A Multi-Attribute Method for Ranking the Risks from Multiple Hazards in a Small Community

By

Hua Li

B.S. Information Engineering
Xi'an Jiaotong University, Xi'an, China, 2000

M.S. Nuclear Energy Science and Engineering
Tsinghua University, Beijing, China, 2003

Submitted to the Engineering Systems Division
in Partial Fulfillment of the Requirements for the Degree of

Master of Science in Engineering Systems
at the
Massachusetts Institute of Technology
[February 2008]
December 2007

Signature of Author ....
Engineering Systems Division
December 12, 2007

Certified by ....
George E. Apostolakis
Professor of Engineering Systems, and Professor of Nuclear Science and Engineering
Thesis Supervisor

Accepted by ....
Richard de Neufville
Professor of Engineering Systems, and Professor of Civil and Environmental Engineering
Chair of Education Committee, Engineering Systems Division

A Multi-Attribute Method for Ranking the Risks from Multiple Hazards in a Small Community

By

Hua Li

Submitted to the Engineering Systems Division on December 12, 2007
in Partial Fulfillment of the Requirements for
the Degree of Master of Science in Engineering Systems

Abstract

Natural hazards, human-induced accidents, and malicious acts have caused great losses and disruptions to society. After September 11, 2001, critical infrastructure protection has become a national focus in the United States and is likely to remain one for the foreseeable future. Damage to the infrastructures and assets could be mitigated through pre-disaster planning and actions.

A systematic method has been developed to assess and rank the risks from these multiple hazards in a small community of 20,000 people. It is an interdisciplinary study that includes probabilistic risk assessment, decision analysis, and expert judgment. Scenarios are constructed to show how the initiating events evolve into undesirable consequences. A value tree, based on multi-attribute utility theory, is used to capture the decision maker's preferences about the impacts on the infrastructures and other assets. The risks from random failures are ranked according to their Expected Performance Index values, which is the product of frequency, probability, and consequence of a scenario. Risks from malicious acts are ranked according to their Performance Index values as the frequency of attack is not available. A deliberative process is used to capture the factors that could not be addressed in the analysis and to scrutinize the results.

This method provides a framework for the development of a risk-informed decision strategy. Although this study uses the Massachusetts Institute of Technology campus as a test-bed, it is a general methodology that could be used by other similar communities and municipalities.

Thesis Supervisor: George E. Apostolakis
Professor of Engineering Systems, and Professor of Nuclear Science and Engineering

Acknowledgement

My foremost thank goes to my thesis adviser, Professor George E. Apostolakis, for his guidance during my study at MIT. He sets an example of a world-class researcher for his rigor and passion on research. I thank him for his insights and suggestions that helped to shape my research skills.

I thank the Federal Emergency Management Agency for their consideration and funding of the study. I would extend my appreciation to the Massachusetts Emergency Management Agency, and its representative Mr. Scott MacLeod, who offered valuable guidance in the study. I gratefully acknowledge the support of my project team: Joseph Gifun, William VanSchalkwyk, Susan Leite, David Barber, William McShea, and Gerald Isaacson. Without them, this thesis would not have been possible. I thank them for their support and encouragement. I enjoyed all the vivid discussions we had on various topics and had lots of fun being a member of this fantastic group. They are my team forever! Finally, I thank the Institute's stakeholders for their insightful discussions and commitment to this study.

I am also grateful to the faculty, staff, and students in ESD. I appreciate their countless help during my study in ESD. What I have learned in ESD are important treasures in my life, and what I have experienced during this period of time will become an unforgettable memory to me.

I would like to extend my thanks to my friends at MIT and elsewhere. Their friendship makes my life wonderful and joyful. I especially want to thank my friend, Ji-yong. I cherish the time when we studied together.

I am also deeply indebted to the many others who provided help, support and encouragement in various ways, especially during the stressful times. Thanks for their advice and help that carried me on.

My deepest gratitude goes to my parents. They always offer me support and encouragement. Thanks for their love.

Finally, I would like to dedicate this thesis to my husband, Ke, for enduring this long process with me. I thank him for believing in me, understanding me, and supporting me all along. He has always been a constant source of encouragement in my life. Without his love, I would never have made it so far.

Table of Contents

List of Figures

List of Tables

1 Introduction

Terrorist attacks in New York City and Washington DC on September 11, 2001, the thwarted attempt that resulted in the crashing of United Airlines Flight 93 in Shanksville, PA, as well as hurricanes Katrina and Rita remind us of the importance of mitigating the consequences of disasters. Natural disasters, human-induced accidents, and malicious acts have great potential for death, injury, economic losses, and disruption of service to society. The damage to infrastructures and assets could be mitigated through pre-disaster planning and actions. An important element to planning is the prioritization of risks according to criteria acceptable to the decision makers and the stakeholders.

Risk has different definitions in different fields, and there is no consistent definition of risk to counter the hazards. In Probabilistic Risk Assessment (PRA), risk is defined as the answer to the following three basic questions, also called the "triplet definition of risk" (Kaplan and Garrick, 1981; Garrick, Hall et al., 2004):

1. *What can go wrong?*
2. *How likely is it to happen?*
3. *What are the consequences if it does happen?*

These questions provide a general framework for risk assessment. Even so, this definition may lead to various explanations. For example, what do the term *consequences* mean? Does it mean the economic losses or number of fatalities only? If not, how should the consequences be determined and evaluated?

Furthermore, although risk assessment has been implemented for hazards such as earthquakes and hurricanes, systematical risk assessment concerning multiple hazards is still a considerable technical challenge. Especially, for malicious acts, probability of attack is not available. How to assess and manage the risks due to malicious acts is still a challenge. In addition, since the infrastructures and assets involve multiple stakeholders, it is important to capture their preferences. Here, *Stakeholders* refer to the entities that have a stake in the decision process, that is, the individuals or organizations that are interested in, involved in, or potentially affected by the decisions (National Research Council, 1996; Accorsi, Zio et al., 1999).

The objectives of the research are:

1. Develop a systematic methodology to assess and rank the risks from multiple hazards in a small community. The hazards include natural hazards, human-induced accidents, and malicious acts. Natural hazards and human-induced accidents refer to the ones that happen probabilistically, and they can also be regarded as random failures. Malicious acts refer to intentional attacks. In this study, vandalism, that is, intentional attacks on the infrastructures, is addressed. Multiple infrastructures and assets together with multiple stakeholders who have stakes on these infrastructures and assets are addressed as well.
2. Provides the framework for the development of a risk-informed decision strategy to understand and manage the above risks. The risk-informed approach is different from the risk-based approach. *Risk-Based approach* means that a safety decision is solely based on the numerical results of the risk assessment. This places heavy reliance on risk assessment results. *Risk-Informed approach* represents a philosophy whereby risk results and insights are considered together with other factors to establish requirements that better focus on the issues commensurate with their importance to stakeholder values.

This study was conducted for the campus of the Massachusetts Institute of Technology (MIT) as part of the Disaster Resistant University (DRU) program. Federal Emergency Management Agency (FEMA) has provided the DRU program to protect U.S. government investment in academic research and to protect the country's higher education capability. MIT is participating in this program to better understand and mitigate all hazard potentials that face the institution. In addition, the MIT campus is a good representation of a community. It can be considered a town with approximately 6,000 residents and 14,000 commuters. It operates a utility plant, data network, cable television station, phone system, and has its own police and medical personnel. The method conducted here can be applied to many similar communities such as other academic research organizations located in similar settings as well as small municipalities.

Chapter 2 reviews the literature about risk assessment, risk ranking, probabilistic risk assessment technique, and decision analysis. Chapter 3 shows the overall framework. Chapter 4 addresses the details of the methodology. In particular, Section 4.1 defines the study scope. Section 4.2 discusses hazard identification and screening, followed by the classifications of critical infrastructures and assets, as is shown in Section 4.3. Section 4.4 introduces how scenarios are constructed using Probabilistic Risk Assessment, and lists the steps used to collect data from the stakeholders through a formal expert elicitation process. The impacts from the scenarios are evaluated by a hierarchical decision framework and are presented in Section 4.5. Chapter 5 outlines the deliberative process used on the technical results. Chapter 6 provides preliminary risk management strategies. The contributions of the method and its limitations are discussed in Chapter 7, followed by Chapter 8 addressing the future research.

2 Literature Review

2.1 Risk Assessment and Ranking

Several universities have participated in the DRU program, including University of California at Berkeley (UC Berkeley) and University of North Carolina at Wilmington (UNCW). The UC Berkeley study (Comerio, Bertero et al., 2000; Comerio, Stallmeyer et al., 2003; Office of the Vice Provost and Disaster-Resistant University Steering Committee, 2000) developed a scenario-based approach to assess the risk to the campus from earthquakes. Three scenarios (magnitude 6.5, 7.0, and 7.5 on the Richter scale) were used to estimate the structural and non-structural losses (in dollars). The conclusion was that non-structural losses dominated the structural losses. Then, the cost of mitigation was evaluated by considering three attributes: *life safety*, *value* (i.e., the purchase price of the equipment), and *importance* (to research).

The UNCW study (UNCW, 2003) addressed multiple hazards in their DRU project, including hurricanes, wildfires, earthquakes, tornadoes, and severe winter weather. Multiple attributes were used to evaluate the potential impact from these hazards to people, property, and business. The hazards were ranked by the *Hazard Priority Score*, defined as the product of frequency and potential impact. Qualitative scales were developed for each attribute, and the score for each attribute was given by faculty and staff. The study is based on subjective qualitative analysis rather than quantitative assessment.

In addition to the DRU studies, methods for evaluating multiple hazards have been proposed in the literature. The Carnegie Mellon University (Florig, Morgan et al., 2001) developed a deliberative risk ranking method that described the risks in multi-attribute terms and employs groups of laypeople to perform the risk ranking. The authors used the Centerville Middle School and DePaul County as test-beds. Multiple risks were considered such as accidental injuries, airplane crashes, bites and stings, common infectious diseases, and lightning. The methodology featured an iterative deliberative process in which each participant provided holistic and multi-attribute risk ranking individually, and then subjected his/her risk ranking to deliberation and revision through group interactions. Several runs of the individual-group risk ranking process were implemented until the participants were satisfied. Risk scenarios were not identified. For example, the expected number of deaths per year was estimated directly and was used to represent the risk of death from a particular hazard.

In the New Jersey Comparative Risk Project (NJCRP), the authors (Andrews, Hassenzahl et al., 2003) developed a hazard ranking methodology by sorting multiple environmental threats. The NJCRP was designed to involve experts and stakeholders through focus groups, surveys, newsletters, open meetings, and a website. This was a consequence-based approach containing multiple impact categories, i.e., human health, ecological, and socioeconomic. Deliberation was included in the process, but probabilities were not considered.

University of Maryland (Ayyub, McGill et al., 2007) developed a quantitative all-hazards framework for critical asset and portfolio risk analysis considering both natural and human-induced hazards. The formula for risk analysis was obtained based on the traditional model, that is, the notional product of consequence, vulnerability, and threat. The consequence model had four loss dimensions, i.e. Casualty (unit: number of fatality equivalents), Economic (unit: dollars), Mission Disruption (unit: percentage reduction in available production capacity), and Recuperation Time (unit: days or years), and yielded direct losses and first-order estimates of interdependency effects. The likelihood of the hazards was expressed as the product of the attractiveness terms and the baseline annual rate of occurrence. For malicious acts, the attractiveness terms can be determined based on the perceived utilities; for natural hazards, the attractiveness terms are set equal to one. A sensitivity measure was defined to show how small changes in each risk parameter contributed to the results so as to provide insights for cost-effective risk reduction. However, the method only included key elements in the scenarios. It did not show how the events evolved into the consequences. Thus, even though the risk contributors could be ranked according to the sensitivity measure, its support for providing actionable risk information and targeting the risk reduction alternatives was still very limited.

2.2 Probabilistic Risk Assessment

Probabilistic Risk Assessment (PRA), also called Probabilistic Safety Assessment (PSA) or Quantitative Risk Assessment (QRA), is a proven, well established, and systematic process aimed at producing quantitative estimates of the risks associated with complex engineering systems. "The identification of the most likely failure scenarios and the major sources of uncertainty is an essential part of PRA (Apostolakis, 1990)".

For a given system, PRA proceeds as follows (Apostolakis, 2004):

1. Determine a set of undesirable end states. An end state is the set of conditions at the end of an event sequence that characterizes the impact of the sequence.
2. Determine the first significant deviation from the normal situation that may lead to the end states. 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, *scenarios* are generated.
4. The probabilities of these scenarios are evaluated using the available evidence, i.e. historical data and expert judgment.

Results are used to provide insights to educate participants. PRA is a planning-as-learning exercise, not simply an analysis tool.

After the scenarios have been constructed, they will show how the initiating events evolve into undesirable consequences, and the evaluation of their probabilities will enable us to rank these scenarios. Therefore, PRA is a scenario-based methodology.

The evaluation of the probabilities of the scenarios is a major challenge. PRA utilizes the Bayesian (degree-of-belief) interpretation of probability that allows using all evidence available, i.e., statistical, experiential, and expert judgment (Apostolakis, 1990). When the statistical evidence is hard to obtain, expert judgment must be relied on. Methods for formal expert opinion elicitation have been developed and applied in major risk studies (Keeney and von Winterfeldt, 1991; Forester, Bley et al., 2004).

PRA strengthens in its quantification. It provides a way of understanding the risks associated with the system and expressing the uncertainties involved. PRA forms the basis for risk-informed decision making. It provides a framework to understand the problem and facilitate communication among various stakeholder groups. It enables to integrate diverse disciplines such as the engineering and social sciences to solve the problem. Although human errors and design and manufacturing error have not been handled well or not handled at all by current PRA, its platform encourages identifying the complex interactions between the systems or events.

2.3 Decision Analysis

Decision problems nowadays are more complex than before. A technical definition of decision analysis is "a philosophy, articulated by a set of logical axioms, and a methodology and collection of systematic procedures, based upon those axioms, for responsibly analyzing the complexities inherent in decision problems (Keeney, 1982)".

The foundation of the Multi-Attribute Utility Theory (MAUT) is a set of axioms, that is, von Neumann and Morgenstern axioms (VNM axioms). Through the use of utility functions, the multiple criteria can be transformed into a dimensionless scale of utility. MAUT assumes that the decision maker is rational, and consistent in his/her judgments. The utility functions reflect the decision maker's attitude towards uncertainties (risk averse, risk neutral, or risk seeking). The Expected Utility Theory tells people "what should do".

However, MAUT is suited for single decision maker problems, a condition that sometimes not the characteristic of the decision context. Besides, experimental evidence has challenged the VNM axioms, for example, the Allais paradox (Kleindorfer, Kunreuther et al., 1993). The situation has stimulated much interest in understanding the factors that influence the valuation and choice process, and several alternative descriptive approaches are generated for dealing with these problems, such as the Regret Models and the Prospect Theory.

Despite of the limitations, decision analysis still has its value. Decision analysis not only provides framework to compare the alternatives, but also has the ability to provide structured methods to involve the stakeholders' opinions into the analysis. McCord and de Neufville (McCord and de Neufville, 1983) also mentioned: "Professional experience confirms that there is much value in helping people structure their choices; think about their preferences are a nonlinear response to risk and quantity. Just this limited exercise is often valuable in that it encourages decision makers to identify strategies that provide insurance against calamities or opportunities to obtain particularly excellent results." We should realize that "decision analysis will not solve a decision problem, nor is it intended to. Its purpose is to produce insight and promote creativity to help decision makers make better decisions (Keeney, 1982)."

Weil and Apostolakis (Weil and Apostolakis, 2001) propose a hierarchy decision framework which includes the following five steps:

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

In decision analysis, the objectives are fundamental to the decision maker in considering the decision problem. The categories and the number of objectives vary depending on the complexity of the decision and the preferences of the decision maker.

Attributes, also called performance measures, criterions, or metrics, are determined to measure the achievement of the objectives. Generally, there are three types of attributes (Keeney and Gregory, 2005): natural attributes, constructed attributes, and proxy attributes. To select attributes for each of the objectives in an analysis, one first tries to identify natural attributes and selects one if a good choice is found. If not, then try to use a constructed scale for that attribute. If neither good natural attributes nor good constructed attributes are available, then one uses a proxy attribute. However, no matter what types of attributes are used, the attributes should be unambiguous, comprehensive, direct, operational, and understandable (Keeney and Gregory, 2005).

After the weights and attributes are constructed, the next step is to weight the objectives and the attributes, and assess the utility functions of the attributes. Many methods are available to fulfill these tasks: the certainty equivalents method (Keeney and Raiffa, 1993), the pricing out method (Keeney and Raiffa, 1993), the ratio method (Clemen, 1995), the swing method (Clemen, 1995), lottery equivalent (LEP) method (McCord and de Neufville, 1986), AHP pairwise comparisons (Hughes, 1986). However, comparison of some of the weighting judgments (Borcherding, Eppel et al., 1991) shows that:

> *"Thus, it appears more prudent to reduce reliance on these approximation methods and concentrate on designing appropriate elicitation procedures... Using carefully designed interactive procedures for elicitation should increase the internal consistency ... "*

Other researchers drew the similar conclusion (von Nitzsch and Weber, 1993; Triantaphyllou and Sanchez, 1997; Fischer, 1995). The statement reminds us to pay more attention to the elicitation procedures.

When weighting the objectives and attributes, and assessing the utility functions of the attributes, the decision maker does not weight them generally, but rather, should be aware of the ranges of the consequences. Different ranges of the consequences may lead to different weights. Finally, eliciting value judgments is subject to bias and random errors. Hence, it is important to check the reasonableness and consistency of the elements in decision analysis.

3 Overall Framework

The objectives of this study are to develop a systematic methodology to assess and rank the risks from multiple hazards in a small community, and provide a framework for the development of a risk-informed decision strategy to understand and manage the risks. The proposed method is scenario-based and involves the decision makers and the stakeholders in each step. It implements and expands the analytic-deliberative process (National Research Council, 1996). Figure 1 illustrates the overall methodology framework, and Figure 2 magnifies each step.

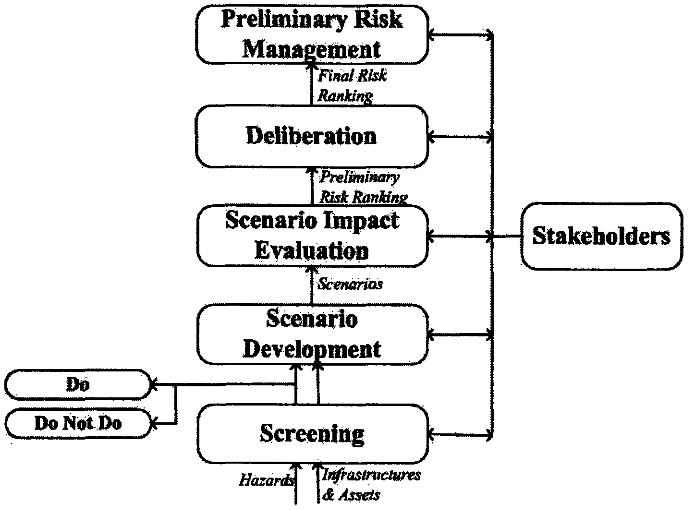

Figure 1: Methodology Framework

The first step (bottom of the figure) is to gather the data and information from a variety of sources. Using the information, the following hazards, infrastructures and assets are screened out: the ones that are addressed by other projects ("Do") due to their significance, and the ones that are judged to be insignificant ("Do Not Do"). The screening is necessitated by the large number of hazards, infrastructures and assets that must be investigated.

Second, using Probabilistic Risk Assessment (PRA) techniques, scenarios are constructed for these infrastructures, assets and hazards. A scenario is a well-defined sequence of events leading to the loss of one of the end states. Each scenario starts from an initiating event and proceeds through a series of subsequent events to a number of undesirable physical consequences, i.e., the end states. Since the infrastructures are interconnected, the dependencies among them are included in the scenarios; otherwise, the consequences would be underestimated. Moreover, the assets are categorized into *Macro-Groups* according to their activities and operations.

