SANDIA REPORT
SAND2008-6098
Unlimited Release
Printed August 2008

National SCADA Test Bed Consequence Modeling Tool

Bryan T. Richardson and Lozanne Chavez

Prepared by:
Sandia National Laboratories
Albuquerque, New Mexico 87185 and Livermore, California 94550

Sandia is a multiprogram laboratory operated by Sandia Corporation,
a Lockheed Martin Company, for the United States Department of Energy's
National Nuclear Security Administration under Contract DE-AC04-94AL85000.

Issued by Sandia National Laboratories, operated for the United States Department of Energy by Sandia Corporation.

Available to DOE and DOE contractors from:
U.S. Department of Energy
Office of Scientific and Technical Information
P.O. Box 62
Oak Ridge, TN 37831

Telephone: (865)576-8401
Facsimile: (865)576-5728
E-Mail: reports@adonis.osti.gov
Online ordering: http://www.doe.gov/bridge

Available to the public from:
U.S. Department of Commerce
National Technical Information Service
5285 Port Royal Rd
Springfield, VA 22161

Telephone: (800)553-6847
Facsimile: (703)605-6900
E-Mail: orders@ntis.fedworld.gov
Online ordering: http://www.ntis.gov/help/ordermethods.asp?loc=7-4-0#online

SAND2008-6098
Unlimited Release
Printed August 2008

National SCADA Test Bed Consequence Modeling Tool

Bryan T. Richardson
Information Assurance and Survivability
Sandia National Laboratories
P.O. Box 5800
Albuquerque, New Mexico 87185

Lozanne Chavez
Partnership Development and Business Intelligence
Sandia National Laboratories
P.O. Box 5800
Albuquerque, New Mexico 87185

Abstract

This document presents a consequence modeling tool that provides, for asset owners, the *cost* (in dollars and consequences) associated with an electric power disruption.

Acknowledgments

The authors of this report wish to thank Massachusetts Institute of Technology and the internal Sandia Laboratory Directed Research and Development organization for their work on "Insights and Analysis Methodologies from a Focused Study of the Bulk Power Grid."[1] That report provided the basis for the National SCADA Test Bed Consequence Modeling Tool.

[1] LaViolette, Randal A., et al. "Towards Risk-Based Management of Critical Infrastructures: Enabling Insights and Analysis Methodologies from a Focused Study of the Bulk Power Grid," Sandia National Laboratories, February 2008, SAND2008-0910.

Contents

Figures

Tables

Acronyms

AHP	Analytical Hierarchy Process
CMT	Consequence Modeling Tool
GNU	(free Unix-style operating system)
JAHP	Java Analytic Hierarchy Process
LDRD	Laboratory Directed Research and Development
NSTB	National SCADA Test Bed
SCADA	Supervisory Control and Data Acquisition
XML	Extensible Markup Language

Executive Summary

The National SCADA Test Bed Consequence Modeling Tool (CMT) was developed to provide utility owners the power to quickly assess which physical assets are at the highest risk and to explore mitigation options that provide the greatest reduction in risk. Based on the consequence-ranking framework[2], the software tool provides asset owners the cost—that is, loss in several dimensions—associated with an electronic power disruption; the CMT also provides an estimation of the consequences of a system failure to the serving utility at a local level. The information provided in this analysis enables 1) utility owners/operators to get the most out of their mitigation budgets and 2) cyber security providers to prioritize their development efforts.

Understanding the consequences of utility system failure is necessary to reduce critical infrastructure risk, which is made up of threat, vulnerability, and consequence. Understanding the consequences of cyber threats is vital to meeting many of the goals outlined in the Roadmap to Secure Control Systems in the Energy Sector, such as 1) developing and integrating protective measures, 2) detecting intrusion and implementing response strategies, and 3) identifying strategic risks, to name just a few goals.

[2] Koonce, A. M. et al, "Bulk Power Grid Risk Analysis: Ranking Infrastructure Elements According To Their Risk Significance," Massachusetts Institute of Technology, Engineering Systems Division, September 2006. http://esd.mit.edu/WPS/esd-wp-2006-19.pdf

1. Introduction

1.1 Background

The consequence analysis method and framework developed by Sandia National Laboratories and Massachusetts Institute of Technology provided the basis for the National SCADA Test Bed Consequences Modeling Tool (CMT). This method for modeling electric power grid consequences on a local level was developed as part of a Sandia Laboratory Directed Research and Development (LDRD)[3] project. The method begins with a utility-ranked list of consequence categories (environment, safety, economics, etc.) and produces a *value tree* that represents the consequences, to a utility, that are associated with losing physical system elements. Also, the method calculates a performance index to describe the overall consequence that a threat scenario creates. Utilizing the infrastructure impact rankings generated from the consequence models helps to identify which threats are of greatest consequence to a utility.

