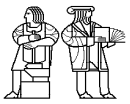

Massachusetts Institute of Technology

Engineering Systems Division

Working Paper Series

ESD-WP-2004-01

A METHODOLOGY FOR THE IDENTIFICATION OF CRITICAL LOCATIONS IN INFRASTRUCTURES

Douglas M. Lemon and George E. Apostolakis
Engineering Systems Division
Department of Nuclear Engineering
Massachusetts Institute of Technology
apostola@mit.edu

June, 2004

ABSTRACT

The extreme importance of critical infrastructures to modern society is widely recognized. These infrastructures are complex, interdependent, and ubiquitous; they are sensitive to disruptions that can lead to cascading failures with serious consequences. Protecting the critical infrastructures from terrorism, human generated malevolent attack directed toward maximum social disruption, presents an enormous challenge. Recognizing that society cannot afford the costs associated with absolute protection, it is necessary to identify the critical locations in these infrastructures. By protecting the critical locations society achieves the greatest benefit for the protection investment. This paper presents a methodology for the identification of critical locations in infrastructures. The framework models the infrastructures as interconnected digraphs and employs graph theory and reliability theory to identify the vulnerable points. The vulnerable points are screened for their susceptibility to a terrorist attack, and a prioritized list of critical locations is produced. The prioritization methodology is based on multi-attribute utility theory. The methodology is illustrated through the presentation of a portion on the analysis conducted on the campus of the Massachusetts Institute of Technology.

Acknowledgments

We are thankful for the support we received from Mr. Joseph F. Gifun, Assistant Director of Facilities for Infrastructure and Special Projects, MIT Facilities Department. One of us (DML) thanks the United States Navy for providing him with such a challenging and rewarding assignment.

Table of Contents

List of Figures

List of Tables

I. Introduction

Critical Infrastructures provide the very foundation for the standard of living in the United States and other Western Democracies. These infrastructures form an over-arching net covering the modern way of life. The infrastructures are large, diffuse, heterogeneous, inter-connected networks, and while critically important, the infrastructures are difficult to control reliably. They include numerous interaction points and local disturbances can cascade very quickly. The complexity of these networks leads to difficulty in modeling and control methodologies. The importance of these infrastructures has long been recognized. Executive Order 13010, July 15, 1996, [Clinton, 1996] stated:

> *America's critical infrastructures underpin every aspect of our lives. They are the foundations of our prosperity, enablers of our defense, and the vanguard of our future. They empower every element of our society. There is no more urgent priority than assuring the security, continuity, and availability of our critical infrastructures…*

Two recent events highlight the vulnerability of the critical infrastructures. First, the terrorist attacks on September 11, 2001, were conducted through exploitation of the Transportation infrastructure. The great oceans no longer provide sufficient protection; America must defend itself against malicious attack. Second, the East Coast blackout of August 14, 2003, demonstrated the fragility of one particular infrastructure, the electrical generation and distribution networks. Roughly 50 million people across the North Eastern United States and Eastern Canada suffered one of North America's worst ever electric power outages. The loss of electricity cascaded through several other critical infrastructures. For example, water was lost due to loss of power at the pumping stations, and transportation was hampered due to the loss of air and ground traffic control. Terrorist acts have similarities and differences with natural and technological disasters, but are distinguished by a malevolent intelligence directed toward maximum social disruption. One subset of the potential targets of terrorist acts is the nation's critical infrastructures [OHS, 2002]. Critical infrastructures are complex, interdependent, and ubiquitous; they are sensitive to disruptions that can lead to cascading failures with serious consequences. Complex national infrastructures have critical nodes or choke points that, if attacked, could lead to significant disruption or destruction. [Garrick, 2004] Conventional assaults with truck bombs, dynamite, or cable cutting, as well as

computer generated attacks, could unleash a chain of events in which a service grid, an oil of gas pipeline, or an air traffic control system collapses with cascading effect. [Garrick, 2004]

After September 11th, critical infrastructure protection became a national focus and is likely to remain one for the foreseeable future. The federal government has reorganized agencies into a Department of Homeland Security, and all levels of government have been increasing resources and taking specific measures (such as tightening airline security) for infrastructure protection. An excellent overview of the terrorist threat is presented in the article *Infrastructure Issues for Cities – Countering Terrorist Threat* [Gilbert, et al, 2003]. The authors identify the importance of the critical infrastructures to the United States' cities; over 80% of the US population lives in and around the cities. [U.S. Census 2000] The challenges in protecting United States' cities from multiple coordinated attacks are addressed. A key point presented by the authors is that the infrastructure systems were never intended by their designers to resist the consequences of planned malicious destruction. [Gilbert, et al, 2003] Additional perspectives are available on the state of the terrorist threat (for example [Garrick, 2002; Deisler, 2002; and Haimes, 2002]. The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets [Bush, 2003] identifies critical infrastructures and key assets, Table I.1.

Critical Infrastructures	**Key Assets**
Agriculture and Food	National Monuments, Icons
Water	Nuclear Power Plants
Public Health	Dams
Emergency Services	Government Facilities
Defense Industrial Base	Commercial Key Assets
Telecommunications	
Energy	
Transportation	
Banking and Finance	
Chemicals, Hazardous Materials	
Postal and Shipping	

Table I.1 Critical Infrastructures and Key Assets

A systematic approach to the identification of the significant relevant risks from terrorism, and the development of effective measures for managing them, has not yet been undertaken [OHS, 2002]. Society has limited resources and can ill-afford to use them on

measures that have not been demonstrated effective. An example is the recent National Research Council report on countering terrorism [NRC, 2002]. This report offers numerous recommendations for the reduction of vulnerabilities in transportation systems, information technology, energy systems, and other infrastructures. Implementing all of them would impose a considerable financial burden on the nation and would ignore the probabilities of these vulnerabilities. Furthermore, the costs and risk-reduction potential of proposed counter-terrorism measures have not yet been evaluated systematically. A framework that would allow for a rigorous evaluation of the merits of such proposals would be highly desirable. This project takes steps toward creating a screening methodology for the identification of critical locations. Developing the complete framework requires overcoming significant challenges, including the geographic and organizational diffusiveness of infrastructure systems, and the importance of multi-organizational responses in disaster prevention, mitigation, and response.

Protecting a complex and interconnected system of infrastructures at the national level creates major technical challenges because of the complexity and diffuse nature of this system. Historically, critical infrastructure protection has tended to be addressed on an infrastructure-specific basis by individual engineering communities (e.g., the electric power industry). Traditional safety methods such as risk assessment are enabled by features of the analytical context such as the standardization of the technology, the bounded number of event triggers of accidents, and the spatial compactness of components. In contrast, societal infrastructures are far more idiosyncratic, interconnected across systems, and spread out geographically (see, for example, [Haimes, 2002; Kunreuther and Lerner-Lam, 2002; Stewart and Bostrom, 2002]). Further, societal infrastructures have overlapping ownership and responsibility in private organizations and local, state, and national government. Therefore, technical complexity is matched or exceeded by sociopolitical complexity. There are many practical and theoretical challenges to developing effective methods for representing and planning for infrastructure threats and coordinating actual responses.

Of particular importance are human actions. For engineering systems, it is the actions of the facility operators that are modeled using the work of human error theorists [e.g., Reason, 1990; Sträter and Bubb, 1999]. Organizational influences on operator performance are still in a state of development. [Paté-Cornell, 1990; Davoudian et al, 1994; Reason, 1997;

Marcinkowski et al, 2001] The case of infrastructures is very different in that there is not a well-defined operator crew that attempts to mitigate the accident but, rather, a number of organizations that would participate in preventing, mitigating, and responding to an event (e.g., local infrastructure operators, first responders, disaster-recovery agencies). Drabek [1985] describes the response to emergencies as "emergent multiorganizational networks" because the relationships among overlapping responder organizations emerge during the event rather than from prior planning. Inter-organizational preparedness is critical to effective response. [Gillespie and Streeter, 1987] It is evident, therefore, that the development of sequences of events leading to undesirable end states will require innovative approaches to the "recovery" actions. Building multi-organizational responses into the measurement of critical infrastructure risk, safety, and priority is a theoretical and practical challenge.

Scenario-based methodologies have been developed to manage the safety of complex systems such as space systems (the International Space Station [Futron, 2002] and the Shuttle [SAIC, 1995]), waste repositories [Rechard, 1996], nuclear power plants [USNRC, 1990], large incinerators [SAIC, 1996], chemical process facilities [CCPS, 1989], municipal water distribution systems [Ezell et al, 2000], and other systems [Hokstad et al, 2001; Melchers and Feutril, 2001]. It has also been used to identify research needs. [Apostolakis et al, 1995] This methodology is known as Probabilistic Risk Assessment (PRA), Quantitative Risk Assessment (QRA), or Performance Assessment. This approach has been found useful because it:

1. Provides a common understanding of the problem, thus facilitating communication among various stakeholder groups.

2. Reduces the probability of emotional reactions because it provides a framework for the evaluation of various risk management proposals.

3. Offers an integrated approach, thus identifying the needs for contributions from diverse disciplines such as the engineering and the social and behavioral sciences.

4. Encourages identification of complex interactions between events/systems.

To better understand the relevant issues facing the nation as a whole, it is often useful to examine a smaller-scale system to uncover insights and issues. This project pushes deeper

into the infrastructure protection issue by analyzing the campus of the Massachusetts Institute of Technology (MIT), which is a small community embedded within the city of Cambridge, Massachusetts. Cambridge is a diverse community, a small city of over 100,000, with disaster planning coordinated through its own Local Emergency Planning Committee that includes participation from MIT. MIT itself can be considered a small town with approximately six thousand residents and an additional fourteen thousand commuters. MIT operates a utility plant, data network, cable television station, and phone system, and has its own police and medical personnel. This project has the full cooperation on the MIT Department of Facilities (DOF), which provided complete information on the infrastructures. Completeness of the documentation supporting national infrastructures is uncertain. Some estimates list up to ten percent of natural gas distribution lines and up to twenty percent of water distribution lines as undocumented. The MIT campus contains a Critical Infrastructure, the Central Utilities Plant (CUP). The CUP houses a natural gas fired turbine generator which provides for MIT's electrical, steam, and air conditioning needs. Additionally, the CUP contains the electrical distribution system, controlling on-site generation and back-up electricity from the local electric utility. The MIT campus also contains a Key Asset, the Nuclear Research Reactor. Although the research reactor is not a power plant as defined by the National Strategy, it is an excellent representation of Key Asset.

This project examined three critical infrastructures, electric power, water (domestic and fire protection), and natural gas, and the interactions between them. The focus was to develop a methodology for the identification of critical locations in infrastructures. A critical location is defined as a point against which a successfully attacked could lead to significant consequences. The more serve the consequences, the more critical the location. On a national scale many potentially critical locations, such as the George Washington Bridge, in New York City, or the Hoover Dam, in Boulder City, Nevada, may be easily identified. Other locations may only be revealed through analysis of the infrastructures. For example, a Financial Institution may have a main communication line for the processing of monetary transactions and a "completely" independent, back-up communication line, both of which run underground and connect to the telecommunications network, under the street, at separate points. In the event of failure of the main communication line, data is automatically routed

over the back-up line with minimal disruption. On initial review the data transmission system appears secure from a single point failure affecting either data transmission line. What if both telecommunication lines pass through the same physical conduit between the building and the telecommunications network? Or both lines are, at some point, accessible from the same manhole? In that case the data transmission system is subject to a single point failure in the form of a physical attack on the transmission conduit.

A single point failure is not limited to an individual infrastructure, but may affect multiple infrastructures. For example, in portions of Washington, DC, water and electrical distribution systems occupy the same service tunnels. The concept of service tunnels and man-way access points is appealing to many people in urban design and city planning. By burying the infrastructures, with limited access points, they are secure from common vandals and moderate environmental disruptions, and are "out-of-sight" so they don't distract from beautification. Putting multiple infrastructures in common service tunnels creates the potential for the unintended development of critical locations.

This work discusses a methodology for the identification of individual critical locations. Also, the methodology addresses combinations of locations, which when attacked through simultaneous or sequential events could lead to significant consequences. The critical locations, and location combinations, and there ranking according to potential impact will be the basis of risk informed decision making.

II. Background

II.1 Quantitative Risk Assessment

Quantitative Risk Assessment (QRA) is a proven, well established, and systematic process for examining engineered systems to produce an understanding of the associated risks. QRA is typically used to examine systems whose operation is based on design requirements, and defined human and computer controlled actions. The quantitative process combines the probability of an event with the anticipated consequences of the event to produce an overall risk picture of the system. QRA is helpful in recognizing the components and failure modes which contribute the greatest to risk. In general terms, QRA asks the following questions [Kaplan and Garrick, 1981]:

- What can go wrong?
- What are the consequences?
- How likely is it?

For a given system, QRA proceeds as follows:

1. A set of undesirable *end states* is defined, e.g., in terms of individual or societal risk.

2. For each end state, a set of disturbances to normal operation is defined which, if uncontained or unmitigated, can lead to the end state. These are called *initiating events (IEs).*

3. *Event* and *fault trees* are employed to identify sequences of events that start with an IE and end at an end state. Thus, *accident scenarios* are generated.

4. The probabilities of these scenarios are evaluated using all available evidence, primarily past experience and expert judgment.

5. Results are used for "insight" to educate participants, help define priorities, reveal interdependencies, and show leverage points. QRA is a planning-as-learning exercise, not simply an analysis tool.

The definition of end states and IEs is a critical part of risk assessment because it may lead to an incomplete analysis. For well-understood systems such as nuclear power plants, standardized lists of end states and IEs have been developed. For infrastructures, these must

be identified using a systematic approach. The MIT Department of Facilities has developed a methodology using multiattribute decision analysis for prioritizing maintenance work. [Karydas and Gifun, 2002] This work identifies an initial list of end states applicable to MIT as follows: Impact on Health, Safety, and the Environment; Economic Impact (physical property, intellectual property; interruption of academic activities and operations); and Impact on Public Image. These end states will serve as the starting point of an iterative process to identify end states appropriate to terrorist threats.

The next step is to identify the IEs for each end state. A systematic method for doing this is to employ a *Master Logic Diagram (MLD)*. [USNRC, 1982; NASA, 2002] The MLD is a fault-tree (top-down) type logic diagram that helps to identify the IEs. Once the IEs have been identified, standard event/fault trees can be employed to develop sequences of events that may lead from each IE to each end state. These sequences include hardware failures, natural phenomena, and human errors (e.g., during recovery actions).

The evaluation of the probabilities of the scenarios will be another major challenge. QRAs utilize the Bayesian (degree-of-belief) interpretation of probability that allows the use of all evidence, i.e., statistical, experiential, and expert judgment. [Apostolakis, 1990] While statistical evidence would be the most desirable basis for this evaluation, in reality the project will have to rely on expert judgment. Methods for the structured elicitation and utilization of expert judgment have been developed and applied in major risk studies. [e.g., Keeney and von Winterfeldt, 1991; Cooke, 1991; Draper, 1995; Budnitz et al, 1995]

It is recognized that QRA models rare events, some which have never happened and others with very infrequent occurrences. Additionally, human behavior and the severity of some events may be challenging to understand. These factors leave the risk assessment with some recognized degree of uncertainty. QRA highlights these issues and incorporates a systematic process for treating them. The importance of the uncertainties, and the degree to which they are assessed, varies based on the decision requirements.

The successful application of Quantitative Risk Assessment provides an understanding of the risks associated with the system and an expression of the uncertainties involved, which together produce a relative risk ranking. QRA forms the basis for risk-informed decision making.

II.2 Decision Analysis

Decision Analysis (DA) is a formal process, Figure II.1, designed to structure complex problems for analysis, deal with tradeoffs between multiple objectives, identify and quantify sources of uncertainty, and incorporate subjective judgments. DA is a methodology to assist

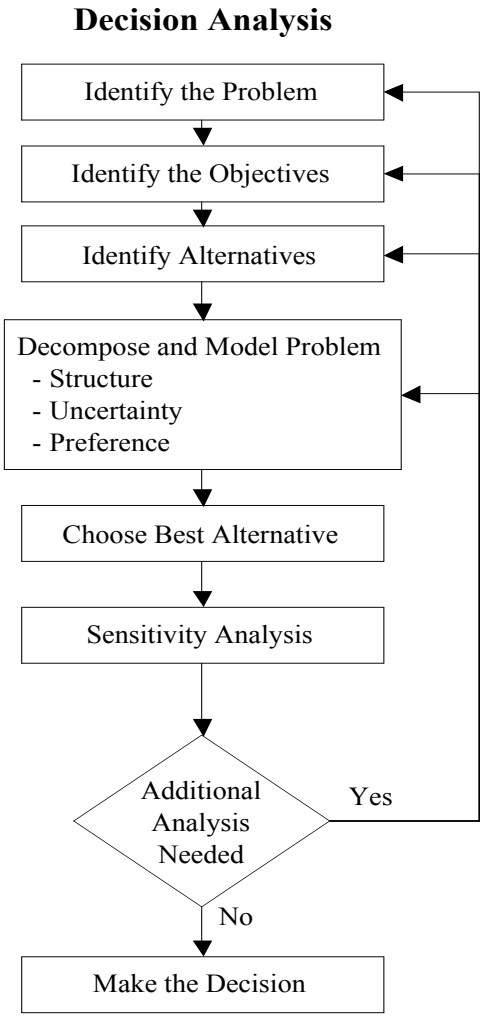

Figure II.1 Decision Analysis [Loerch, 1996]

decision makers in achieving appropriate decisions. Decision Analysis is applied to the case of identifying the critical locations in infrastructures to assist in establishing the prioritization methodology. The prioritization methodology provides a guideline for rank ordering events in many situations. While the methodology is a general approach, which may be applied in

numerous situations, the analysis is specific to each decision case. The methodology is portable, but the analysis must be repeated for each specific application.

The prioritization methodology is a structured approach that determines the most appropriate prioritization based on a performance index (PI) calculated for each item. [Weil and Apostolakis, 2001] The priority of each item is ranked according to the PI. The PI is the sum of the weights of individual performance measures (PM) multiplied by the disutilities of each item for that particular PM. The PMs are measures of the community's objectives.

$$PI_j = \sum_i^{K_{pm}} w_i d_{ij}$$

where

PI_j is the performance index for item *j*
w_i is the weight of the performance measure *i*
d_{ij} is the disutility of performance measure *i* for item *j*
K_{pm} is the number of performance measures

In this application, $PI_A > PI_B$ when the decision maker assess alternative A to cause more disutility than alternative B. The performance measures are designed to be independent, meaning the preference for the consequences depend only on the individual levels of the separate PMs, not on the way they are combined. PMs are independent to prevent a double count. Pairs of PMs are Preference Independent of other PMs if preferences for the levels of these two PMs do not depend on the value of any other PMs. Also, a PM is Utility Independent of other PMs of preferences for risky situations involving probabilities of the different levels of the PM do not depend on the fixed level of any other PM. Performance measure independence leads to use of the above Additive Value Function for Disutility. [Loerch, 1996] In cases where the PMs are not independent the Multiplicative Value Function must be employed. In the analysis of critical infrastructures the PMs have been designed to be independent.