A preliminary ranking of the scenarios is achieved by using methods from Multi-Attribute Utility Theory. In particular, the objectives of the decision makers are represented in a "value tree," as shown in Figure 2. Disutilities measure the impact of the scenarios on these objectives. The expected disutilities of the scenarios form the basis for a preliminary ranking, i.e., the higher the disutility the less desirable a scenario. The expected disutilities of scenarios emanating from natural events can be evaluated because their frequencies are known. This is not the case for malicious acts and therefore other methods for ranking are developed.

The final risk ranking is determined through a deliberative process in which the results are evaluated by the decision makers and the stakeholders. Based on this ranking, risk management alternatives can be proposed.

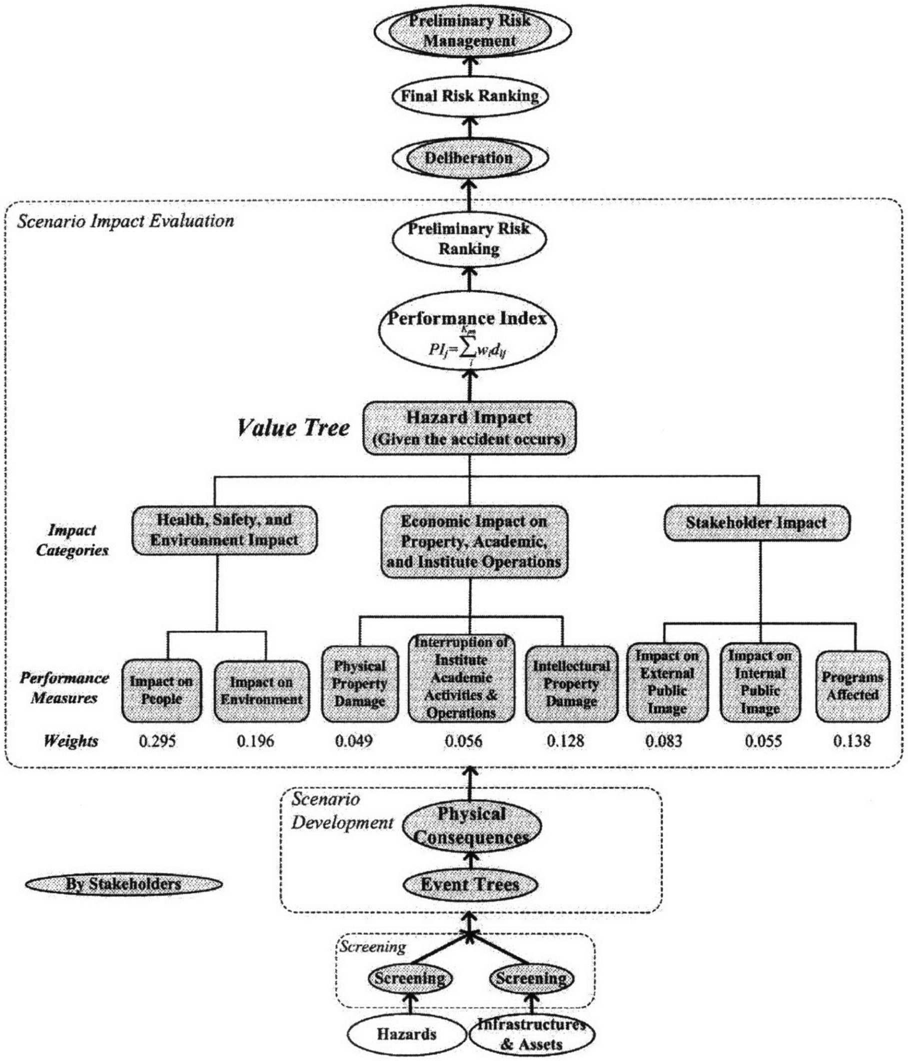

Figure 2: Overall Methodology

4 Methodology

4.1 Study Scope

The National Research Council (National Research Council, 1994) has recommended that the decision-maker include all the stakeholders in the decision-making process from the beginning. They recommend an analytic/deliberative process that not only clarifies the technical risk assessments but also enables the stakeholders to express their preferences. More than 50 lab-level and department-level stakeholders were interviewed in this study. Their participation is key to obtain their perspective in terms of the vulnerabilities and risks to the MIT campus. In addition, the stakeholders play important roles in eliciting information for formal technical analysis. Finally, they are the key participants for the deliberation process.

The infrastructures and assets that are critical for MIT's research and teaching mission are identified and addressed; these include the buildings and physical assets, utility generation facilities, utility distribution systems, and other assets within the campus. Natural and human-induced hazards that could potentially lead to damage and interruption for the Institute are considered. Other issues such as thefts, which are not directly involved in the disaster and emergency response, are beyond the scope of this analysis.

Both local damage and campus-wide damage are analyzed. The former refers to the initiating events that occur in a single location and will be bounded to local damage unless propagated; the latter refers to the initiating events that lead to multi-location failures simultaneously. The starting point for the analysis is the single point failure or attack, that is, the analysis of the consequences and vulnerability if a single location is damaged, a single system fails, or a single asset is out of service. This enables a broad perspective on how the impact is distributed across the campus.

The utility infrastructures are distributed networks. While network algorithms could have been used to analyze the nodes in the distribution systems, they are not used in this study, because the assets in this project are the end-users of the utilities, and the probability of large propagation onto the distribution network, given a single end-user failure, is very low. The utility generation units as key assets, however, play an important role in the utility infrastructure. The risks of losing the utility generation units and the resulting campus-wide failures are therefore analyzed.

4.2 Hazard Identification and Screening

4.2.1 Screening Criteria

The following hazards may potentially present risks to a small community similar to the MIT campus:

- Natural Hazards: Earthquakes, Tornados, Hurricanes, Winter storms, Freezing, and Heavy rain
- Human-Induced Hazards: Fires, Explosions, Internal flooding, Vandalism, Outbreaks of infectious diseases, and Cyber/IT attacks

Here, internal flooding means the flooding due to broken water pipes, plugged drains, condensation, faulty plumbing, or sprinkler system failure; all internal to the building. Vandalism describes the malicious actions on the infrastructures that result in operation disruption, property or facilities damage.

Screening is used to find out the most important or credible hazards so that mitigation resources can be concentrated on the most important ones. The criteria for screening the hazards are (Karydas, 2002; Pillay and Wang, 2003):

- *Frequency*: occurrence of events per year;
- *Severity:* the consequence level due to the hazard;
- *Warning/Detectability:* the extent to which warning information is available;
- *Awareness:* how much work has historically been done to mitigate the hazard and the extent to which MIT grasps the damage due to the hazard

- *Importance:* the extent of urgency or necessity of doing work to address the hazard; and,
- *Satisfaction*: degree of personal acceptance of the level at which MIT is currently working to prepare for, respond to, or mitigate a potential hazard.

See Table 1 to Table 6 for details.

Each hazard is compared against each of these six criteria, and evaluated using a subjective 0-4 scale. The objective of these criteria is not to find the exact scale for each hazard (detailed quantitative analysis will be done in the following steps) but to determine qualitatively the properties of all the hazards and screen out the hazards that are beyond the scope of the analysis. For this reason, the criteria aim to provide a platform to the decision makers and enable them to develop an overview of the hazards. Thus, each decision maker can select the hazards that should be screened out in his/her opinion. After the screening, the decision makers discuss the hazards, and reach consensus on the hazards that do not require further analysis. The results of this screening process are shown in Table 8.

Table 1: Frequency

Description	Level
High (occurs >3 times /year)	4
Moderate (occurs 1-3 times /year)	3
Low (occurs 0.1-1 time /year)	2
Very Low (occurs <0.1 time /year)	1
Extremely low or not available	0

Table 2: Severity

Description	Level
Catastrophic	4
Critical	3
Limited	2
Negligible	1
No adverse impact	0

Table 3: Warning / Detectability

Description	Level
Extremely low detectability (no warning information)	4
Very low detectability (minimal warning information)	3
Low detectability (warning information available 1 to 12 hours before occurrence)	2
Moderate detectability (warning information available 12 to 24 hours before occurrence)	1
High detectability (warning information available more than 24 hours before occurrence)	0

Table 4: Awareness

Description	Level
Much work has been done to mitigate the hazard; MIT knows the hazard and its impact well.	4
Significant work has been done to mitigate the hazard; MIT knows the hazard and its impact moderately.	3
Some work has been done to mitigate the hazard; MIT knows the hazard and its impact limitedly.	2
Little work has been done to mitigate the hazard; MIT knows the hazard and its impact little.	1
No work has been done to mitigate the hazard; MIT knows nothing about its impact.	0

Table 5: Importance

Description	Level
Essential	4
Very important	3
Somewhat important	2
Not important	1
I do not know	0

Table 6: Satisfaction

Description	Level
Very satisfied	4
Somewhat Satisfied	3
Neutral	2
Somewhat dissatisfied	1
Very dissatisfied	0

4.2.2 Hazards Screening

Earthquakes

Earthquakes with magnitude lower than 4.5 on the Richter scale do not tend to lead to structural damage. Table 7 lists the probabilities of earthquakes with different magnitudes in Cambridge (http://earthquake.usgs.org). It can be concluded that Cambridge has very low probability for a severe earthquake (magnitude is greater than 4.5).

Table 7: Probability of Earthquake with Various Magnitudes (within 500years & 50km Area)

Magnitude	Probability (Cambridge MA)
≥ 5.0	0.4
≥ 6.0	0.05
≥ 6.5	0.02
≥ 7.0	0.008

Based on the data in Table 7 for the City of Cambridge, the probability of severe earthquake for the MIT campus is very low. MIT considers mitigating the earthquake consequences as not worthy in terms of the benefit-cost perspective. Earthquake is therefore screened out from further analysis.

Outbreaks of Infectious Diseases

Outbreak of infectious diseases like pandemic flu is a catastrophic issue for the whole campus. At present, the United States is facing a threat from the pandemic flu. It is such an important and urgent issue that MIT has a specific project to address the outbreak of infectious diseases. Thus, this hazard is screened out from further analysis.

Winter Storms

Cambridge, Massachusetts, is located at the northeastern part of the United States. MIT suffers from snow and wind storms, as well as extreme low temperature events annually. Since these hazards always come in winter, they are referred as winter storms.

The Cambridge area has a long history of severe and damaging winter storms. According to FEMA data, the average annual snowfall for the eastern half of Cambridge is 36.1 to 48 inches and for the western half, 48.1 to 72 inches. There had been a risk of structural damage due to excessive accumulation of snow at two locations on campus. At one location, the tennis bubble, there are procedures that are followed during times of heavy snow that call for controlled deflation, while at the other structural reinforcements were installed. The depth of snow on other roofs is monitored and if becoming potentially dangerous, it is removed. Thus, this risk was screened out.

Wind storms are another natural hazard that impacts MIT. In winter, snow storms are often accompanied by strong wind that may lead to more loss than a snow storm alone or a wind storm alone. Hurricane, with its high wind speeds and substantial rain, and tornado, a kind of wind storm, are also potential hazards. Research on damage to residential structures shows that wind is responsible for greater property loss than water (Ayscue, 1996). Cambridge has been impacted by hurricanes throughout its history. Since 1900, there have been effects from 24 hurricanes and 14 tropical storms, in which Hurricane Edna (September 11, 1954), Hurricane Carol (August 31, 1954), Great Atlantic Hurricane (September 14-15, 1944), and Great New England Hurricane (September 21, 1938) are indicated as Category 3 (111-133mph central speed). Historical data also show that there are 16 tornados in Massachusetts from 1950 to 2002 (http://www.ncdc.noaa.gov/oa/climate/severeweather/tornadoes.html#19902003). No records are available showing whether and how much these hurricanes and tornados impacted the MIT campus. In all, Cambridge has a 100-year wind speed of 110mph, that is, a speed of 110mph wind would occur once within 100 years.

Buildings on campus, including those buildings with extensive glass facades, are constructed to withstand strong winds. Thus, the structural damage due to wind storms should be screened out of the study, however, indirect damage from wind storms should be taken into consideration. For example, trees would fall down during wind storms, and they may damage the utility transmission lines (e.g., electricity), thus impacting the utility end-users.

MIT records show that utility pipes that were frozen and broken in the cold days have cost $832,019 loss in the past ten years. Weather records in the past five years show that there are on-average 6 days with extreme low temperature (below 10F). Therefore, a detailed analysis is required for freezing and its impact on the campus.

Rain Flooding

Heavy rain may lead to flooding (especially in basements) and structural damage, thus damaging the facilities and research equipment. Since 1999, the campus has experienced a loss of roughly $380,000 due to flooding from rainstorms. On July 14, 1996, heavy rain resulted in flooding of a building's sub-basement; the precipitation was 3.36 inches that day. On April 21, 1997, the basement of another building was flooded. The precipitation was 1.69 inches that day. According to 5 years of weather records, in a year, there are 10 days on average with the rain precipitation above 1 inch. For this reason, flooding due to heavy rain is not screened out of the detail analysis.

Fires and Explosions

Fire, either accidental or intentional such as arson, is an issue of concern for MIT. There are approximately 8-10 fire incidents each year, although around 300 fire calls and alarms are recorded annually. Furthermore, MIT operates the laboratory facilities that may lead to explosion. The probable causes and the consequences need to be investigated for these hazards.

Internal Flooding

Internal flooding means flooding due to broken water pipes, plugged drains, condensation, faulty plumbing, or sprinkler system failure. Every year, tens of internal flooding incidents are recorded. The stakeholders believe internal flooding is a high-frequency hazard, and the consequences due to internal flooding could also be very high. Internal flooding is therefore assessed in detail.

Terrorism (or Vandalism)

Terrorism is defined by the Department of Defense as (Department of Defense, 1999):

> *"The calculated use of violence or threat of violence to inculcate fear; intended to coerce or to intimidate governments or societies in the pursuit of goals that are generally political, religious, or ideological."*

The campus has very low probability for severe terrorist events such as bombings. MIT may, however, suffer from a minor attack. *Vandalism* is used to describe such actions and is defined as:

> *"Any intentional act that results in operation disruption, property or facilities damage."*

The consequences of such intentional attack on the key assets could be very high or even catastrophic, for example, an attack on MIT research reactor. Therefore, it is very essential to systematically analyze the vulnerabilities regarding vandalism.

Cyber Attacks

The U.S. National Infrastructure Protection Center (NIPC) defines *Cyber Attacks* as (Garrison and Grand, 2001):

> *"A criminal act perpetrated by the use of computers and telecommunications capabilities, resulting in violence, destruction and/or disruption of services to create fear by causing confusion and uncertainty within a given population, with the goal of influencing a government or population to conform to particular political, social or ideological agenda."*

Cyber attacks are the malicious actions by use of the computer network tools, and are thus differentiated from other malicious actions that depend on physical attacks. The action whereby one attacks the internet network by perpetrating a software virus is defined as a cyber attack, while the sabotage action that an attacker takes to intentionally damage the physical bus is referred as vandalism.

Cyber attacks are beyond the scope, because they have been handled by the MIT Department of Information Services and Technology with a specific and continuous effort.

Table 8: Hazards in Scope and Hazards Screened Out

Hazards in-Scope	Hazards Screened Out and Reasons
Internal flooding; Fires; Explosions; Winter Storms (snow storms, wind storms) Rain flooding; Vandalism	Earthquakes • Because of the low probability of severe earthquakes, mitigating the earthquake consequences is not cost-effective; • The efforts for reducing the impacts from earthquakes are considered as "Do Not Do". Outbreaks of infectious diseases • This hazard is so important and urgent that it is the subject of a specific study; • The efforts for reducing the impacts from infectious diseases are considered as "Do". Cyber attacks • They have been handled by another organization.

4.3 Infrastructures, Assets, and Macro-Groups

4.3.1 Critical Infrastructures and Key Assets

The President's *National Strategy for Homeland Security* (NSHS), issued in July 2002 (U.S. Office of Homeland Security, July 2002), lists critical infrastructures and key assets, as is shown in Table 9. The MIT critical infrastructures include the utilities and the emergency and security elements (see Figure 3). Electricity is a fundamental utility for the equipment of research and education and the facilities of other utilities, such as the production of chilled water. Water and steam also provide a necessary utility to MIT and its activities. For MIT, natural gas is a fundamental component of the power generation infrastructure. Tel-data refers to the facilities that support data and telephone systems. The chilled water generation and distribution system is a critical infrastructure for MIT, since chilled water is an important utility for the operations and activities of some laboratories and provides the resource to cool interior spaces. HVAC (Heating, Ventilation and Air Conditioning) and Controls refers to the infrastructures that provide both process and temperature controls for the comfort of building occupants, as well as research equipment. The emergency and security elements listed in the right hand side of Figure 3 play a major role in the emergency planning and response system. Fire alarm systems, sprinkler systems, and the access-control systems provide physical defense to hazards. When an incident occurs in the campus, the Operations Center, the Police, EHS, and the Department of Facilities are involved in the emergency response process.

The key assets of MIT can be classified into three sectors (Figure 4):

1. Mission-Related Assets refer to the assets that are academic and research related, including research and education offices, laboratories, classrooms;
2. Support and Services Assets refer to medical center, administration offices (Human Resources Office, Payroll Office, etc.), athletics centers, and residential halls;
3. Other key assets refer to the assets such as the Central Utility Plant (CUP) which provides multiple utilities (electricity, steam, and chilled water) to the whole campus, Data Center which is the database for the administration offices, MIT Research Reactor, and the key assets in Information Services and Technology Department (IST) such as switches and servers. To be specific, although MIT Research Reactor is a key asset, it is screened out of further analysis, because the Nuclear Regulatory Commission supervises its operation and security issues. Security issues have been considered as the reactor was designed, built, and as it

has been operated. Additionally, the security was enhanced after September 11, 2001.

Table 9: Critical Infrastructures and Key Assets

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	

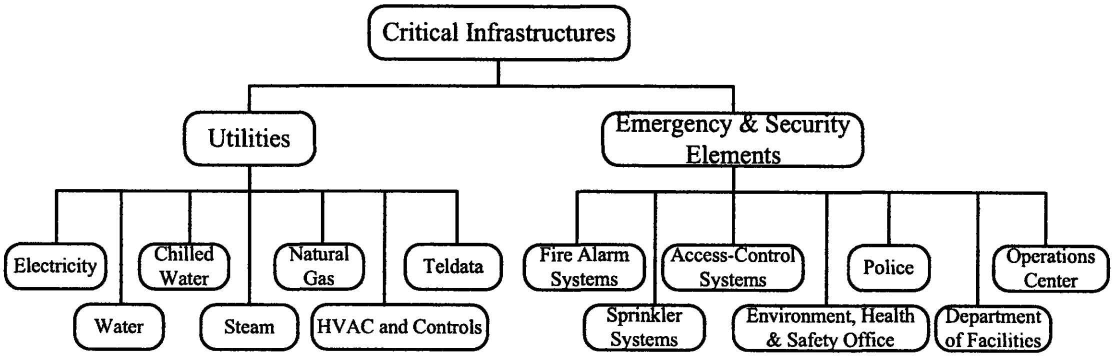

Figure 3: MIT Campus Critical Infrastructures

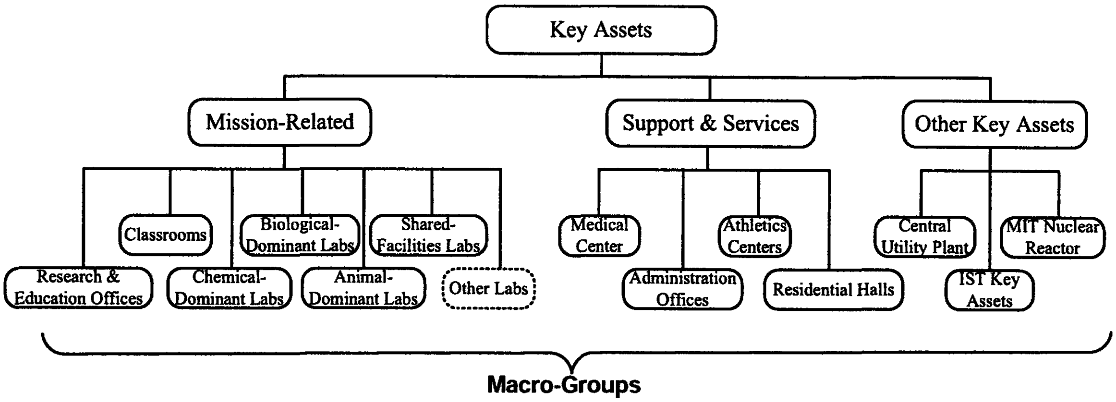

Figure 4: MIT Campus Key Assets

4.3.2 Macro-Groups

Since there are more than 155 buildings on the MIT campus, the assets are further categorized into *Macro-Groups* according to their activities and operations, as is shown in Table 10. A *Macro-Group* is defined as a group of assets that have similar activities and operations. For example, the faculty members' offices, staff's offices, and other researchers' offices can be considered as the Research and Education Offices Macro-Group. Data are collected from a representative of the Macro-Group, and is considered transferable for all the assets within the Macro-Group. The Macro-Group concept is extended from the one that Patterson (Patterson and Apostolakis, 2007) used in his study about minor intentional attack on the MIT campus' infrastructures. He classified the infrastructures in the MIT campus to the following four Macro-Groups: Residential (dorms, etc), Academic and Research (classrooms and laboratories), Support Facilities (utility plants, etc), and Athletics (sports, gym, etc). In this study, more than 13 Macro-Groups are constructed.

