
# Performance Index for Transmission Line T-4 (Random Failures)

| PM | Level | Disutility | Weighted Disutility |
|---|---|---|---|
| Lost Revenue | 3 | 0.1761 | 0.0368 |
| Repair / Replace | 2 | 0.0687 | 0.0024 |
| Public Image | 2 | 0.1873 | 0.0073 |
| Political Image | 0 | 0.0000 | 0.0000 |
| Customer Image | 3 | 0.3317 | 0.0324 |
| General Public | 0 | 0.0000 | 0.0000 |
| Utility Workers | 1 | 0.0707 | 0.0094 |
| Fauna | 0 | 0.0000 | 0.0000 |
| Failure Frequency | 0.39 outage/yr | PI | 0.0883 |
| | | $\overline{\text{PI}}$ | 0.0345 |

# Results (S-1)
# (random failures)

| Component | PI | $\overline{\text{PI}}$ |
|---|---|---|
| T – 13 | 0.1833 | 0.0806 |
| T – 5 | 0.1055 | 0.0506 |
| T – 30 | 0.0883 | 0.0477 |
| T – 21 | 0.0883 | 0.0459 |
| T – 2 | 0.0883 | 0.0451 |

# Results (S-1)
# (random failures)



# Susceptibility Categories (Malevolent Acts)

| Level | Description |
|---|---|
| 5 – Extreme | Completely open, no controls, no barriers |
| 4 – High | Unlocked, non-complex barriers (door or access panel) |
| 3 – Moderate | Complex barrier, security patrols, video surveillance |
| 2 – Low | Secure area, locked, complex barrier |
| 1 – Very Low | Guarded, secure area, locked, alarmed, complex closure |
| 0 – Zero | Completely secure, inaccessible |