Determination of the performance index follows a six step procedure. [Weil and Apostolakis, 2001]

1. Structure the objectives
2. Determine the appropriate performance measures

3. Weighting objectives and performance measures
4. Assessing disutility functions of performance measures
5. Performing consistency checks
6. Validating the results

Structuring the objectives is necessary to identify the fundamental objectives, those fundamental to the decision maker in analyzing the environment. Structuring also identifies the means objectives, those not specifically important to the decision maker but which support the fundamental objectives. [Clemen, 1991] A value tree, a hierarchical relationship, is employed to structure the objectives and applicable performance measures. The value tree for the efficient prioritization of infrastructure renewal projects is shown in Figure II.2. At the

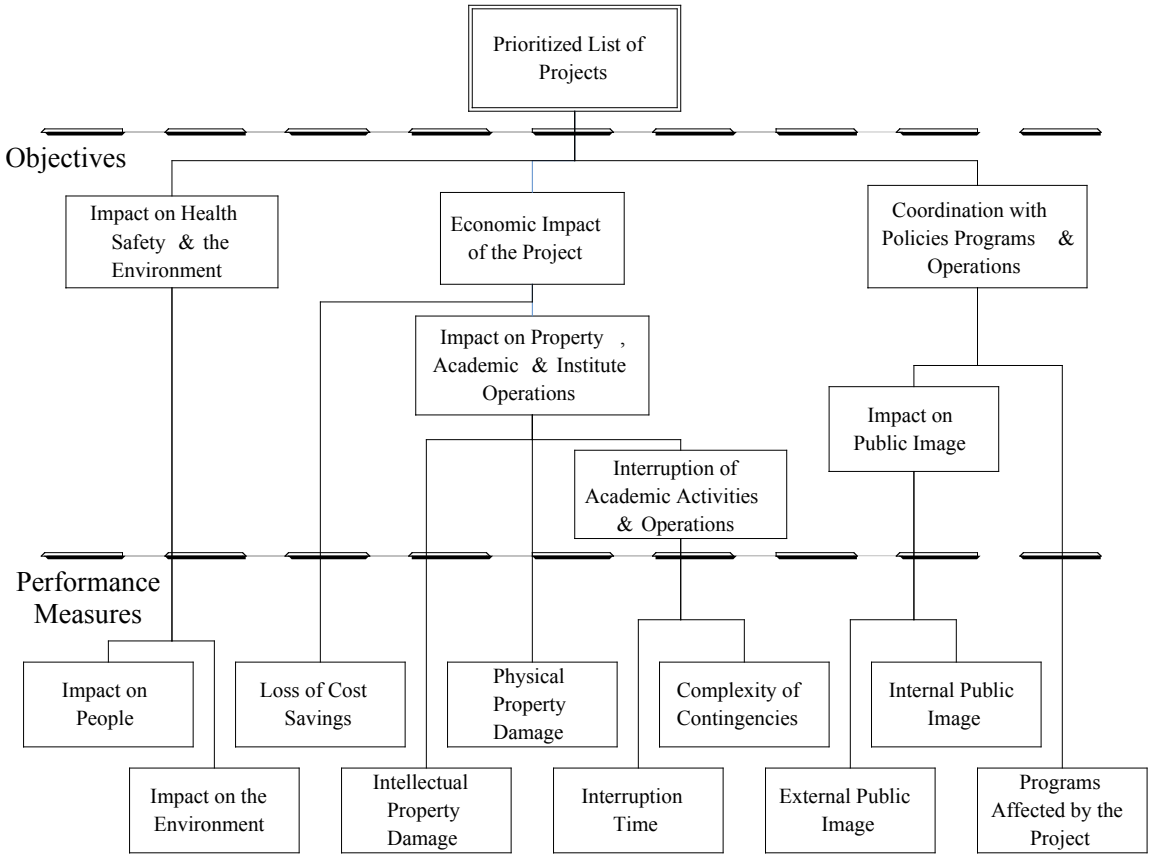

Figure II.2 MIT DOF Value Tree for infrastructure renewal projects. [Karydas and Gifun, 2002]

top of the value tree is the overall goal. In this example the Department of Facilities developed the value tree specifically as a decision tool to help the decision makers prioritize

infrastructure renewal projects. [Karydas and Gifun, 2002] Below the overall goal are the fundamental objectives. Next down the tree are the means objectives, where appropriate. Finally, the lowest level contains the performance measures. The number of elements and even the number of levels in the tree varies depending on the complexity of the decision and the desires to the decision maker.

Performance measures, sometimes referred to as attributes, are used to determine the extent to which the objectives are satisfied. Natural scales often exist for the assessment of PMs, like dollars for an economic objective or lost work days for a safety objective. When natural scales are not obvious, or not convenient, constructed scales are often used. [Keeney and Merkhofer, 1987] Often times the decision maker would prefer to use constructed scales for all the performance measures, even the ones with clearly defined natural scales. Constructed scales reduce the difficulty of assessment and allow the decision maker to combine multiple metrics into a single PM. A constructed scale is divided into zone levels with a description of the criteria appropriate to that level. The number of levels in each constructed scale is determined by the decision maker, but there should be sufficient levels to provide accurate results and not so many levels that the decision maker is overwhelmed. Constructed scales are developed for all the performance measures. A preliminary constructed scale from the analysis of infrastructure networks, for physical property damage, is shown in Table II.1.

Level	**Description**
3	Catastrophic physical property damage, Greater than $10 million
2	Major physical property damage $1 million to $10 million
1	Minor physical property damage Less than $1 million
0	No physical property damage

Table II.1 Preliminary Constructed Scale for physical property damage

The decision maker next assigns weights to the performance measures using the Analytic Hierarchy Process (AHP.) [Saaty, 1980] The decision maker begins with a series of

pair-wise comparisons between the fundamental objectives with respect to the primary goal. The comparisons are made using linguistic scale shown in Table II.2.

Intensity of Importance	Definition	Explanation
1	Equal importance	Two activities contribute equally to the objective.
3	Weak importance of one over another	Experience and judgment slightly favor one activity over another.
5	Essential or strong importance	Experience and judgment strongly favor one activity over another.
7	Very strong or demonstrated importance	An activity is favored very strongly over another; its dominance demonstrated in practice.
9	Absolute importance	The evidence favoring one activity over another is of the highest possible order of affirmation.
2,4,6,8	Intermediate values	When compromise is needed.

Table II.2 AHP Comparison scale [Saaty, 1980]

After completing the comparisons among the fundamental objectives, the decision maker moves down the value tree analyzing each level of objectives. The weight of the fundamental objective is passed down the value tree to the objectives below, with the weight being split among the objectives using AHP. [Weil and Apostolakis, 2001] The value tree is completed when all weights have been passed down the tree to the performance measures. The value tree is examined for consistence in AHP, with the decision maker determining the inconsistencies and correcting the value tree to eliminate them. [Saaty, 1980] The weights are converted into a 0 to 1 scale using a linear transformation. The weights for the DOF value tree for infrastructure renewal projects, Figure II.2, are shown in Table II.3. The local weight

describes the value of the objective, in relation to its siblings, to its parent objective. The global weight describes the value of the objective to the overall goal.

Objective	Local Weight	Global Weight
I. Impact on Health, Safety, and the Environment	0.491	0.491
A. Impact on People	0.600	0.295
B. Impact on the Environment	0.400	0.196
II. Economic Impact of the Project	0.233	0.233
C. Economic Impact on Property, Academic and Institute Operations	0.600	0.140
1. Physical Property Damage	0.210	0.029
2. Intellectual Property Damage	0.550	0.077
3. Interruption of Academic Activities and Operations	0.240	0.034
a. Interruption Time	0.500	0.017
b. Complexity of Contingencies	0.500	0.017
D. Loss of Cost Savings	0.400	0.093
III. Coordination with Policies, Programs, and Operations	0.276	0.276
E. Impact on Public Image	0.500	0.138
4. Internal Public Image	0.400	0.055
5. External Public Image	0.600	0.083
F. Programs Affected	0.500	0.138

Table II.3 Value tree weights for infrastructure renewal projects [Karydas and Gifun, 2002]

With the value tree and weights established, the decision maker assesses the disutility functions associated with the performance measures. The AHP is applied to the constructed scale for each performance measure to develop the disutility function. [Hughes, 1986] For each PM, the process follows the familiar pair-wise comparisons of the levels in the appropriate constructed scale. Once the weights have been assigned, and passed consistency checks, they are converted into a 0 to 1 scale by a linear transformation. The worst case disutility has the value 1 (full impact of the PM), and the least case disutility has the value 0 (no impact from the PM.) A constructed scale from the analysis of infrastructure networks, for physical property damage, which the disutility weights included, is shown in Table II.4.

Level	Description	Disutility
3	Catastrophic physical property damage Greater than $10 million	1.00
2	Major physical property damage $1 million to $10 million	0.27
1	Minor physical property damage Less than $1 million	0.03
0	No physical property damage	0.00

Table II.4 Constructed Scale for physical property damage

Once the value tree (including all weights) and the constructed scales (with disutility values) are complete the decision maker checks for consistency across the PMs. For example, compare the decision makers' preferences between physical property damage and impact on the environment, constructed scale displayed in Table II.5. The contribution

Level	Description	Disutility
3	Major Environmental Impact	1.00
2	Moderate Environmental Impact	0.34
1	Minor Environmental Impact	0.04
0	No Environmental Impact	0.00

Table II.5 Constructed Scale for environmental impact

to the overall assessment from each performance measure is the product of the weights of the PM and the disutility from the constructed scale. Comparing major physical property damage with a minor environmental impact reveals the contribution from each PM to the overall goal to be equal (less than 0.1% difference.)

PI (physical property damage) = weight (0.029) * disutility (0.27) = 0.00783
PI (environmental impact) = weight (0.196) * disutility (0.04) = 0.00784

So, the decision maker should be indifferent to suffering major physical property damage or minor environmental impact. If not, the decision maker may adjust the value tree weights and constructed scales disutility values until consistency is satisfied.

Finally, the decision analysis tool is benchmarked to validate the results. The prioritization tool is applied to several previously investigate cases and the results are compared to the historical data. The comparison serves to satisfy the decision maker that the prioritization tool is producing the desired results.

II.3 Networks and Minimal Cut Sets

In the search for understanding the vulnerabilities of critical infrastructures the concept of modeling the infrastructures as networks has been discussed. [Pate-Cornell and Gikema, 2002; Amin, 1999; Ezell, et al, 2000; Ballocco, et al, 2003] The network model and underlying graph theory provides for mathematical analysis of the infrastructures in the effort to identify the critical locations.

A graph G is an ordered triplet (V(G), E(G), $\__G$) consisting of a nonempty set V(G) of vertices, a set E(G), disjoint from V(G), of edges, and an incidence function $\__G$ that associates with each edge of G an unordered pair of (not necessarily distinct) vertices of G. If *e* is an edge and *u* and *v* are vertices such that $\__G(e)=u,v$ then *e* is said to join *u* and *v*; the vertices *u* and *v* are called ends of *e*. [Bondy and Murty, 1980]

For example, let

$G = (V(G), E(G), \__G)$

where

V(G) = {v1, v2, v3, v4, v5, v6, v7, v8}

E(G) = {e1, e2, e3, e4, e5, e6, e7, e8}

$\__G$(e1) = v1,v2 $\__G$(e2) = v2,v3 $\__G$(e3) = v3,v4 $\__G$(e4) = v2,v5

$\__G$(e5) = v5,v7 $\__G$(e6) = v5,v6 $\__G$(e7) = v7,v8 $\__G$(e8) = v6,v8

The graph G is displayed in Figure II.3.

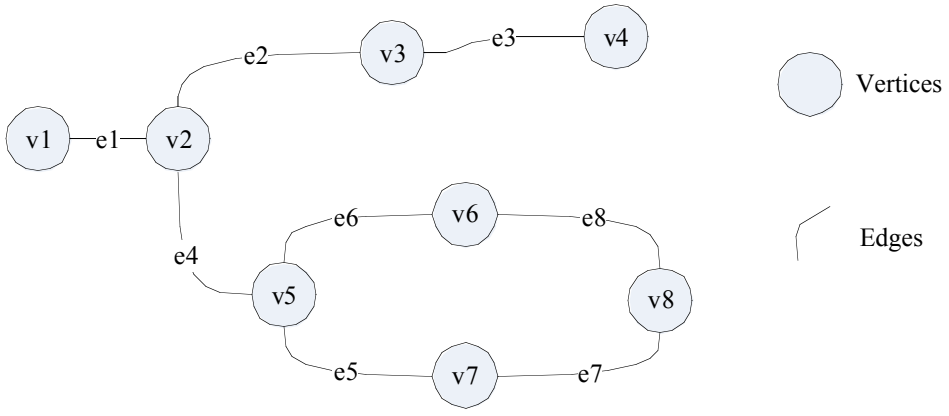

Figure II.3 Diagram of graph G

For any graph H, with *v* vertices and *e* edges, there corresponds a *vxe* matrix called the incident matrix of H. The incident matrix M(H) = [m_{ij}], where m_{ij} is the number of times (0, 1, or 2) that v_i and e_j are incident [Bondy and Murty, 1980]. When m_{ij} equals 0, the vertex *i* and the edge *j* are not incident. When m_{ij} equals 1, edge *j* either begins or ends at the vertex *i*. When m_{ij} equals 2, edge *j* both begins and ends at the vertex *i*, making edge *j* a loop. For the graph G shown in Figure II.3 the incident matrix M(G) is displayed in Table II.6. The incident

		Edges							
		e1	e2	e3	e4	e5	e6	e7	e8
Vertices	v1	1	0	0	0	0	0	0	0
	v2	1	1	0	1	0	0	0	0
	v3	0	1	1	0	0	0	0	0
	v4	0	0	1	0	0	0	0	0
	v5	0	0	0	1	1	1	0	0
	v6	0	0	0	0	0	1	0	1
	v7	0	0	0	0	1	0	1	0
	v8	0	0	0	0	0	0	1	1

Table II.6 Incident matrix M(G) for graph G

matrix is created to serve as the input table for computer analysis. This project employed *Mathematica*® as a graph analysis tool.

Two vertices *u* and *v* are connected if there is a path between them. In graph G vertices v5 and v4 are connected along path v5, e4, v2, e2, v3, e3, and v4. A cut edge (vertex) is an edge (vertex) that, if removed from the graph, would separate the graph into two distinct sections, having no path between them. A terminal vertex, i.e., a vertex with only one incident edge, can be a cut vertex in that it would separate that vertex from the rest of the graph. Examples of cut edges in graph G include edges e1, e2, e3, and e4; cut vertices include vertex v1, v2, v3, v4, v5, and v8. Edges e5, e6, e7, and e8 are not cut edges since the removal of one of them does not separate the graph. Similarly, vertices v6 and v7 are not cut vertices. A cut set K is a set of components (edges and/or vertices) that, if removed from the graph, would separate the graph into two distinct sections. [Bondy and Murty, 1980]

The discussion of edges has assumed the path to be bi-directional. For example, in graph G vertex v3 may be reached from vertex v3 via edge e2, and vertex v2 may be reached

from vertex v3 via edge e2 (in the opposite direction.) In such cases, graph G is non-directed, i.e., the edge allows "flow" in either direction. In some problems, such as interstate traffic flow or some utility distribution systems, the edges in the graph should be modeled to allow flow in one direction only. A directed graph D is an ordered triplet (V(D), A(D), $\__D$) consisting of a nonempty set V(D) of vertices, a set A(D), disjoint from V(D), of arcs, and an incidence function $\__D$ that associates with each arc of D an ordered pair of (not necessarily distinct) vertices of D. If *a* is an arc and *u* and *v* are vertices such that $\__D(a)=u,v$ then *a* is said to join *u* and *v*; *u* is the tail of *a* and *v* is its head. [Bondy and Murty, 1980] Arc *a* allows flow from vertex *u* to vertex *v*, but not from vertex *v* to vertex *u*. A directed graph is frequently referred to as a digraph. [Bondy and Murty, 1980]

For example, let

D = (V(D), A(D), $\__D$)

where

V(D) = {v1, v2, v3, v4, v5, v6, v7, v8}

A(D) = {a1, a2, a3, a4, a5, a6, a7, a8}

$\__D$(a1) = v1,v2 $\__D$(a2) = v2,v3 $\__D$(a3) = v3,v4 $\__D$(a4) = v2,v5

$\__D$(a5) = v5,v7 $\__D$(a6) = v5,v6 $\__D$(a7) = v7,v8 $\__D$(a8) = v6,v8

Digraph D is displayed in Figure II.4.

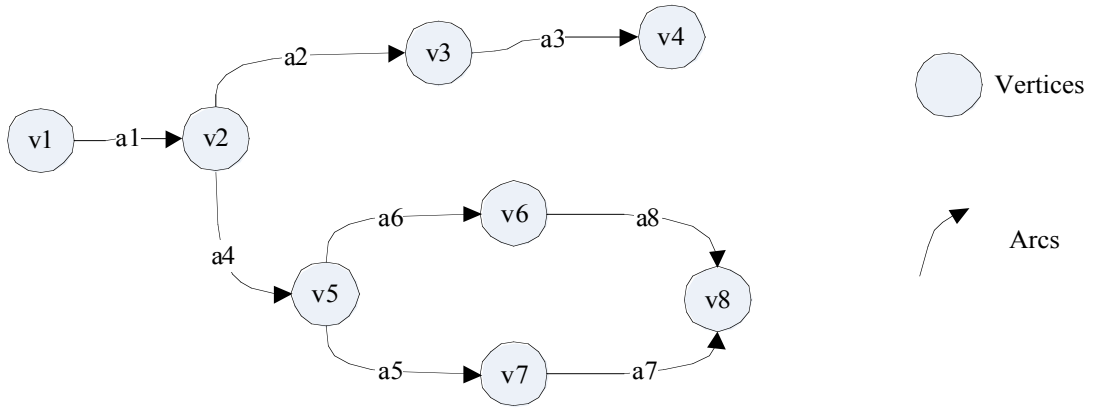

Figure II.4 Diagram of digraph D

Digraphs have an incident matrix similar to graphs. The incident matrix N(H) = [n_{ij}], where n_{ij} (-1, 0, 1, or 2) is the incidence relationship between vertex v_i and arc a_j [Bondy and Murty, 1980]. When n_{ij} equals 0, the vertex *i* and the arc *j* are not incident. When n_{ij} equals 1, the head of arc *j* is incident with vertex *i*. When n_{ij} equals -1, the tail of arc *j* is incident with vertex *i*. When n_{ij} equals 2, arc *j* both begins (tail) and ends (head) at the vertex *i*, making arc *j* a loop. For the digraph D shown in Figure II.4 the incident matrix N(D) is displayed in Table II.7.

		Arcs							
		a1	a2	a3	a4	a5	a6	a7	a8
Vertices	v1	-1	0	0	0	0	0	0	0
	v2	1	-1	0	-1	0	0	0	0
	v3	0	1	-1	0	0	0	0	0
	v4	0	0	1	0	0	0	0	0
	v5	0	0	0	1	-1	-1	0	0
	v6	0	0	0	0	0	1	0	-1
	v7	0	0	0	0	1	0	-1	0
	v8	0	0	0	0	0	0	1	1

Table II.7 Incident matrix N(D) for digraph D

Similar to the discussion concerning graphs, in a digraph two vertices *u* and *v* are connected, if there is a directed path between them. In digraph D, vertex v4 is connected to vertex v2 along the directed path v2, a2, v3, a3, and v4. But, vertex v2 is not connected to vertex v4 because there is not a directed path from vertex v4 to vertex v2. The concept of a cut arc (vertex) is the same for digraphs as graphs.

To model an infrastructure, say water distribution, with a digraph, we let vertices represent the valves, branches in the pipe, and the sources (supply vertices) and sinks (user vertices.) Arcs represent the water pipes. We are interested in identifying the events that interrupt service to the users. Let digraph D represent a water distribution system, Figure II.5, with one supplier (vertex v1) and two users, user A (vertex v4) and user B (vertex v8.) The supply node may be the actual water pumping station or it may just be a point in the water distribution network. In either case, the vertex is treated the same in the digraph analysis. We want to identify the cut sets (cut arcs and vertices, and sets of cut arcs and vertices) that interrupt service to each user. If the infrastructure service is interrupted from the user, we will

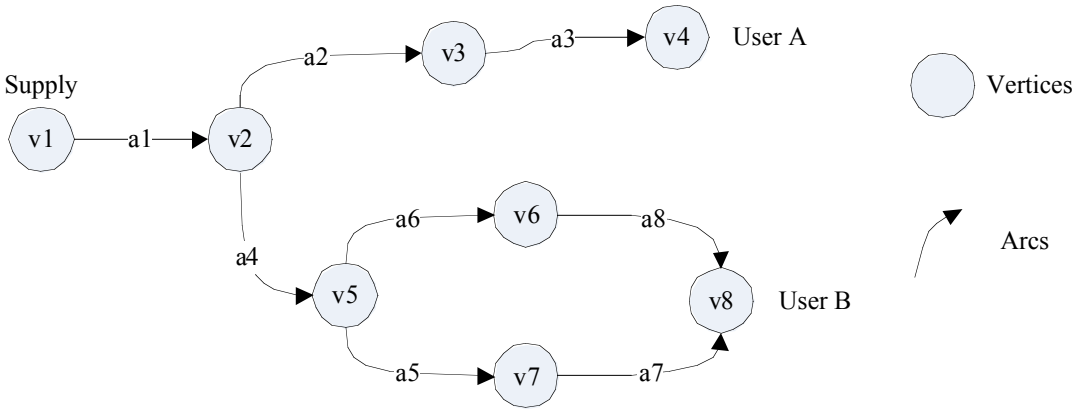

Figure II.5 Digraph D of a water distribution network

consider the system to have failed, and we are interested in the cut set(s) responsible for that failure. For a set of components (arcs and vertices) C = {1, 2, 3, ..., n}. A cut set K is a set of components in C, which by failing causes the system to fail, interrupts the infrastructure service to the user. A cut set is said to be minimal if it cannot be reduced without losing its status as a cut set [Bondy and Murty, 1980; Hoyland and Rausand, 1994]

For the analysis of infrastructures we will examine the cuts sets associated with each user. For example, analyzing digraph D in Figure II.5 for user A would produce many cut sets, K_A = {(a2), (a2,v3), (a2,a3), (a3,v3),…}. The cut sets that can be reduced, i.e., (a2,v3) and (a3,v3), are not minimal cut sets. The cut sets that cannot be reduced, i.e., (a2) and (a3), are minimal cut sets.