Given a hazard, the consequences for the Macro-Groups are different. In terms of internal flooding, for example, the consequences for the research and education offices are the loss of the documents and computers (loss of electronic data and research documents), but the consequences for the animal-dominant laboratories could be more severe since the laboratories may lose animals, which could result in long-term research damage.

4.3.3 Interdependencies

Protecting these infrastructures and assets creates major technical challenges, because the infrastructures are complex and interconnected systems. Infrastructure interdependencies refer to "relationships or influences that an element in one infrastructure imparts upon another infrastructure (Dudenhoeffer, Permann et al., 2006b)". Ignoring these interdependencies results in underestimation of the physical consequences, and thus underestimates the risks.

Interdependencies can be classified into different types. Bühne (Bühne, Halmans et al., 2003) defines the following dependencies: *Requires Dependency, Exclusive Dependency, Hints Dependency, Hinders Dependency.* Dudenhoeffer (Dudenhoeffer, Permann et al., 2006a) describes dependencies in terms of four general categories *Physical Dependency, Geospatial Dependency, Policy Dependency,* and *Informational Dependency.* Rinaldi (Rinaldi, Peerenboom et al., 2001) proposes a slightly different but similar categorization, which is adopted in this study:

- *Physical Dependency* refers to a physical reliance on material flow from one infrastructure to another. The dependency of water pumps on electricity is an example of physical dependency.
- *Cyber Dependency* refers to a reliance on information transfer between the infrastructures. For example, the Human Resources Department depends on the Data Center to transfer, update, and store personnel data.
- *Geographic Dependency* refers to the dependency that a local environmental event affects components across multiple infrastructures due to physical proximity. If a utility manhole containing the valves of water pipes, electric power lines, and steam lines is flooded, the result could be a loss of several utilities because of geographic dependency.
- *Geographic Dependency* refers to the dependency between a local event and the affect of this event on multiple infrastructures due to physical proximity. For example, if a natural gas main exploded in the vicinity of water and steam mains and an electric duct bank, the result could be the loss of three additional utility services because of geographic dependency.

- *Logical Dependency* refers to the dependency between infrastructures that do not fall into one of the above categories. The dependency among the Institute's police, Environmental Health and Safety Programs, Emergency Operations Center, and Department of Facilities, and local fire services when responding to a fire is an instance of logical dependency.

The four categories of dependencies enable us to check whether all the dependencies have been included into the analysis. Figure 5 illustrates the interdependencies among the infrastructures and assets during a campus-wide power outage.

Table 10: Definitions, Activities, Operations, and Characteristics of Macro-Groups

ro-Group	Definitions, Activities and Operations	Characteristics	Representati
arch and ation Offices	Occupants use computers and documents to do research and education.	Computer failure or documents loss impacts the research.	Faculty offic
ical- inant ratories	Experiments using chemicals and associated equipment	Feature in high potential environmental and people safety impact. A backup power system is installed.	Chemistry Laboratories
gical- inant ratories	Experiments examining live tissues or life processes.	The biological samples store at the freezers. Loss of the biological samples leads to long-term research damage.	Bio Engineering Laboratories
al-Dominant ratories	Manage animals and improve the quality of control.	The animals are sensitive to pressure, temperature, and humidity. Loss of the animals leads to long-term research damage. A backup power system is installed.	Division Comparative Medicine
d-Facilities ratories	Laboratories with facilities shared with the researchers.	The facilities are shared by hundreds of researchers. The facilities failure may lead to high physical property damage. Most of the experiments can be re-performed after the facilities are restored.	Center of Material Sciences and Engineering
rooms	Instructor teaches students w/o multimedia equipment.	Feature in hundreds of students' safety and schedule of their classes.	Classrooms i Building 24
cal Center	Provide health service to the Institute members. Activities and operations involved critical systems (e.g. HVAC, proper lighting), in-patient unit, clinic hours, urgent care, and critical out-patient visits for patients.	Feature in the patients' safety. A backup power system is installed.	Medical Cent

ro-Group	Definitions, Activities and Operations	Characteristics	Representati
inistration es	Activities including communicate with data center to communicate, transfer, update, and store the data, and provide administrative service for Institute members.	Computer failure or document loss impacts the function of the administration offices. The activities and operations of the administration offices can be recovered by relocation.	Human Resources Office
lential Halls	Places for people to live.	Feature in hundreds of residents' safety. The potential physical property damage is not as high as other Macro-Groups.	West-Gate Residential Hall
tics Centers	Places for members to play sports and relax.	Feature in hundreds of Institute members' safety. The potential physical property damage is not so high.	Johnson Athletics Center
al Utility Plant	Generate utilities to provide electricity, steam, and chilled water for the whole campus.	Important utilities generator for the whole campus. Its failure impacts the campus severely.	Center Utilit Plant
Research tor	Key asset for research experiments.	Catastrophic impact to the campus or the nearby community.	MIT Researc Reactor
ey Assets	Key assets to provide Tel-data and wireless service for the Institute, including 5ESS Telephone Switches, cell tower, data center, and other key systems of information service to the campus.	Important assets to provide the communication service for the campus. Their failures impact the campus severely. High potential physical property damage.	IST telephon switches (Building E1

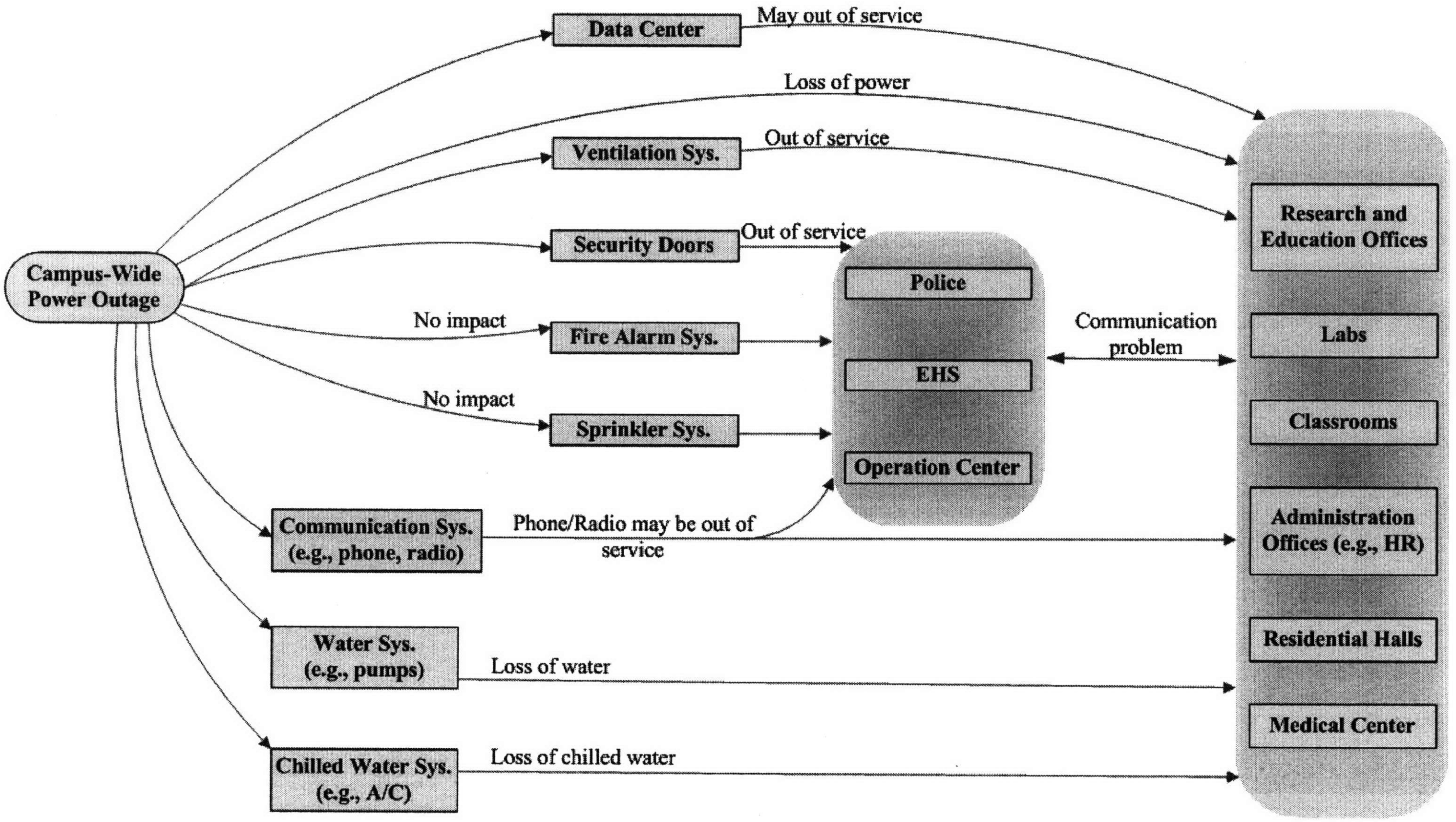

Figure 5: Infrastructures and Assets Interdependencies During Campus-Wide Power Outage

4.4 Scenario Development

4.4.1 Assumptions

The general risk process shown in Figure 6 provides the basis for constructing the scenarios. A scenario starts with an initiating event. If installed, the physical defense system responds right after the initiating event occurs. Emergency responders, i.e., police, EHS, and other departments, act to mitigate the consequences. In the subsequent events, utility systems such as electricity, water, and steam may fail. The final consequences for the Macro-Group depend on the activities and operations within the Macro-Group. For example, when a fire occurs at a location, the sprinkler system reacts, and the fire alarm system is activated. The Police, EHS Officer, fire fighters, and other emergency responders take actions for evacuation and mitigation. Fire damages the property and may also result in utilities supply failure.

The series of events between the initiating events and the end states could interfere with each other. For example, when an incident occurs, the Police, EHS, and other emergency responders must cooperate to mitigate the damage as much as possible. The emergency and security elements interact with each other. Whether they can communicate and collaborate well determines the action efficiency. This interaction is a dynamic process, however, and is difficult to quantify. Thus, the focus in this study is on the first responder instead of quantifying the dynamic process of emergency response teamwork.

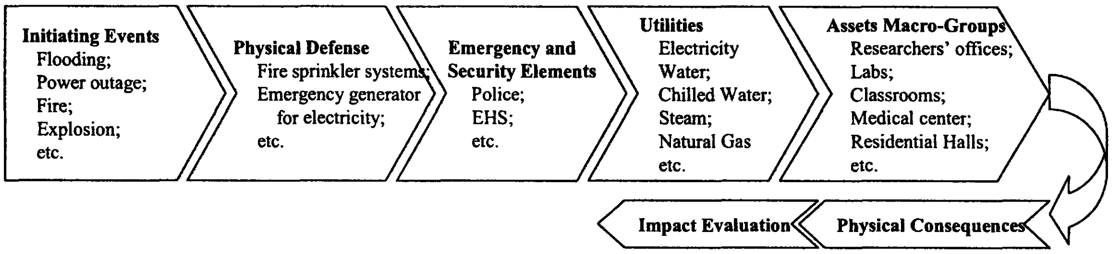

Figure 6: Risk Process

Two categories of failures are described: those that lead to local damage and those that lead to campus-wide damage. It is assumed the local-damage failures are bounded to building-level, or even room-size. This assumption works well for hazards such as fire and flooding. For incidents such as loss of utilities, however, it may propagate to other buildings. Because the utility systems are distributed networks, losing one node may extend to a broader area in the networks. In this study, the key assets are the users of the utilities. As the end nodes of the distribution systems, the probability of propagation due to losing a specific user is very low, assuming the failure is bounded in the Macro-Group building is reasonable. On the other hand, if the utility generation unit fails, it impacts the whole distribution system, since the generation unit is the source node of the network.

It is assumed that the duration of the local impact failures does not last more than one week, e.g., when a single building loses power supply, the power outage duration is not more than one week. The Managing Director of EHS Programs indicated: "When there is a single failure in a location, all the response resources can be concentrated on that location." This implies that the emergency responders could take action actively once there is single point of failure. For this reason, one week is a reasonable assumption for the duration.

Furthermore, the physical structure of the buildings is assumed the same for all the Macro-Group buildings. The age and the construction type of the buildings are not differentiated. With this assumption, the historical incidents due to the same initiating event are homogenously distributed across the Macro-Group buildings, that is, the frequency of a specific initiating event is the same across the Macro-Group buildings.

4.4.2 Initiating Events

Probabilistic risk assessment requires constructing a complete set of scenarios. Each scenario starts from the Initiating Event (IE) and proceeds through a series of subsequent events, then ends with the End States (ES) which reflect the levels of consequences. An example of a scenario is that a heavy rain floods the basement of a building, thus leading to property loss and other damage.

The hazards are the causes of the initiating events. Instead of starting from the hazards, the scenarios are constructed from the initiating events. For example, different origins of fires, such as domestic carelessness, industrial accidents, natural disasters, and arson, generate a number of scenarios. If the various origins of fires lead to different subsequent events, different scenarios must be constructed for the origins. Otherwise, one must start from the initiating event (fire in this case) and delineate the series of events leading to the end states.

The initiating events for scenario development are shown in Table 11. In this study, the initiating events are designed to be common for all the Macro-Groups. The initiating events could lead to local damage or campus-wide damage. Flooding due to the sprinkler system failure in a room is an example of the former. Water may flood the documents and the electronic equipment in the room. Even though the water may also propagate to other rooms.. the impact is still limited to the local location. Loss of utility supply (electricity, water, chilled water, steam, or natural gas) is another example of such initiating events, which is bounded in the Macro-Group building. On the other hand, there are a few such critical locations or key assets that if the initiating events occur in these places, the physical consequences would be wide-spread across the whole campus. For example, if the main bus of Central Utility Plant fails, the whole campus loses the electricity; if the city main pipe of water fails, no water is available to the campus.

Table 11: Initiating Events

Initiating Event	Scope
Loss of electricity	Leading to local damage (building-level)
Loss of water	Leading to local damage (building-level)
Loss of chilled water	Leading to local damage (building-level)
Loss of steam	Leading to local damage (building-level)
Loss of natural gas	Leading to local damage (building-level)
Internal flooding	Leading to local damage (room-size, multi-room-size, or building-level)
Fire	Leading to local damage (room-size, multi-room-size, or building-level)
Explosion	Leading to local damage (building-level)

Initiating Event	Scope
Campus-wide power outage	Leading to Campus-Wide Damage
Loss of water supply from City	Leading to Campus-Wide Damage
Rain storm	Leading to Campus-Wide Damage
Winter storm	Leading to Campus-Wide Damage

4.4.3 Event Trees and Physical Consequences

After the initiating events are determined, the next step is to analyze the subsequent events and the end states of the scenarios. Event Trees are used to describe the scenarios. The event trees start from the initiating event. The branches of the tree denote the subsequent events. The end node of a branch is the end-state of a scenario. Figure 7 is the event tree for internal flooding (more event trees are shown in Appendix 2). Table 12 is the corresponding physical consequences for the Shared-Facilities Macro-Group. This tree, as well as the physical consequences of the scenarios, are obtained from historical records and stakeholder input.

To quantify the scenario, probabilities of the events are required. Three sources of information were used to evaluate the probabilities:

1. Statistical analysis on the historical incidents: for example, the historical records on the number of flooding incidents.
2. Literature reviews: for example, papers evaluating the reliability of s fire sprinkler system (Bukowski, Budnick et al., 1999).
3. Stakeholder input: for example, the probability of flooding that propagates to lower-level rooms is elicited from the stakeholders, as will be shown in next section.

Figure 7: Event Tree for IE Internal Flooding

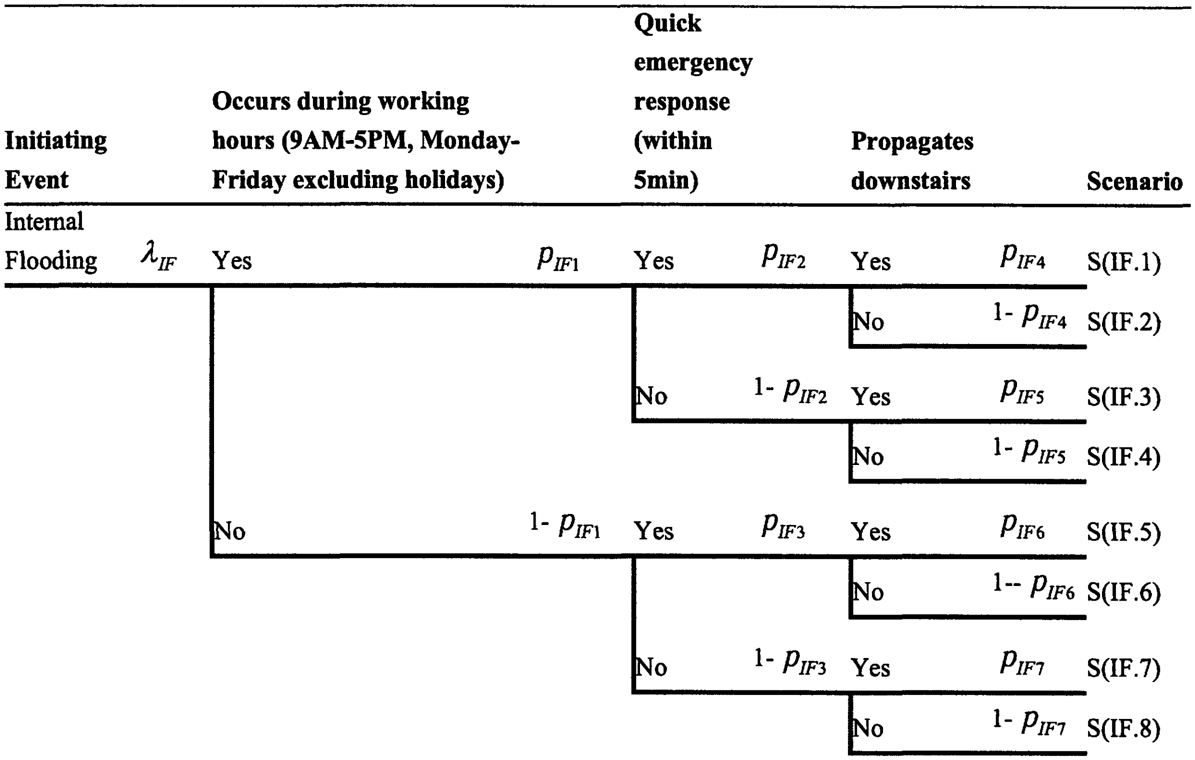

Table 12: Physical Consequences for Shared-Facilities Macro-Group Due to Internal Flooding

Scenario	Physical Consequences for Shared-Facilities Macro-Group
IF.1	Water damage facilities and propagate downstairs. Hundreds of researchers can not work due to the water damage. Most experiments can be redone after recovery.
IF.2	Small damage due to the quick response.
IF.3	Water damage facilities and propagate downstairs. The physical damage could be doubled or even more because of delayed response and propagation. Hundreds of researchers can not work due to the water damage. Most experiments can be redone after recovery.
IF.4	Water damage facilities. Tens to hundreds of researchers can not work due to the water damage. Most experiments can be redone after recovery.
IF.5	Water damage facilities and propagate downstairs. Hundreds of researchers can not work due to the water damage. Most experiments can be redone after recovery.
IF.6	Small damage due to the quick response.
IF.7	Water damages facilities and propagates downstairs. The physical damage could be doubled or even more because of delayed response and propagation. Hundreds of researchers can not work due to the water damage. Most experiments can be redone after recovery.
IF.8	Water damages facilities. Tens to hundreds of researchers can not work due to the water damage. Most experiments can be redone after recovery.