In the area of critical infrastructure protection, consequences can be defined at local, regional, and national levels. Each level can contain consequences that affect other critical infrastructures. To identify the threats and threat vectors that a control system requires protection against, we need methods to model physical-impact consequences that would result from a cyber attack on a critical-infrastructure–protection control system.

Physical system impacts do not affect all end-users in the same way. For example, losing power to several residences for several hours may have little impact on dollar cost, but losing the same amount of power over the same several hours at an industrial plant could lead to millions of dollars in lost production; this, in turn, could lead to adverse consequences in other critical infrastructures. Understanding only the impacts associated with a particular infrastructure does not accurately depict the *true* loss to the asset owner. The CMT was designed to give the utility owners a picture of the *total-costs* associated with an outage. Before the CMT can be used, stakeholders must define a value tree that reflects importance rankings for the individual components within their system.

1.2 Purpose

The *consequence* of an event is its cost, in any of several forms: dollars, loss of health, reduced quality of life, etc. Consequence differs from impact.

Impact refers to the effects of an event on a utility system; for example, ‘Generator #65 will not be able to produce power for the next 12 hours.’

Consequence refers to the *cost* associated with that impact; for example, ‘Four people died as a result of yesterday’s power failure.’

Reducing impacts to consequence (cost) terms has several benefits.

[3] SAND2008-0910

First, otherwise dissimilar events can be compared. For example, which is worse: Losing 20 megawatts of transmission or losing 20 megawatts of generation? This tool compares costs incurred in the two situations.

Second, anyone can understand often-complex physical impact descriptions when they are translated into consequences.

Third, mitigation effectiveness can be stated in cost terms for cost/benefit and return-on-investment analyses.

Finally, calculation of risk requires knowledge of consequence.

2. Approach

The CMT enables stakeholders to determine the cost of an outage based on what the stakeholders themselves value with respect to the service that the infrastructure provides. The word *cost* represents loss in several dimensions (capital expenditure, lost revenue, health effects, perceived stature, etc.); these are defined as part of the CMT process. Determining cost using the CMT is a six-step process:

1. Define the categories of impact.
2. State the importance of each category relative to the others.
3. Define the measures of impact for each category.
4. Define the relationships between physical effects and impact measures.
5. Define the power system and its customers.
6. Define the event in terms of power system impact.

When the steps have been completed, the CMT calculates the consequence result. Although arrival at the first result can be a lengthy process, variations for the first case can be obtained rapidly. The step outcomes can be 'mixed and matched' to some extent; for example, one set of importance measures can be used with different power systems. The CMT can be used also to assess mitigation-technique effectiveness. Step 4 and 5 outcomes are modified to reflect the mitigation effects, and the consequences are re-calculated. This enables a direct cost-benefit result for a given mitigation strategy and is useful for selecting from among alternatives.

2.1 Value Tree Creation

The consequence analysis engine is used to quantify the consequences of the input threat vectors for a given utility. A software implementation of the consequence-ranking framework was developed to assist in creating the value tree. The resulting software is used to analyze the results generated from the analysis engine against the value tree. The tool provides a total consequence *performance index* for each threat vector class analyzed; it also provides a value for each impact category that illustrates the negative effect (disutility) imposed by the threat vector on the impact category.

The Java Analytic Hierarchy Process (JAHP)[4] tool was used as a basis to create the value tree. JAHP consists of a swing-based user interface to the analytical hierarchy process (AHP). JAHP is licensed under the GNU General Public License. This tool was modified to support the criteria, alternatives, hierarchy, and calculated weights as outlined in the consequence modeling framework.

[4] Morge, M., "Java Analytic Hierarchy Process," July 2003, http://www.di.unipi.it/~morge/software/JAHP.html

Impact Categories

To build the value tree, stakeholders first define their impact categories. In this example, the categories were defined as economics, image, health and safety, and environment. Next, stakeholders perform a pairwise comparison for the impact categories. Pairwise comparisions allow the stakeholder to identify the most important item with an indication of how important one item is over another. In this example, the stakeholder has said that image is intermediate between SLIGHTLY and STRONGLY more important than economics; and economics is intermediate between SLIGHTLY and STRONGLY more important than environment. The AHP process results in a value tree weighted by importance. In this scenario, image was ranked to be the most important impact category. Figure 1 defines the impact categories and shows pairwise comparisons.