Minimal Cut Sets for digraph D in Figure II.5 are

User A, K_A = {(a1), (a2), (a3), (v1), (v2), (v3), (v4)}

User B, K_B = {(a1), (a4), (v1), (v2), (v5), (v8), (a6,a5), (a6,v7), (a6,a7), (a8,a5), (a8,v7), (a8,a7), (v6,a5), (v6,v7), (v6,a7)}

In analyzing the infrastructure network (digraph) for all users we are interested in discovering those cut sets which have the greatest impact, those which, when successfully attacked by terrorists, cause the greatest disutility among the user community. When looking at Figure II.4 one can intuitively see that cut sets (a1), (v1), and (v2) are more important than

any of the others because their loss causes an interruption of service to both user A and user B. Inspection is sufficient for very small system, but the decision maker would quickly become overwhelmed as the size of the infrastructure grows.

II.4 Risk Analysis Model

The Risk Analysis Model from the National Infrastructure Protection Center, NIPC, [NIPC, 2002] forms the framework for the assessment of the MIT infrastructure. This model follows the following five steps: Asset Assessment, Threat Assessment, Vulnerability Assessment, Risk Assessment, and Identification of Countermeasure Options. The Infrastructure Critical Location Risk Analysis Methodology, outlined in Figure II.6, is a decision analysis tool to assist the decision makers to fully evaluate the terrorism risk to the MIT community.

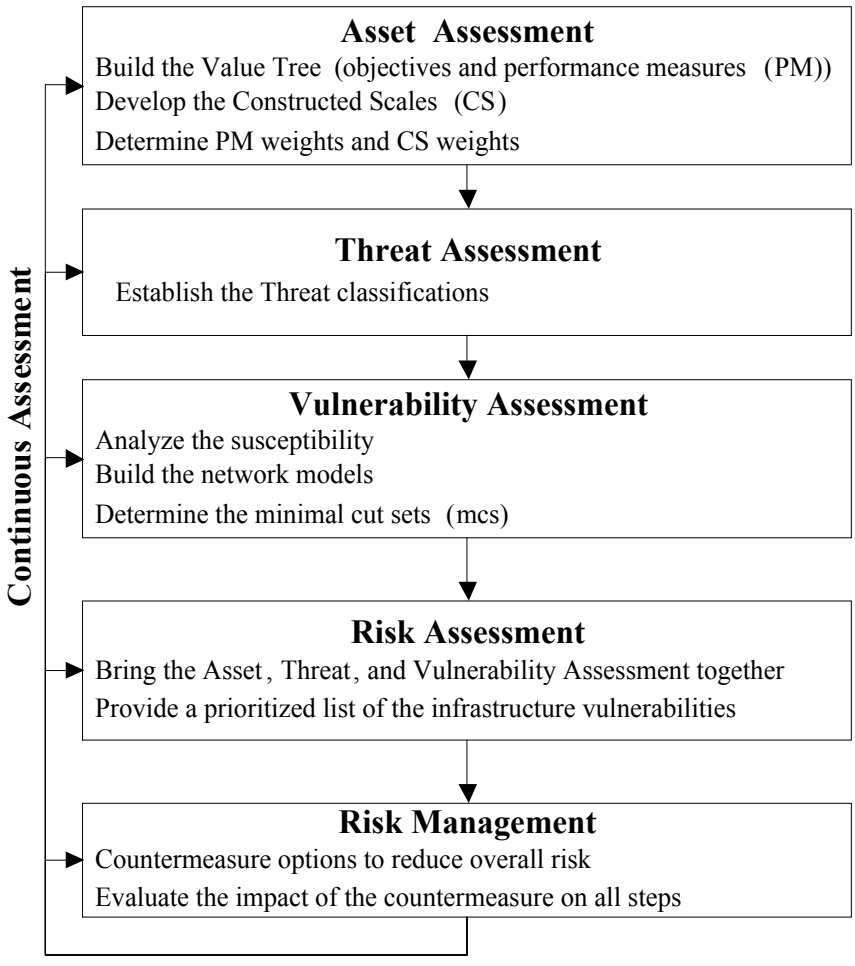

Figure II.6 Infrastructure Critical Location
Risk Analysis Methodology

II.4.A Asset Assessment

Asset Assessment is the process of understanding the "value" of the organization being analyzed. In the case of infrastructures the value is divided into distinct categories. First is the value of the infrastructures themselves. For example, the Hoover Dam has a certain value based on the repair or replacement costs (i.e. excavation, concrete, steel, machinery, and so on). Hoover Dam also has value because it is a national monument, which classifies it as a key asset. Additionally, the dam has value from the services is provides to the infrastructure users. It supplies electricity to the national electric grid, and recreation to the users of Lake Meade. In many cases the contribution to the infrastructures, and the associated end users, will significantly outweigh the repair costs or monumental "costs." The asset value can be expressed in terms of consequences of an undesirable event impacting a user. A detailed asset assessment of the MIT community was conducted by the MIT Department of Facilities. [Karydas and Gifun, 2002] This assessment established a baseline value of the assets, and will be discussed further in a following section.

II.4.B Threat Assessment

The Threat Assessment is specific to the community assets as established during the Asset Assessment. In a traditional threat assessment, the analyst would consider threats from all sources, including natural disasters, accidents, and human-generated attacks. This project is focused on the terrorist threat and, therefore, it is limited to human-generated malicious attack. The Threat Assessment requires identification and detailed assessment of the adversaries. For the MIT community the threat could be an international terrorist group, domestic terrorists, disgruntled community members, or others. For each threat (or threat group) the analyst will normally assess the intent, capability, as history of success of the particular adversary to develop a profile for the threat. The specific Threat Assessment is left to the security specialists, and additional details are not discussed here.

For this analysis of the MIT community we will make use of three threat profiles. These profiles are not the result of detailed threat assessments of security specialists, and should not be considered real life threats to MIT. The threat profiles are chosen to represent a few of the possibilities facing the community. The three scenarios we examine are:

Major Threat	A major threat is from an organization, group, or individual with significant capabilities. The threat may constitute a severe pinpoint attack against one or more infrastructures or a coordinated multi-axis attack against multiple locations. The attack would result in damage requiring long term restoration (greater than 1 month) and causing significant impact on the community.
Moderate Threat	A moderate threat is from a capable organization, group, or individual. The threat may constitute a pinpoint attack against one or more infrastructures or a coordinated multi-axis attack against two locations. The attack would result in damage requiring short term restoration (less than 1 month) and causing moderate impact on the community.
Minor Threat	A minor threat is from an organization, group, or individual with limited capabilities. The threat may constitute a single pinpoint attack against one or more infrastructures. The attack would result in minor damage requiring minimal restoration (less than one week) and causing minor impact on the community.

II.4.C Vulnerability Assessment

Vulnerability is defined as the susceptibility of an entity to attack. The Vulnerability Assessment reviews the environment to develop an understanding of the system weaknesses. In the case of critical infrastructures the analyst identifies and characterizes exploitable situations in these infrastructures. Susceptibilities may appear as poor access controls, such as open systems connected to the internet or the physically open MIT community. The lack of locks, guards, or security procedures is a potential vulnerability. The Vulnerability Analyst typically asks the question, "If I were a terrorist, I would..." This leads to a vide variety of points for consideration as initiating events.

Through the application of expert judgment vulnerability may be classified into broad categories to assist the analyst in describing the systems. Definitions for each category will depend on the specific environment and threat. An example of susceptibility classifications is presented in Table II.8.

Level	Description (examples)
Extreme	Completely open, no controls, no barriers
High	Unlocked, non-complex barriers (door or access panel)
Moderate	Complex barrier, security patrols, video surveillance
Low	Secure area, locked, complex closure
Very Low	Guarded, secure area, locked, alarmed, complex closure
Zero	Completely secure, no vulnerability (very unlikely)

Table II.8 Susceptibility categories

A second piece to the understanding of vulnerability is the importance of the point being described. Consider that a street light, which is completely open with no controls or barriers for protection, is extremely susceptible to attack. This would lead to initially classifying the street light as extremely vulnerable. However, to complete the description the analyst must consider the "value" of the street light. The replacement costs of the bulb, or even the entire light, are minimal. The street light is not a key asset, nor does it hold any monumental value. The likelihood of the loss of a street light cascading through the electrical distribution system is extremely small. There are some societal costs for continuing life with the street light out, but they should also be minor. So, while the street light is extremely susceptible to an attack it has very low value in the environment. Therefore, the street light is not a point that should be considered a critical location. The vulnerability of a point is a function of the susceptibility to attack and the value (from the asset assessment) of the point in the environment (infrastructure.) ***Vulnerability = f (Susceptibility, Value).*** Vulnerability categories are defined in Table II.9 and described in Table II.10.

Susceptibility	**Value**					
	Extreme	High	Moderate	Low	Very Low	Zero
Extreme	Red	Red	Orange	Yellow	Blue	Green
High	Red	Orange	Orange	Yellow	Blue	Green
Moderate	Orange	Orange	Yellow	Blue	Blue	Green
Low	Yellow	Yellow	Blue	Green	Green	Green
Very Low	Blue	Blue	Green	Green	Green	Green
Zero	Green	Green	Green	Green	Green	Green

Table II.9 Vulnerability Categories

Vulnerability	Description
Red	This category represents a sever vulnerability in the infrastructure. It is reserved for the most critical locations. Red vulnerabilities are those requiring the most immediate attention and prompt action.
Orange	The Orange vulnerability condition is the second priority for counter terrorism efforts. These locations are generally moderately to extremely valuable and moderately to extremely susceptible.
Yellow	The Yellow vulnerability condition is the third priority for counter terrorism efforts. These locations are normally less vulnerable because they are either less susceptible or less valuable that the terrorist desires.
Blue	The Blue vulnerability condition is the fourth priority for counter terrorism efforts.
Green	This is the final category for action. It gathers all locations not included in the more sever cases, typically those which are low (and below) on the susceptibility scale and low (and below) on the value scale. It is recognized that constrained fiscal resources is likely to limit efforts in this category, but it should not be ignored.

Table II.10 Vulnerability descriptions

II.4.D Risk Assessment

The Risk Assessment brings all the details together to provide the decision maker with a framework to analyze the community and understand the global risk. A prioritized list of infrastructure vulnerabilities is produced dependent upon the value of the assets, the threat specified by the security specialist, and the vulnerability of the infrastructures. The decision makers analyze the specified threat using the value tree and constructed scales developed during the Asset Assessment. A performance index (PI) table is compiled to represent the disutility of each user for each infrastructure. An example and full description of the PI table is presented in Table III.8, in section III.C. The decision maker combines the susceptibility of the infrastructures with the value, represented by the performance index, to produce a prioritized list of infrastructure vulnerabilities.

II.4.E Identification of Countermeasure Options (Risk Management)

Risk management build on the risk assessment process by seeking answers to a second set of three questions [Haimes, 1991]:

- What can be done and what options are available?
- What are the trade-offs in terms of costs, benefits, and risks?
- What are the impacts of current management decisions on future operations?

Countermeasures are intended to lower the overall risk to the assets. For each countermeasure the analyst must review the impact on each assessment for the entire community of assets. The risk assessment is repeated to account for the impact of the countermeasure. In assessing the countermeasure options, the analyst must ensure to account for the ongoing cost of the countermeasure. Also, it is important to account for any negative contribution the countermeasure may have to the overall risk. For example, many infrastructures run underground and are accessible via manholes. To protect services in a manhole the analyst may recommend welding the manhole covers in place to prevent unauthorized access. The ongoing cost of cutting the weld and re-welding the cover whenever access is required must be considered. Additionally, any cost (additional damage) incurred while emergency personnel wait to cut the weld to gain access to the manhole must be accounted for in the analysis.

II.4.F Continuous Assessment

Risk Assessment is not a one-time event, is must be a continuous process to achieve success. The analyst is required to vigilantly monitor the environment for changes that could impact the analysis. Asset values may change leading to a shift in consequences. New threats may emerge, old threats may fade away. Vulnerability may also change. Continuous assessment is necessary to timely address new risks.

III. Screening Methodology for Critical Infrastructures

III.1 Overview

To analyze infrastructures for vulnerabilities this project models each of the MIT campus infrastructures as an interconnected digraph. Arcs represent conduits for service, i.e. pipes for water and natural gas, and electrical cable for electricity. Vertices represent everything else in the infrastructure, including suppliers, users, pumps, valves, switches, and branches. Additionally, service access points are modeled as vertices. The impact of losing a service is modeled by the Performance Index (PI) measured through the disutility of the user losing the service. The PI is determined through analysis of the individual users with a value tree and performance measure constructed scales. Each user is analyzed to determine the minimal cut sets (mcs), arcs and vertices, which produced an interruption of an infrastructure supplied service. A mcs may be impact more than one user and/or more than one infrastructure. Once all the users have been examined, a database is compiled of the mcs, with the associated PI representing the "value" of the mcs to the infrastructure. The susceptibility of each mcs is assessed and combined with the value of the mcs to produce a vulnerability assessment of the mcs. A prioritized list of mcs for consideration is developed.

The infrastructure analysis model is a decision analysis tool to assist the decision maker in identifying the critical locations in infrastructures. The methodology for the efficient prioritization of infrastructure renewal projects [Karydas and Gifun, 2002] served as a starting point for the identification of critical locations in infrastructures. Through the application of expert judgment the value tree for the efficient prioritization of infrastructure renewal projects was modified to serve as the value tree for the identification of critical locations in infrastructures. The constructed scales for the analysis of the performance measures were adapted from the infrastructure renewal project for use in the critical location analysis. Network models of the selected infrastructures were developed and analyzed using graph theory to identify potential critical locations, i.e. the points in the network which, if lost, would lead to the greatest disutility among the user community. The susceptibility of the infrastructure network points were analyzed and combined with the performance index to establish the vulnerability of each location. Prioritization of the vulnerability list leads to the identification of critical locations in infrastructures.

III.2 The Value Tree

The Value Tree developed by the Department of Facilities (DOF) for the prioritization of infrastructure renewal projects is shown in Figure II.2. The objective and performance measure weights for the value tree were developed through expert judgment in workshops organized by DOF and are shown in Table II.3. The value tree and associated weights were developed using the AHP [Karydas and Gifun, 2002; Saaty, 1980] as described in section II.2. The value tree is hierarchical in nature, i.e. information is passed from an objective to its parent or children, and there is no information flow from an objective directly to a sibling. Recall, the local weight represents the contribution by the objective to its parent objective, and the global weight represents the contribution by the objective to the overall objective.

The DOF value tree contains many objectives and performances measures that are appropriate for the identification of critical locations in infrastructures. Rather than starting from ground zero, we adapted the DOF value tree into a value tree for the identification of critical locations in infrastructures. A review was conducted on the DOF value tree to assess the applicability of the objectives. Loss of Cost Savings, objective II-D, does not apply. This objective captures the economic loss incurred if a particular infrastructure renewal project is not completed. For example, consider a section of water supply piping that requires periodic maintenance to flush the water lines to prevent the build-up of undesirable material. A renewal project could replace the water supply line with an advanced material and eliminate the required periodic system flush, saving maintenance costs. There would be some impact to the community during the project to replace the piping, which would be modeled with the value tree. A decision not to replace the piping would generate a "loss of cost savings" as the periodic maintenance flush would be required to continue. The Loss of Cost Savings objective would capture that value. For a terrorist event there is no opportunity to experience a "loss of cost savings," so that objective requires elimination.

Additionally, Complexity of Contingencies, objective II-C-3-b, does not apply. This objective is designed to capture the pre-planning impact costs of a renewal project. For example, replacement of floors in a building with Asbestos tiles requires relocation of the building activities. The cost to relocate the users, such as establishing temporary laboratories, computing facilities, offices, and classrooms is modeled in the Complexity of Contingencies

objective. The actual impact from temporary relocation is captured in objective II-C-3-a, Interruption Time. Action taken in response to an immediate terrorist threat is not considered in the complexity of contingencies objective, but is accounted for in the vulnerability assessment. No additional objectives were identified, therefore none was added.

The two objectives, Loss of Cost Savings and Complexity of Contingencies, are eliminated from the value tree for terrorist event impact. The Loss of Cost Savings objective is eliminated first. Figure III.1a shows a portion of the DOF value tree with the changes

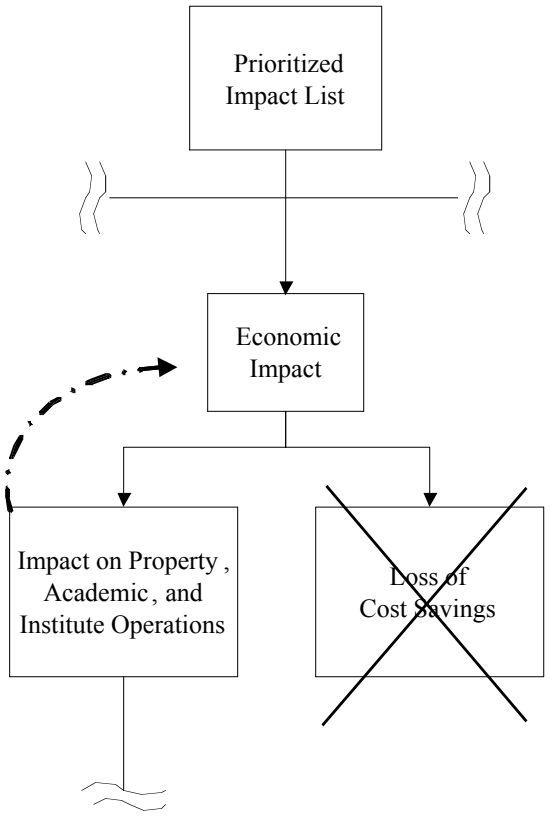

Figure III.1a DOF Value Tree (portion) [Karydas and Gifun, 2002]

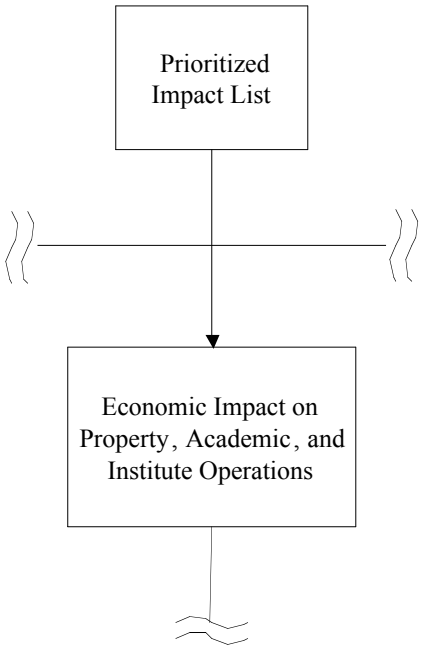

Figure III.1b Value Tree (portion)

outlined. The Loss of Cost Savings is simply eliminated and the Impact on Property, Academic, and Institute Operations is absorbed by the Economic Impact objective. The Economic Impact is renamed as the Economic Impact on Property, Academic, and Institute Operations to more accurately reflect the objective, Figure III.1b.

The Complexity of Contingencies objective was eliminated following the same process. Figure III.2a shows a portion of the DOF value tree with the changes highlighted.

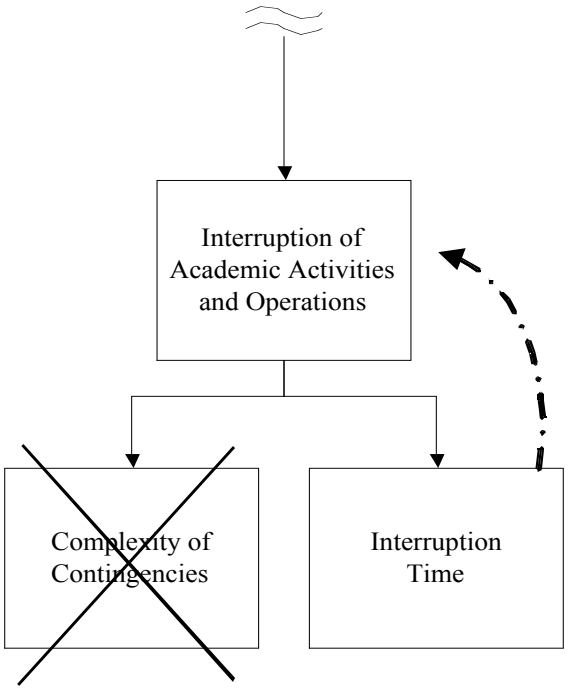

Figure III.2a DOF Value Tree (portion)
[Karydas and Gifun, 2002]

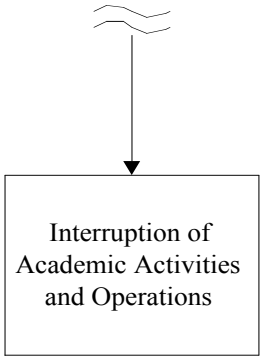

Figure III.2b – Value Tree (portion)

The Complexity of Contingencies objective was simply eliminated and its sibling, Interruption Time, was absorbed by the Impact on Property, Academic, and Institute Operations, Figure III.2b. Additionally, Coordination with Policies, Programs, and Operations, objective III, was renamed Stakeholder Impact to more accurately reflect the fundamental meaning of the impact category in the terrorism analysis.

