SAND2009-2971C

Consequence Analysis

Bryan T. Richardson
Senior Member of Technical Staff
Critical Infrastructure Systems
Sandia National Laboratories

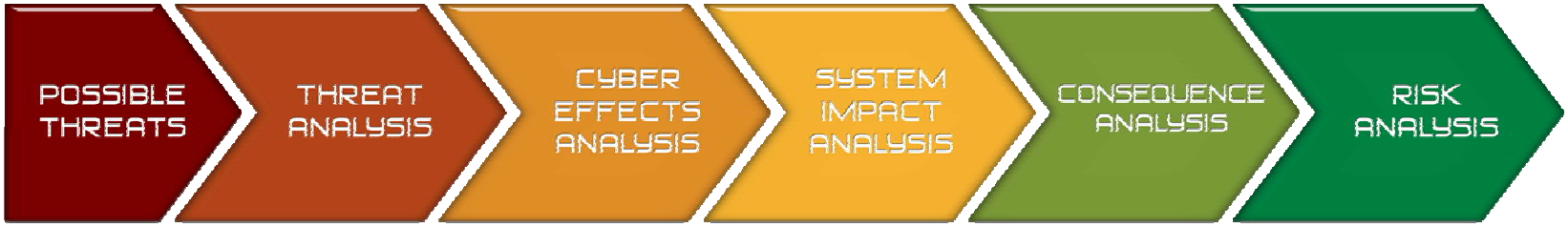
btricha@sandia.gov
(505) 845-2386

NSTB
National SCADA Test Bed

Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company, for the United States Department of Energy under contract DE-AC04-94AL85000.

NNSA National Nuclear Security Administration
Sandia National Laboratories

Threat to Consequence Framework



- How can cyber attack result in electrical outages?
- Might particular cyber vulnerabilities result in significant impacts?
- Are there scenarios for cyber attack that would cause high grid impacts that we were previously unaware of?
- How can we prioritize cyber security mitigation to reduce potential impacts?
- What dynamic impacts can tampering of control systems have on an electric power grid?
- What are the most attractive control system parameters to an adversary for a significant electrical impact?

Consequence Analysis

- Are the consequences quantifiable in a way that is relevant to the stakeholder's business/operational roles?
- What are the consequences of the impacts in terms of the stakeholder's business/operational roles?
- What infrastructure components need to be protected the most?
- Where could mitigations be implemented to lower the consequences?

What is Consequence?

- **In terms of the Threat to Consequence Framework, consequence is the higher-level result of an operational impact.**
  - The consequence of losing an electric power generator (the impact) could be lost revenue or a diminished public image.
  - The consequence of losing an electric transmission line (the impact) could be causalities or increased government oversight.
- **How one defines these higher-level results depends on the metrics most relevant to the business and/or operational roles.**

Consequence Metrics

- Some are readily quantified
  - Casualties
  - Economic loss
- Others... not so much
  - Psychological Impacts
  - Confidence in Government
  - Loss of Governance
- Even the readily quantified require clear definition
  - Casualties: Deaths? Injuries? Both?
  - Economic loss: Over what time frame?
- Combination of the readily quantified can be a nightmare
  - How much is a life worth? Are you willing to commit it to print?