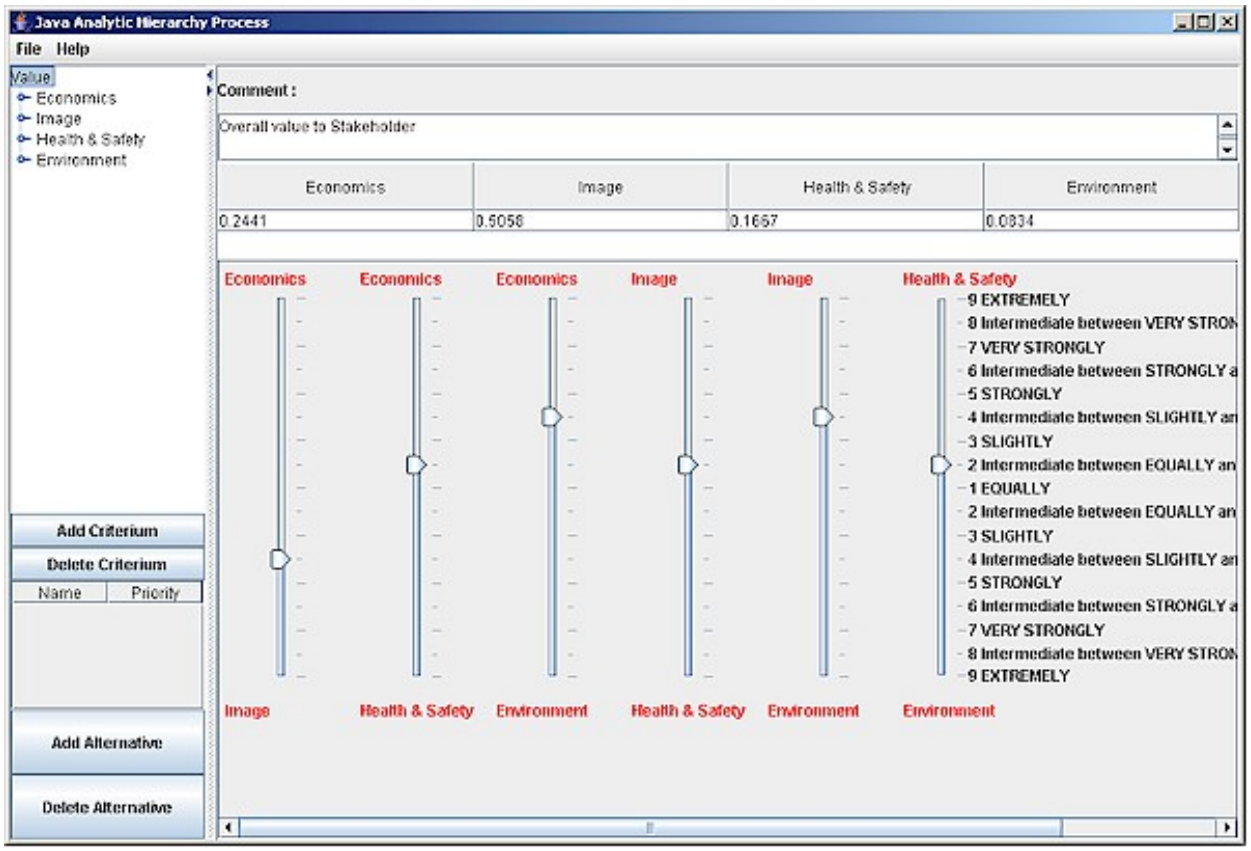

Figure 1. Impact categories defined in the CMT user interface for value tree construction

Performance Measures

Each impact category is broken down into a set of performance measures that describe how consequences can cause stakeholder impacts, as shown in Figure 2. These performance measures are then ranked using pairwise comparisons. In this example, political impact was ranked to be the most important performance measure for the image impact category.