The final value tree for the Impact of a Terrorist event is shown in Figure III.3. This value tree looks like it would if we had started from scratch and followed the decision analysis process described in section II.2. It represents the decision maker's fundamental objectives necessary in order to analyze the vulnerability of MIT community from terrorist activities. The value tree developed by a different decision maker may look different, as would a value tree we designed to analyze a different problem.

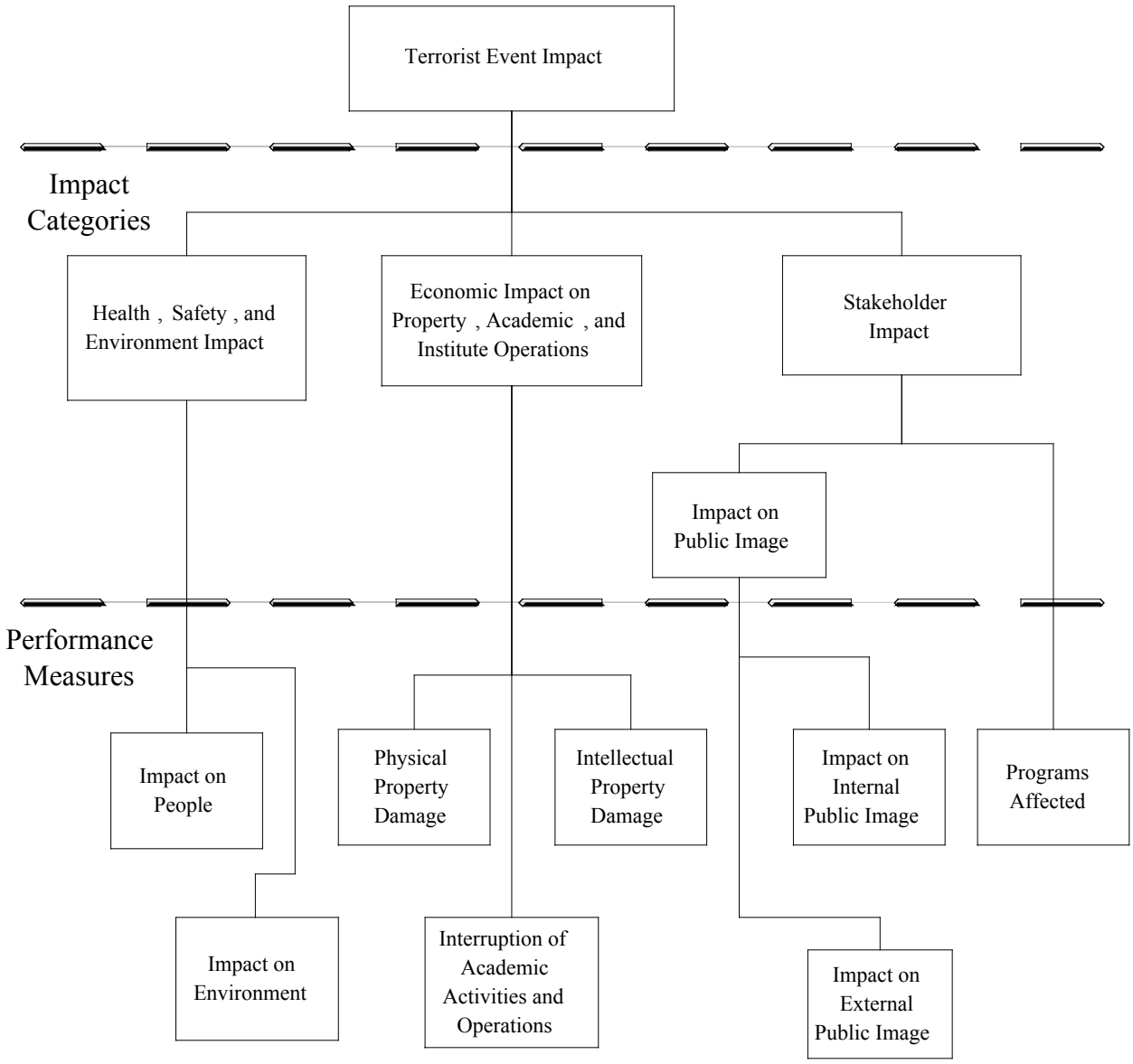

Figure III.3 Value Tree for Impact of Terrorism

The intent of this analysis is to identify the critical locations in infrastructures. We have replaced the classification "objective" with "impact categories" as it is more representative of the nature of this methodology. We assigned the value tree weights using the AHP as discussed in section II.2. Since many of the impact categories and performance measures were carried over from the infrastructure renewal project the weights associated with those attributes were used as a starting point. The importance of the three impact

categories worked out the same for the two projects. And, the weight of the Economic Impact on Property, Academic, and Institute Operations (Economic Impact in the DOF value tree) remains unchanged with respect to the sibling impact category (Impact on Health, Safety, and the Environment; and Coordination with Policies, Programs, and Operations). The Economic Impact on Property, Academic, and Institute Operations objective retains weight 0.233.

In the DOF value tree the impact on property, academic, and institute operations carries 60 percent of the economic impact, and loss of cost savings accounted for the remaining 40 percent. The 60 percent passed to the impact on property, academic, and institute operations was further split among the three children (PMs.) The split allocated 21 percent to physical property damage, 55 percent to intellectual property damage, and 24 percent to interruption of academic activities and operations. So, the PM weight for intellectual property damage in the DOF value tree was determined by:

$$W_{PM\_ipd} = W_{econ\_imp} * W_{impact\_pai} * W_{intel\_prop\_dam}$$

$$W_{PM\_ipd} = 0.233 * 0.600 * 0.550$$

$$W_{PM\_ipd} = 0.077$$

where

W_{PM_ipd} is the global weight of the intellectual property damage PM.

W_{econ_imp} is the global weight of the economic impact fundamental impact category.

W_{impact_pai} is the fractional split of the economic impact dedicated to the impact on property, academic, and institute operations.

$W_{intel\_prop\_dam}$ is the fractional split of the impact on property, academic, and institute operations dedicated to intellectual property damage.

The weight of the Loss of Cost Savings objective, just eliminated, was absorbed by the sibling objective (Impact on Property, Academic, and Institute Operations). The new fundamental impact category (Economic Impact on Property, Academic, and Institute Operations) passes its entire weight (0.233) to its new children (Physical Property Damage, Intellectual Property Damage, and Interruption of Academic Activities and Operations). The weight is split among the children in the same proportion as in the DOF value tree, where the

three attributes were siblings. In the critical infrastructure value tree the PM weight for intellectual property damage in the DOF value tree is determined by:

$$W_{PM\_ipd} = W_{ei\_pai} * W_{intel\_prop\_dam}$$

$$W_{PM\_ipd} = 0.233 * 0.550$$

$$W_{PM\_ipd} = 0.128$$

where

W_{PM_ipd} is the global weight of the intellectual property damage PM.

W_{ei_pai} is the global weight of the economic impact on property, academic, and institute operations fundamental impact category.

$W_{intel\_prop\_dam}$ is the fractional split of the economic impact on property, academic, and institute operations dedicated to intellectual property damage.

The weight of the Complexity of Contingencies objective, eliminated, was absorbed by the sibling objective (Interruption Time), leaving the objective for the Interruption of Academic Activities and Operations with one performance measure (Interruption Time). The PM was merged with the objective, creating a new performance measure (Interruption of Academic Activities and Operations.) The weight of the objective (Interruption of Academic Activities and Operations) in the DOF value tree becomes the local weight of the PM in the terrorism value tree. The global weight is recalculated following the method illustrated for the intellectual property damage PM.

The terrorism value tree, Figure III.3, and weights, Table III.1, are specific to the MIT campus and the particular decision makers conducting the analysis. These tools, the impact categories, value tree, and weights are specific to the MIT community analysis for the identification of critical locations in infrastructures. Application of this methodology in another environment would require development of applicable impact categories, value tree and weights.

Impact Category	Local Weight	Global Weight
I. Impact on Health, Safety, and the Environment	0.491	0.491
A. Impact on People	0.600	0.295
B. Impact on the Environment	0.400	0.196
II. Economic Impact on Property, Academic and Institute Operations	0.233	0.233
C. Physical Property Damage	0.210	0.049
D. Intellectual Property Damage	0.550	0.128
E. Interruption of Academic Activities and Operations	0.240	0.056
III. Coordination with Policies, Programs, and Operations	0.276	0.276
F. Impact on Public Image	0.500	0.138
1. Internal Public Image	0.400	0.055
2. External Public Image	0.600	0.083
G. Programs Affected	0.500	0.138

Table III.1 Value Tree impact category and performance measure weights

III.3 Disutility and Constructed Scales

In the standard application of Decision Analysis the utility function produces a measure of preference. In this case the desire to avoid undesirable outcomes led to the employment of disutility, i.e., the higher the disutility value the lower the desirability. The most and least desirable levels are represented by the extreme values of d=0 and d=1, respectively. The impact of each event is evaluated against the performance measures defined in the value tree. The constructed scales developed by the DOF were used as a starting point for the critical infrastructure analysis. DOF generated the constructed scales by following the AHP method described in section II.2. We applied the AHP methods as described in section II.2 in developing the constructed scales for the identification of critical locations in infrastructure value tree.

Constructed scales for physical property damage and environmental impact were presented in Table II.4 and Table II.5 respectively. The remaining constructed scales are displayed in Tables III.2 through III.7.

Level	Description	Disutility
4	Extreme Interruption Greater than 6 months, entire buildings evacuated and activities relocated.	1.00
3	Major Interruption 1 to 6 months, laboratories evacuated and activities relocated.	0.57
2	Moderate Interruption 1 to 4 weeks, specialty classrooms evacuated and activities relocated.	0.19
1	Minor Interruption Less than 1 week, a few administrative units or small classrooms evacuated and activities relocated.	0.06
0	No Interruption	0.00

Table III.2 Constructed Scale for interruption of academic activities & operations

Level	Description	Disutility
3	Fatality or Lethal Exposure Ex. Roof Collapse, Falling Brick, Inhalation of Gas	1.00
2	Major Exposure with Long Term Effects Ex. Lead Poisoning	0.46
1	Minor Injury or Exposure Ex. Broken Arm, Laceration	0.05
0	No personal injury	0.00

Table III.3 Constructed Scale for impact on people

Level	Description	Disutility
3	Catastrophic intellectual property damage Long-term experiments	1.00
2	Major intellectual property damage Artifacts and rare documents	0.46
1	Minor intellectual property damage Non-backed up electronic data	0.05
0	No intellectual property damage	0.00

Table III.4 Constructed Scale for intellectual property damage

Level	Description	Disutility
3	Major degree of adverse publicity Petitions, sit-ins, demonstrations	1.00
2	Moderate degree of adverse publicity Negative articles published	0.34
1	Minor degree of adverse publicity Verbal complaints	0.04
0	No adverse publicity	0.00

Table III.5 Constructed Scale for internal public image

Level	Description	Disutility
3	Major degree of adverse publicity Affects enrollment, contributions, program funding, or faculty recruiting	1.00
2	Moderate degree of adverse publicity National / International Media	0.57
1	Minor degree of adverse publicity Local media	0.06
0	No adverse publicity	0.00

Table III.6 Constructed Scale for external public image

Level	Description	Disutility
4	Extreme Impact Greater than $20 million and/or impacting greater than 250 students	1.00
3	Major Impact $10 million to $20 million and/or impacting 50 to 250 students	0.50
2	Moderate Impact $1 million to $10 million and/or impacting 5 to 50 students	0.23
1	Minor Impact Up to $1 million and/or impacting up to 5 students	0.02
0	No Impact	0.00

Table III.7 Constructed Scale for programs affected

Following completion of the value tree (including all weights) and the constructed scales (with disutility values) we checked for consistency across the PMs. For example, we compared our preferences between programs affected, Table III.7, and interruption of academic activities and operations, Table III.2. The contribution to the overall assessment from each performance measure is the product of the weights of the PM and the disutility from the constructed scale. Comparing a moderate impact on programs affected with a major

interruption of academic activities and operations reveals the contribution from each PM to the overall goal to be very close.

PI (programs affected) = weight (0.138) * disutility (0.23) = 0.0318

PI (interruption of academic activities and operations) =
weight (0.056) * disutility (0.57) = 0.0319

The consistency check suggests that we should be indifferent to suffering a moderate impact on programs affected or suffering a major interruption of academic activities and operations. If we are not indifferent then we would adjust the value tree weights and constructed scale disutility values to reflect our preference.

As another example we performed a three way comparison among intellectual property damage (major intellectual property damage), Table III.4, internal public image (major degree of adverse publicity), Table III.5, and interruption of academic activities and operations (extreme interruption), Table III.2.

PI (intellectual property damage) = weight (0.128) * disutility (0.46) = .0589

PI (internal public image) = weight (0.055) * disutility (1.00) = 0.0550

PI (interruption of academic activities and operations) =
weight (0.056) * disutility (1.00) = 0.0560

The consistency check suggests we are indifferent to suffering a major degree of adverse publicity or an extreme interruption of academic activities and operations. Also, that we value major intellectual property damage as slight more damaging (these are disutilities) than a major degree of adverse publicity or an extreme interruption of academic activities and operations. If these do not reflect our preferences then we would adjust the value tree weights and constructed scale disutility values as necessary.

III.4 Network Models

The infrastructures are modeled using networks to take advantage of existing network analysis in our investigation. For this study the analysis is limited to three interconnected hard infrastructures: Natural Gas, Water, and Electricity. Wireless networks, both telephone and data, present different challenges and are not addressed in this work. The original analysis contains actual locations and infrastructure designations that are MIT campus specific. The work presented in this report is from the MIT analysis, but the names and designators have been changed to prevent any inadvertent release of potentially sensitive information.

Figure III.4 shows a portion on the Natural Gas distribution system. This section of the MIT community is isolable from the remainder of the natural gas distribution system with an isolation valve upstream of the Supply point. This particular section of the campus

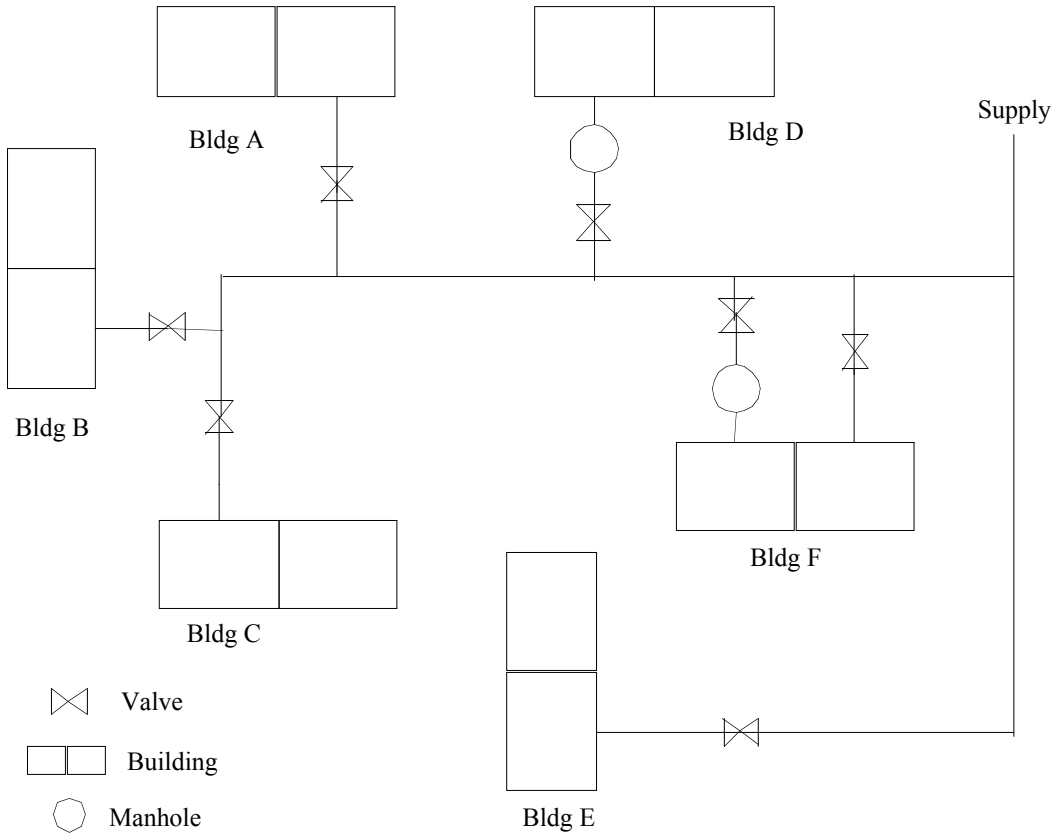

Figure III.4 Natural Gas distribution schematic (partial)

represents one supply and six users, five end users and one user (building F) configured to allow gas flow through to other portions of the network.

The network representation of this portion of the natural gas distribution system is shown in Figure III.5. The network vertices, shown as circles, represent the supply, users, valves, branches, and manhole access points in the piping system. All connected vertices

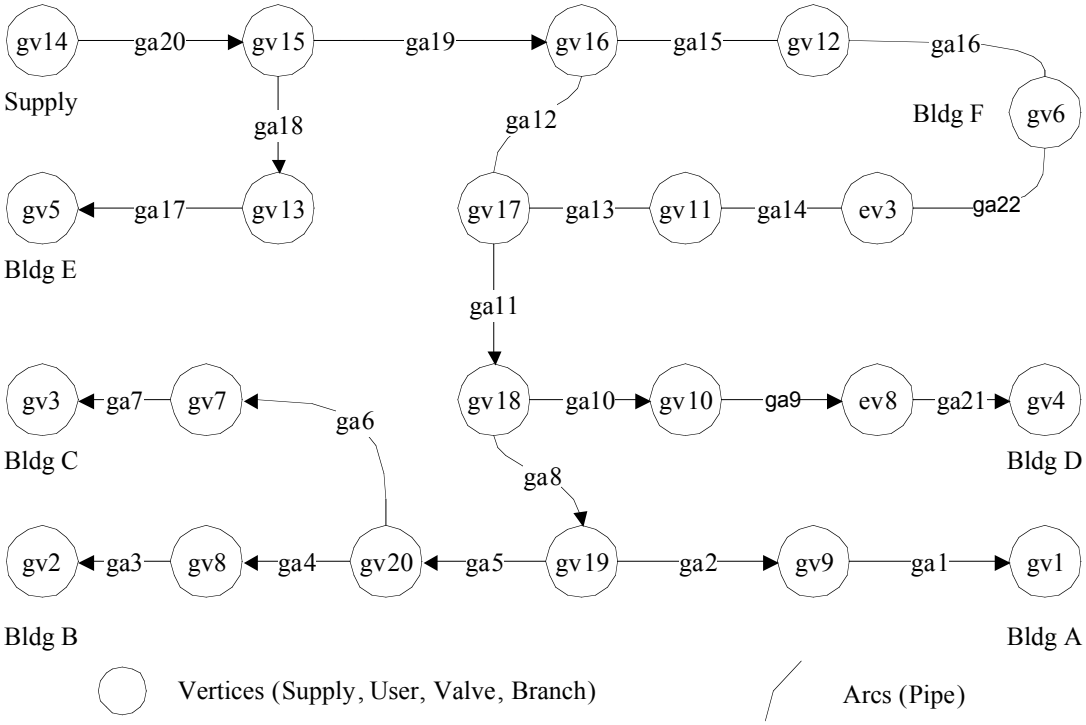

Figure III.5 – Natural Gas distribution network digraph

have one or more associated arcs. The vertices are numbered, inside the circles, for identification purposes to support network analysis. The arcs, shown as lines, represent the piping. All arcs have two, and only two, associated vertices. An arc may be incident to the same vertex at both its tail and head, in which case the arc forms a loop starting and ending at the same vertex. A dead end pipe would have an originating vertex and a dummy vertex at the "dead end." The arcs are numbers, adjacent to each arc.