4.4.4 Data Collection and Stakeholder Input

To collect data and evaluate the scenario probabilities, more than 50 stakeholders were interviewed over the course of approximately 30 workshops. The workshops were organized and conducted by a team of analysts. The preparation for each workshop followed five steps, as discussed below (Keeney and von Winterfeldt, 1991; Forester, Bley et al., 2004):

- Stage 1: Interview preparation;
- Stage 2: Introduction of the study and gathering of general information from the stakeholders;
- Stage 3: Construction of the initial event trees and description of the physical consequences;
- Stage 4: Elicitation of probabilities to quantify the scenarios;
- Stage 5: Validation of collected input.

Stage 1: Interview preparation

The first task is to determine and select the stakeholders for interview. The stakeholders were selected to represent diverse interests including faculty, emergency coordinators, administrative staff, engineers, and others. They also represented different levels of the organization: lab-level, department-level, and Institute-level. See Appendix 3 for the list of stakeholders. In addition, before interviewing the stakeholders, a document was prepared and sent to the stakeholders to provide general information about the study and help the stakeholders fully understand the context.

Stage 2: Introduction of the study and gathering of general information from the stakeholders

Each session started with a presentation on the background, framework, and objectives of the project, as well as the benefits to the entire Institute. In this step, the information gathered from the interview was qualitative. The following questions were asked of the stakeholders:

- Question 1: What are the critical operations and activities in your department?

- Question 2: What are the critical hazards for your department, e.g., floods, fires, explosions, loss of utilities (e.g., power, water, chilled water, steam, natural gas)?
- Question 3: What are the potential consequences when the incidents occur in your department due to the above hazards?
- Question 4: How do you perceive vandalism for your department?
- Question 5: What would you do if you had the funding to mitigate the impact?

Stage 3: Construction of the initial event trees and description of the physical consequences

The stakeholders were trained on the concept of the event trees through examples. Scenarios were generated and the physical consequences of the scenarios were gathered from the stakeholders. The interdependencies among the infrastructures, assets, and utilities within the department were also determined.

Stage 4: Elicitation of probabilities to quantify the scenarios

It was found that stakeholders were reluctant to provide probability values. To assist the stakeholders who had no background in probability, some guidance was provided. They were encouraged to try to imagine how many times out of 10 (or 100, etc.) would an event happen, given the preceding events in the event tree had occurred. In addition, in order to help control anchoring bias, they were asked to provide a lower bound and an upper bound, instead of just a best estimate of the probability (Forester, Bley et al., 2004). To estimate the probabilities that lead to two disjoint consequences, such as p_{IF3} in Figure 7, the stakeholders were asked to estimate the ratio of the two outcomes out of 10 (or 100, etc.) times incidents.

Stage 5: Validation of collected input

The data that had been collected were sent to the stakeholders. The stakeholders reviewed, discussed, and refined the data until they agreed that the data provided satisfactory information.

4.5 Scenario Impact Evaluation

4.5.1 Value Tree

Given that a failure occurs, the physical consequences could be physical property loss, personal injury, environmental pollution due to release of hazardous chemicals, loss of research data, or even long-term research damage. Not all of the impacts are commensurate. The impact that these consequences have on the decision makers were evaluated by borrowing the idea of objectives hierarchy and utilities from the Multi-Attribute Utility Theory. In this study, the terms “impact categories” and “performance measures” were used in lieu of “objectives”. This hierarchy decision framework (Weil and Apostolakis, 2001), also called Value Tree because of its hierarchical structure and dimensionless scale, contains the following four steps:

1. Structuring the impact categories and performance measures;
2. Weighting objectives and performance measures;
3. Assessing disutility functions for the performance measures;
4. Performing consistency checks.

The benefit of an analysis that combines MAUT with PRA is that it provides a framework for the stakeholders to discuss the issues in detail, thus enhancing the chances that the stakeholders will reach consensus. It also provides opportunities for the stakeholders to create new decision alternatives (in the light of the PRA results) to better satisfy their preferences (Apostolakis and Pickett, 1998).

In this study, rather than starting from ground zero, the value tree is revised from the one developed by MIT stakeholders. The initial value tree was developed by the MIT Department of Facilities (DOF), to prioritize infrastructure renewal projects (Karydas and Gifun, 2006), as shown in Figure 9. Later, Apostolakis and Lemon (Apostolakis and Lemon, 2005) revised this value tree in order to use it in the context of malicious acts (see Figure 10). The DRU’s value tree, shown in Figure 8, is a revision of the Apostolakis and Lemon value tree. The stakeholders agreed with the elements in the value tree, thus only one value tree was constructed. The reason for these revisions is that these investigators were dealing with different decision-making problems and their value trees had to reflect the preferences of their decision makers and stakeholders.

4.5.1.1 Steps to Construct a Value Tree

Step 1: Structuring the impact categories and performance measures;

The objectives are defined to capture the decision makers' fundamental concerns toward the physical consequences. The consequences can be classified as three fundamental impact categories (see Figure 8):

1. Health, safety, and environment impact;
2. Economic impact on property, academic, and Institute operations;
3. Stakeholder impact.

The objectives are then followed by the identification of the *Performance Measures (PM)*, also called *Attributes*, which are used to measure the magnitude of the impact of each scenario. Generally, there are three types of attributes (Keeney and Gregory, 2005): natural attributes, constructed attributes, and proxy attributes. Natural scales directly measure the degree to which the objective is met, such as dollars for an economic impact, or lost work days for a safety impact. Proxy attributes do not directly measure quality. When the natural scales are not obvious, constructed scales are often used. Each constructed scale is divided into several levels with a description for that level. The constructed scales are developed for all the performance measures, as is shown in Table 13.

The construction of the PMs impacts the value model for the preferences among the objectives. The PMs could be Preference Independent, Utility Independent, or Additive Independent, thus leading to various value models (Keeney and Raiffa, 1993). Obviously, the Additive Value Model is so simple and understandable that is preferred in the real world, and it is used in this study. Here, the Additive Value Model means that "the preferences for the consequences depend only on the individual levels of the separate attributes and not on the manner in which the levels of the different attributes are combined (Keeney, 1994)". Keeney (Keeney, 1981) provides some guidance to help construct additive independent attributes. Even though the additive assumption can not be verified in some practical cases, it provides a good approximation.

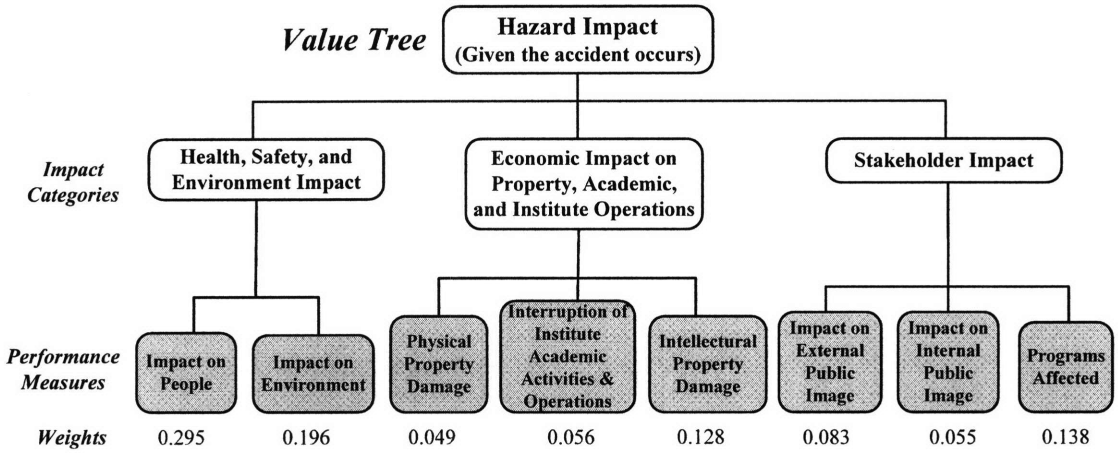

Figure 8: DRU's Value Tree

Table 13: The Constructed Scales and Disutility Values for DRU's Value Tree

(the Global Weight is the product of the PM's weight and the disutility)

1 Impact on people **Weight 0.295**

PM1: death, injury and illness (excluding psychological impact) on individuals. Major injuries are chronic injuries or acute injuries that require hospitalization; Minor injuries are acute injuries that do not require hospitalization.

Level	Description	Explanation	Disutility	Global Weight
4	Catastrophic safety impact	Hundreds of minor and major injuries and/or tens of fatalities	1	0.295
3	Extreme safety impact	Tens of major injuries and/or several fatalities	0.67	0.19765
2	Major safety impact (need hospitalization)	Tens of minor injuries and/or several major injuries	0.46	0.1357
1	Minor safety impact (no need hospitalization)	Several minor injuries	0.05	0.01475
0	No safety impact	No personal impact	0	0

2 Impact on the environment **Weight 0.196**

PM2: the degree of impact on the environment of scenarios.

Level	Description	Explanation	Disutility	Global Weight
3	Major Environmental Impact	Quantity of chemical involved in the incident reaches federal regulatory reporting thresholds	1	0.196
2	Moderate Environmental Impact	Quantity of chemical involved in the incident reaches state regulatory reporting thresholds	0.34	0.06664
1	Minor Environmental Impact	Quantity of chemical involved in the incident is below regulatory reporting thresholds	0.04	0.00784
0	No Environmental Impact		0	0

3 Physical property damage **Weight 0.049**

PM3: the cost to restore the affected physical property and contents (land, buildings, and equipment).

Level	Description	Explanation	Disutility	Global Weight
4	Catastrophic physical property and contents damage	More than $10M	1	0.049
3	Extreme physical property and contents damage	$1M to $10M	0.27	0.01323
2	Major physical property and contents damage	$10K to $1M	0.03	0.00147
1	Minor physical property and contents damage	Less than 10K	0.01	0.00049
0	No physical property and contents damage		0	0

4 Interruption of Institute academic activities and operations **Weight 0.056**

PM4: the length of time needed to restore the academic activities and institute operations (teaching, research, and other supporting activities, such as work environment or living accommodations).

Level	Description	Explanation	Disutility	Global Weight
5	Catastrophic Interruption	More than 6 months to restore	1	0.056
4	Extreme Interruption	1 to 6 months to restore	0.57	0.03192
3	Major Interruption	Less than 1 month to restore	0.19	0.01064
2	Moderate Interruption	Less than 1 week to restore	0.06	0.00336
1	Minor Interruption	Less than 1 day to restore	0.02	0.00112
0	No Interruption		0	0

5 Intellectual property damage **Weight 0.128**

PM5: the degree of damage on the affected intellectual and intangible property.

Level	Description	Explanation	Disutility	Global Weight
3	Catastrophic Intellectual Property Damage	E.g. Long-term Experiments Lost	1	0.128
2	Major Intellectual Property Damage;	E.g. Artifacts and Rare Documents Lost	0.46	0.05888
1	Minor Intellectual Property Damage;	E.g. Non-backed up Electronic Data Lost	0.05	0.0064
0	No Intellectual Property Damage		0	0

6 Impact on external public image **Weight 0.083**

PM6: the degree of the negative image held by parents of prospective students, prospective students, granting agencies, donors, and regulatory agencies.

Level	Description	Explanation	Disutility	Global Weight
3	Major Degree of Adverse Publicity	E.g. National/International Media and affects Enrollment, Contributions, Program Funding, or Faculty Recruiting	1	0.083
2	Moderate Degree of Adverse Publicity	E.g. National Media	0.57	0.04731
1	Minor Degree of Adverse Publicity	E.g. Local Media	0.06	0.00498
0	No Adverse Publicity		0	0

7 Impact on internal public image **Weight 0.055**

PM7: the degree of the negative image held by parents of existing students, students, faculty, staff, and other members of the MIT community.

Level	Description	Explanation	Disutility	Global Weight
3	Major Degree of Adverse Publicity	E.g. Petitions, Demonstrations	1	0.055
2	Moderate Degree of Adverse Publicity	E.g. Negative Articles Published	0.34	0.0187
1	Minor Degree of Adverse Publicity	E.g. Verbal Complaints	0.04	0.0022
0	No Adverse Publicity		0	0

8 Program affected **Weight 0.138**

PM8: the impact on the business, operation, employment, and objectives of the Institute programs (departments, laboratories or centers).

Level	Description	Explanation	Disutility	Global Weight
4	Catastrophic impact on Institute programs	Tens of departments and/or thousands of employees are affected	1	0.138
3	Major impact on Institute programs	Several departments and/or hundreds of employees are affected	0.5	0.069
2	Moderate impact on Institute programs	1 department is affected and/or tens of employees are affected	0.23	0.03174
1	Minor impact on Institute programs	1 department is affected and/or several employees are affected. The activity can be restored by relocation.	0.02	0.00276
0	No Impact		0	0

Step 2. Weighting objectives and performance measures

After constructing the PMs, the next step is to assign weights to the objectives and the PMs. These weights represent the preferences of the decision makers. When expressing preferences among the impact categories and PMs, the decision makers should not do so in a general sense, but rather, should be aware of the ranges of the consequences. When the range of the consequences changes, the preferences also change. Therefore, the range of the consequences should be determined before weighting.

In this study, a first set of weights were produced by asking the decision makers to perform pairwise comparisons as prescribed by the Analytic Hierarchy Process (AHP) (Saaty, 2000). The decision maker is asked to make a series of pairwise comparisons between the three impact categories using the linguistic scale shown in Table 14. Afterwards, similar pairwise comparisons are implemented in the performance measures within the same fundamental objective. The weight of the fundamental objective then split among its performance measures. The value tree is completed when each performance measure has been assigned a weight. These preliminary weights are then discussed and possibly modified by the decision makers who must ultimately accept the weights as representing their preferences.

Table 14: AHP Comparison Scale

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.

Step 3. Assessing disutility functions for the performance measures

Disutilities are measures of the undesirability of the various levels of the PMs. The concept of *disutility* is the same as *utility* but for convenience to describe losses. Through the use of disutility functions, the multiple criteria can be transformed into a dimensionless scale. Strictly speaking, the disutility functions in this study are not the utility functions elicited by simple lotteries but the value functions which show the nonlinear preferences on the certain consequences.

AHP is also applied to the performance measures to develop a first set of diutilities (Hughes, 1986). For each PM, similar pair-wise comparisons among the levels in the constructed scale are implemented. Once the disutility values have been determined for the PM, they are normalized into a 0 to 1 scale by a linear transformation. The disutility for the worst impact has the value of unity and the disutility for no impact has the value of zero (see Table 13).

Eliciting value judgments is subject to bias and random errors; hence, it is important to check the consistency of the elements in the decision analysis. One advantage of using AHP is that it provides a numerical indicator, *Consistency Ratio (CR)* to ensure consistency in pairwise comparisons. This is so-called internal consistency check, that is, to check the consistency across the disutility function of the constructed scales in the PM.

Step 4. Performing consistency checks

Once the value tree is complete, the decision maker checks the preference consistency across the PMs, that is, external consistency check. For example, to check the preference consistency between the interruption and impact on programs, one would compare the product of the weights of the PM and the disutility for the impact level in the constructed scale. Using Table 13, the product of extreme interruption and the product of moderate impact on Institute programs are:

*PI (extreme interruption) = weight (0.056) * disutility (0.57) = 0.03192*

*PI (moderate impact on Institute programs) = weight (0.183) * disutility (0.23) = 0.03174*

The same *Global Weight* (the product of weight and disutility value) means the decision maker should be indifferent with the two levels of impact. If this is not the case, the weights and/or the disutilities should be re-examined. The consistency checks are done for all the PMs until the decision maker is satisfied with all of the preferences.

4.5.1.2 Revisions to Construct the DRU's Value Tree

The initial value tree, DOF's value tree is shown in Figure 9. It is built through the process introduced in Section 4.5.1.1. Later, Lemon revised DOF's value tree for the research of malicious acts. The performance measures *Loss of Cost Savings* and *Complexity of Contingencies* were eliminated. Furthermore, *Economic Impact* was renamed as *Economic Impact on Property, Academic, and Institute Operations.* Additionally, *Coordination with Policies, Programs, and Operations*, was renamed by *Stakeholder Impact* to more accurately reflect the fundamental meaning. In addition, the weights for the performance measures were modified accordingly. Lemon's value tree is shown in Figure 10.

For the DRU's value tree, the decision makers consider that the attributes in Lemon's value tree represent their fundamental objectives of assessing the impact due to the hazards. No additional attributes need to be added into Lemon's value tree. Yet, the constructed scales may not work for the DRU project. DOF's value tree works for the building-level infrastructure renewable projects, and Lemon's value tree captures the minor terrorism threat to the buildings, while the DRU project not only includes the minor failure which is bounded in the building or even room-size level, but also includes campus-wide incidents. For this reason, the constructed scales were rebuilt after assessing the potential scope of the impact due to the hazards. More levels were added into the constructed scales for the performance measure *Impact on People*; Additional level of impact was added into the constructed scales for the performance measures *Physical Property Damage* and *Interruption of Institute Academic Activities and Operations* each to capture the lower level of impact than *Level 1* as defined in DOF's value tree and Lemon's value tree. The definitions and descriptions for the performance measures and the constructed scales were revised accordingly in the DRU project.

The next step was to create new disutilities for the constructed scales. These disutility values were obtained through the decision analysis processes presented in Section 4.5.1.1, followed by consistency check. The final DRU value tree is shown in Figure 8. The constructed scales and the disutility values are listed in Table 13.