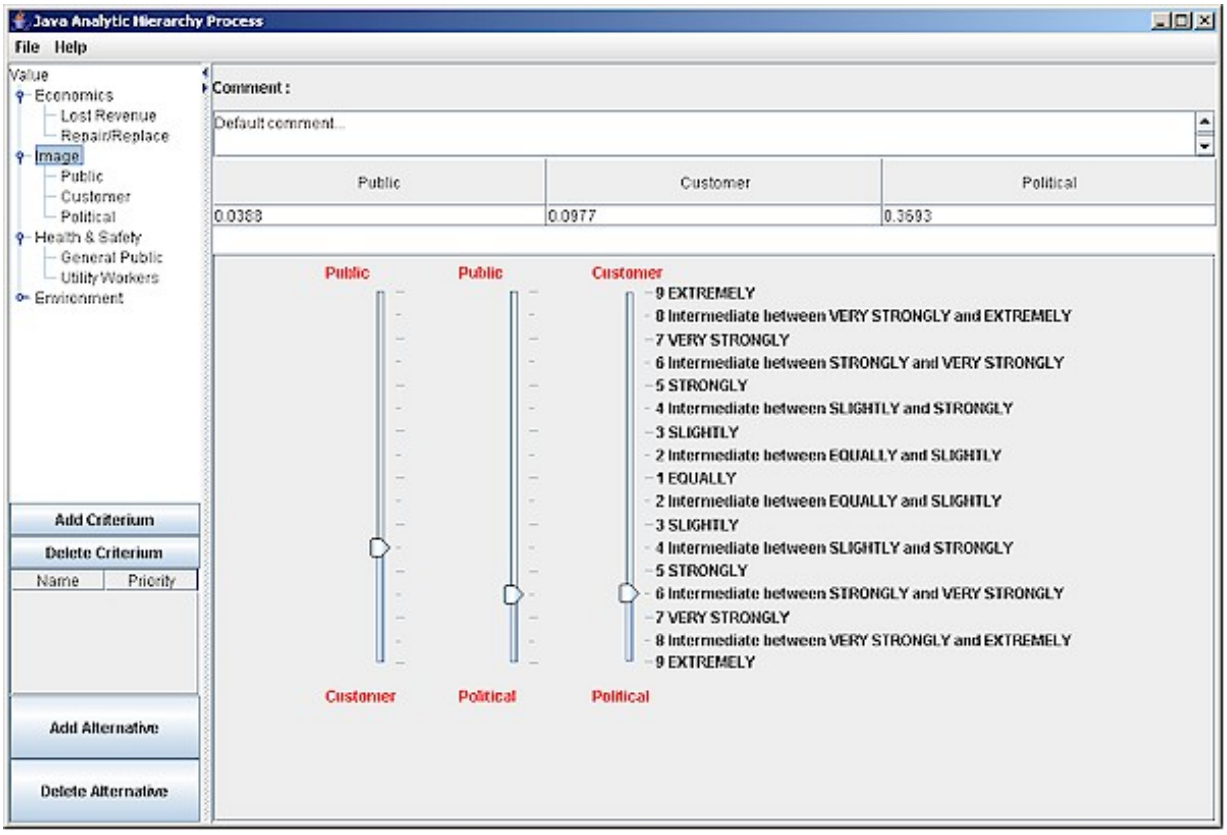

Figure 2. Performance measures defined in the CMT user interface for value tree construction

Constructed Scales

Each performance measure is divided into a set of constructed scales, which represent the amount of impact the physical consequences have on the stakeholder through each performance measure. The constructed scales are also ranked using pairwise comparisons. In this example, Level 3 represents a political push for major regulation reform. Level 2 represents a moderate political push for additional regulations. Level 1 represents a low political influence on industry regulations. Level 0 represents no impact. Figure 3 illustrates constructed scales.