The natural gas system contains few flow directors, such as check valves or pressure reducers. Direction of gas flow is determined by the pressure gradient. Normally the supply

will be at relatively high pressure and user at relatively low pressure, so gas will flow from supply to user. The network is represented in the incident matrix shown in Table III.8.

Vertices - Natural Gas (gv) / Electric (ev)	Natural Gas Arcs (ga)																					
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22
3	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	1
8	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	-1	0
1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0
5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0
6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	1
7	0	0	0	0	0	1	-1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
8	0	0	-1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
9	-1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0	0	-1	1	0	0	0	0	0	0	0	0	0	0	0	0
11	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	0	0	0	0	0	0	0
12	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	0	0	0	0	0
13	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	-1	1	0	0	0	0
14	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	-1	0	0
15	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	-1	-1	1	0	0
16	0	0	0	0	0	0	0	0	0	0	0	1	0	0	1	0	0	0	1	0	0	0
17	0	0	0	0	0	0	0	0	0	0	-1	1	1	0	0	0	0	0	0	0	0	0
18	0	0	0	0	0	0	0	-1	0	-1	1	0	0	0	0	0	0	0	0	0	0	0
19	0	-1	0	0	-1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
20	0	0	0	-1	1	-1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Table III.8 Incident matrix for natural gas distribution

Most arcs are directed, having a specific tail (-1) and head (1), because flow goes in one direction only. Some arcs, ga16 for example, are non-directed. These arcs, indicated with two 1s, one for each incident vertex, permit flow in either direction depending on the network configuration and pressure gradient. The natural gas distribution system contains two vertices (ev3 and ev8) which are part of the electrical distribution system. These vertices are electric manholes designed primarily to serve as access points to the electric distribution switching network. The natural gas piping runs through, or adjacent to, the two identified manholes. The electrical and natural gas networks are not physically connected at the manhole, but are

geographically coincident. The two infrastructures are connected in cases where electricity is powering a natural gas pressurizing pump or a natural gas fired turbine is generating electricity. In the case of connected infrastructures the natural network modeling would use a vertex to model the incidence of the two networks. In modeling the MIT infrastructures, we included vertices to account for those geographic locations where two or more infrastructures are coincident. A vertex is also used to model the situations where an infrastructure is geographically coincident with itself. For example, this can occur when two gas pipes (not physically connected to allow flow) are located in the same service man-way.

Figure III.6 shows a portion of the Water distribution system. This section of the MIT community is isolable from the remainder of the water distribution system with an isolation

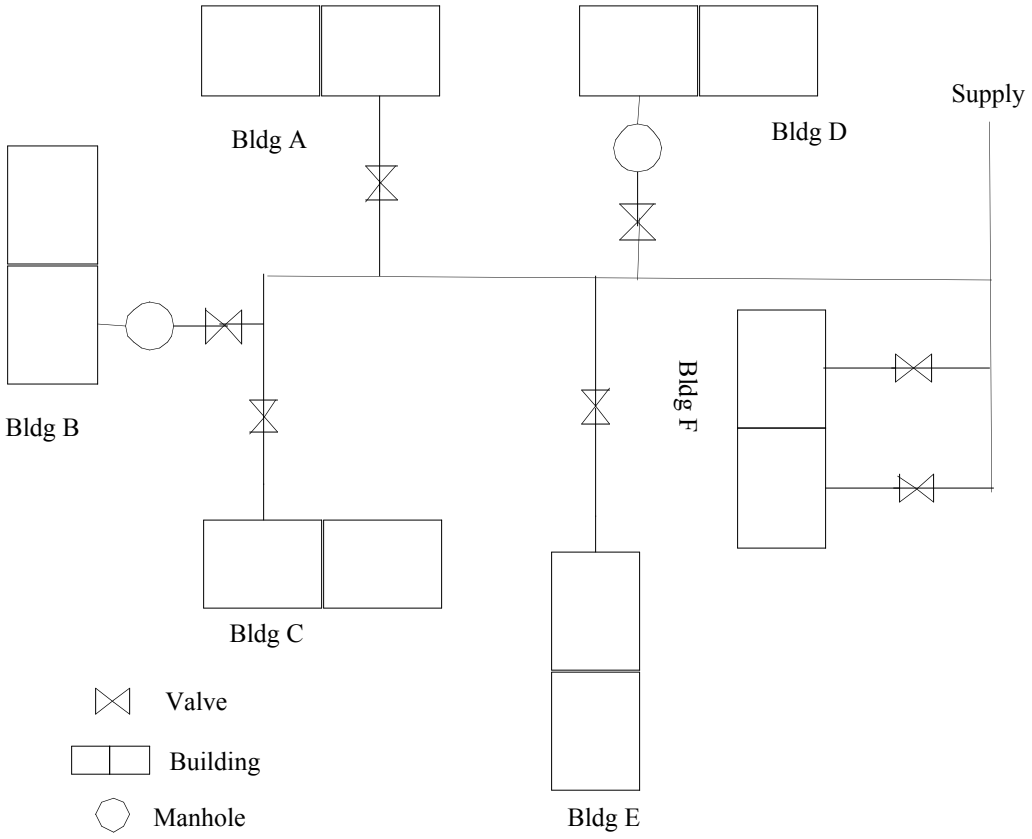

Figure III.6 Water distribution schematic (partial)

valve upstream of the Supply point. This particular section of the campus represents one supply and the same six users modeled in the natural gas network.

The network representation of this portion of the water distribution system is shown in Figure III.7. The network vertices, shown as circles, represent the supply, users, valves,

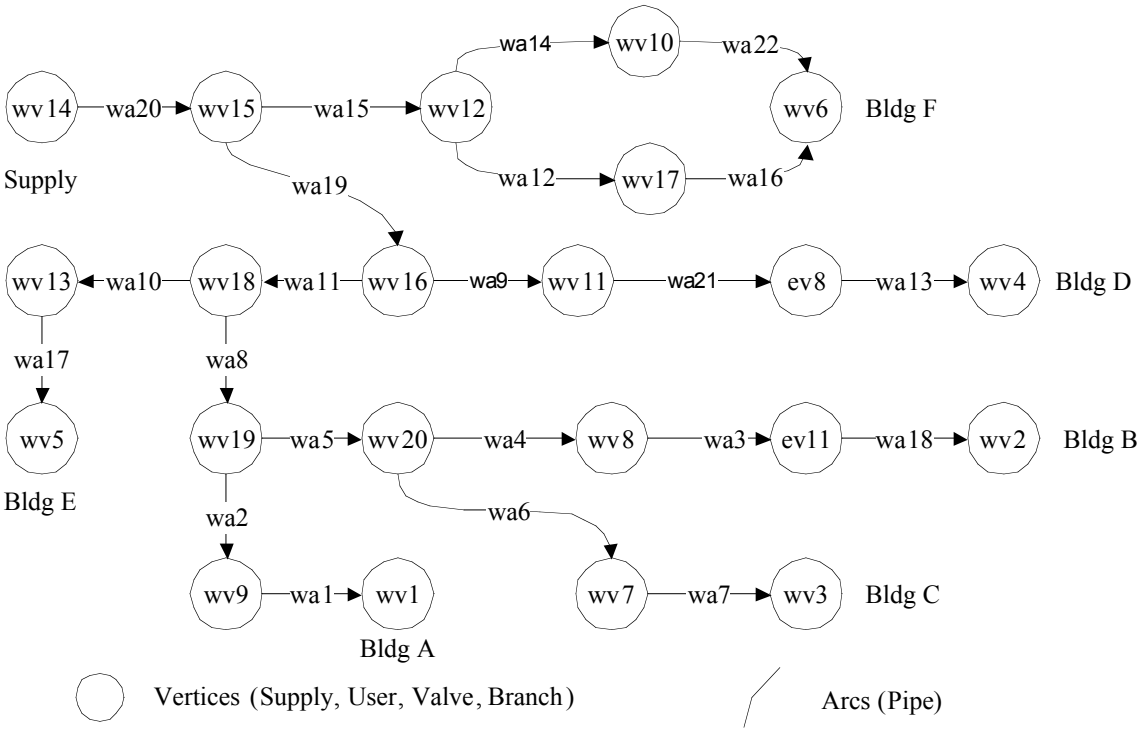

Figure III.7 – Water distribution network digraph

branches, and manhole access points in the piping system. All connected vertices have one or more associated arcs. The vertices are numbered for identification purposes to support network analysis. The arcs, shown as lines, represent the piping.

The water system contains few flow directors, such as check valves or pressure reducers. Direction of water flow is determined by the pressure gradient. Normally the supply will be at relatively high pressure and user at relatively low pressure, so water will flow from supply to user. The network is represented in the incident matrix shown in Table III.9. All the water distribution arcs in the displayed section are directed, having a specific tail (-1) and head (1), because flow goes in one direction only. The water distribution network may have sections which allow water flow in either direction, similar to the natural

gas network discussed previously. In the case of non-directed flow, the arc is indicated with two 1s, one for each incident vertex, permitting flow in either direction depending on the network configuration and pressure gradient.

Vertices - Electric (ev) / Water (wv)	Water Arcs (wa) 1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22
8	0	0	0	0	0	0	0	0	0	0	0	0	-1	0	0	0	0	0	0	0	1	0
11	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	-1	0	0	0	0
1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0
3	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0
6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	1
7	0	0	0	0	0	1	-1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
8	0	0	-1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
9	-1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	-1
11	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	-1	0
12	0	0	0	0	0	0	0	0	0	0	0	-1	0	-1	1	0	0	0	0	0	0	0
13	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	-1	0	0	0	0	0
14	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	-1	0	0
15	0	0	0	0	0	0	0	0	0	0	0	0	0	0	-1	0	0	0	-1	1	0	0
16	0	0	0	0	0	0	0	0	-1	0	-1	0	0	0	0	0	0	0	1	0	0	0
17	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	-1	0	0	0	0	0	0
18	0	0	0	0	0	0	0	-1	0	-1	1	0	0	0	0	0	0	0	0	0	0	0
19	0	-1	0	0	-1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
20	0	0	0	-1	1	-1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Table III.9 Incident matrix for water distribution

The water distribution system contains two vertices (ev8 and ev11) which are part of the electrical distribution system. These vertices are electric manholes designed primarily to serve as access points to the electric distribution switching network. As with the natural gas piping passing through the electric manhole, the electrical and water networks are not physically connected at the manhole, but are geographically coincident. The modeling is consistent with the previous description.

The MIT electrical system, both generation and distribution, is handled in the Central Utilities Plant. Major electrical buses are energized from the natural gas fired turbine generator or back-up generation. The electrical buses feed the electrical cables disbursed through campus to provide electricity to the users (buildings.) An electrical cable forms a loop on the campus, beginning at bus 'A', winding through campus in service ducts, and ending at bus 'B.' Electricity may originate from either bus. Switches places along the cable direct electricity to various buildings. The system is made up of a number of loops, with each loop providing electricity to several buildings. A schematic, Figure III.8, shows two

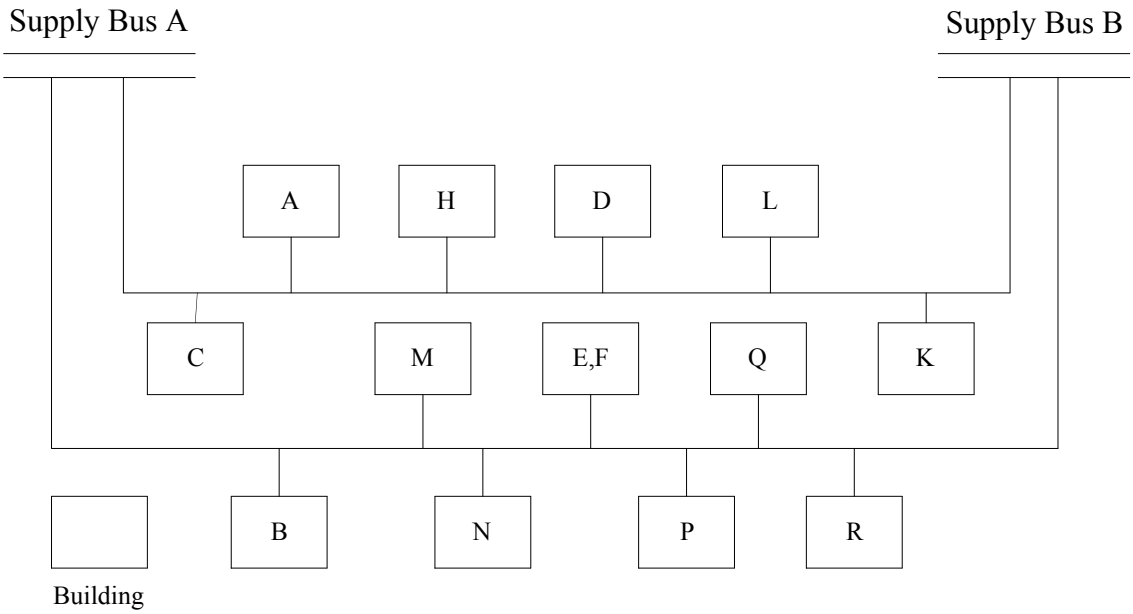

Figure III.8 Electrical distribution schematic (partial)

distribution loops for the section of campus coinciding with the natural gas and water infrastructures. The loops are modeled with non-directed edges, as electricity can flow in either direction around the loop. The electric lines from the switches to the buildings are modeled with directed arcs, as electricity only flows from the distribution loop to the building.

The network representation of these portions of the electrical distribution system are shown in Figure III.9 (loop one) and Figure III.10 (loop two.) The network vertices, shown as circles, represent the supply, users, switches, branches, and manhole access points in the

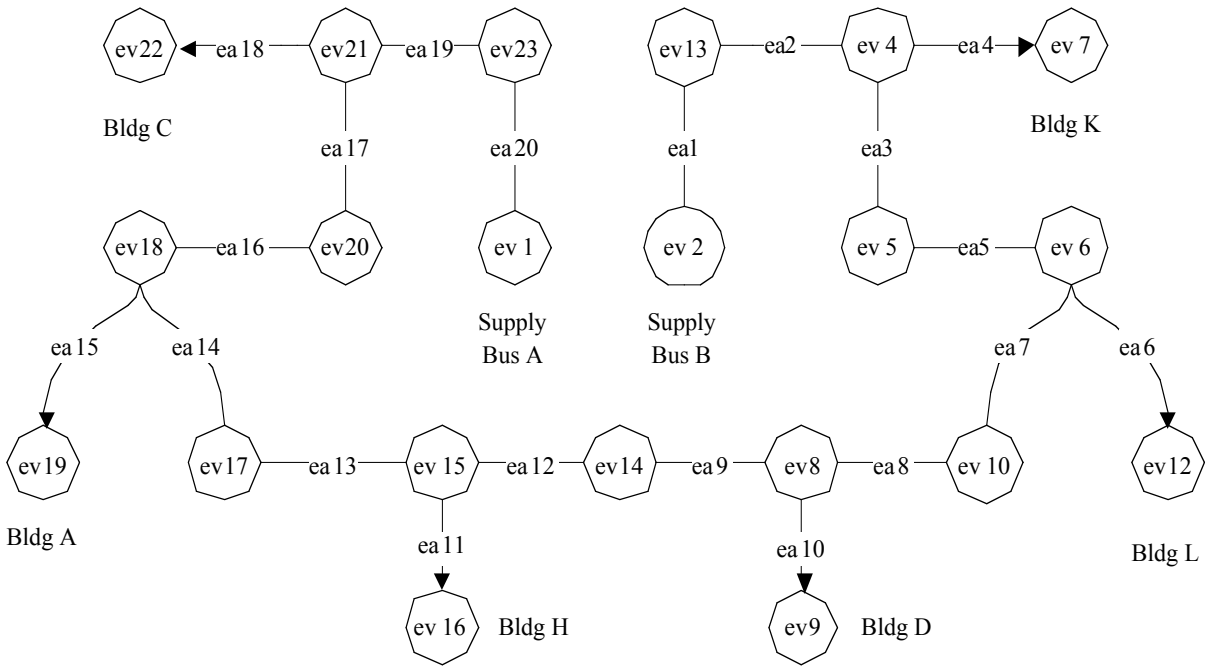

Figure III.9 Electrical distribution network digraph (loop one)

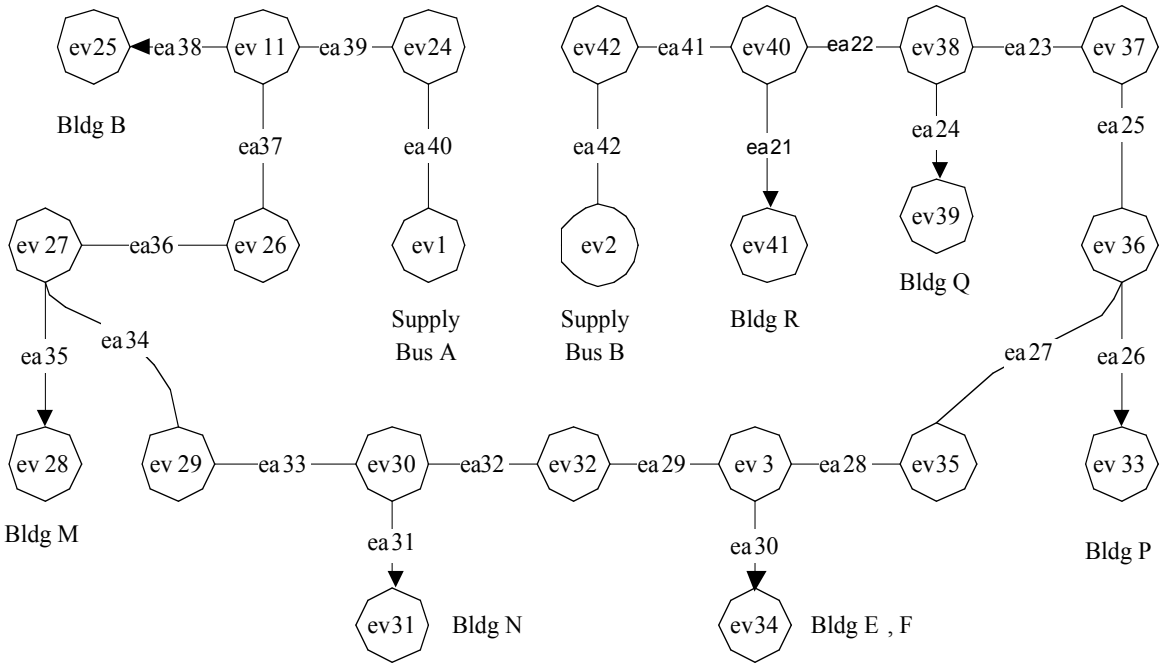

Figure III.10 Electrical distribution network digraph (loop two)

cabling system. The vertices are numbered, inside the circles, for identification purposes to support network analysis. The edges and arcs, shown as lines, represent the electrical cables. The electrical service ducts run primarily underground and are accessible from a number of manholes located throughout campus. The manholes provide service access for technicians to conduct maintenance. The electric manholes (there is an independent set of telecommunications manholes on campus) are primarily associated with the electrical distribution system, however in some cases other infrastructure services run through or immediately adjacent to the manholes. Some of the manholes contain only cabling; these are modeled by a vertex with two incident arcs (or edges), and electricity simply flows through these manholes. Other manholes contain switches which accept electricity from either loop direction and provide current to the user (building.) These points are modeled by a vertex

Elecrtic Vertices (ev) \ Electric Arcs (wa)	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
2	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
4	0	1	1	-1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
5	0	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
6	0	0	0	0	1	-1	1	0	0	0	0	0	0	0	0	0	0	0	0	0
7	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	1	1	-1	0	0	0	0	0	0	0	0	0	0
9	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0
10	0	0	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0
12	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
13	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
14	0	0	0	0	0	0	0	0	1	0	0	1	0	0	0	0	0	0	0	0
15	0	0	0	0	0	0	0	0	0	0	-1	1	1	0	0	0	0	0	0	0
16	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0
17	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	0	0	0	0	0
18	0	0	0	0	0	0	0	0	0	0	0	0	0	1	-1	1	0	0	0	0
19	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0
20	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	0	0
21	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	-1	1	0
22	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0
23	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1

Table III.10 Incident matrix for electrical distribution (loop one)

with three or more incident vertices to account for splitting the electricity flow. The incident matrices for loops one and two of the electrical distribution system are displayed in Table III.10 and Table III.11, respectively.