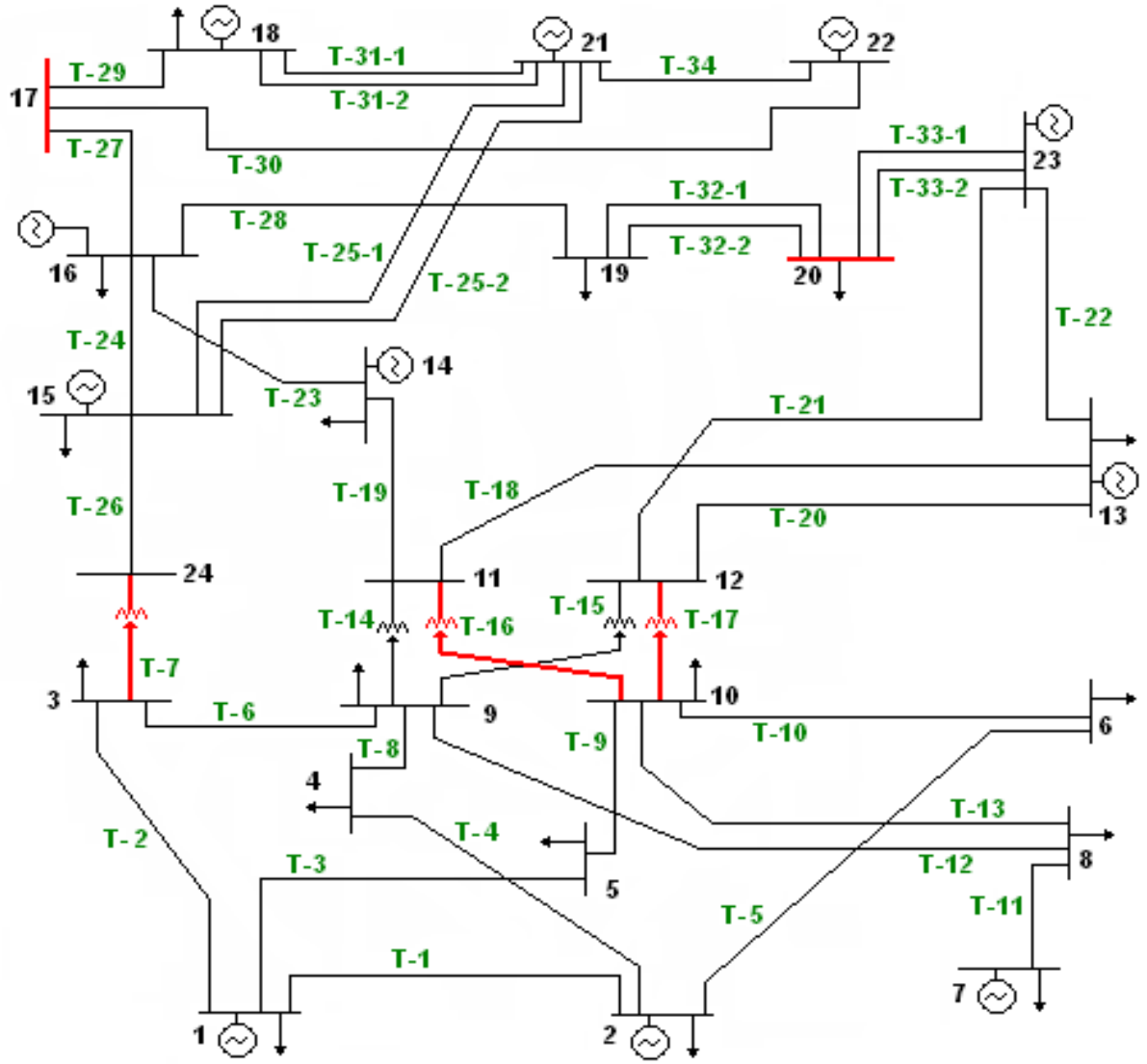
# Vulnerability / Risk Categories

| Category | Description |
|---|---|
| I (Red) | 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. |
| II (Orange) | This category represents the second priority for counter-terrorism efforts. These locations are generally moderately to extremely valuable and moderately to extremely susceptible. |
| III (Yellow) | 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. |
| IV (Blue) | This category represents the fourth priority for counter terrorism efforts. |
| V (Green) | 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. |

# Results (S-1)
# (malevolent acts)

| Component | PI | Vulnerability Category |
|---|---|---|
| T – 16 | 0.4021 | I |
| T – 17 | 0.4021 | I |
| T – 7 | 0.2583 | I |
| B – 17 | 0.2246 | II |
| B – 20 | 0.2246 | II |

# 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.**
- **The amount of load shed alone does not determine the order in which the components are ranked. The high susceptibility level (extreme) and higher failure frequencies of the transmission lines are the key factors that elevated them in the rankings above the other types of components even though the amount of load is usually smaller.**

# References


- Apostolakis, G.E., and Lemon, D.M., "A Screening Methodology for the Identification and Ranking of Infrastructure Vulnerabilities due to Terrorism," *Risk Analysis,* 25:361-376, 2005.
- Koonce, A.M., Apostolakis, G.E., and Cook, B.K., "Bulk Power Grid Risk Analysis: Ranking Infrastructure Elements According to their Risk Significance," *International Journal of Electrical Power and Energy Systems,* 30:169-183, 2008.
- Li, H., Apostolakis, G.E., Gifun, J., VanSchalkwyk, W., Leite, S., and Barber, D., "Ranking the Risks from Multiple Hazards in a Small Community," *Risk Analysis*, accepted for publication, 2008.
- Michaud, D., and Apostolakis, G.E., "Methodology for Ranking the Elements of Water-Supply Networks," *Journal of Infrastructure Systems,* 12:230-242, 2006.
- Patterson, S.A., and Apostolakis, G.E., "Identification of Critical Locations across Multiple Infrastructures for Terrorist Actions," *Reliability Engineering and System Safety*, 92:1183-1203, 2007.