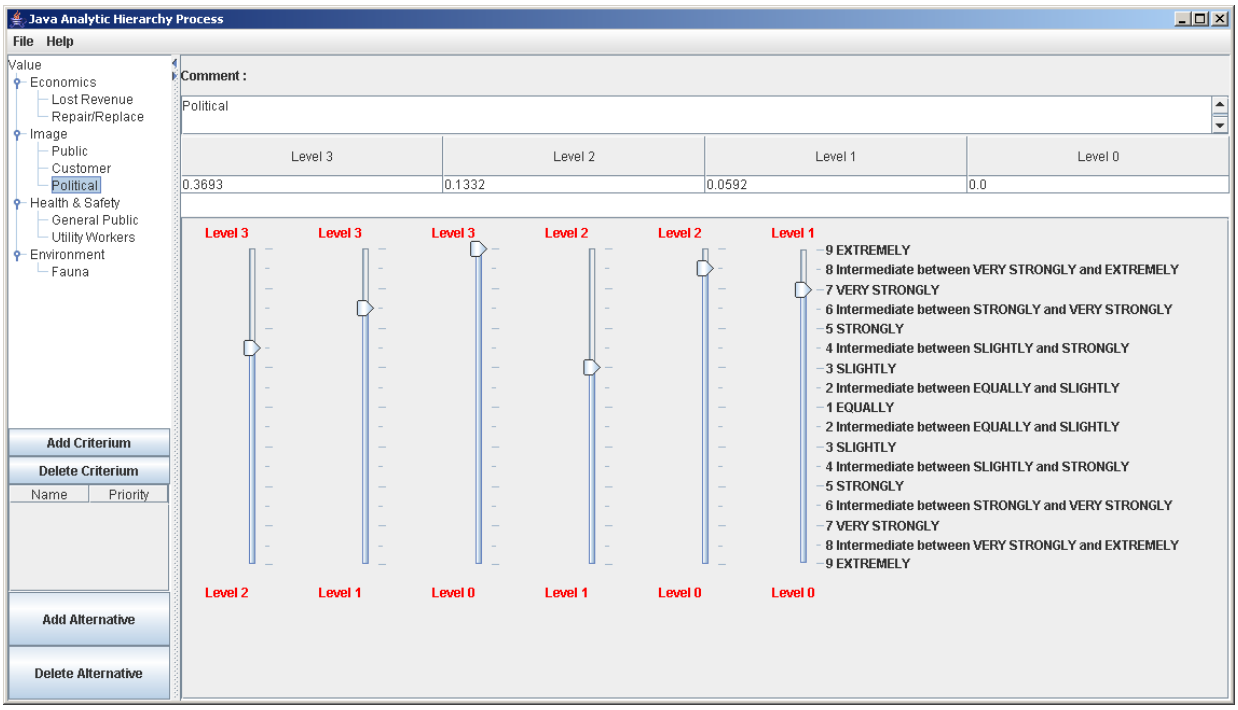

Figure 3. Constructed scales defined in the CMT user interface for value tree construction

The constructed value tree is used to generate a total consequence *performance index* for each impact category that illustrates the negative effects (disutility) that the threat vector imposes on the impact category.

2.2 CMT User Interface

The CMT provides a user interface that utilizes the value tree, performance index, and disutility values generated in the consequence modeling framework, as shown in Figure 4.

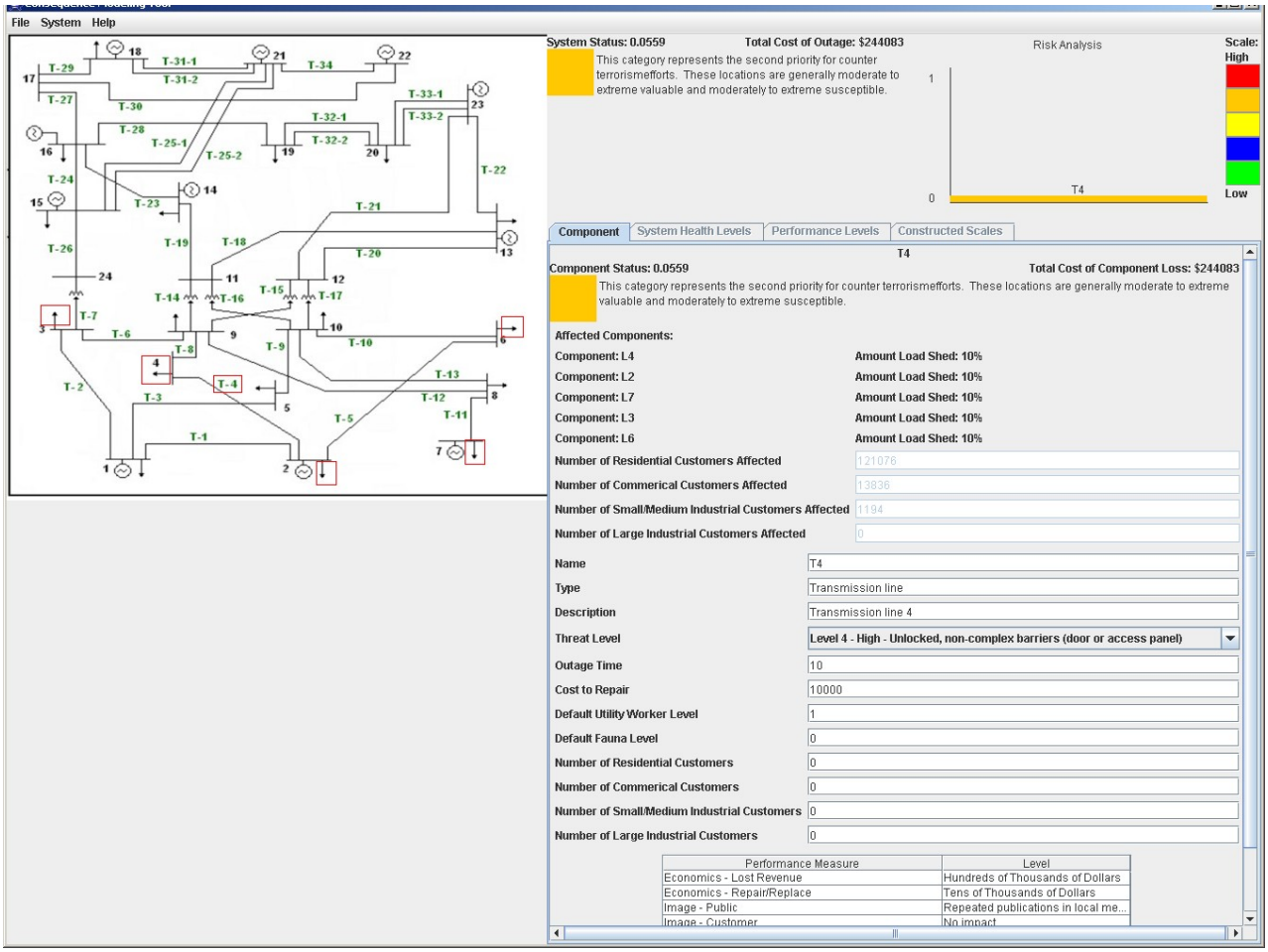

Figure 4. CMT user interface overview

Within this interface, users are presented with an interactive visual representation of the system, as shown in Figure 5. Users may click on any component to identify it as affected. A selected component is represented by a red box. Multiple components can be selected.