Electric Vertices (ev) \ Electric Arcs (wa)	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42
1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0
2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
3	0	0	0	0	0	0	0	1	1	-1	0	0	0	0	0	0	0	0	0	0	0	0
11	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	-1	1	0	0	0
24	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	0
25	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0
26	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	0	0	0	0
27	0	0	0	0	0	0	0	0	0	0	0	0	0	1	-1	1	0	0	0	0	0	0
28	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0
29	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	0	0	0	0	0	0	0
30	0	0	0	0	0	0	0	0	0	0	-1	1	1	0	0	0	0	0	0	0	0	0
31	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0
32	0	0	0	0	0	0	0	0	1	0	0	1	0	0	0	0	0	0	0	0	0	0
33	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
34	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0
35	0	0	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
36	0	0	0	0	1	-1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
37	0	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
38	0	1	1	-1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
39	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
40	-1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0
41	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
42	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1

Table III.11 Incident matrix for electrical distribution (loop two)

We analyzed the network digraphs, using *Mathematica*®, to produce the minimal cut sets for each user for each infrastructure. The complete listing of mcs, by infrastructure and user, is provided in Appendix A.1. When reviewing the complete listing of mcs the reader will find over 1,000 mcs listed. The list is meshed to account for mcs which impact more than one user and/or more than one infrastructure. For example the cut set (ea5,ea16) impacts electricity to two users, building A and building D. The user-infrastructure combination

impacted by the mcs is recorded, the mcs listed once, and the duplicates are eliminated. A user-infrastructure combination refers to one infrastructure supplied to one user. For example, water service to building A is one user-infrastructure combination and water service to building B is another user-infrastructure combination. This example contains eighteen user-infrastructure combinations, three infrastructures (natural gas, water, and electricity) for each of six users (buildings A, B, C, D, E, and F.) We sorted and analyzed the sets using *Microsoft Excel*®. Following the elimination of duplicates, there remain 663 unique mcs for the section of the MIT community being analyzed. That is, there are 663 different locations (or combination of locations) that, if attacked, would lead to the loss of one or more infrastructures to one or more users. There are seven mcs which impact six user-infrastructure combinations. For example mcs (ev1,ev2) impacts electrical service to all six buildings, and mcs (wv15) impacts water to all six users. The complete breakdown of the number of user-infrastructure combinations affected by mcs is shown in Table III.12. While the mcs which impact the most user-infrastructure combinations would seem to provide hints as to the prioritization, the analysis is not complete until the vulnerability is incorporated.

Number of mcs	Number of user-infrastructure combinations impacted
7	6
7	5
11	4
107	3
256	2
275	1

Table III.12 mcs impact on User-Infrastructure combinations

III.5 Critical Infrastructure Vulnerabilities

Having completed the framework for the analysis of the infrastructures, we analyze the community for the specified threat. For this example, we will analyze for a minor threat, section II.4.B, which is from an organization, group, or individual with limited capabilities. The threat may constitute a single pinpoint attack against one or more infrastructures. The attack would result in minor damage leading to minimal restoration and causing a minor impact on the community. Using the constructed scales, we determined the level representative of the damage and impact. Looking at the constructed scale for the interruption of academic activities and operations, Table III.13, for electrical service to building A, we classified the impact from the selected threat as level 1, minor interruption. So, if the attack

Assessment	Level	Description	Disutility
	4	Extreme Interruption Greater than 6 months, entire buildings evacuated and activities relocated.	1.00
	3	Major Interruption 1 to 6 months, laboratories evacuated and activities relocated.	0.57
	2	Moderate Interruption 1 to 4 weeks, specialty classrooms evacuated and activities relocated.	0.19
—	1	Minor Interruption Less than 1 week, a few administrative units or small classrooms evacuated and relocated.	0.06
	0	No Interruption	0.00

Table III.13 Constructed Scale for interruption of academic activities & operations

caused an interruption in electrical service to building A, the contribution to the Performance Index, for building A electrical service, from the interruption of academic activities and operations would be the global weight of the performance measure (0.056) multiplied by the assessed disutility (0.06), which is 0.00336.

The remaining constructed scales are used to determine the contribution from the other performance measures to the PI for electrical service to building A. When the summation

across all the PMs in completed, the resulting PI for electrical service to building A is 0.02117. The other infrastructure services to building A are analyzed following the same methodology, resulting in a PI for natural gas service to building A of 0.00865 and a PI for water service to building A of 0.01477. Once the building A assessment was completed we analyzed the other five users (buildings B, C, D, E, and F) for each infrastructure by following the same process. The PIs are likely to be different because the users are heterogeneous, have different infrastructure service needs, and perform functions of differing value to the community. In this example building E and F are very similar, so there PIs are the same in many cases. The result is a PI for each of the eighteen user-infrastructure combinations considered in the example. The detailed constructed scales are provided in Appendix A.2, and the Performance Index for each user-infrastructure is summarized in Table III.14.

	Infrastructure		
User	Electric	Natural Gas	Water
Building A	0.02117	0.00865	0.01477
Building B	0.02901	0.01505	0.02117
Building C	0.06490	0.01141	0.00979
Building D	0.07274	0.02117	0.02117
Building E	0.02980	0.00865	0.02340
Building F	0.02980	0.00865	0.02340

Table III.14 Performance Index for user-infrastructure combination

Once the PI is calculated for each user-infrastructure combination, the PI of each mcs is calculated as follows:

$$PI_{mcsk} = \sum_{k=1}^{MCS} \sum_{i} \sum_{j} (mcs_{ijk} * PI_{ij})$$

where

PI_{mcsk} is the performance index for minimal cut set mcsk
MCS is the total number of mcs
mcs_{ijk} is a Boolean operator (1 when the mcs*k* impacts the user-infrastructure combination *ij*, and 0 otherwise)
PI_{ij} is the performance index for the combination of user *i* and infrastructure *j*
i is the user (1 – 6, for building A, B, C, D, E, F)
j is the infrastructure (1 – 3, for electric, natural gas, water)

For example, mcs (ea5, ea16) impacts electrical service to building A and building D, and no other user-infrastructure combinations. The Boolean operator mcs_{ijk}, for *k* representing the mcs (ea5, ea16), equals one when *i* equals 1 (electric) and *j* equals 1 (building A) or when *i* equals 1 (electric) and *j* equals 4 (building D), and zero in the remaining sixteen user-infrastructure combinations. So, the PI_{mcsk}, where *k* representing the mcs (ea5, ea16), equals the PI for electrical service to building A (0.02117) plus the PI for electrical service to building D (0.07274), which is 0.09391. This process is repeated for every mcs to assign a PI to each mcs, using *Microsoft Excel*®. The PI tabulations for each mcs are presented in Appendix A.3. Some of the mcs with the highest PI are shown in Table III.15.

PI	Number of mcs	mcs
0.24742	1	(ev1,ev2)
0.15881	47	(ev23,ev6), (ev1,ev5), (ea20,ev4), (ea19,ev2), ….
0.11508	1	(ev8)
0.11370	3	(wv14), (wv15), (wa20)
0.09391	48	(ev21,ev6), (ev20,ev5), (ea17,ev2), (ev21,ev10), ….
0.09030	2	(wv16), (wa19)
0.08861	55	(ev24,ev42), (ea40,ev42), (ea39,ev38), (ev1,ev37), …

Table III.15 Performance Index values associated with minimal cut sets

The list of mcs, ordered by PI, indicates which mcs, which if successfully attacked, would lead to the greatest disutility in the MIT community. The mcs (ev1, ev2), because it carries the greatest PI, would cause the most significant impact. The ordered list suggests which mcs should be considered as critical locations, but the analysis is not complete, the vulnerability assessment must be completed to determine the actual critical locations.

The PI for each mcs is the "value" portion of the vulnerability, so the susceptibility is analyzed following the guidelines established in section II.4.C. The susceptibility of each mcs is categorized in a level described by Table II.8. For example a successful attack against mcs (ev1, ev2) requires an attack against *ev1* and a separate attack against *ev2*. The susceptibility depends on the nature of the attack, for example the explosive range of a truck

bomb is quite different from the explosive range of a suitcase bomb. The susceptibility of each must be analyzed and then combined to establish the susceptibility of mcs (ev1, ev2). For example, if we assessed the susceptibility of ev1 to be high and the susceptibility of ev2 to be low, we would assess the combined susceptibility (both ev1 and ev2) to be low. In general a mcs with multiple components would be no more susceptible than the most secure of the individual pieces, but could be less susceptible than the most secure piece when the combination of all components is considered.

The threat for the particular example presented is a minor threat, which includes only a single point attack (i.e., an attack against one location.) Since a minor threat is not capable of a multi-axis attack, we may simplify the susceptibility analysis by classifying all mcs with two or more elements as zero susceptibility. We must consider this simplification carefully, however, as it is not appropriate for more advanced threats in which a coordinated multiple location attack must be considered. We assessed the susceptibility of each mcs using the classification levels presented in Table II.8, the complete susceptibility assessments, for the mcs with assessed to have susceptibility of very low or greater, are listed in Appendix A.4.

Having established the value of each mcs (the PI) and the susceptibility, we combine the two using the guidelines established in Table II.9, to assign each mcs a vulnerability category. For example, looking at mcs wa20 we find it corresponds to the main water line serving the selected portion of campus. Failure of this line would result in loss of water service to all six users. The PI for mcs wa20 places it in the extreme value category. Since the water line is buried with no service access, it would be difficult to attack. As a result we classified the susceptibility of the water line as very low. Applying the guidelines in Table II.9, we intersect extreme value with very low susceptibility resulting in Blue vulnerability. The complete vulnerability categorizations are detailed in Appendix A.5, and summarized in Table III.16.

Through application of the infrastructure risk analysis model, we now have a prioritized list of mcs for consideration in risk management. The single mcs (ev8) with vulnerability red is dealt with first. We trace ev8 back to the network digraph and schematics to determine its identity. In this case, ev8 is identified as an electric service manhole in the selected portion of campus. The manhole has a specific identifier which uniquely identifies

the location. In order to prevent the inadvertent release of the location, this manhole is referred to as EM-X by this analysis. Manhole EM-X contains the main electrical service

Vulnerability Category	Number of mcs	mcs
Red	1	(ev8)
Orange	0	none
Yellow	5	(ev21), (ev22), (ev3), (ev34), (ev9)
Blue	19	(wa20), (wv14), (wv15), (ev11), (ev18), (ev19), (ev25), (gv1), (gv2), (gv3), (gv4), (gv5), (gv6), (wv1), (wv2), (wv3), (wv4), (wv5), (wv6)
Green	60	(ea10), (ea18), (ea30), (ga11), (ga19), (ga20), (gv14), (gv15), (gv16), (gv17), (gv18), (wa11), (wa8), (wv18), (wv19), (wa19), (wv16), (ea15), (ea38), (ga1), (ga10), (ga17), (ga18), (ga2), (ga21), (ga3), (ga4), (ga5), (ga6), (ga7), (ga8), (ga9), (gv10), (gv13), (gv19), (gv20), (gv7), (gv8), (gv9), (wa1), (wa10), (wa13), (wa15), (wa17), (wa18), (wa2), (wa21), (wa3), (wa4), (wa5), (wa6), (wa7), (wa9), (wv11), (wv12), (wv13), (wv20), (wv7), (wv8), (wv9)

Table III.16 Vulnerability Categories for the minimal cut sets

switch to building D, so a successful attack against this manhole would interrupt electrical service to the building. Additionally, the natural gas and water service to building D also run through, or immediately adjacent to, manhole EM-X. A successful attack against this manhole would also interrupt the natural gas and water service to building D. A schematic of manhole EM-X is presented in Figure III.11. The electric switches are designed to allow electricity flow in either direction (from EM-A to EM-X to EM-B, or from EM-B to EM-X to EM-A) and split the feed to provide electric service to building D. The natural gas and water service both come from their corresponding service network, via a building isolation valve, through the manhole to building D. This manhole shows a geographic vulnerability of multiple infrastructures which are not physically connected. None of the three services

(electric, natural gas, or water) are connected to each other inside the manhole, yet all three are vulnerable to a single attack.

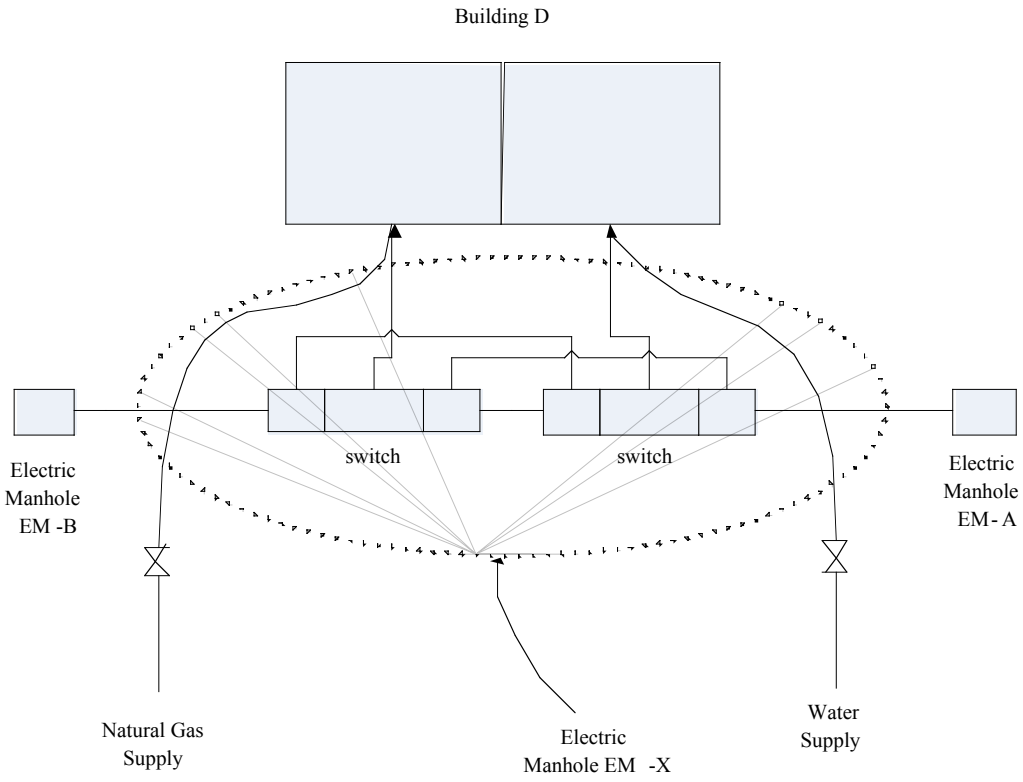

Figure III.11 Electric Manhole EM-X

III.6 Risk Management

We now proceed to risk management of the vulnerabilities. The protection of the critical locations is accomplished by reducing the susceptibility of the location, reducing the value of the location, or some combination of the two. In reality the threats could be eliminated, but that is a law enforcement issue which is beyond the scope of this analysis. Many options for countermeasures are available and one must consider the options and the associated risks and benefits carefully. Potential actions are analyzed to support the selection of an appropriate countermeasure or combination of countermeasures. Each potential countermeasure is assessed against a set of common attributes to support comparison among the possibilities. We have chosen the set of attributes (security method, control method, cost, on-going cost, supply reliability, service quality) as shown in Figure III.12. The number of attributes, and the attributes themselves, are chosen by the decision makers. Just as with the value tree, a different set of decision makers is likely to have different attributes, and we would have different attributes when addressing a different problem.

From our example, the starting point is the red category (mcs ev8, manhole EM-X), which has the highest priority for countermeasure actions. Some possible countermeasures, not an exhaustive list, to address susceptibility and value of the critical location are shown in Table III.17. We review the possible countermeasures to select the most appropriate for the situation, recognizing that taking no action is always a possibility which must be considered.

Category	**Possible Countermeasures**
Reduce Susceptibility	Weld the manhole cover Alarm the manhole cover Monitor the manhole cover Increase the security patrols
Reduce Value	Install additional independent infrastructure supply lines Install internal (to the building) back-up sources

Table III.17 Possible Countermeasures

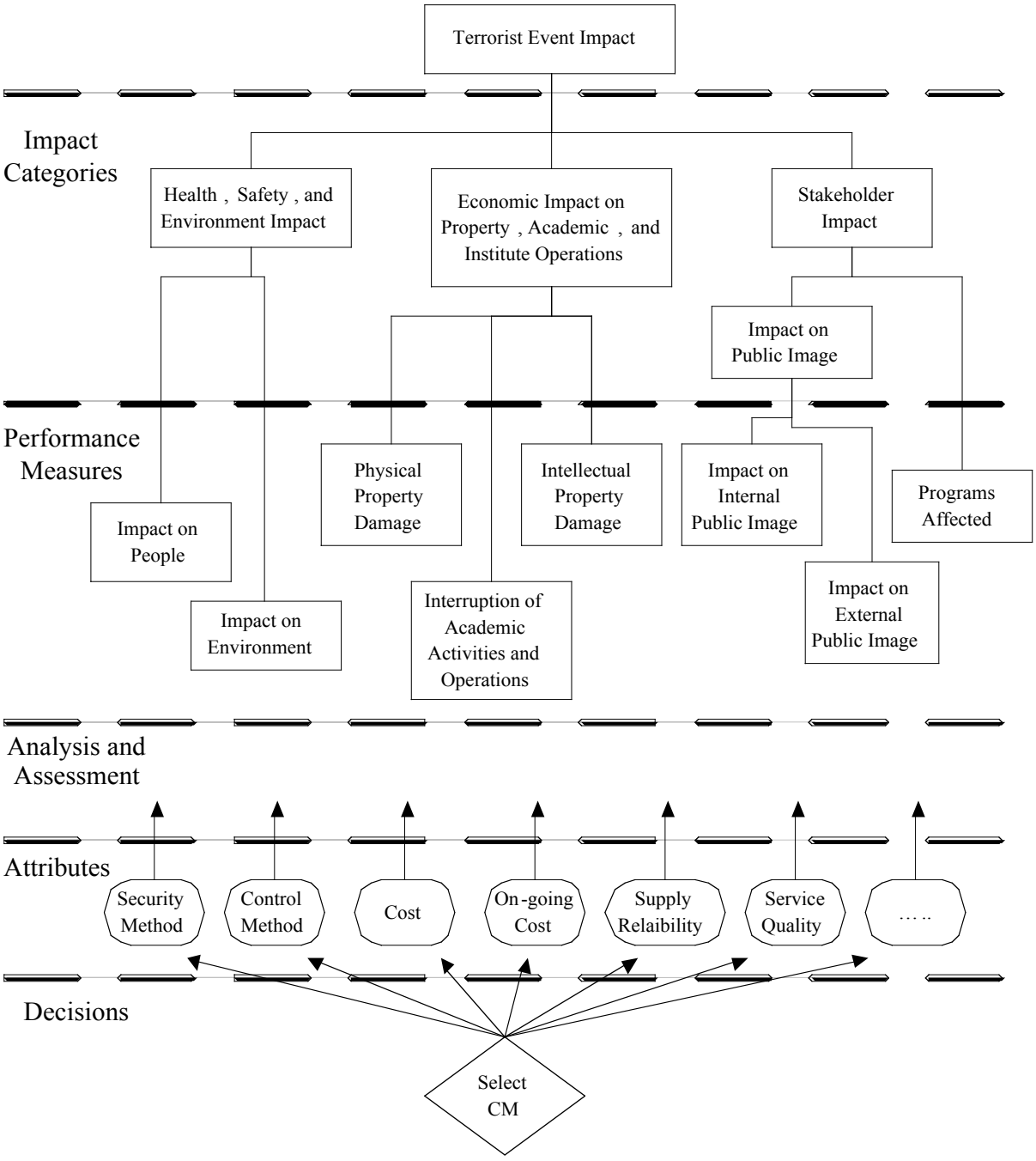

Figure III.12 Decision Analysis and Risk Management

For example, to review the possibility of welding the manhole cover to reduce the susceptibility we consider the attributes in Figure III.12. The security method is a physical barrier (the weld) to access of the manhole. The access is controlled by cutting and re-

welding the cover as required. Cutting the weld would require tools and sufficient time. Our assessment is that welding the cover would reduce the susceptibility from high to low. There is no change in the value of the location; the supply reliability and service quality remain unchanged. The cost of welding is low; as is the on-going cost (the manhole is not routinely accessed.) The new vulnerability category for manhole EM-X (mcs ev8) is Yellow (low susceptibility and extreme value.)

To look at the value portion of the equation, we consider the installation of additional infrastructure service to the affected user (building D.) Additional services are considered for each of the infrastructures. The PI for building D, for all three services, is 0.11508, as presented in Appendix A.3. The electric service accounts for 63 percent of that value, or 0.07274, with water and gas accounting for the rest. Installing an additional electrical feed to the building would reduce the PI of the manhole to 0.04234 (low). Considering only the additional electrical service the new vulnerability category for manhole EM-X (mcs ev8) is Yellow (high susceptibility and low value.) The costs of installing and maintaining the service is significant and must be considered.