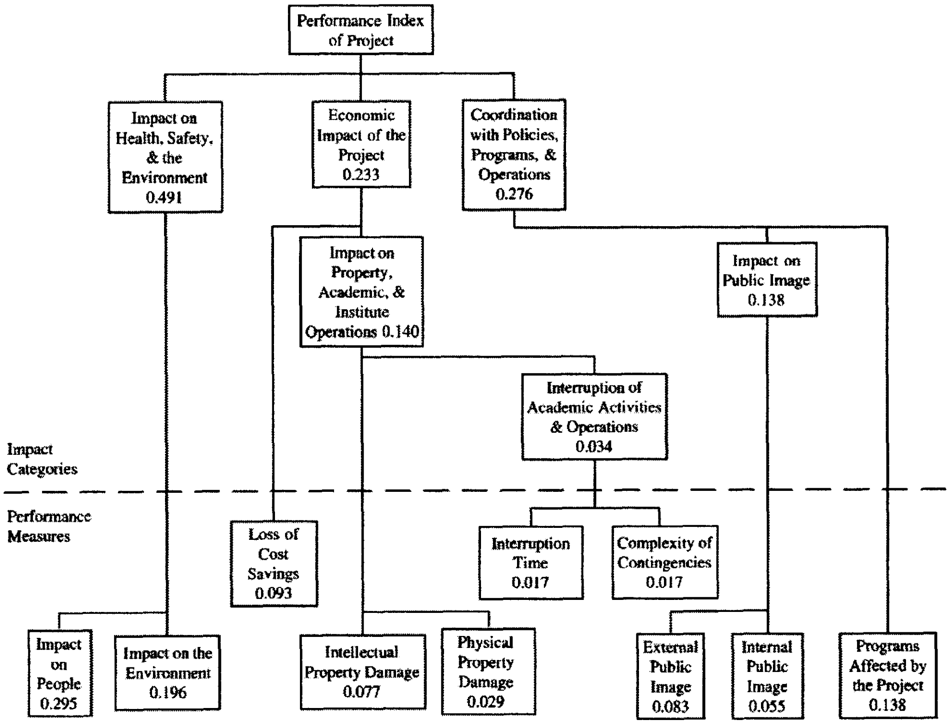

Figure 9: DOF's Value Tree

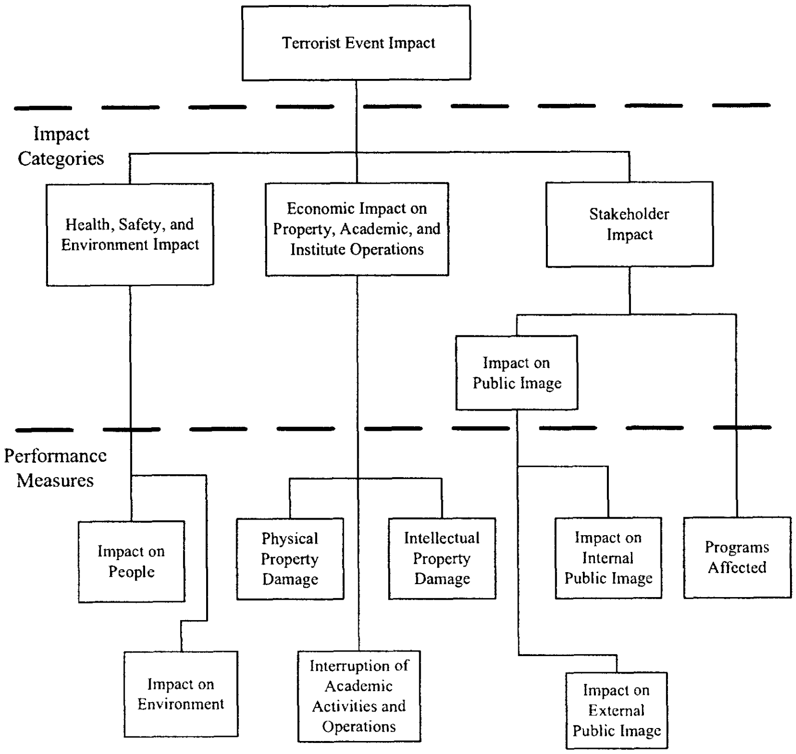

Figure 10: Lemon's Value Tree

4.5.2 Performance Index

4.5.2.1 Definition of Performance Index

Performance Index (PI) is the sum of the weights of an individual PM multiplied by the disutility value of the level of impact on that PM of this scenario. It is a measure of the physical consequences for each scenario. PI is defined as (Weil and Apostolakis, 2001):

$$PI_j = \sum_{i}^{K_{pm}} w_i d_{ij} \quad \textbf{(Equation 1)}$$

Where

PI_j is the performance index for scenario j;

w_i is the weight of the performance measure i;

d_{ij} is the disutility of the level of the performance measure i impacted by scenario j;

K_{pm} is the number of performance measures.

$PI_i > PI_m$ means the decision maker assesses that the consequences (undesirability) of scenario *i* is higher than that of scenario *m*.

When the probabilities of the scenarios are available, the *Expected Performance Index (EPI)*, can be calculated by the following equation:

$$\overline{PI}_j = \sum_{i}^{K_{pm}} w_i \overline{d}_{ij} \quad \textbf{(Equation 2)}$$

Where $\overline{d}_{ij}$ is the expected disutility of performance measure i for scenario j

Using the constructed scales shown in Table 13, the proper levels of impact are selected to describe the physical consequences of the Macro-Groups given a specific scenario. The values then substitute into Equation 1 to obtain the performance index of the scenario for the Macro-Group.

In this study, two kinds of risks are distinguished: random failures and malicious acts. For random failures, the probability of occurrence (or frequency of occurrence) can be estimated from the historical records. Therefore, the expected performance index was used to rank the risks from random failures. However, for malicious acts, the probability of attack is not available. Performance indices were used to denote the magnitude of such risks.

Equation 1 and Equation 2 imply that the additive value model is used in this study. The model is valid only if the performance measures are additive independent. Although much effort has been made to assure additive independence among the PMs, such independence is difficult to ensure. This model is viewed as an approximation whose results will be scrutinized by the decision makers. As Clemen (Clemen, 1995) stated, "in extremely complicated situations with many attributes, the additive model may be a useful rough-cut approximation."

4.5.2.2 Performance Index of Local-Damage Random Occurrences

PI of Loss of Electricity

Although the event tree *loss of electricity* has 28 scenarios, the end states could absorb the scenarios into several dominant scenarios. If one considers the Macro-Groups as users of electricity, the scenarios S(LE,3), S(LE,5), and S(LE,7) have the same end states "the users lose electricity supply for less than 8 hours during the working hours (9AM-5PM, Monday-Friday excluding holidays)". Thus, the scenarios for the initiating event loss of electricity can be absorbed into three dominant ones, as are shown in Figure 11:

1. S(LE,a): Users lose electricity supply for less than 8 hours during the working hours ;
2. S(LE,b): Users lose electricity supply for less than 8 hours in the off-working hours; and
3. S(LE,c): Users lose electricity supply for 1 day to 1 week.

The mission-related Macro-Groups with the exception of *Classrooms* rank higher than the support and services Macro-Groups such as *the Administration Offices* and *the Residential Halls. The Animal-Dominant* and *the Biological-Dominant Macro-Groups* have higher level of impact on the intellectual damage, because losing the animals for the former and losing the samples for the latter result in long-term damage of research. *The Shared-Facilities Macro-Group* has high physical property damage. Since most of the research can be re-operated after the electricity is recovered, however, the intellectual damage for *the Shared-Facilities Macro-Group* is not as high as that for *the Animal-Dominant* and *Biological-Dominant Macro-Groups.*

PI of Loss of Other Utilities

Steam provides heating for the whole campus. Losing the steam supply for *the Animal-Dominant Macro-Group* and *the Residential Halls* is significant (see Figure 13). *The Animal-Dominant Macro-Group* is very sensitive to variations in temperature, humidity, and pressure. Loss of steam may lead to animal injuries or deaths, resulting in long-term damage to the research. Another issue for this initiating event is the scenario of *loss of steam in the extreme cold days* in which the personal health and safety is compromised. Higher PI values demonstrate that this specific scenario is considerable.

The situations are quite similar for the initiating event *loss of chilled water. The Animal-Dominant Macro-Group* still have high PI, and the scenario that *losing the chilled water in the extreme hot days* is considerable, as is shown in Figure 14.

Internal Flooding

The dominant scenarios for internal flooding are (see Figure 15):

1. S(IF,a): Local flooding with quick response;
2. S(IF,b): Local flooding with delayed response; and
3. S(IF,c): Propagated flooding.

Still, the mission-related assets rank higher than the support and services assets. More importantly, when *the Chemical-Dominant Macro-Group* is flooded, potential chemical releases may result in an environmental impact, especially when the flooding propagates downstairs. The PI values in Figure 15 illustrate the situation.

PI of Fire

The PI values of the Macro-Groups for fire are shown in the Figure 16. The levels of the performance measures indicate that the PI value is dominated by life safety for all the Macro-Groups. If other impacts (physical property damage, intellectual damage, image, etc.) are factored in, the mission-related assets with the exception of *Classrooms* rank higher than the support and services assets such as *the Administration Offices* and *the Residential Halls. The Animal-Dominant Macro-Group* and *the Biological-Dominant Macro-Group* have higher level of impact on the intellectual damage. *The Shared-Facilities Macro-Group* has high physical property damage in fire. *The Classrooms* and *the Residential Halls* are only dominated by the people safety.

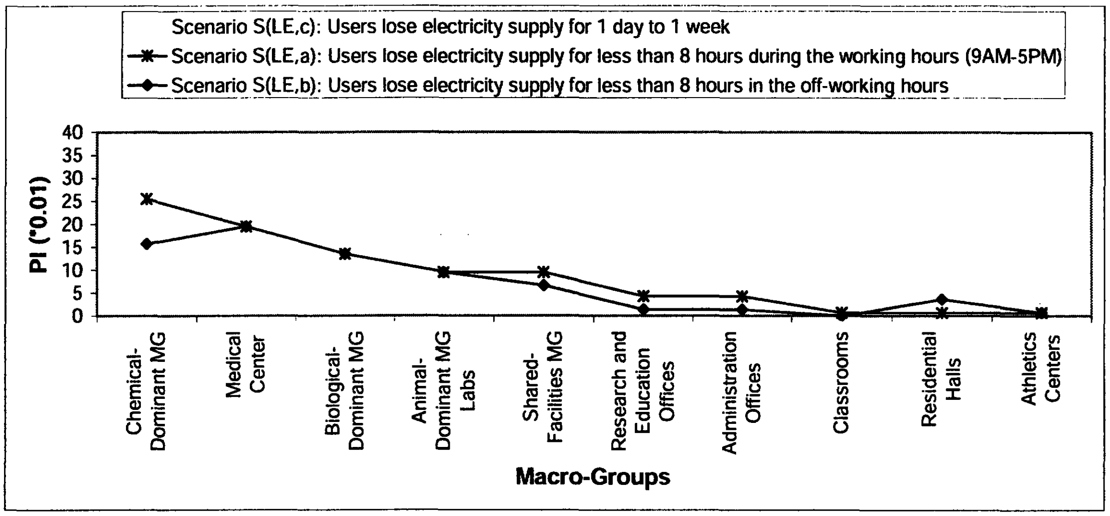

Figure 11: The PI Values of the Macro-Groups for Loss of Electricity

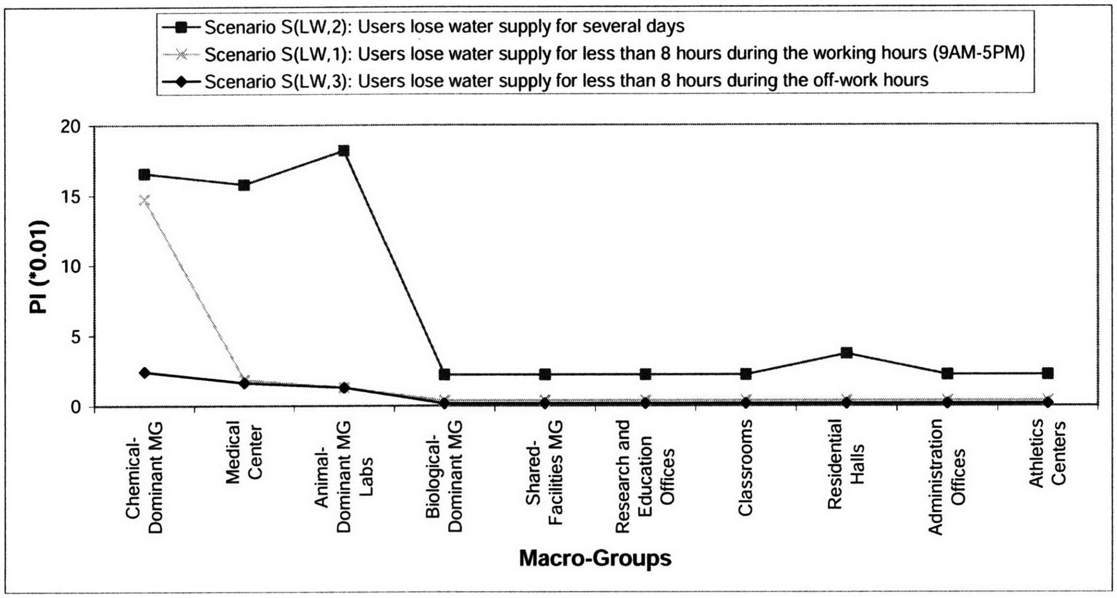

Figure 12: The PI Values of the Macro-Groups for Loss of Water

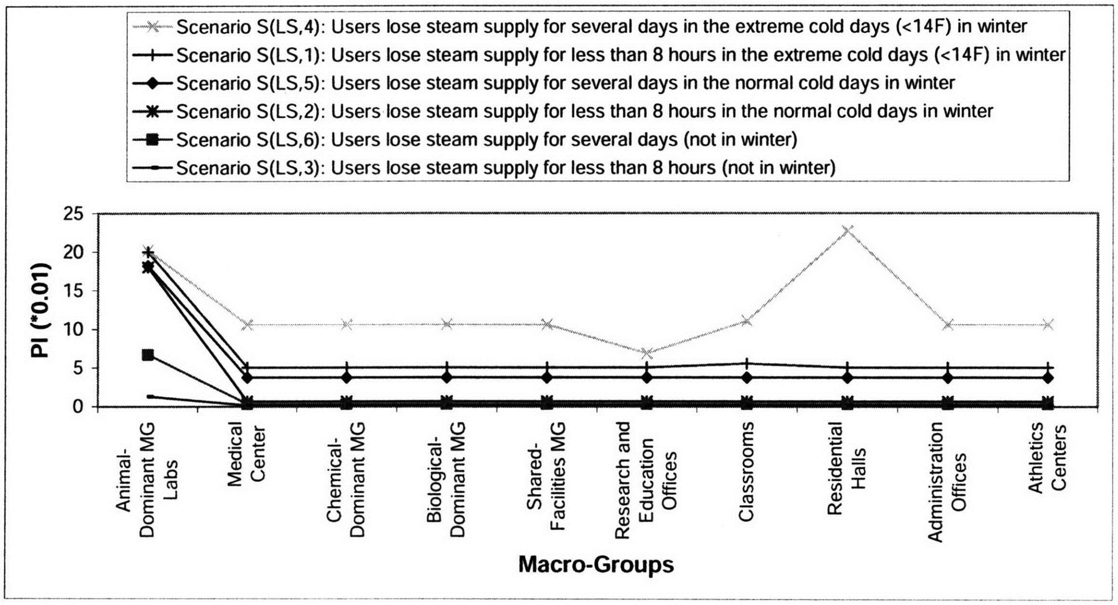

Figure 13: The PI Values of the Macro-Groups for Loss of Steam

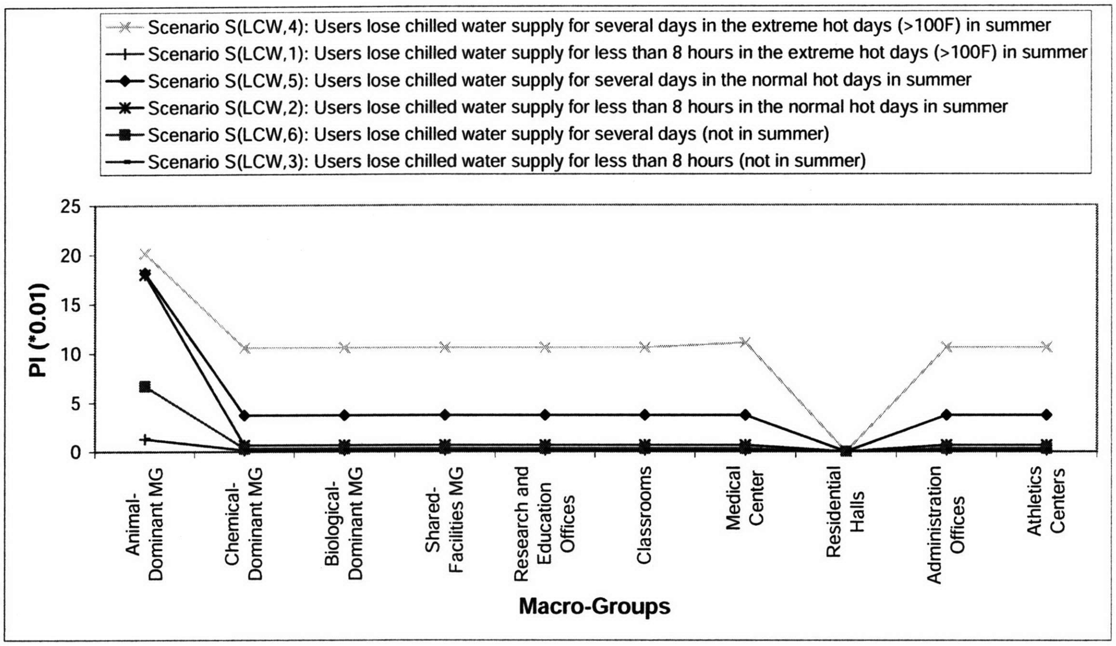

Figure 14: The PI Values of the Macro-Groups for Loss of Chilled Water

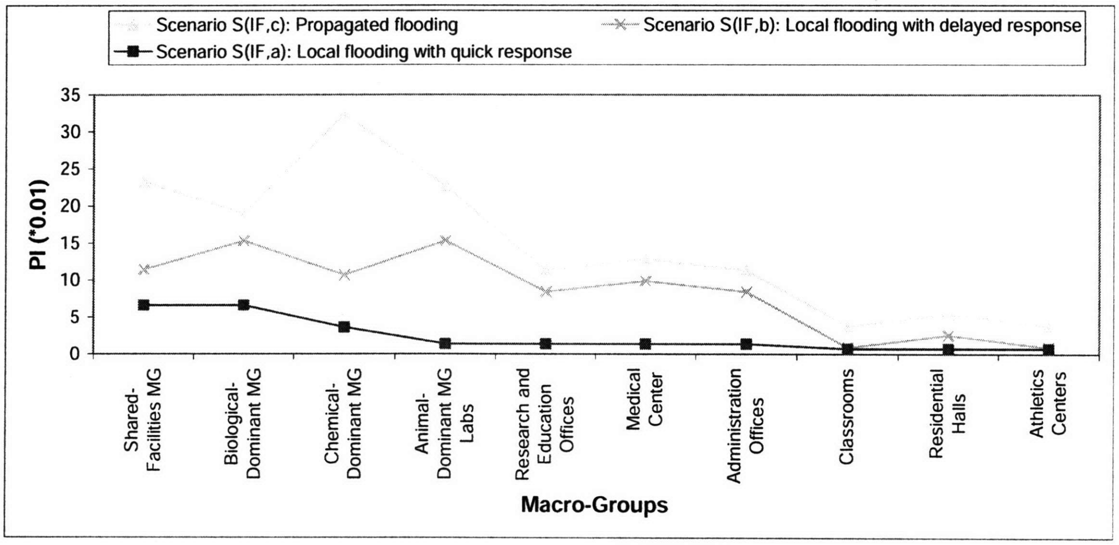

Figure 15: The PI Values of the Macro-Groups for Internal Flooding

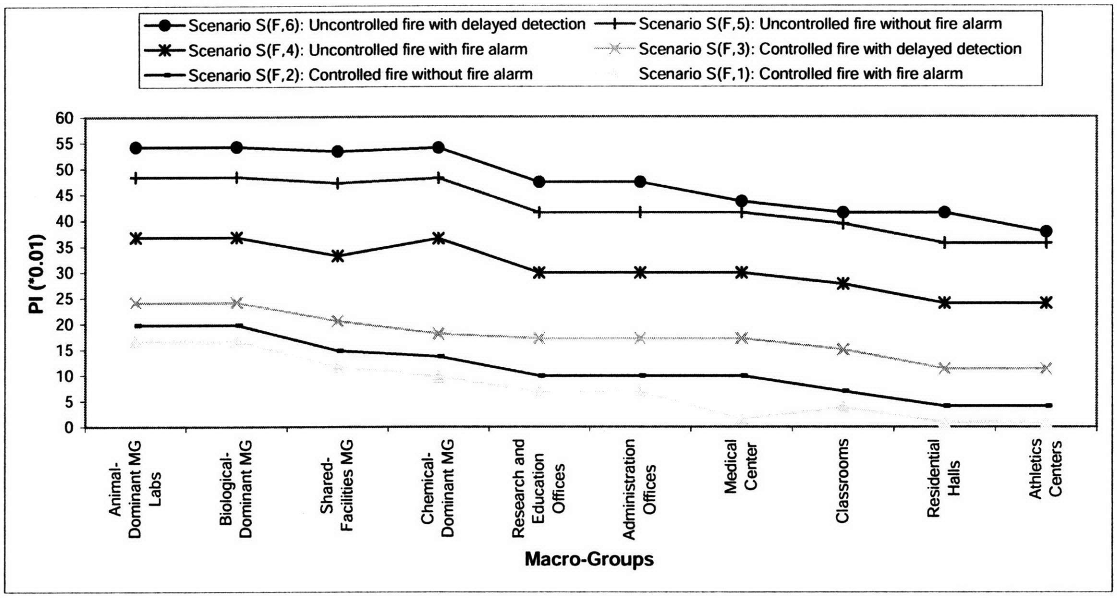

Figure 16: The PI Values of the Macro-Groups for Fire

4.5.2.3 Expected Performance Index of Local-Damage Random Occurrences

The *Frequency* of the initiating event is defined as the mean number of occurrences per year. MIT insurance data record the historical incidents in the past twelve years (1994-2005) that are deductible for insurance. These data provide much information about the frequency of the initiating events. Starting from the records, one can estimate the base case frequency of the initiating events, as is shown in Table 15.