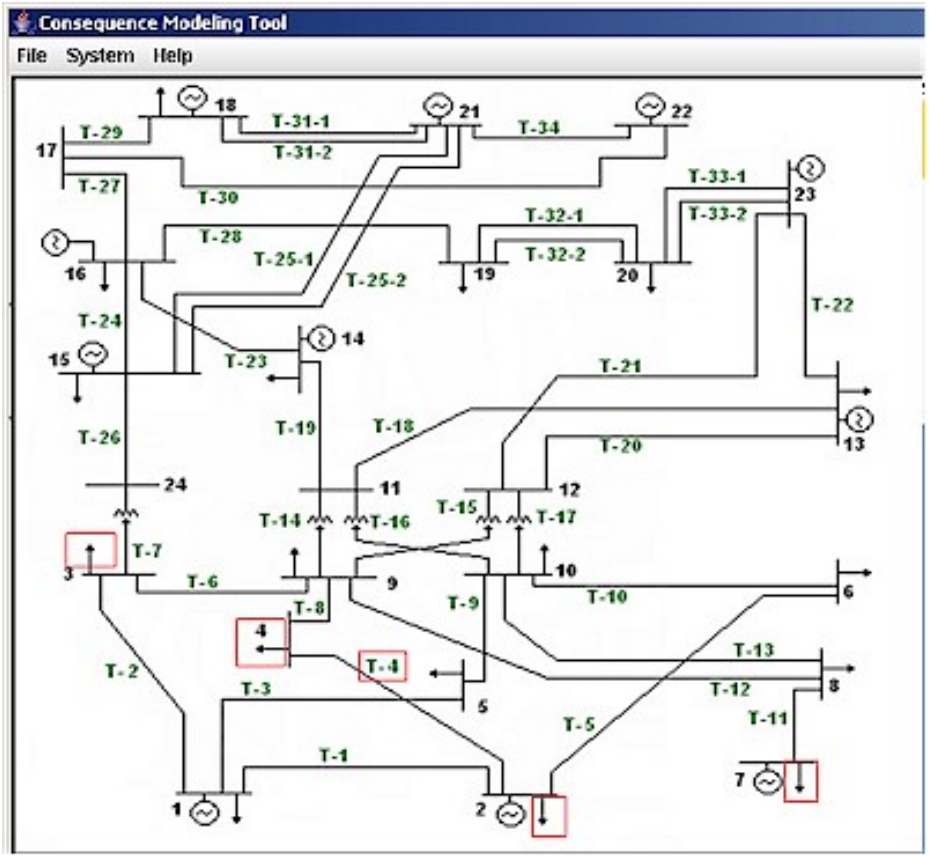

Figure 5. CMT system overview

By clicking on a component in the system diagram, users can identify the consequences of a loss by a single component in the component details section, as shown in Figure 6. Here, users are presented with editable component details, such as the following:Component type

- Description
- Threat level
- Time to bring the component back up, in the event of a failure
- Cost to repair
- Number of customers served.

The component performance index and status are displayed, as well as the total cost of the component loss. In this scenario, the loss of transmission line 4 caused components L2, L3, L4, L6, and L7 to each shed 10% of the load. The number of customers affected by the outage is also displayed, as shown in Figure 6.