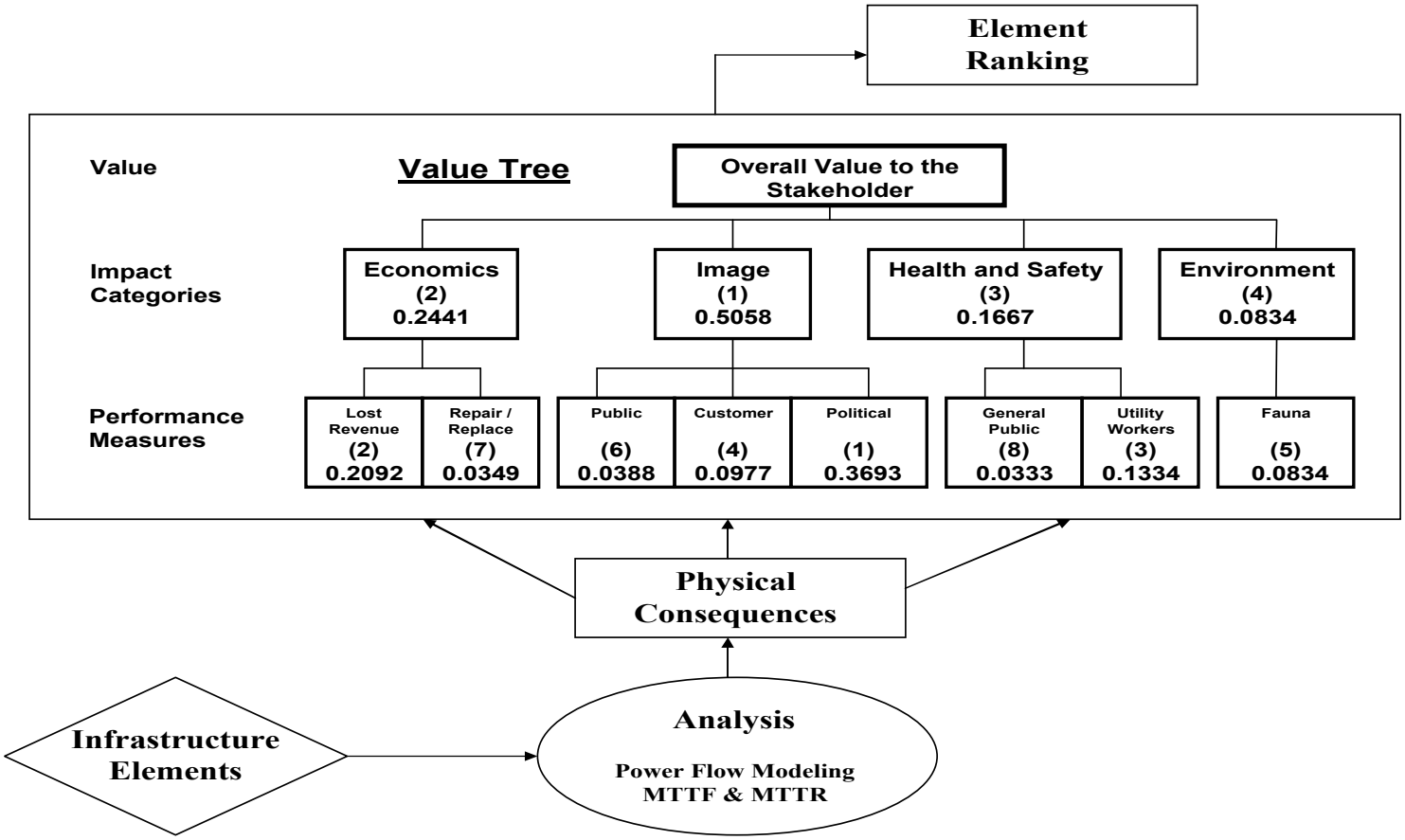
Overview of Consequence Estimation

- **Stakeholders have a need to base consequence on metrics they care about**
  - Economics, public image, health and safety, etc.
- **Physical impacts must somehow be mapped to metrics**
- **Metrics most likely will not be equally important to everyone and in every situation**
  - Can use pairwise comparison techniques to weigh metrics
- **As impacts occur, metrics and specific system data can be used to calculate a numerical value (the performance index) for consequence**
- **Metrics can also highlight areas of concern within the system that mitigations could be applied to**

Approach for Consequence Estimation

- **Utilize value tree analysis to:**
  - Identify the consequence to the stakeholder
    - In the case of Consequence Analysis, the desired consequence of an impact is always zero.
  - Clarify the consequence's meaning with more specific Impact Categories (IM)
  - Describe each Impact Category with one or more Performance Measures (PM) that can be directly associated with an impact
- **Given metrics of concern, develop a value tree that describes these metrics**
  - Metrics can most often be used as a PM directly
  - Similar PMs are grouped into IMs
  - Pair-wise comparison is then used to assign a numerical value to each IM and PM

Example Consequence Value Tree



Sandia National Laboratories

Constructed Scales

- **Once the value tree has been developed, Constructed Scales (CS) can be used to associate Performance Measures (PM) with an impact**
  - Constructed Scales define how much to scale a particular Performance Measure due to an impact
  - Constructed Scales are in terms of the Performance Measure they belong to
    - For example, each level of a CS for a Lost Revenue PM would be in terms of dollars
  - An impact must be definable in these terms as well, and must already be known
    - For example, losing a generator might lead to loss of an industrial load, which would cost X amount of dollars due to contract penalties
- **Constructed Scales can be considered the 'linkage' between an impact and the value tree analysis of that impact**

Expected Disutility

- ***Expected Disutility* describes the likelihood of an impact occuring due to random failures**
  - Given an impact scenario, the expected disutility is calculated by multiplying the frequency of the failure scenario by the scenario's performance index.
- **The expected disutility is based on random failure values for physical system components (historical data)**
- **Knowing the expected disutility of different failure scenarios enables the different scenarios to be ranked, and also helps to identify areas of improvement.**
  - If a particular failure scenario has a very high expected disutility, one might focus efforts on how to lower the random failure value(s) for that particular scenario.