The occurrences of the initiating events are assumed homogenously distributed across the campus. After consulting an officer of Department of Facilities to estimate the number of buildings with considerable size and contents, 120 is used approximately to denote the number of the Macro-Group assets. Therefore, the base case frequency for each Macro-Group asset is the base case frequency divided by the total number of Macro-Group assets (i.e. 120). Other two sources for the probabilities of the subsequent events in the event trees are: the literature (e.g., the reliability of the sprinkler systems) and the stakeholder input (e.g., the probability of propagation given an internal flooding incident occurs).

Table 15: Frequency of the Initiating Events

Classifications	**Initiating Event (IE)**	**Base Case Frequency** (Number of Occurrences per Year)	**Base Case Frequency per MG Asset** (Base Case Frequency/120)
IEs Leading to Local Damage	Loss of electricity	0.92	0.0076
	Loss of water	5	0.083
	Loss of chilled water	3	0.042
	Loss of steam	3	0.042
	Internal flooding	21	0.175
	Fire	1.57	0.013

The expected performance index is obtained by substituting all the quantitative data (the frequency of the initiating event and the probabilities of the subsequent events) into Equation 2. Figure 17 shows the expected performance index of the random failures that lead to local damage, counting all the scenarios of a specific initiating event. For example, there are 8 scenarios for the initiating event internal flooding. The base case frequency for a Macro-Group asset is 0.013/year, and the probabilities for the subsequent events are shown in Figure 7. The expected performance index for a MG is obtained by summarizing the expected performance index values for all the 8 scenarios, as is shown in the first bar of Figure 17.

In Figure 17, the expected performance index of internal flooding ranks the highest. Fire is second highest one in the figure. Although the frequency of power outage can be compared with that of fire, loss of electricity is not as severe as fire, partially because backup power supply equipment has been installed for some mission-related assets. The expected performance index of loss of steam and loss of chilled water rank the lowest. In addition, it is observed that generally, the mission-related Macro-Groups have higher percentage contribution than the support and services Macro-Groups for each initiating event.

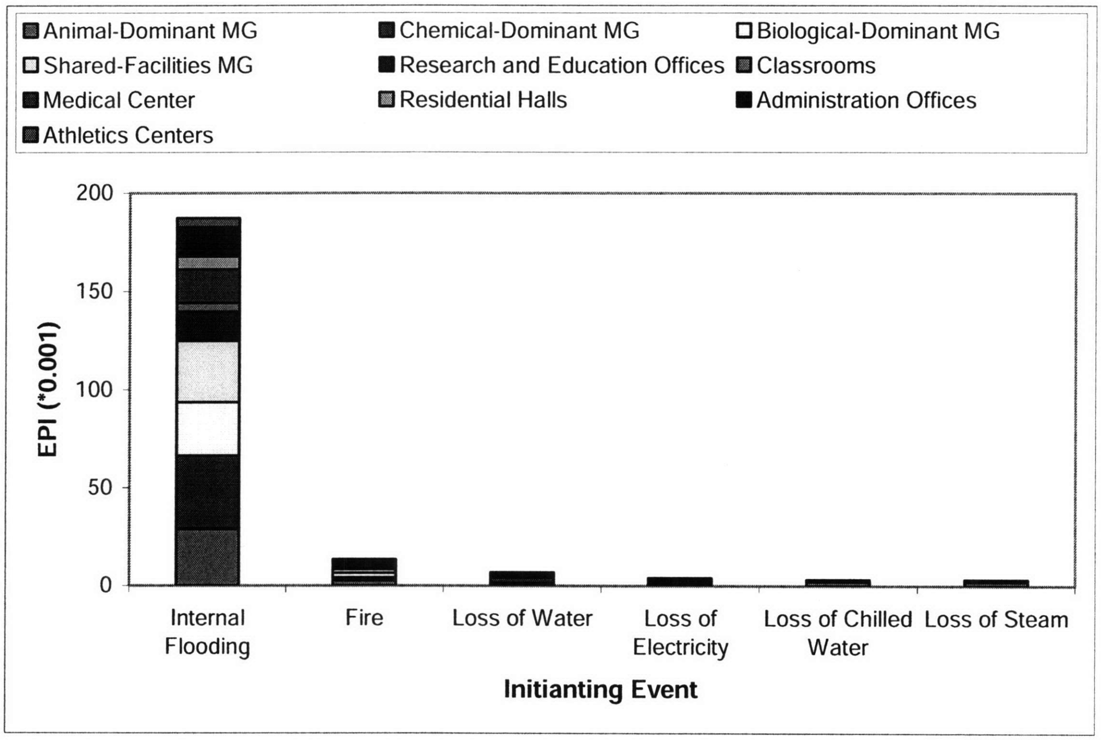

Figure 17: Expected Performance Index of Local-Damage Random Failures

4.5.2.4 Campus-Wide Random Occurrences

Four scenarios concerning campus-wide random failures are addressed:

1. S(LE_C): Campus-wide power outage for less than 8 hours during the working hours;
2. S(LW_C): Loss of water supply from City less than 8 hours during the working hours;
3. S(RS_C): Campus-wide rain storm damage; and
4. S(WS_C): Campus-wide winter storm damage.

Table 16 shows the frequency of these scenarios, demonstrating that all of the scenarios have occurred at least once in the past ten years. Figure 18 is the performance index and expected performance index for these campus-wide scenarios.

The scenarios are not complete. For example, for campus-wide power outage, other scenarios such as campus-wide power outage for several days or even longer are not addressed. Furthermore, the consequences are estimated conservatively.

Table 16: Base Case Frequency of Campus-Wide Random Failures

Scenarios	**Base Case Frequency**	**Number of Occurrence (in the past n years)**
Campus-wide power outage for less than 8 hours during working hours	0.25	3 (in 11 years)
Loss of water supply from City less than 8 hours during working hours	0.083	1 (in 12 years)
Campus-wide rain storm damage	0.33	4 (in 8 years)
Campus-wide winter storm damage	0.17	2 (in 8 years)

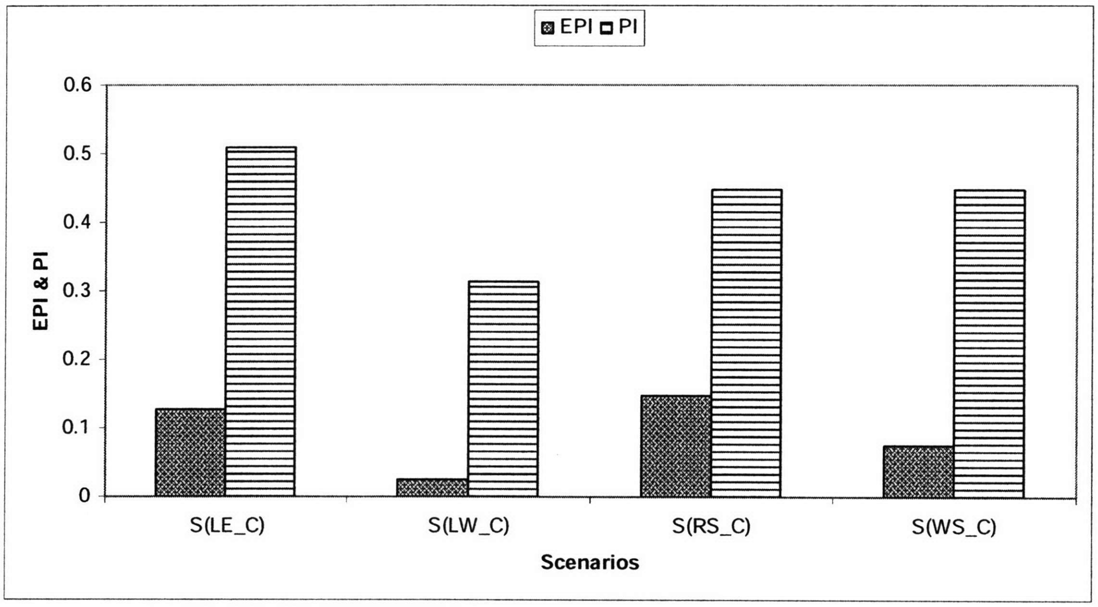

Figure 18: Performance Index and Expected Performance Index of Campus-Wide Random Failures

Where:
S(LE_C) refers to the scenario that campus-wide power outage for less than 8 hours during working hours;
S(LW_C) refers to the scenario that loss of water supply from City less than 8 hours during working hours;
S(RS_C) refers to the scenario that campus-wide rain storm damage;
S(WS_C) refers to the scenario that campus-wide winter storm damage.

4.5.2.5 Vandalism

Vandalism refers to intentional, targeted actions, that is, malicious acts. The execution of an attack depends upon the attractiveness of the target, the resources, and the plan. The probability of attack for a potential target is believed to be a function of its value and susceptibility. The higher the value, and the higher the susceptibility, the higher the probability of attack would be, as is shown below.

Probability of Attack = function (Value, Susceptibility)

where *Value* is denoted by the Performance Index, that is, the consequences given a successful attack. *Susceptibility* is defined as the matrix in Table 17. However, the probability of attack on a target "require extensive use of expert judgment and extremely difficult to obtain (Apostolakis and Lemon, 2005)". For this study, the information for vandalism is shown in Figure 19. However, the detail information is reserved.

Table 17: Susceptibility Definition

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

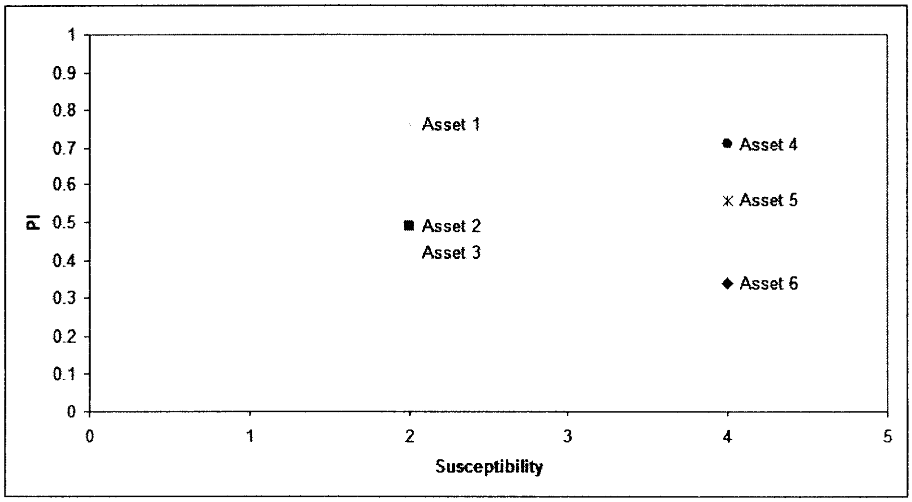

Figure 19: Performance Index and Susceptibility Levels of Key Assets

4.5.3 Sensitivity Analysis

The risk ranking may change due to the uncertainty in the parameters (or inputs) in Eq. (1) and Eq. (2). A sensitivity analysis was performed on the frequencies of occurrence and the probabilities used in the event trees. A list of parameters can be found in Table 18. The second column of the table shows the values used for the base case calculation. The third and fourth columns list the upper and lower bounds of the parameters. The distribution of the frequency of occurrence was assumed to be lognormal and the 5th and 95th percentiles of the lognormal distribution were obtained from the stakeholder inputs. The reliability of the fire sprinkler systems and fire alarm system comes from the literature (Bukowski, Budnick et al., 1999). For the parameters elicited from the stakeholders, the uncertainty was modeled by a uniform distribution or triangular distribution, and their minimum and maximum values came from the stakeholder inputs.

Monte Carlo analysis, by the *Crystal Ball* software, was performed for the parameters. Sensitivity analysis demonstrated that the top uncertain parameter is the frequency of the initiating event. The risk ranking was very sensitive to this parameter. The second uncertain parameter is the probability of the emergency responder, such as the speed of response when flooding occurs, or the speed of manual detection when the fire alarm system does not work in case of fire. The probability of failure of physical systems, such as emergency generators, backup batteries, fire sprinkler systems, and fire alarm systems, contributed little to the variation of ranking. This was because of the high reliability of these systems and the narrow range of the uncertain values.

Table 18: Parameters and Their Ranges for Uncertainty Analysis

Classifications	Initiating Event	Parameter	Base Case Value	Lower Bound	Upper Bound	Distribution
IEs Leading to Local Damage	Loss of electricity	λ_{LE}	0.92	0.2	2	Lognormal
		p_{LE1}	0.3	0.2	0.4	Uniform
		p_{LE2}	0.9	0.8	0.98	Triangular
		p_{LE3}	0.95	0.92	0.98	Triangular
		p_{LE4}	0.95	0.92	0.98	Triangular
		p_{LE5}	0.95	0.92	0.98	Triangular
	Loss of water	λ_{LW}	5	1.7	15	Lognormal
		p_{LW1}	0.3	0.2	0.4	Uniform
		p_{LW2}	0.9	0.8	0.95	Triangular
	Loss of chilled water	λ_{LCW}	3	1	9	Lognormal
		p_{LCW1}	0.9	0.8	0.95	Triangular
		p_{LCW2}	0.003	0.001	0.009	Triangular
		p_{LCW3}	0.6	0.5	0.7	Triangular
	Loss of steam	λ_{LS}	3	1	9	Lognormal
		p_{LS1}	0.9	0.8	0.98	Triangular
		p_{LS2}	0.003	0.001	0.009	Triangular
		p_{LS3}	0.6	0.5	0.7	Triangular

Classifications	**Initiating Event**	**Parameter**	**Base Case Value**	**Lower Bound**	**Upper Bound**	**Distribution**
	Internal flooding	λ_{IF}	21	10	40	Lognormal
		p_{IF1}	0.3	0.2	0.4	Uniform
		p_{IF2}	0.75	0.6	0.9	Uniform
		p_{IF3}	0.5	0.25	0.75	Uniform
		p_{IF4}	0.25	0.1	0.4	Uniform
	Fire	λ_{F}	1.57	0.7	3	Lognormal
		p_{F1}	0.95	0.922	0.971	Triangular
		p_{F2}	0.778	0.751	0.806	Triangular
		p_{F3}	0.7	0.5	0.9	Uniform
IEs Leading to Campus-Wide Damage	Loss of electricity supply from NSTAR in the working hours for less than 8 hours	λ_{CLE}	0.25	0.08	0.75	Lognormal
	Loss of water supply from City in the working hours for less than 8 hours	λ_{CLW}	0.083	0.03	0.25	Lognormal
	Campus-wide rain storm damage	λ_{CRS}	0.33	0.1	1	Lognormal
	Campus-wide winter storm damage	λ_{CWS}	0.17	0.06	0.5	Lognormal

4.5.4 Preliminary Risk Ranking

4.5.4.1 Preliminary Risk Ranking for Local-Damage Random Failures

The risks from the random failures are ranked by the mean value of expected performance index, which is obtained from the numerical analysis. There are more than 270 scenarios for the risks from random failures (10 Macro-Groups with 27 end states for each plus several campus-wide random failures). Figure 20 lists the risk ranking for local-damage random failures according to the expected performance index. Figure 21 shows the top 100 scenarios that lead to local damage and their PI and EPI (for simplicity, the names of the scenarios and the EPI and PI values are not shown). According to the magnitude, the scenarios can be classified as 3 categories (see Table 19). In the following sections, each category is analyzed separately. In addition, $S(i,j)$ and $S(i,j,k)$ are used to differentiate two kinds of scenarios, where $S(i,j)$ refers to the j^{th} scenario of the i^{th} initiating event, and $S(i,j,k)$ refers to the j^{th} scenario of the i^{th} initiating event for the Macro-Group k.

Table 19: Information of EPI Category I, II, and III

EPI Category	**EPI Magnitude**	**# of Scenarios**	**Explanation**
Category I	10^{-3}~10^{-2}	20	High risk and high PI values
Category II	10^{-4}~10^{-3}	14	Moderate risk and high PI values
Category III	10^{-7}~10^{-4}	236	Low risk values but the risks with low probability but severe damage need to be addressed
Category III-1	10^{-4}	58	
Category III-2	10^{-5}	118	
Category III-3	10^{-7}~10^{-6}	60	

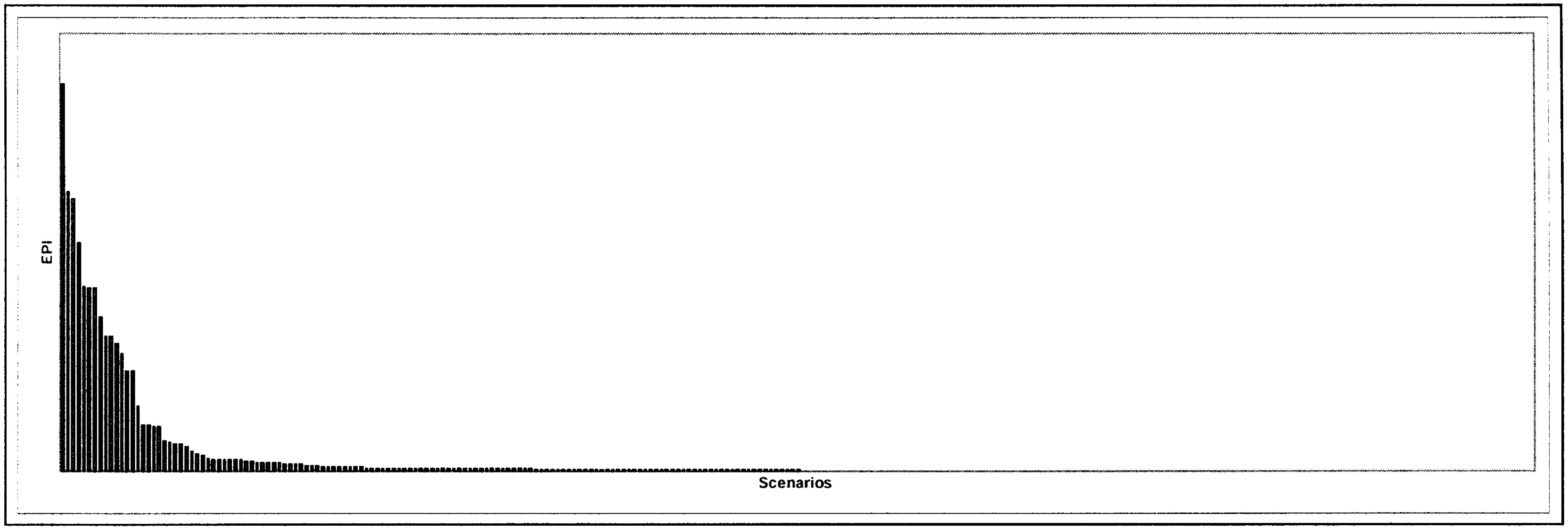

Figure 20: Risk Ranking for Local-Damage Random Failures According to the Expected Performance Index (270 Scenarios)