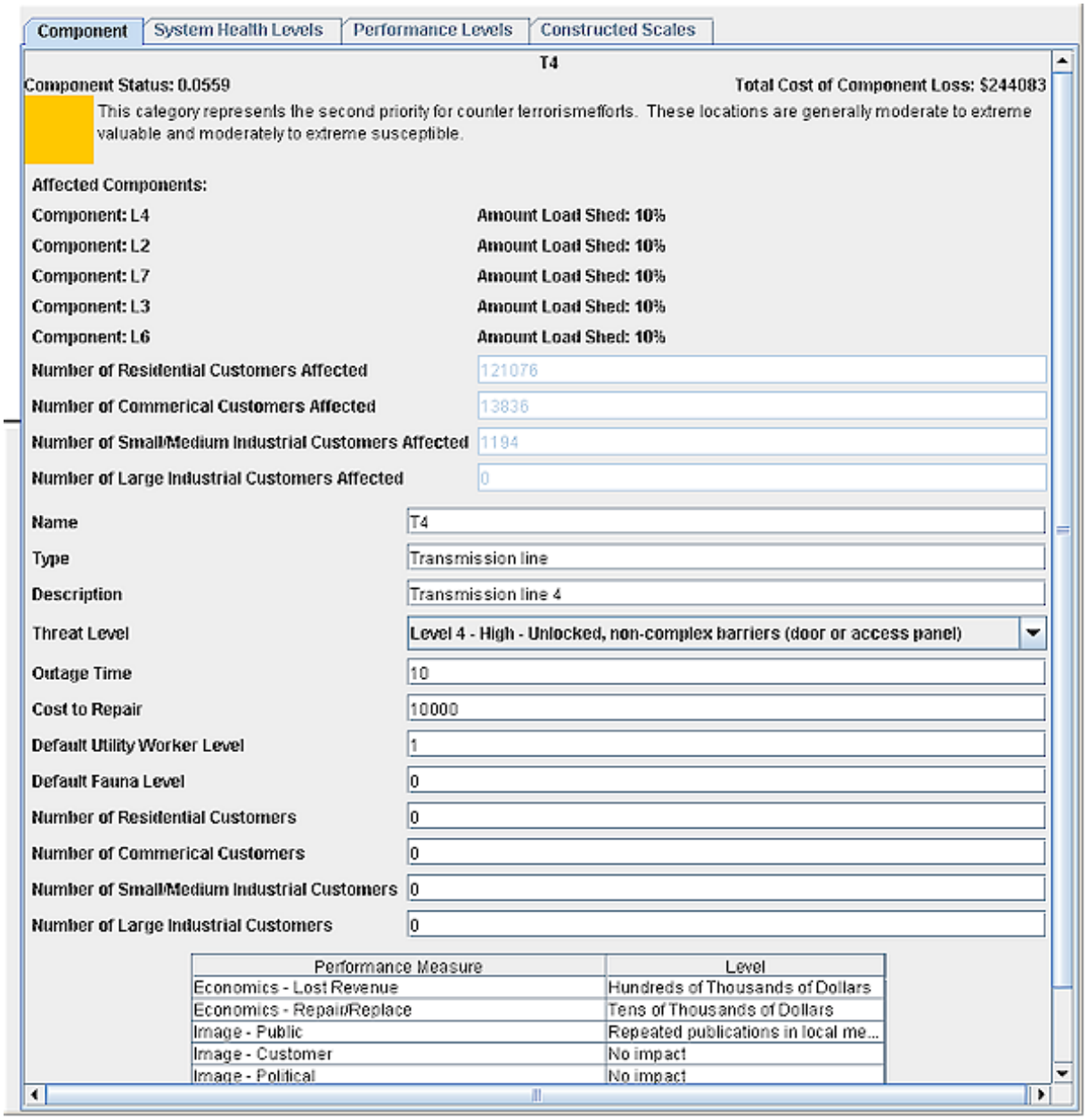

Figure 6. CMT component details

Users are able to test *what-if* scenarios for each component by changing any of the component information and specifying different levels for each performance measure, as shown in Table 1.

Table 1. CMT Performance Measures

Performance Measure	Level
ECONOMICS—Lost revenue	Hundreds of thousands of dollars
ECONOMICS—Repair/replace	Tens of thousands of dollars
IMAGE—Public	Repeated publications in local media
IMAGE—Customer	No impact
IMAGE—Political	No impact
HEALTH & SAFETY—General public	No impact
HEALTH & SAFETY—Utility workers	Low safety impact on worker associated with repairs
ENVIRONMENT—Fauna	No impact

The consequences for all affected components are displayed in the system status section, as shown in Figure 7. The component susceptibility level is a default value read into the system based on component type.