Vulnerability Levels

- ***Vulnerability Levels* categorize consequences of impacts caused by malevolent acts**
  - Requires each physical system component to have a susceptibility *level* associated with it.
- **For each failure scenario, a vulnerability matrix is used to determine the vulnerability level of the scenario.**
  - The vulnerability matrix uses the performance index of the scenario, along with the susceptibility level of the component involved in the scenario, to determine the vulnerability level.
- **Knowing the vulnerability levels of different failure scenarios enables the different scenarios to be ranked, and also helps to identify mitigation opportunities.**
  - If a particular failure scenario has a high vulnerability level, one might focus efforts on how to lower the susceptability level for components involved in that particular scenario.

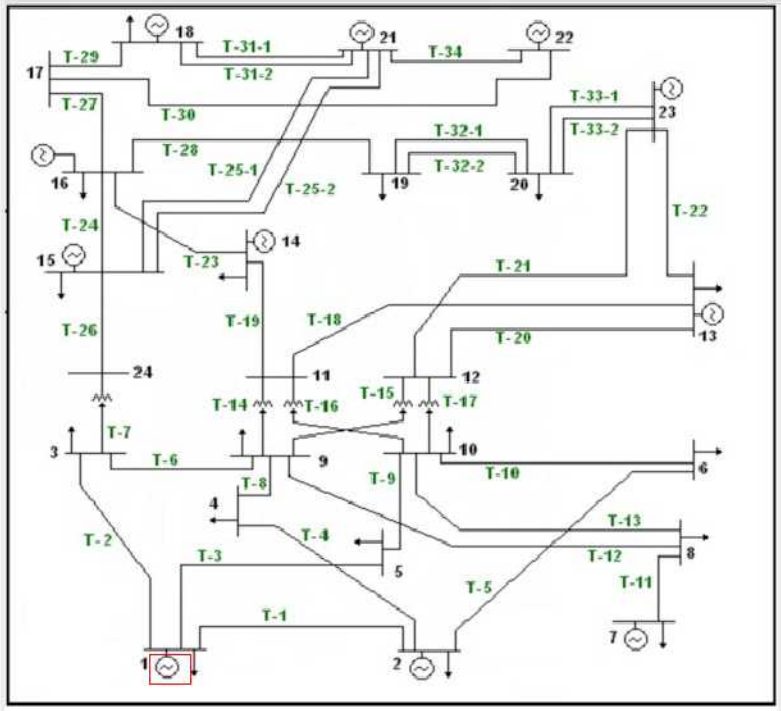
Prototype Consequence Estimator

- Allows for creation of a value tree
- Allows for pair-wise comparison of value tree components
- Implements expected disutility and vulnerability rankings using the methodology described in the previous slides
- Provides a graphical user interface to the methodology
- Allows for analysis of failure scenarios using either the GUI or using data from a file (generated by other software tools)

Example Consequence Results

Consequence Modeling Tool

File System Help



Component Status: 0.0889

This category represents the second priority for counter-terrorismefforts. These locations are generally moderate to extreme valuable and moderately to extremesusceptible.

Risk Analysis

Lost Revenue: 1265388

Component | System Health Levels | Performance Levels | Constructed Scales

Name	G1
Type	Generator
Description	Generator 1
Threat Level	4.0
Outage Time	40
Cost to Repair	10000
Utility Worker Level	1
Fauna Level	0
Number of Residential Customers	161110
Number of Commerical Customers	18946
Number of Small/Medium Industrial Customers	1623
Number of Large Industrial Customers	2

Performance Measure	Level
Economics – Lost Revenue	Millions of Dollars
Economics – Repair/Replace	Tens of Thousands of Dollars
Image – Public	No impact
Image – Customer	No impact
Image – Political	No impact
Health & Safety – General Public	No impact
Health & Safety – Utility Workers	Low safety impact on worker as...
Environment – Fauna	No impact

Sandia National Laboratories

Summary

- **In Sandia's Threat-to-Consequence Framework, consequence is the higher-level result of an operational impact**
- **Metrics used to determine consequence can be difficult to define and/or measure, and vary by persons and situations**
- **The consequence estimation methodology described here enables the following:**
  - Multiple viewpoints on the importance of each consequence metric can be taken into consideration
  - Physical impacts can be mapped to metrics of concern
  - Impact scenarios, both random and malicious, can be ranked according to their consequence
  - Areas of improvement for equipment outages and impact mitigation opportunities can be discovered via the rankings

Questions?