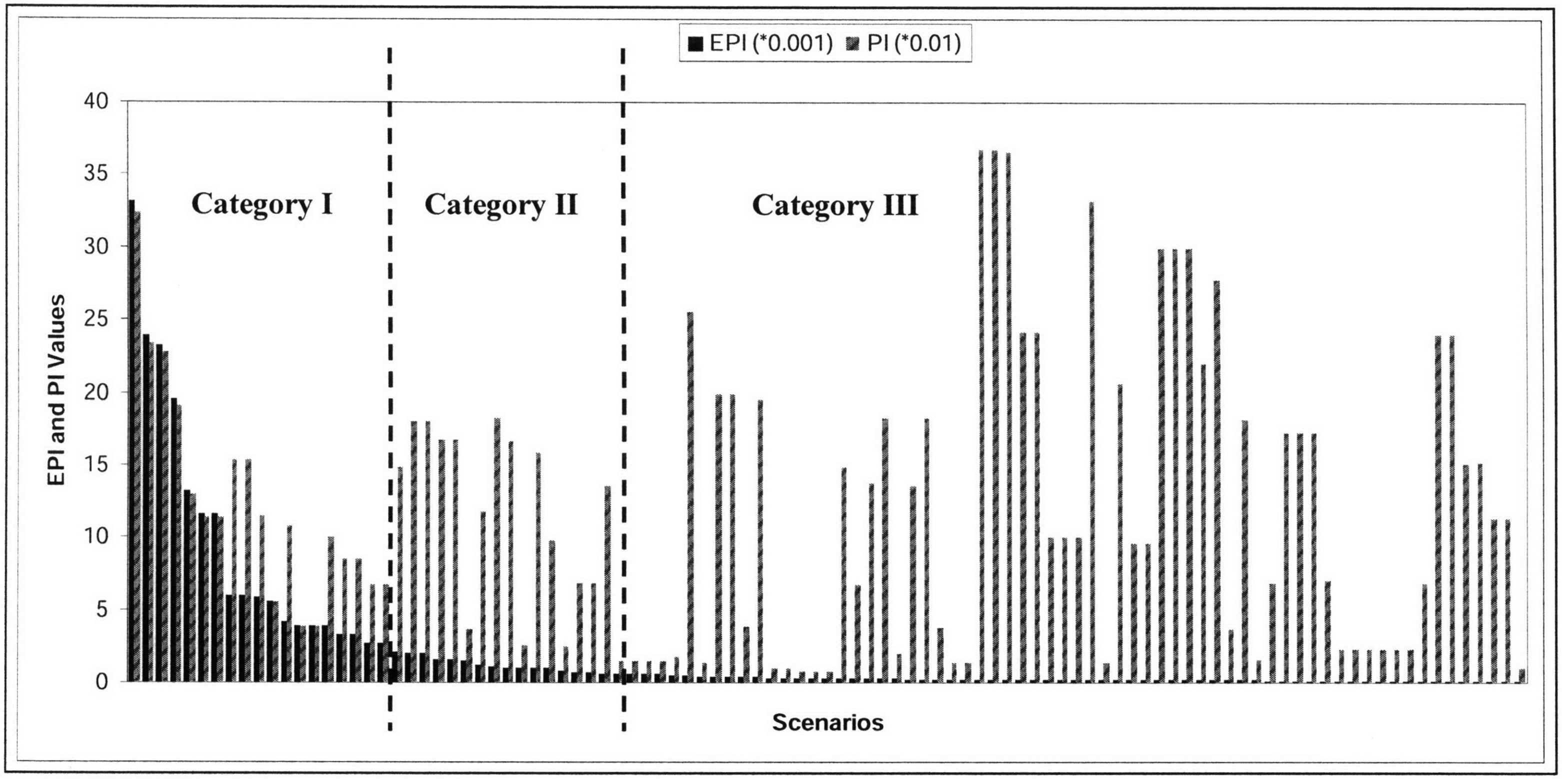

Figure 21: Risk Ranking According to EPI for the Top 100 Local-Damage Scenarios

4.5.4.2 EPI Category I for Local-Damage Random Failures

The risks in EPI Category I (see Figure 22) are the following internal flooding scenarios on the Macro-Groups:

1. S(IF,1): Quick response to the internal flooding, and water damage is localized;
2. S(IF,2): Delayed response to the internal flooding but still localized water damage; and
3. S(IF,3): Delayed response to the internal flooding and water damage propagates downstairs.

Obviously, from scenario S(IF,1) to scenario S(IF,3), the severity of the physical consequences increases. The risk of scenario S(IF,3) ranks higher than the other scenarios for all Macro-Groups.

Next, the Macro-Groups are prioritized according to their internal flooding risks. The higher the priority of the Macro-Group, the more severe the damage is for that Macro-Group, and the more it should be concerned in the risk mitigation and emergency response planning. The priority list for the Macro-Groups is:

1. Chemical-Dominant MG (MG2)
2. Shared-Facilities MG (MG4)
3. Animal-Dominant MG (MG1)
4. Biological-Dominant MG (MG3)
5. Medical Center (MG7)
6. Research and Education Offices (MG5)
7. Administration Offices (MG9)
8. Classrooms (MG6)
9. Residential Halls (MG8)
10. Athletics Centers (MG10)

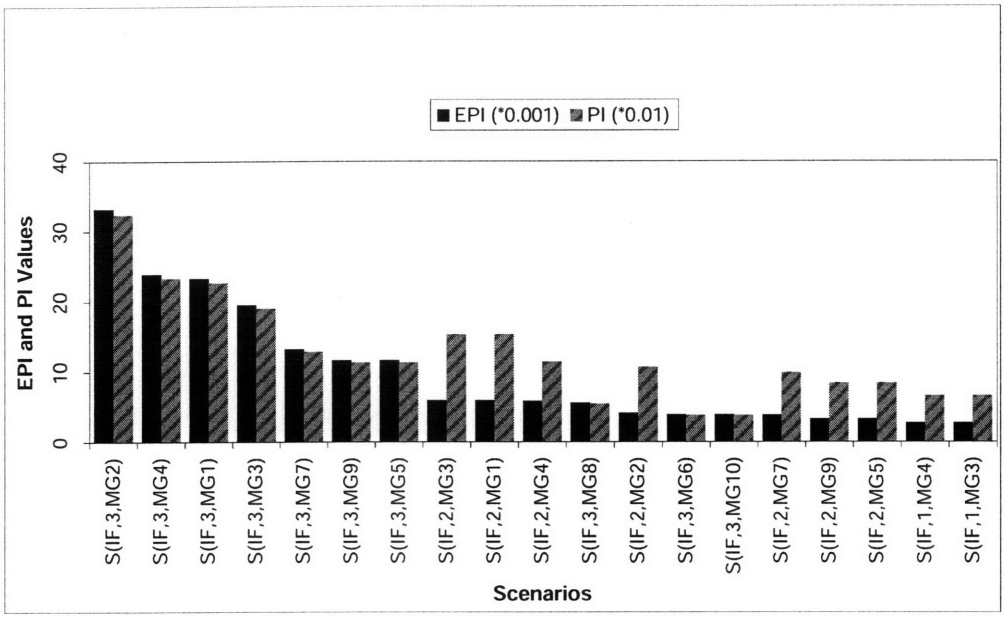

Figure 22: Category I Risk Ranking According to EPI (Local-Damage Scenarios Only)

4.5.4.3 EPI Category II for Local-Damage Random Failures

The significant scenarios in Category II (see Figure 23) are:

1. The Chemical-Dominant MG loses water supply;
2. The Animal-Dominant MG loses chilled water supply in hot days;
3. The Animal-Dominant MG loses steam supply in cold days;
4. Controlled fire with fire alarm;
5. The Animal-Dominant MG, the Chemical-Dominant Assets and Medical Center lose water supply for several days; and
6. Biological-Dominant MG loses electricity supply.

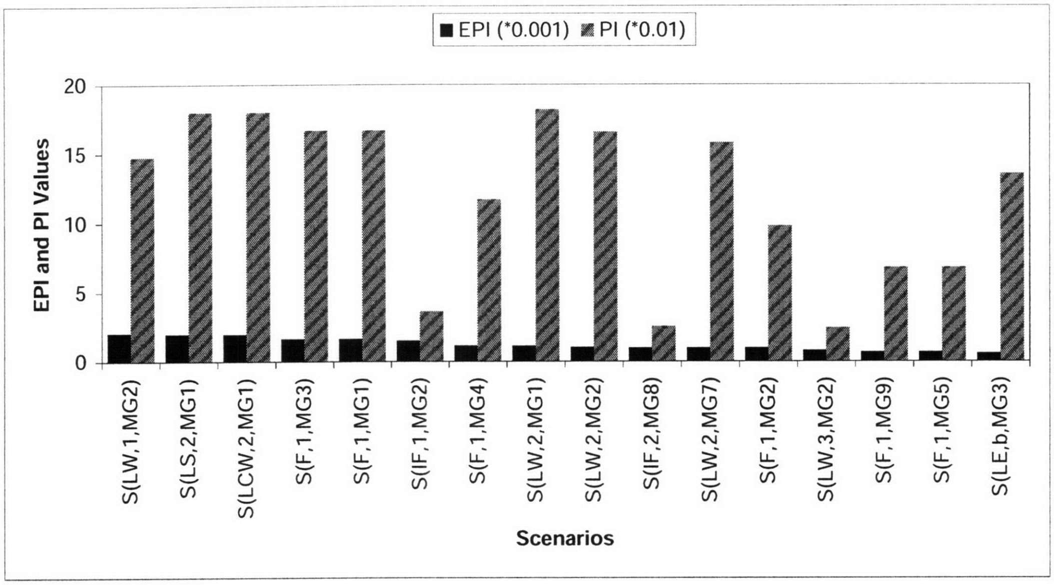

Figure 23: Category II Risk Ranking According to EPI (Local-Damage Scenarios Only)

4.5.4.4 EPI Category III for Local-Damage Random Failures

The magnitude of the scenarios in EPI Category III is quite small compared to the scenarios in EPI Category I and Category II. The purpose of analyzing EPI Category III is to determine the essential scenarios with low probability but high (or even catastrophic) impact. Category III contains approximately 200 scenarios. Category III is subdivided into 3 sub-categories, i.e., Category III-1, Category III-2, and Category III-3, according to the magnitude of the EPI values.

Since the EPI magnitude of the scenarios in Category III is very low, the scenarios are sorted according to their performance index values (see Figure 24). The rare but high impact scenarios are:

1. Uncontrolled fire with/without fire alarm;
2. Medical Center and Chemical-Dominant Macro-Groups lose electricity supply for several days;
3. Residential Halls Macro-Group loses steam for several days in extreme cold weather;

4. Animal-Dominant Macro-Group loses steam supply for several days in extreme cold weather; and
5. Animal-Dominant Macro-Group loses chilled water supply for several days in extreme hot weather.

4.5.4.5 Preliminary Risk Ranking According to EPI for All Random Failures

Figure 25 shows the preliminary risk ranking according to the EPI values. The scenarios in this figure include both campus-wide random failures and local-damage random failures. The risks in Category I are the significant ones and include all the campus-wide random failures and a few scenarios for local internal flooding. Category II contains the moderate risks. The low-probability, high-consequence scenarios lie in Category III. Since the EPI is calculated from the product of probabilities and a performance index representing the magnitude of the impact of the physical consequences, it makes sense that these scenarios have low EPI values because of their very low frequency of occurrence; however, these scenarios are still of concern due to their potential high impacts. Table 20 provides further description and explanation for this risk ranking.

4.5.4.6 Preliminary Risk Ranking According to PI

Figure 26 shows the scenarios ranked according to the performance index values. The scenarios for vandalism, which can not be shown in Figure 25 because of lack of probabilities of occurrence, are shown in Figure 26. According to the PI values, the risks are classified into four categories (Category A; Category B; Category C; Category D). The scenarios for vandalism on the key assets lie in the left side of the figure indicating their significant severe damage. These risks are followed by campus-wide random failures and fire-related scenarios. Table 21 provides the information in detail.

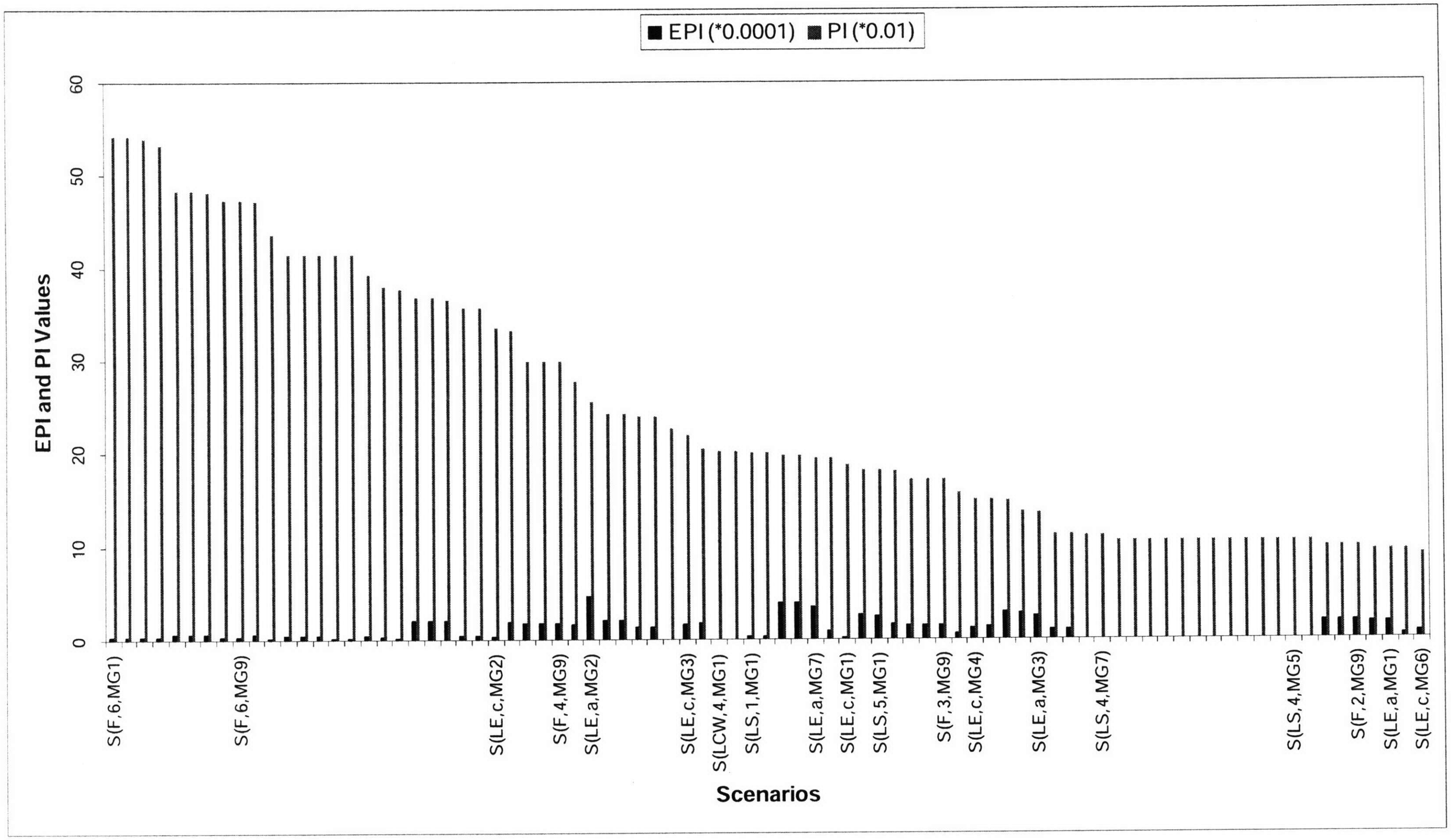

Figure 24: Category III Risk Ranking According to PI (Local-Damage Scenarios Only)

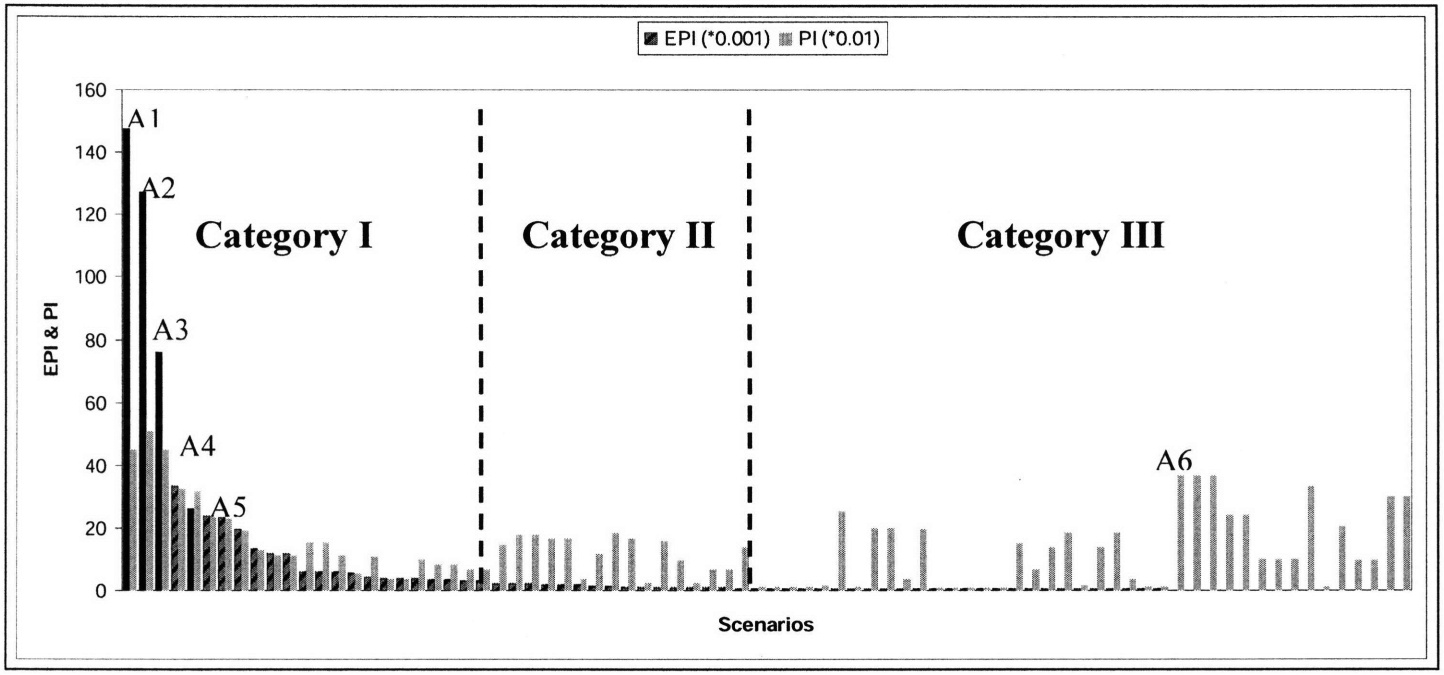

Figure 25: Preliminary Risk Ranking According to EPI for the First 80 Scenarios

The dark bars show the EPI for campus-wide random failures, the cross-hatched bars show the EPI for local-damage random failures, and the grey bars show the PI for the corresponding scenarios.

For example, A1 (the 1st dark bar) refers to the scenario S(RS_C), i.e. campus-wide rain storm damage;
A2 (the 2nd dark bar) refers to the scenario S(LE_C), i.e. campus-wide power outage for less than 8 hours during working hours;
A3 (the 3rd dark bar) refers to the scenario S(WS_C), i.e. campus-wide winter storm damage;
A4 (the 4th dark bar) refers to the scenario S(LW_C), i.e. loss of water supply from City for less than 8 hours during working hours;
A5 (the 2nd cross-hatched bar) refers to the scenario for internal flooding at a specific MG;
A6 (gray bar) refers to the scenario for uncontrolled fire (sprinkler system failure if installed or sprinkler system is not installed) with fire alarm at a specific MG.