If we choose to take both steps, installing the additional electrical service and welding the manhole cover, the new vulnerability category for manhole EM-X (mcs ev8) would be Green (low susceptibility and low value.) Once a countermeasure is selected, the analysis is repeated taking into account the impact of the countermeasure. The decision maker should review the entire process to ensure there are no unintended consequences of the countermeasure. Once satisfied, the decision maker would move to the next vulnerability. In the event that no countermeasure is chosen, the decision maker just proceeds to the next vulnerability. In this example, there are no mcs categorized as Orange, so the decision makers proceed to the Yellow category. The process repeats until the decision maker feels satisfied in the risk management efforts. Continuous assessment ensures the community risk profile is reviewed on a regular basis.

IV. Comments

The analysis of the MIT community served to validate the screening methodology for the identification of critical locations in infrastructures. We gained significant insight into the infrastructure system through the development of the network digraphs. In the case where the decision makers are interested solely in the number of user-infrastructure combinations impacted by each location, the network models provide that information without further analysis. However, this approach would ignore the vulnerability portion of the analysis. By excluding the vulnerability assessment, the analyst could remove the human judgment from the prioritization. In effect, the decision maker would be presented with a list of infrastructure locations ordered by the number of user-infrastructure combinations they impact. To develop a more realistic prioritization of the locations the vulnerability must be included in the analysis. The treatment of uncertainties and expert judgment become important in this process. The threat assessment is limited in that terrorist risk assessment studies are generally classified. [Garrick, 2002] This study worked with fixed threat parameters and the uncertainties were incorporated through expert judgment at the performance measure level. This methodology is a screening methodology to identify the candidate critical locations. These locations are subjected to a review panel and the critical locations are identified through expert judgment. Another way of looking at it is that we have developed a methodology for initial screening and identification of critical locations. A rigorous uncertainty analysis, including organizational response, would be done for these critical locations.

The MIT case study revealed some issues with regard to the screening of critical locations in infrastructures and infrastructure analysis. The availability of infrastructure documentation cannot be overlooked. The MIT study had the benefit of full, unrestricted access to the infrastructure design, layout, location, and operating instructions. In expanding the analysis beyond the confines of MIT, it is anticipated that obtaining infrastructure documentation will be challenging. The data mining task itself could prove complicated, as the data must be gathered from multiple utilities and various governmental agencies. It is recognized that commercial data may be proprietary and governmental data may be classified. Also, the issue of data completeness must be faced. Even if the analyst had full access to the

industry and government data there is a concern the information may not be complete. During some of the older construction of utility infrastructures good records were not kept concerning the location of lines. Data accuracy must also be addressed, for it is not certain that accurate records exist concerning growth and changes. Unauthorized modifications may exist and authorized modifications may not be properly documented.

Another issue which must be considered by the analyst is the impact of isolation for the damaged portion of the networks. For example, consider again the sample water distribution network reviewed in Figure II.5. If a successful attack were conducted against *v5,* the analyst could immediately determine that water would be denied to user B. The impact on user A requires a more detailed review. The likely upstream isolation point for the damage at *v5* is the next upstream valve; in this case assume that valve to be *v2*, see Figure IV.1. While

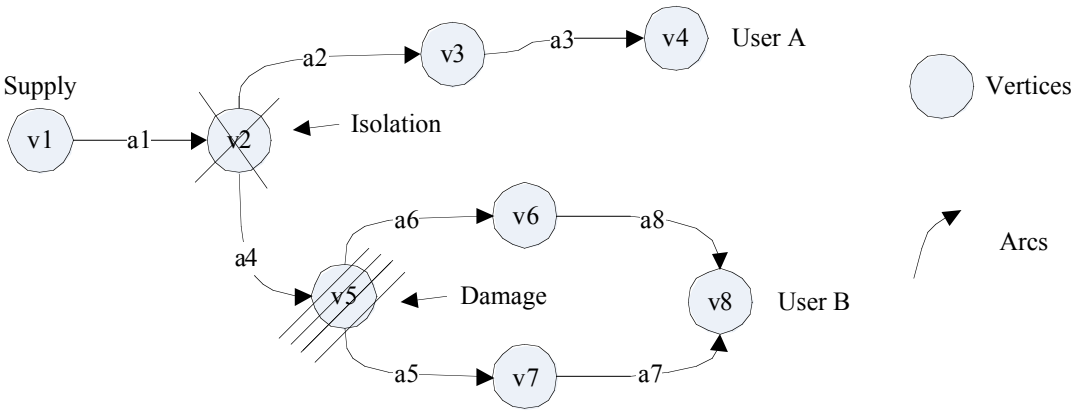

Figure IV.1 Water distribution network with damage and isolation

the damage to *v5* is the direct cause of the loss of water suffered by user B, the isolation required is the cause of the loss of water to user A. The loss of water to the users may be of different durations. The restoration to user B may require replacement of valve *v5* and repair of the associated water pipes, which may be moderate in duration. Water pipe *a4* may be temporarily capped to provide isolation, so the valve *v2* maybe reopened to restore service to user A; which could be minor in duration. The analyst must take care to ensure the true impact of potential attacks is included in the analysis.

The MIT campus contains sufficient infrastructure components that it provides a good prototype. MIT operates a utility plant, utilities distribution network, data network, cable

television station, and phone system, and has its own police and medical personnel. The MIT campus contains a Critical Infrastructure, the Central Utilities Plant, and a Key Asset, the Nuclear Research Reactor. The Reactor does not use natural gas, so there would be no impact in the event of an interruption of natural gas service. Sufficient water inventory is maintained within the reactor complex to withstand a water outage of significant duration. The loss of electrical service would possibly be an impact. The Reactor Operations team has sufficiently analyzed the impact of loss of the electrical service, and no additional risks are anticipated from the infrastructure analysis.

Several drawbacks were uncovered. First, there are very limited physical dependencies between the infrastructures on the MIT campus. The natural gas fired electric generation turbine and electric driven domestic water pumps account for most of the infrastructure ties. There is no water pumping stations or natural gas pressurization points on the campus. Second, the campus could be viewed as homogeneous with regard to mission; MIT is primarily a research institution. This eased our determination of the disutility on the users. In expanding the scope to model a city, for example, the decision makers may have more difficulty comparing disutility across society. Political influence, which was not experienced in the MIT study, may become a factor. Finally, the impact of a loss of one or multiple infrastructures on law enforcement and firefighting was not included in the MIT prototype. Faced with a significant electric power or water outage society must address the issue of rioting and looting. Those objectives may influence the decision.

The issues of outages and maintenance, both preventative and corrective, were not included in the analysis. Clearly, the unavailability of certain components could impact the prioritization index. To gain additional accuracy the unavailability periods should be included.

The screening methodology may be expanded beyond MIT to a smaller scale (larger area). The decision makers will make an assessment of the level of detail to be analyzed, which will impact the complexity of the model. Trying to model every building in the nation, or even the state, would likely prove exhausting. At the city level the decision makers may decide, for a first look, to represent each neighborhood as a vertex and model the ties between the cities with arcs. The second level analysis could look deeper into each neighborhood. On

a national level the decision makers may, for example, choose to look at the interstate transmission voltage network for electricity. By focusing on a specific voltage the decision makers should be able to bound the problem. Another approach could be to identify the critical facilities in a region like hospitals, emergency response units, water pumping stations, electrical generation (and distribution substations), etc. Then model their infrastructure supplies using the network digraphs. The methodology could then be used to identify the critical locations in the infrastructures serving the identified facilities.

V. Conclusions

This project presents a screening methodology to analyze infrastructures to identify the critical locations. The methodology itself is a general approach which may be used in a number of prioritization situations. The general portions include the development and application of the value tree, constructed scales, and the AHP to assign weights to the objectives and performance measures. These techniques are commonly applied in decision analysis. The infrastructures are "valued" through application of this general approach. The details of the process reviewed in this project apply only to the specific decision considered for the specific decision makers. A different set of decision makers, applying the methodology to the same problem, may arrive at a different ending. However, using such an explicit methodology may help the disagreeing parties to reach consensus, because their disagreements will be specific. And, the same decision makers using the process to prioritize a different problem would achieve different results. The methodology makes use of a quantitative approach which supports a specific numerical comparison of the effects of different threats and different targets.

The portion of the methodology specific to the MIT campus infrastructures is the modeling of the infrastructures as interconnected digraphs and accompanying application of graph theory and reliability theory to identify the vulnerable points, modeled as minimal cut sets. A mcs may be impact more than one user and/or more than one infrastructure. Once all the users have been examined, a database is compiled of the mcs, with the associated PI representing the "value" of the mcs to the infrastructure. The susceptibility of each mcs is assessed and combined with the value of the mcs to produce a vulnerability assessment of the mcs. A prioritized list of mcs for consideration is developed.

References

Amin M. 1999. National Infrastructures as Complex Interactive Networks. Automation, Control, and Complexity: New Developments and Directions. Palo Alto, CA: John Wiley and Sons.

Amin M. 2002. "Toward Secure and Resilient Interdependent Infrastructures." *Journal of Infrastructure Systems*, 8: 67-75.

Apostolakis GE. 1990. "The Concept of Probability in Safety Assessments of Technological Systems." Science, 250: 1359-1364.

Apostolakis GE, Catton I, Issacci F, Jones S, Paul M, Paulos T, Paxton K. 1995. "Risk-Based Spacecraft Fire Safety Experiments." *Reliability Engineering and System Safety*, 49: 275-291.

Ballocco G, Carpignano A, Gargiulo M. 2003. Merging cut sets and reliability indexes for reliability and availability of highly meshed networks. *Proceedings of ESREL 2003, European Safety and Reliability Conference*, 15-18 June 2003, Maastricht, The Netherlands. Sewts and Zeitlinger BV, Lisse, The Netherlands.

Bondy JA, Murty USR. 1980. *Graph Theory with Applications*. New York: North-Holland.

Budnitz RJ, Apostolakis GE, Boore DM, Cluff LS, Coppersmith KJ, Cornell CA, Morris PA. *1995. Recommendations for Probabilistic Seismic Hazard Analysis: Guidance on Uncertainty and Use of Experts.* Report NUREG/CR-6372, U. S. Nuclear Regulatory Commission, Washington, DC.

Bush GW. 2003. *The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*. Washington DC: White House.

CCPS. 1989. Center for Chemical Process Safety, *Guidelines for Chemical Process Quantitative Risk Analysis.* New York.

Clemen RT. 1991. *Making hard decisions*. Belmont, CA: Duxbury Press.

Clinton WJ. 1996. *Presidential Executive Order 13010*. Washington DC: White House.

Cooke RM. 1991. *Experts in Uncertainty: Expert Opinion and Subjective Probability in Science*. Oxford University Press, New York.

Davoudian K, Wu JS, Apostolakis GE. 1994. "Incorporating Organizational Factors Into Risk Assessment Through the Analysis of Work Processes." *Reliability Engineering and System Safety*, 45: 85-105.

Deisler PF Jr. 2002. "A Perspective: Risk Analysis as a Tool for Reducing the Risk of Terrorism." *Risk Analysis*, 22: 405-413.

Drabek TE. 1985. "Managing the Emergency Response." *Public Administration Review*, 45: 85-92.

Draper D. 1995. "Assessment and Propagation of Model Uncertainty." *Journal of the Royal Statistical Society*, B, 57: 45-97.

Ezell BC, Farr JV, Wiese I. 2000. "Infrastructure Risk Analysis Model." *Journal of Infrastructure Systems*, 6: 114-117.

Ezell BC, Farr JV, Wiese I. 2000. "Infrastructure Risk Analysis of Municipal Water Distribution System." *Journal of Infrastructure Systems*, 6: 118-122.

Futron. 2002. Futron Corporation, *Probabilistic Risk Assessment of the International Space Station. Phase III – Stage 12A.1 Configuration*. Washington, DC.

Garrick BJ. 2002. "Perspectives on the Use of Risk Assessment to Address Terrorism." *Risk Analysis*, 22: 421-423.

Garrick BJ. 2004. "Confronting the Risks of Terrorism: Making the Right Decisions," Special Study Group on Combating Terrorism, B. John Garrick, Chair. *Reliability Engineering and System Safety*, to appear.

Gilbert PH, Isenberg J, Baecher GB, Papay LT, Spielvoget LG, Woodard JB, Badolato EV. 2003. "Infrastructure Issues for Cities-Countering Terrorist Threat." *Journal of Infrastructure Systems*, 9: 44-54.

Gillespie DF, Streeter CL. 1987. "Conceptualizing and Measuring Disaster Preparedness." *International Journal of Mass Emergencies and Disasters*, 5: 155-176.

Haimes YY. 1991. "Total Risk Management." *Risk Analysis*, Vol. 11: 169-171.

Haimes YY. 2002. "Roadmap for Modeling Risks of Terrorism to the Homeland." *Journal of Infrastructure Systems*, 8: 35-41.

Haimes YY, Longstaff T. 2002. "The Role of Risk Analysis in the Protection of Critical Infrastructures against Terrorism." *Risk Analysis*, 22: 439-444.

Hokstad P, Jersin E, Sten T. 2001. "A Risk Influence Model Applied to North Sea Helicopter Transport." *Reliability Engineering and System Safety*, 74: 311-322.

Hoyland A, Rausand M. 1994. *System Reliability Theory: Models and Statistical Methods*. New York: John Wiley and Sons.

Hughes WR. 1986. "Deriving utilities using the analytic hierarchy process." *Socio-Economic Planning Science*, 20: 393-395.

Kaplan S, Garrick BJ. 1981. "On the Quantitative Definition of Risk." *Risk Analysis*, 1: 11-27.

Karydas DM, Gifun JF. 2002. "A Methodology for the Efficient Prioritization of Infrastructure Renewal Projects." *Proceedings of the 6th International Conference on Probabilistic Safety Assessment and Management (PSAM 6),* San Juan, Puerto Rico, 23-28 June 2002, E.J. Bonano, Editor, Elsevier Science Ltd., United Kingdom.

Kazarians M, Siu NO. 1986. *Spatial Interaction Analysis in Probabilistic Risk Assessment*. International ANS/ENS Topical meeting on Thermal Reactor Safety. San Diego, CA, February 2-6.

Keeney RL, Merkhofer MW. 1987. "A multiattribute utility analysis of alternative sights for the disposal of nuclear waste." *Risk Analysis*, 7: 173-194.

Keeney RL, von Winterfeldt D. 1991. "Eliciting Probabilities from Experts in Complex Technical Problems." *IEEE Transactions on Engineering Management*, 38: 191-201.

Kunreuther H, Lerner-Lam A. 2002. *Risk Assessment and Risk Management Strategies in an Uncertain World*. Palisades, New Jersey, April 12-13.

Loerch A. 1996. Proceedings of Computer Based Decision Support Systems. April 1996, Fairfax, VA.

Marcinkowski K, Apostolakis GE, Weil R. 2001. "A Computer-Aided Technique for Identifying Latent Conditions (CATILaC)." *Cognition, Technology & Work*, 3: 111-126.

Melchers RE, Feutril WR. 2001. "Risk Assessment of LPG Automotive Refueling Facilities." *Reliability Engineering and System Safety*, 74: 283-290.

NASA. 2002. National Aeronautics and Space Administration, *Probabilistic Risk Assessment Procedures Guide for NASA Managers and Practitioners*. Office of Safety and Mission Assurance, Washington, DC.

NIPC. 2002. National Infrastructure Protection Center. *Risk Management: As essential Guide to Protecting Critical Assets*. National Infrastructure Protection Center, Wahsington, DC.

NRC. 2002. National Research Council. *Making the Nation Safer*. National Academy Press Washington, DC.

OHS. 2002. Office of Homeland Security, *National Strategy for Homeland Security*. U.S. Executive Office of the President, Office of Homeland Security, Washington, DC.

Paté-Cornell ME. 1990. "Organizational Aspects of Engineering System Safety: The Case of Offshore Platforms." *Science*, 250: 1210-1217.

Paté-Cornell ME, Guikema S. 2002. "Probabilistic Modeling of Terrorist Threats: A Systems Analysis Approach to Setting Priorities Among Countermeasures." *Military Operations Research*, 7: 5-20.

Reason JT. 1990. *Human error*. Cambridge University Press, New York.

Reason JT. 1997. *Managing the Risks of Organizational Accidents*. Ashgate, Aldershot, UK.

Rechard RP. 1996. "Historical Background on Performance Assessment for the Waste Isolation Pilot Plant." *Reliability Engineering and System Safety*, 69: 5-46.

Saaty TL. 1980. *The analytic hierarchy process: planning, priority setting, and resource allocation.* New York: McGraw-Hill.

SAIC. 1995. Science Applications International Corporation, *Probabilistic Risk Assessment of the Space Shuttle*. Report SAIC, NY95-02-25, New York.

SAIC. 1996. Science Applications International Corporation, *Tooele Chemical Agent Disposal Facility Quantitative Risk Assessment*. Report SAIC-96/2600, Abingdon, MD.

Stewart TR, Bostrom A. 2002. *Extreme Event Decision Making: Workshop Report.* Arlington, Virginia, April 29-30, 2001.

Sträter O, Bubb H. 1999. "Assessment of Human Reliability Based on Evaluation of Plant Experience; Requirements and Implementation." *Reliability Engineering and System Safety*, 63: 199-219.

Tan Z. 2003. "Minimal cut sets of s-t networks with k-out-of-n nodes." *Reliability Engineering and System Safety*, 82: 49-54.

U.S. Census. 2000. "Population change and distribution." U.S. Census Bureau, Department of Commerce, Washington, DC.

USNRC. 1982. U. S. Nuclear Regulatory Commission, *PRA Procedures Guide*. Report NUREG/CR-2300, Vol. 1, Rev. 1, Washington, DC.

USNRC. 1990. U. S. Nuclear Regulatory Commission, *Severe Accident Risks: An Assessment for Five US Nuclear Power Plants*. Report NUREG-1150, Washington, DC.

Weil R, Apostolakis GE. 2001. "A methodology for the prioritization of operating experience in nuclear power plants." *Reliability Engineering and System Safety*, 74: 23-42.

Yeh WC. 2004. "A simple algorithm for evaluating the k-out-of-n network reliability." *Reliability Engineering and System Safety*, 83: 93-101.

Zimmerman R. 2001. "Social Implications of Infrastructure Network Interactions." *Journal of Urban Technology*, 8: 79-119.