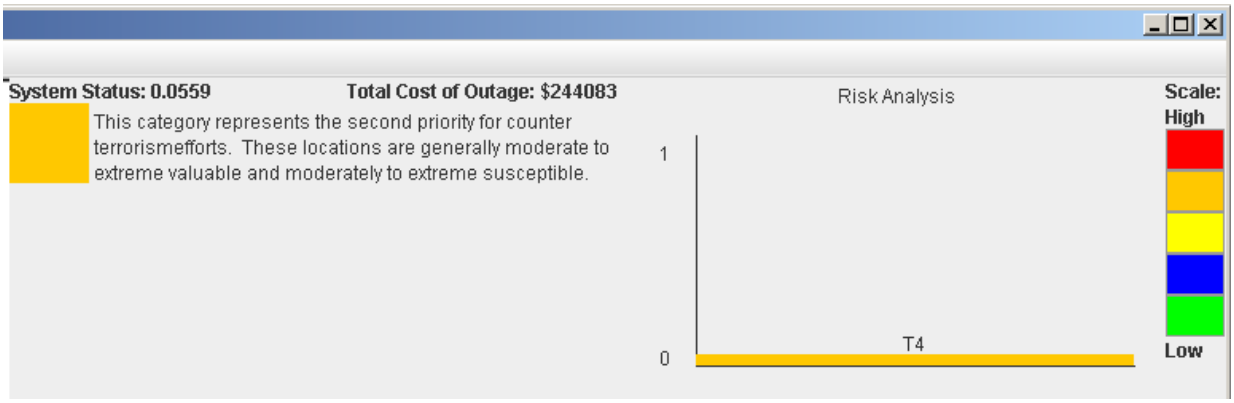

Figure 7. CMT system status

Table 2 summarizes the different susceptibility levels defined for this scenario. By default, generators were set to a susceptibility level 1. Transmission lines without a transformer were set to a level 4; transmissions lines with a transformer were set to a level 3. Loads with a generator were set to a level 2; loads without a generator were set to a level 3. Buses with a generator were set to a level 2; buses without a generator were set to a level 3.

Table 2. Susceptibility Levels of Infrastructure Elements

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 closure
1—VERY LOW	Guarded, secure area, locked, alarmed, complex closure
0—ZERO	Completely secure, inaccessible

The system susceptibility was calculated by taking the highest susceptibility level among all affected components. The system performance index was calculated by taking the highest performance index among all affected components. The total cost of all component loss resulting from the outage is also calculated and displayed, along with a graph of affected components. A change in any of the component details will update the system status details as well.

2.3 Interactions with Other Systems

Users are able to load scenarios generated by hand or by other systems. An XML schema was designed and integrated to accept information from other models. Using this schema, scenarios can be loaded and run to see the consequences. The following specifications were used to read in the scenario pictured in the figures above.

```
<outages>
      <outage>
            <component>T4</component>
            <loadShed>
                  <component>L2</component>
                  <percentshed>10</percentshed>
            </loadShed>
            <loadShed>
                  <component>L3</component>
                  <percentshed>10</percentshed>
            </loadShed>
            <loadShed>
                  <component>L4</component>
                  <percentshed>10</percentshed>
            </loadShed>
            <loadShed>
                  <component>L6</component>
                  <percentshed>10</percentshed>
            </loadShed>
            <loadShed>
                  <component>L7</component>
                  <percentshed>10</percentshed>
            </loadShed>
      </outage>
</outages>
```

3. Results and Discussion

The CMT was built based the consequence modeling framework to give asset owners the associated *cost* of an outage. The tool provides mechanisms to input the value tree, which is the basis of the framework. The graphical user interface uses the results of the value tree to present an interactive tool for stakeholders to assess system impacts during an electrical outage.

Data gathered to research the consequence analysis framework was used to seed the system. The data included the following:

- Outage time—number of hours before the component can be restored to function.
- Numbers of residential customers, commercial customers, small/medium industrial customers, large customers—fictional number of customers based on LDRD research.
- Repair cost of the component.
- Default level for utility workers—component specific value that was used based on the LDRD research.
- Default level for fauna—component specific value that was used based on the LDRD research.
- System status scales.
- Lookup table to determine overall system health.
- System health level descriptions.
- Performance measures and constructed scales for the value tree, along with the weights from stakeholder S-1.

Additional data used included image coordinates of the components in the system diagram (to visually highlight the component).

4. Conclusions and Recommendations

The current CMT implementation provides a basis for further development. It would be highly beneficial to continue the development of a customizable framework that could easily be setup for use in other systems and utilities. Included in this customization would be the ability to easily incorporate and define system diagrams and components, as well as a wizard-like interface to step users through the process of setting up a new system or utility.

The current tool allows users to load scenarios generated by hand or by other tools. However, it would be beneficial to also allow users the ability to generate and save scenarios developed within the CMT.

The value tree in the current CMT implementation is based solely on the insights of a single stakeholder. As noted in the LDRD research, different stakeholders hold different beliefs about the system. The ability to combine rankings from various stakeholders within the utility would provide additional CMT benefits. Also, the ability to gather these inputs through a distributed interface, such as a web-based interface, would facilitate the gathering process.

Moreover, the current CMT implementation looks for the worst-case component susceptibility level and the worst-case component performance index to use in the overall system status. It would be beneficial to develop an algorithm that calculates the overall system status based on a weighted factor of all affected components in the system.

These enhancements would greatly improve CMT usability.

Appendix A. Contact Information

For more information, contact:

Jennifer DePoy, Manager (505) 844-0891, jdepoy@sandia.gov

Bryan T. Richardson (505) 845-2386, btricha@sandia.gov

Lozanne Chavez (505) 844-0008, lmchave@sandia.gov

Distribution List

1	MS 0899	Technical Library, 09536


Sandia National Laboratories