Appendix A.1 Minimal Cut Sets by Infrastructure and User

Minimal Cut Sets – Natural Gas

Bldg E (vertex gv5)

{(gv14),	(ga20),	(gv15),	(ga18),	(gv13),	(ga17),
(gv5)}					

Bldg C (vertex gv3)

{(gv14),	(ga20),	(gv15),	(ga19),	(gv16),	(gv17),
(ga11),	(gv18),	(ga8),	(gv19),	(ga5),	(gv20),
(ga6),	(gv7),	(ga7),	(gv3),	(ga12,ga15),	(ga12,gv12),
(ga12,ga16),	(ga12,gv6),	(ga12,ga22),	(ga12,ev3),	(ga12,ga14),	(ga12,gv11),
(ga12,ga13)}					

Bldg B (vertex gv2)

{(gv14),	(ga20),	(gv15),	(ga19),	(gv16),	(gv17),
(ga11),	(gv18),	(ga8),	(gv19),	(ga5),	(gv20),
(ga4),	(gv8),	(ga3),	(gv2),	(ga12,ga15),	(ga12,gv12),
(ga12,ga16),	(ga12,gv6),	(ga12,ga22),	(ga12,ev3),	(ga12,ga14),	(ga12,gv11),
(ga12,ga13)}					

Bldg A (vertex gv1)

{(gv14),	(ga20),	(gv15),	(ga19),	(gv16),	(gv17),
(ga11),	(gv18),	(ga8),	(gv19),	(ga2),	(gv9),
(ga1),	(gv1),	(ga12,ga15),	(ga12,gv12),	(ga12,ga16),	(ga12,gv6),
(ga12,ga22),	(ga12,ev3),	(ga12,ga14),	(ga12,gv11),	(ga12,ga13)}	

Bldg D (vertex gv4)

{(gv14),	(ga20),	(gv15),	(ga19),	(gv16),	(gv17),
(ga11),	(gv18),	(ga10),	(gv10),	(ga9),	(ev8),
(ga21),	(gv4),	(ga12,ga15),	(ga12,gv12),	(ga12,ga16),	(ga12,gv6),
(ga12,ga22),	(ga12,ev3),	(ga12,ga14),	(ga12,gv11),	(ga12,ga13)}	

Bldg F (vertex gv6)

{(gv14),	(ga20),	(gv15),	(ga19),	(gv16),	(gv6),
(ga15,ga12),	(ga15,gv17),	(ga15,ga13),	(ga15,gv11),	(ga15,ga14),	(ga15,ev3),
(ga15,ga22),	(gv12,ga12),	(gv12,gv17),	(gv12,ga13),	(gv12,gv11),	(gv12,ga14),
(gv12,ev3),	(gv12,ga22),	(ga16,ga12),	(ga16,gv17),	(ga16,ga13),	(ga16,gv11),
(ga16,ga14),	(ga16,ev3),	(ga16,ga22)}			

Minimal Cut Sets – Water

Bldg F (vertex wv6)

{(wv14), (wa20), (wv15), (wa15), (wv12), (wv6),
(wa14,wa12), (wa14,wv17), (wa14,wa16), (wv10,wa12), (wv10,wv17), (wv10,wa16),
(wa22,wa12), (wa22,wv17), (wa22,wa16)}

Bldg E (vertex wv5)

{(wv14), (wa20), (wv15), (wa19), (wv16), (wa11),
(wv18), (wa10), (wv13), (wa17), (wv5)}

Bldg D (vertex wv4)

{(wv14), (wa20), (wv15), (wa19), (wv16), (wa9),
(wv11), (wa21), (ev8), (wa13), (wv4)}

Bldg A (vertex wv1)

{(wv14), (wa20), (wv15), (wa19), (wv16), (wa11),
(wv18), (wa8), (wv19), (wa2), (wv9), (wa1),
(wv1)}

Bldg C (vertex wv3)

{(wv14), (wa20), (wv15), (wa19), (wv16), (wa11),
(wv18), (wa8), (wv19), (wa5), (wv20), (wa6),
(wv7), (wa7), (wv3)}

Bldg B (vertex wv2)

{(wv14), (wa20), (wv15), (wa19), (wv16), (wa11),
(wv18), (wa8), (wv19), (wa5), (wv20), (wa4),
(wv8), (wa3), (ev11), (wa18), (wv2)}

Minimal Cut Sets – Electric

Bldg C (vertex ev22)

{(ev22), (ea18), (ev21), (ea19,ea17), (ea19,ev20), (ea19,ea16),
(ea19,ev18), (ea19,ea14), (ea19,ev17), (ea19,ea13), (ea19,ev15), (ea19,ea12),
(ea19,ev14), (ea19,ea9), (ea19,ev8), (ea19,ea8), (ea19,ev10), (ea19,ea7),
(ea19,ev6), (ea19,ea5), (ea19,ev5), (ea19,ea3), (ea19,ev4), (ea19,ea2),
(ea19,ev13), (ea19,ea1), (ea19,ev2), (ev23,ea17), (ev23,ev20), (ev23,ea16),
(ev23,ev18), (ev23,ea14), (ev23,ev17), (ev23,ea13), (ev23,ev15), (ev23,ea12),
(ev23,ev14), (ev23,ea9), (ev23,ev8), (ev23,ea8), (ev23,ev10), (ev23,ea7),
(ev23,ev6), (ev23,ea5), (ev23,ev5), (ev23,ea3), (ev23,ev4), (ev23,ea2),
(ev23,ev13), (ev23,ea1), (ev23,ev2), (ea20,ea17), (ea20,ev20), (ea20,ea16),
(ea20,ev18), (ea20,ea14), (ea20,ev17), (ea20,ea13), (ea20,ev15), (ea20,ea12),
(ea20,ev14), (ea20,ea9), (ea20,ev8), (ea20,ea8), (ea20,ev10), (ea20,ea7),
(ea20,ev6), (ea20,ea5), (ea20,ev5), (ea20,ea3), (ea20,ev4), (ea20,ea2),
(ea20,ev13), (ea20,ea1), (ea20,ev2), (ev1,ea17), (ev1,ev20), (ev1,ea16),
(ev1,ev18), (ev1,ea14), (ev1,ev17), (ev1,ea13), (ev1,ev15), (ev1,ea12),
(ev1,ev14), (ev1,ea9), (ev1,ev8), (ev1,ea8), (ev1,ev10), (ev1,ea7),
(ev1,ev6), (ev1,ea5), (ev1,ev5), (ev1,ea3), (ev1,ev4), (ev1,ea2),
(ev1,ev13), (ev1,ea1), (ev1,ev2)}

Bldg B (vertex ev25)

{(ev25), (ea38), (ev11), (ev24,ea37), (ev24,ev26), (ev24,ea36),
(ev24,ev27), (ev24,ea34), (ev24,ev29), (ev24,ea33), (ev24,ev30), (ev24,ea32),
(ev24,ev32), (ev24,ea29), (ev24,ev3), (ev24,ea28), (ev24,ev35), (ev24,ea27),
(ev24,ev36), (ev24,ea25), (ev24,ev37), (ev24,ea23), (ev24,ev38), (ev24,ea22),
(ev24,ev40), (ev24,ea41), (ev24,ev42), (ev24,ea42), (ev24,ev2), (ea39,ea37),
(ea39,ev26), (ea39,ea36), (ea39,ev27), (ea39,ea34), (ea39,ev29), (ea39,ea33),
(ea39,ev30), (ea39,ea32), (ea39,ev32), (ea39,ea29), (ea39,ev3), (ea39,ea28),
(ea39,ev35), (ea39,ea27), (ea39,ev36), (ea39,ea25), (ea39,ev37), (ea39,ea23),
(ea39,ev38), (ea39,ea22), (ea39,ev40), (ea39,ea41), (ea39,ev42), (ea39,ea42),
(ea39,ev2), (ea40,ea37), (ea40,ev26), (ea40,ea36), (ea40,ev27), (ea40,ea34),
(ea40,ev29), (ea40,ea33), (ea40,ev30), (ea40,ea32), (ea40,ev32), (ea40,ea29),
(ea40,ev3), (ea40,ea28), (ea40,ev35), (ea40,ea27), (ea40,ev36), (ea40,ea25),
(ea40,ev37), (ea40,ea23), (ea40,ev38), (ea40,ea22), (ea40,ev40), (ea40,ea41),
(ea40,ev42), (ea40,ea42), (ea40,ev2), (ev1,ea37), (ev1,ev26), (ev1,ea36),
(ev1,ev27), (ev1,ea34), (ev1,ev29), (ev1,ea33), (ev1,ev30), (ev1,ea32),
(ev1,ev32), (ev1,ea29), (ev1,ev3), (ev1,ea28), (ev1,ev35), (ev1,ea27),
(ev1,ev36), (ev1,ea25), (ev1,ev37), (ev1,ea23), (ev1,ev38), (ev1,ea22),
(ev1,ev40), (ev1,ea41), (ev1,ev42), (ev1,ea42), (ev1,ev2)}

Bldg A (vertex ev19)

{(ev19), (ea15), (ev18), (ea19,ea14), (ea19,ev17), (ea19,ea13),
(ea19,ev15), (ea19,ea12), (ea19,ev14), (ea19,ea9), (ea19,ev8), (ea19,ea8),
(ea19,ev10), (ea19,ea7), (ea19,ev6), (ea19,ea5), (ea19,ev5), (ea19,ea3),
(ea19,ev4), (ea19,ea2), (ea19,ev13), (ea19,ea1), (ea19,ev2), (ev23,ea14),
(ev23,ev17), (ev23,ea13), (ev23,ev15), (ev23,ea12), (ev23,ev14), (ev23,ea9),
(ev23,ev8), (ev23,ea8), (ev23,ev10), (ev23,ea7), (ev23,ev6), (ev23,ea5),
(ev23,ev5), (ev23,ea3), (ev23,ev4), (ev23,ea2), (ev23,ev13), (ev23,ea1),
(ev23,ev2), (ea20,ea14), (ea20,ev17), (ea20,ea13), (ea20,ev15), (ea20,ea12),
(ea20,ev14), (ea20,ea9), (ea20,ev8), (ea20,ea8), (ea20,ev10), (ea20,ea7),
(ea20,ev6), (ea20,ea5), (ea20,ev5), (ea20,ea3), (ea20,ev4), (ea20,ea2),
(ea20,ev13), (ea20,ea1), (ea20,ev2), (ev1,ea14), (ev1,ev17), (ev1,ea13),
(ev1,ev15), (ev1,ea12), (ev1,ev14), (ev1,ea9), (ev1,ev8), (ev1,ea8),
(ev1,ev10), (ev1,ea7), (ev1,ev6), (ev1,ea5), (ev1,ev5), (ev1,ea3),
(ev1,ev4), (ev1,ea2), (ev1,ev13), (ev1,ea1), (ev1,ev2), (ea17,ea14),
(ea17,ev17), (ea17,ea13), (ea17,ev15), (ea17,ea12), (ea17,ev14), (ea17,ea9),
(ea17,ev8), (ea17,ea8), (ea17,ev10), (ea17,ea7), (ea17,ev6), (ea17,ea5),
(ea17,ev5), (ea17,ea3), (ea17,ev4), (ea17,ea2), (ea17,ev13), (ea17,ea1),
(ea17,ev2), (ev20,ea14), (ev20,ev17), (ev20,ea13), (ev20,ev15), (ev20,ea12),
(ev20,ev14), (ev20,ea9), (ev20,ev8), (ev20,ea8), (ev20,ev10), (ev20,ea7),
(ev20,ev6), (ev20,ea5), (ev20,ev5), (ev20,ea3), (ev20,ev4), (ev20,ea2),
(ev20,ev13), (ev20,ea1), (ev20,ev2), (ea16,ea14), (ea16,ev17), (ea16,ea13),
(ea16,ev15), (ea16,ea12), (ea16,ev14), (ea16,ea9), (ea16,ev8), (ea16,ea8),
(ea16,ev10), (ea16,ea7), (ea16,ev6), (ea16,ea5), (ea16,ev5), (ea16,ea3),
(ea16,ev4), (ea16,ea2), (ea16,ev13), (ea16,ea1), (ea16,ev2), (ev21,ea14),
(ev21,ev17), (ev21,ea13), (ev21,ev15), (ev21,ea12), (ev21,ev14), (ev21,ea9),
(ev21,ev8), (ev21,ea8), (ev21,ev10), (ev21,ea7), (ev21,ev6), (ev21,ea5),
(ev21,ev5), (ev21,ea3), (ev21,ev4), (ev21,ea2), (ev21,ev13), (ev21,ea1),
(ev21,ev2)}

Bldg D (vertex ev9)

{(ev9), (ea10), (ev8), (ea19,ea8), (ea19,ev10), (ea19,ea7),
(ea19,ev6), (ea19,ea5), (ea19,ev5), (ea19,ea3), (ea19,ev4), (ea19,ea2),
(ea19,ev13), (ea19,ea1), (ea19,ev2), (ev23,ea8), (ev23,ev10), (ev23,ea7),
(ev23,ev6), (ev23,ea5), (ev23,ev5), (ev23,ea3), (ev23,ev4), (ev23,ea2),
(ev23,ev13), (ev23,ea1), (ev23,ev2), (ea20,ea8), (ea20,ev10), (ea20,ea7),
(ea20,ev6), (ea20,ea5), (ea20,ev5), (ea20,ea3), (ea20,ev4), (ea20,ea2),
(ea20,ev13), (ea20,ea1), (ea20,ev2), (ev1,ea8), (ev1,ev10), (ev1,ea7),
(ev1,ev6), (ev1,ea5), (ev1,ev5), (ev1,ea3), (ev1,ev4), (ev1,ea2),
(ev1,ev13), (ev1,ea1), (ev1,ev2), (ea17,ea8), (ea17,ev10), (ea17,ea7),
(ea17,ev6), (ea17,ea5), (ea17,ev5), (ea17,ea3), (ea17,ev4), (ea17,ea2),
(ea17,ev13), (ea17,ea1), (ea17,ev2), (ev20,ea8), (ev20,ev10), (ev20,ea7),
(ev20,ev6), (ev20,ea5), (ev20,ev5), (ev20,ea3), (ev20,ev4), (ev20,ea2),
(ev20,ev13), (ev20,ea1), (ev20,ev2), (ea16,ea8), (ea16,ev10), (ea16,ea7),
(ea16,ev6), (ea16,ea5), (ea16,ev5), (ea16,ea3), (ea16,ev4), (ea16,ea2),
(ea16,ev13), (ea16,ea1), (ea16,ev2), (ev21,ea8), (ev21,ev10), (ev21,ea7),
(ev21,ev6), (ev21,ea5), (ev21,ev5), (ev21,ea3), (ev21,ev4), (ev21,ea2),
(ev21,ev13), (ev21,ea1), (ev21,ev2), (ea14,ea8), (ea14,ev10), (ea14,ea7),
(ea14,ev6), (ea14,ea5), (ea14,ev5), (ea14,ea3), (ea14,ev4), (ea14,ea2),
(ea14,ev13), (ea14,ea1), (ea14,ev2), (ev17,ea8), (ev17,ev10), (ev17,ea7),
(ev17,ev6), (ev17,ea5), (ev17,ev5), (ev17,ea3), (ev17,ev4), (ev17,ea2),
(ev17,ev13), (ev17,ea1), (ev17,ev2), (ea13,ea8), (ea13,ev10), (ea13,ea7),
(ea13,ev6), (ea13,ea5), (ea13,ev5), (ea13,ea3), (ea13,ev4), (ea13,ea2),
(ea13,ev13), (ea13,ea1), (ea13,ev2), (ev15,ea8), (ev15,ev10), (ev15,ea7),
(ev15,ev6), (ev15,ea5), (ev15,ev5), (ev15,ea3), (ev15,ev4), (ev15,ea2),
(ev15,ev13), (ev15,ea1), (ev15,ev2), (ea12,ea8), (ea12,ev10), (ea12,ea7),
(ea12,ev6), (ea12,ea5), (ea12,ev5), (ea12,ea3), (ea12,ev4), (ea12,ea2),
(ea12,ev13), (ea12,ea1), (ea12,ev2), (ev14,ea8), (ev14,ev10), (ev14,ea7),
(ev14,ev6), (ev14,ea5), (ev14,ev5), (ev14,ea3), (ev14,ev4), (ev14,ea2),
(ev14,ev13), (ev14,ea1), (ev14,ev2), (ea9,ea8), (ea9,ev10), (ea9,ea7),
(ea9,ev6), (ea9,ea5), (ea9,ev5), (ea9,ea3), (ea9,ev4), (ea9,ea2),
(ea9,ev13), (ea9,ea1), (ea9,ev2), (ev18,ea8), (ev18,ev10), (ev18,ea7),
(ev18,ev6), (ev18,ea5), (ev18,ev5), (ev18,ea3), (ev18,ev4), (ev18,ea2),
(ev18,ev13), (ev18,ea1), (ev18,ev2)}

Bldg E, F (vertex ev34)

{(ev34), (ea30), (ev3), (ea40,ea28), (ea40,ev35), (ea40,ea27),
(ea40,ev36), (ea40,ea25), (ea40,ev37), (ea40,ea23), (ea40,ev38), (ea40,ea22),
(ea40,ev40), (ea40,ea41), (ea40,ev42), (ea40,ea42), (ea40,ev2), (ev1,ea28),
(ev1,ev35), (ev1,ea27), (ev1,ev36), (ev1,ea25), (ev1,ev37), (ev1,ea23),
(ev1,ev38), (ev1,ea22), (ev1,ev40), (ev1,ea41), (ev1,ev42), (ev1,ea42),
(ev1,ev2), (ev24,ea28), (ev24,ev35), (ev24,ea27), (ev24,ev36), (ev24,ea25),
(ev24,ev37), (ev24,ea23), (ev24,ev38), (ev24,ea22), (ev24,ev40), (ev24,ea41),
(ev24,ev42), (ev24,ea42), (ev24,ev2), (ea39,ea28), (ea39,ev35), (ea39,ea27),
(ea39,ev36), (ea39,ea25), (ea39,ev37), (ea39,ea23), (ea39,ev38), (ea39,ea22),
(ea39,ev40), (ea39,ea41), (ea39,ev42), (ea39,ea42), (ea39,ev2), (ev11,ea28),
(ev11,ev35), (ev11,ea27), (ev11,ev36), (ev11,ea25), (ev11,ev37), (ev11,ea23),
(ev11,ev38), (ev11,ea22), (ev11,ev40), (ev11,ea41), (ev11,ev42), (ev11,ea42),
(ev11,ev2), (ea37,ea28), (ea37,ev35), (ea37,ea27), (ea37,ev36), (ea37,ea25),
(ea37,ev37), (ea37,ea23), (ea37,ev38), (ea37,ea22), (ea37,ev40), (ea37,ea41),
(ea37,ev42), (ea37,ea42), (ea37,ev2), (ev26,ea28), (ev26,ev35), (ev26,ea27),
(ev26,ev36), (ev26,ea25), (ev26,ev37), (ev26,ea23), (ev26,ev38), (ev26,ea22),
(ev26,ev40), (ev26,ea41), (ev26,ev42), (ev26,ea42), (ev26,ev2), (ea36,ea28),
(ea36,ev35), (ea36,ea27), (ea36,ev36), (ea36,ea25), (ea36,ev37), (ea36,ea23),
(ea36,ev38), (ea36,ea22), (ea36,ev40), (ea36,ea41), (ea36,ev42), (ea36,ea42),
(ea36,ev2), (ev27,ea28), (ev27,ev35), (ev27,ea27), (ev27,ev36), (ev27,ea25),
(ev27,ev37), (ev27,ea23), (ev27,ev38), (ev27,ea22), (ev27,ev40), (ev27,ea41),
(ev27,ev42), (ev27,ea42), (ev27,ev2), (ea34,ea28), (ea34,ev35), (ea34,ea27),
(ea34,ev36), (ea34,ea25), (ea34,ev37), (ea34,ea23), (ea34,ev38), (ea34,ea22),
(ea34,ev40), (ea34,ea41), (ea34,ev42), (ea34,ea42), (ea34,ev2), (ev29,ea28),
(ev29,ev35), (ev29,ea27), (ev29,ev36), (ev29,ea25), (ev29,ev37), (ev29,ea23),
(ev29,ev38), (ev29,ea22), (ev29,ev40), (ev29,ea41), (ev29,ev42), (ev29,ea42),
(ev29,ev2), (ea33,ea28), (ea33,ev35), (ea33,ea27), (ea33,ev36), (ea33,ea25),
(ea33,ev37), (ea33,ea23), (ea33,ev38), (ea33,ea22), (ea33,ev40), (ea33,ea41),
(ea33,ev42), (ea33,ea42), (ea33,ev2), (ev30,ea28), (ev30,ev35), (ev30,ea27),
(ev30,ev36), (ev30,ea25), (ev30,ev37), (ev30,ea23), (ev30,ev38), (ev30,ea22),
(ev30,ev40), (ev30,ea41), (ev30,ev42), (ev30,ea42), (ev30,ev2), (ea32,ea28),
(ea32,ev35), (ea32,ea27), (ea32,ev36), (ea32,ea25), (ea32,ev37), (ea32,ea23),
(ea32,ev38), (ea32,ea22), (ea32,ev40), (ea32,ea41), (ea32,ev42), (ea32,ea42),
(ea32,ev2), (ev32,ea28), (ev32,ev35), (ev32,ea27), (ev32,ev36), (ev32,ea25),
(ev32,ev37), (ev32,ea23), (ev32,ev38), (ev32,ea22), (ev32,ev40), (ev32,ea41),
(ev32,ev42), (ev32,ea42), (ev32,ev2), (ea29,ea28), (ea29,ev35), (ea29,ea27),
(ea29,ev36), (ea29,ea25), (ea29,ev37), (ea29,ea23), (ea29,ev38), (ea29,ea22),
(ea29,ev40), (ea29,ea41), (ea29,ev42), (ea29,ea42), (ea29,ev2)}

Appendix A.2 Performance Index (PI) calculation for each user-infrastructure combination

This appendix presents the constructed scales used by the decision maker to assess the disutility for each user-infrastructure combination. The global weight is contained along side each constructed scale for reference. The scales are presented in user order (building A, building B, …, building F). The decision makers' analysis of the appropriate level on the constructed scale, for the specific threat, is annotated with a 1 in the row indicating the constructed scale level under the appropriate infrastructure column. The columns are designated E for electrical service, NG for natural gas service, and W for water service. When the decision maker has completed the analysis each constructed scale will contain three 1 entries, one for each infrastructure. A summary of the final PI entries is:

	Infrastructure		
User	Electric	Natural Gas	Water
Building A	0.02117	0.00865	0.01477
Building B	0.02901	0.01505	0.02117
Building C	0.06490	0.01141	0.00979
Building D	0.07274	0.02117	0.02117
Building E	0.02980	0.00865	0.02340
Building F	0.02980	0.00865	0.02340