Table 20: Description and Explanation of Risk Ranking According to EPI

Risk Category	Ranking	Explanation
Campus-Wide Failures	• Campus-wide rain storm damage; • Campus-wide power outage for less than 8 hours during working hours; and • Campus-wide winter storm damage.	Campus-wide failures rank higher than others because of their moderate frequency and high (or even catastrophic) consequences.
EPI Category I	• Internal flooding at Chemical-Dominant MG; • Internal flooding at Shared-Facilities MG; • Internal flooding at Animal-Dominant MG; • Internal flooding at Biological-Dominant MG; • Loss of water supply from City for less than 8 hours during the working hours (campus-wide failure); • Internal flooding at Medical Center; • Internal flooding at Research and Education Offices; • Internal flooding at Administration Offices; • Internal flooding at Classrooms; and • Internal flooding at Athletics Centers.	The campus-wide failure, that is, loss of water supply from City for less than 8 hours during the working hours, is in this category because of its low frequency (only once in the past 10 years). Sensitivity analysis shows that the scenarios of internal flooding still in Category I despite of uncertainty. This is because of its high frequency and high (or moderate) impact on the MGs. The frequency of internal flooding is more than 20 incidents per year, which is about 10 times of other initiating events. Furthermore, there is no physical defense system installed to prevent or mitigate the impacts. So, once internal flooding occurs, the consequences are very high for the MGs.

Risk Category	Ranking	Explanation
EPI Category II	• The Chemical-Dominant MG loses water supply for less than 8 hours; • The Animal-Dominant MG loses chilled water supply on a hot day for several hours; • The Animal-Dominant MG loses steam supply in a cold day for several hours; • Controlled fire with fire alarm; • The Animal-Dominant MG loses water supply for several days; • The Chemical-Dominant MG loses water supply for several days; • The Medical Center loses water supply for several days; and • The Biological-Dominant MG loses electricity supply.	Once losing water supply, the safety shower in Chemical-Dominant MG is compromised, leading to high impact on health and safety. Losing utilities supply in the Animal-Dominant MG would impact the animals, because the animals are very sensitive to the temperature, humidity, and pressure. Their injuries and deaths lead to long-term intellectual damage. If the Medical Center loses water supply for several days, patients have to be moved, leading to high impact on patients' health and safety. Biological-Dominant MG does not have backup power systems. When losing electricity supply, the freezers that contain the bio-samples fail to work, leading to long-term intellectual damage. Sensitivity analysis shows that the risks do not move across Category II except that the following two scenarios may move to Category III-1 due to the uncertainty: • The Medical Center lose water supply for several days • Biological-Dominant MG loses electricity supply
EPI Category III-1	• The following assets lose electricity for several hours: • Chemical-Dominant MG; • Medical Center; • Shared-Facilities Assets; and	For the MGs that have backup power systems, losing normal electricity supply has little impact as long as the emergency generators start working during the power outage.

Risk Category	Ranking	Explanation
	• Animal-Dominant MG. • Animal-Dominant MG lose chilled water for several days; • Animal-Dominant MG lose steam for several days; and • Residential Halls lose water supply for several days.	
EPI Category III-2 and III-3	• Uncontrolled fire with/without fire alarm; • Medical Center and Chemical-Dominant MG lose electricity supply for several days; • Residential Halls MG loses steam for several days in extreme cold weather; • Animal-Dominant MG loses steam supply for several days in extreme cold weather; • Animal-Dominant MG loses chilled water supply for several days in extreme hot weather.	For the scenarios in Category III-2 and III-3, the parameter uncertainty does impact their EPI Categories. Here, only the risks with low probability but catastrophic consequences will be considered.

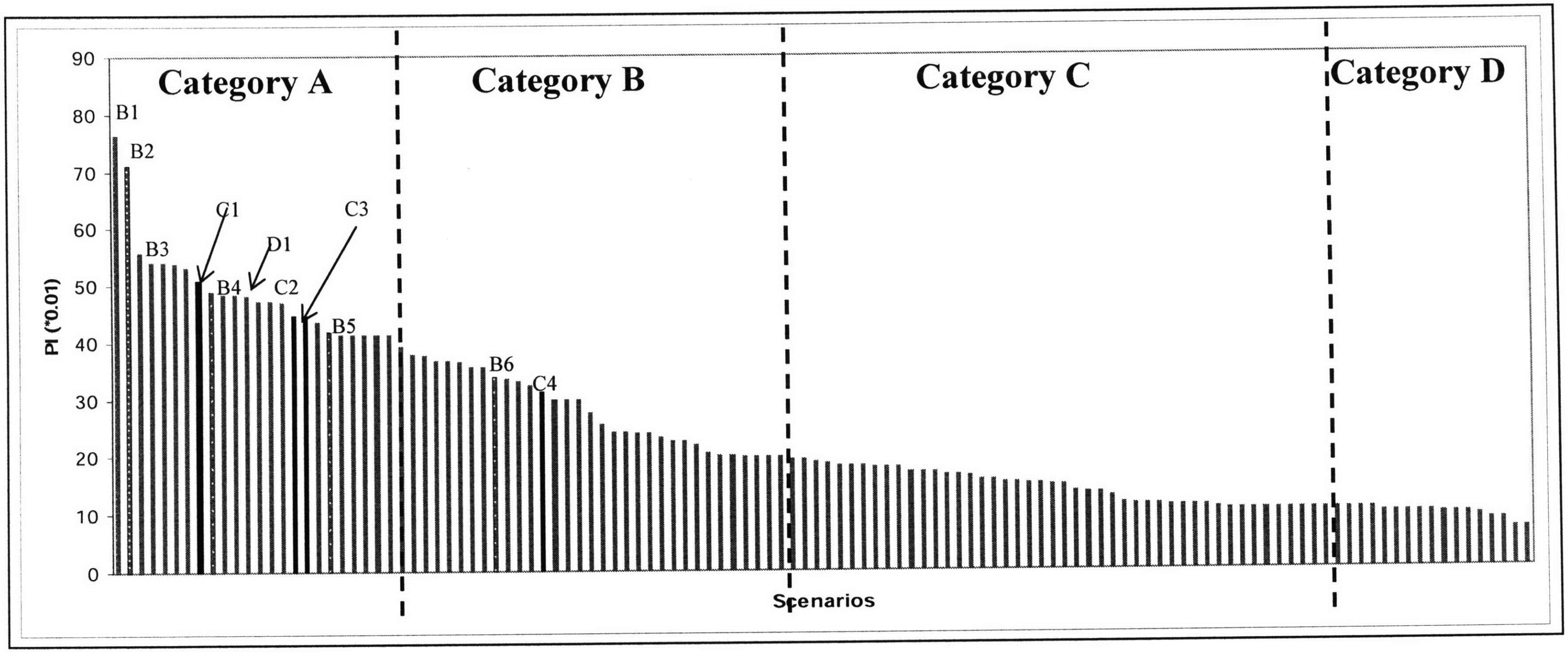

Figure 26: Risk Ranking According to PI for the First 120 Scenarios

The grey bars with black line refer to vandalism on the key assets, and the dark bars refer to the campus-wide random failures.
For example, B1 (the 1st bar, gray with black line) refers to vandalism on Asset 1; B2 refers to vandalism on Asset 4; B3 refers to vandalism on Asset 5; B4 refers to vandalism on Asset 2; B5 refers to vandalism on Asset 3; B6 refers to vandalism on Asset 6;
C1 (the 1st dark bar) refers to campus-wide power outage for less than 8 hours during working hours;
C2 refers to campus-wide rain storm damage; C3 refers to campus-wide winter storm damage;
C4 refers to loss of water supply from City for less than 8 hours during working hours;
D1 (gray bar) refers to uncontrolled fire (sprinkler system failure if installed or sprinkler system is not installed) without fire alarm at a specific MG.

Table 21: Risks Ranking for Local Damage Random Failures According to PI

Scenarios	PI Magnitude	EPI Category
Intentional attack on key assets (e.g. Asset 1, Asset 4)	0.7 ~ 1.0	N/A
Intentional attack on other key assets (e.g. Asset 5, Asset 2, Asset 3)	0.4 ~ 0.6	N/A
Campus-wide random failures: • S(LE_C): Campus-wide power outage for less than 8 hours during the working hours; • S(RS_C): Campus-wide rain storm damage • S(WS_C): Campus-wide winter storm damage	0.4 ~ 0.6	I
Uncontrolled fire without fire alarm	0.4 ~ 0.6	III-2
Medical Center loses electricity supply for several days (with EG failure)	0.3 ~ 0.4	III
The Chemical-Dominant MG loses electricity supply (with EG failure)	0.2 ~ 0.4	III
Uncontrolled fire with fire alarm	0.3 ~ 0.4	
Internal flooding in the Chemical-Dominant MG	0.3 ~ 0.4	I
Internal flooding in the Animal-Dominant MG and Shared-Facilities MG	0.2 ~ 0.3	I
Residential Halls lose steam for several days in extreme cold weather	0.2 ~ 0.3	III-3
The Biological-Dominant MG loses electricity for several days	0.2 ~ 0.3	III-1
The Animal-Dominant MG loses chilled water supply for several days in extreme hot weather	0.2 ~ 0.3	III-3
The Animal-Dominant MG loses steam supply for several days in extreme cold weather	0.2 ~ 0.3	III-3

4.5.5 Consistency Check

The consistency of the PI values was checked among the Macro-Groups. As the severity of physical consequences increases, the PI of the physical consequences also increases. Starting from the least-impact scenario for each initiating event, the PI ranking was checked for each Macro-Group. If inconsistency exists, the description of the physicals consequences and the levels of the constructed scales were examined to determine whether important elements were missing or the values were overestimated (or underestimated). For example, it makes sense that *S(LE,c)> S(LE,b)> S(LE,a)* for *the Shared-Facilities Macro-Group* in Figure 11, where:

S(LE,a): Users lose electricity supply for less than 8 hours during working hours ;
S(LE,b): Users lose electricity supply for less than 8 hours in off-working hours; and
S(LE,c): Users lose electricity supply for 1 day to 1 week.

The next step was to implement comparisons for all the scenarios of a specific initiating event. For example, for the scenario *loss of electricity for less than 8 hours during working hours*, the PI of *Classrooms* is indifferent with the PI of *Residential Halls*, and the PI values of Researcher *and Education Offices* ranks higher than the PI values of *Administration Offices and Athletics Centers*, which can be shown as:

Scenario a: loss of electricity for less than 8 hours during working hours

PI(Residential Halls) = PI(Classrooms)

PI(Researcher and Education Offices) > PI(Administration Offices) > PI(Athletics Centers)

For the scenario *loss of electricity for less than 8 hours during off-working hours*, the PI of *Residential Halls* ranks higher than the PI of *Classrooms*, while the PI ranking of the other three Macro-Groups holds, that is:

Scenario b: loss of electricity for less than 8 hours during off-working hours

PI(Residential Halls) > PI(Classrooms)

PI(Researcher and Education Offices) > PI(Administration Offices) > PI(Athletics Centers)

After comparing *Scenario a* and *Scenario b*, the result is reasonable because if assume no classes in off-working hours, loss of electricity does not have impact on *the Classrooms Macro-Group*, hence the PI of *Classrooms* becomes of zero. The same comparisons were implemented for all the PI values within the same initiating event.

4.6 Insights

Figure 25 and Figure 26 yield the following observations:

- Regardless of whether the probabilities of the scenarios are considered, campus-wide failures dominate local-damage failures. Campus-wide failures are shown in Category I within Figure 25 and in Category A within Figure 26, at the left side of each of the figures.
- If the probabilities of the scenarios are considered, the risk from the internal flooding ranks the highest (in Category I) among all the local-damage risks. If the probabilities of the scenarios are taken out, most of these risks move from Category I to Category C in Figure 26, while a few of them move to Category B.
- For local-damage failures, the risks from uncontrolled fires without fire alarm rank very low (in Category III within Figure 25) if the probabilities of the scenarios are considered. However, these risks rank the highest among all the local-damage risks in Category A within Figure 26, because of the catastrophic consequences.
- Vandalism, whose probability of attack is not available, dominates random failures (see Figure 26) in terms of the consequences. Vandalism on key assets whose failure could lead to campus-wide damage dominates the campus-wide damage scenarios from random failures.

The insights from the risk rankings are:

- When the risks have approximately the same values (EPI or PI), i.e., they are adjacent in the ranking, it is hard to judge whether one risk is higher than the other, since the slight difference in risk value may come from uncertainty in the parameters and variability in subjective judgments. Therefore, it not useful to emphasize the exact ranking order.
- This study has demonstrated that purely ranking the risks according to the expected consequences could prevent one from considering the potential impact of rare events. Thus, rare but catastrophic scenarios should not be discounted but evaluated to determine priority over other risks and in the context of what could

be done to mitigate or eliminate the risk. For example, the risk from an uncontrolled fire in a building (in Category III in Figure 25, yet in Category A in Figure 26) could be reduced by installing fire sprinklers or removing or controlling fuel sources. These mitigation measures could cost much less than the cost due to an uncontrolled fire and such a beneficial outcome might not be realized unless low expected consequence events were discussed.

- Vandalism can only be addressed in the PI ranking, since the probability of attack is not available. The consequences from vandalism on some key assets can be comparable with (or even higher than) the consequences of rare but catastrophic risks, for example, the scenario *uncontrolled fire without fire alarm.*

5 Deliberation

The National Research Council recommends an analytical-deliberative process in the decision-making process. Deliberation (National Research Council, 1996) is defined as:

> *"Any formal or informal process for communication and collective consideration of issues. Participants in deliberation discuss, ponder, exchange observations and views, reflect upon information and judgments concerning matters of mutual interest and attempt to persuade each other."*

Analysis, on the other hand,

> *"Uses rigorous, replicable methods, evaluated under the agreed protocols of an expert community—such as those of disciplines in the natural, social, or decision sciences, as well as mathematics, logic, and law—to arrive at answers to factual questions."*

The whole idea of deliberation is to force the stakeholders to think about the issues in detail by way of logic and a structured format. Thus a truly wise decision can be reached.

An iterative deliberation process was used extensively in every stage of the process. Through deliberation, the stakeholders achieved consensus on the elements in the value tree, i.e., the impact categories, the performance measure, the weights, the constructed scales, the disutility values for the levels in the constructed scales, and even the definitions for these elements in the value tree. After the risk assessment was completed, a deliberative process was used to determine the final risk ranking. In this deliberative process, the results were scrutinized and their validity was evaluated through discussion, reflection, and communication. The deliberation on the results is a very important step for the whole study, because it increases understanding, overcomes the causes for mistrust, and brings new insights to arrive at substantive decisions, thus enhancing the decision-making process.

Three types of participants were involved in this final deliberation process: stakeholders, the analyst, and a facilitator (Apostolakis and Pickett, 1998). The role of the stakeholders is to listen actively and communicate concerns; the role of the analysts is to provide and clarify technical data and results, and explain the technical questions; and the role of the facilitator is to coordinate the agenda, guide the deliberation, and promote a fair process for understanding of all issues. In this study, the stakeholders, who are sound representatives of their organizations (especially those who have been involved in the project before), were invited to the deliberation meeting. To establish equity, an experienced officer served as the facilitator.

The deliberation process commenced with introducing the project background, the goal of the deliberation, and the roles of the participants. The analyst presented the framework, the definitions, and the assumptions used in the method to enable the stakeholders fully understand the context. The stakeholders were informed that the purpose of the analysis was not to simply produce the results but, rather, to help them understand the relative value and quality of the results, and develop insights from these results to arrive at substantive decisions. The analyst not only presented what the risks were and what their ranking was, but also explained why the risks had such a ranking. For example, the risks from internal flooding rank high for the following reasons:

1. The frequency of internal flooding incidents is about 10 times that of other initiating events.
2. There is no centralized campus-wide physical prevention system for flooding, unlike fires for which sprinkler systems and alarm systems are installed.
3. The consequences of flooding could be very high.

Deliberation was an interactive process. The stakeholders raised questions regarding the analysis, methodology, and the results. They also expressed their opinions of the results. For example, a stakeholder mentioned that the potential impact of the scenario *Animal-Dominant Macro-Group loses chilled water supply on hot days* is more severe than the potential impact of the scenario *Animal-Dominant Macro-Group loses steam supply on cold days*; however, in the preliminary risk ranking, these two scenarios had the same ranking. After going back and checking the data, it was found that the reason for this ranking was because of the discrete constructed scales (for example, there are only five levels for the PM *physical property damage*), therefore, these two scenarios cannot be differentiated by their PI values.

6 Preliminary Risk Management

Risk management requires an understanding of hazards, reliable information, teamwork on the part of many segments of society, organizational entities capable of implementing actions, and rigorous supporting technical analyses (Garrick, Hall et al., 2004). Table 22 lists internal flooding, one of the credible risks identified by this study, in the context of the risk scenario, magnitude of impact, root causes, existing mitigation plans and actions, and preliminary mitigation strategies. The information is deliberated by the stakeholders. Similar entries are developed for other risk exposures.

This table is used to display all risks, support the stakeholders to summarize the existing mitigation plans and actions, and generate preliminary mitigation alternatives quickly. Potential risk mitigation strategies could include both engineering/technical and management solutions. In terms of fire, engineering solutions such as upgrading fire alarm and sprinkler systems would mitigate the physical property damages that could potentially result from a fire, while management solutions calling for periodically run fire evacuation drills would mitigate the potential for injuries.

Table 22: Risk Explanation

Risk	**Risk Explanation**	**Causes**	**Existing Mitigation Plans and Actions**	**Preliminary Mitigation Strategies**
Internal flooding	Internal flooding ranks high because of the inherent opportunity for flooding in buildings containing many pipes and the frequency and magnitude of flooding experienced on campus. Currently there is no campus-wide physical defense system to prevent internal flooding or mitigate its damage. One shared facility contains many very expensive experimental devices and serves hundreds of researchers annually. Thus potential for delays in research and high costs associated with damage to equipment and the loss of research income.	Faulty or failed plumbing, overflowing drains, condensation, faulty or accidentally damaged fire sprinkler systems.	1. Plumbers and custodians directed to scene by way of radio and paging system; 2. Water level detection system installed in select locations; 3. Call-in process for additional help if needed; 4. On-campus personnel repair systems when failure is observed and reported; 5. Fire sprinkler water flow alarm system alerts central operations center personnel of water flowing through sprinkler pipes whether or not a fire is present; 6. Sectional valves, where present, prevent impact due to accidental breakage of fire sprinkler heads or piping in active construction sites.	1. Seal penetrations, cracks, and holes through floors; prioritize according to potential for consequences, e.g. floors above shared experimental facility; 2. Install check valves where they could be effective; 3. Increase level of urgency of repair requests associated with potential pipe breaks; 4. Verify call-in procedures and policies for all personnel associated with flood and storm damage response; 5. Study need for additional water detectors; 6. Install sectional valves on fire sprinkler systems; 7. Require that renovation contractors submit and adhere to an agreed upon flood mitigation plan; 8. Insert text in design guidelines that addresses flood mitigation in the early stages of design.

7 Conclusions

Confronting the natural hazards, human-induced accidents, and malicious acts, a systematic method has been developed to assess and rank the risks in a community. This method is based on a formal, self-consistent decision-making process that integrates probabilistic risk assessment, decision analysis, expert judgment, and other disciplines.

One contribution of the study is the development of a scenario-based model. The model not only shows where the risks are and their magnitudes, but also enables to present how the initiating events evolve into the undesirable consequences. It can also help to generate mitigation alternatives to handle the risks through the event trees.

A value tree, which is based on Multi-Attribute Utility Theory, is used in this study. It splits the impacts from the hazards into three fundamental impact categories (health, safety, and environment impact; economic impact on property, academic, and Institute operations; and stakeholder impact), and constructs 8 performance measures to measure the three impact categories. This hierarchical structure enables to incorporate tangible measures (e.g., physical property losses) and intangible measures (e.g., impact on internal image) when evaluating the consequences. This structure also makes it feasible to capture the stakeholders' nonlinear preferences in the analysis.

The risks from random failures are ranked according to their Expected Performance Index, which is the product of frequency, probability, and consequence of a scenario. The risks are also prioritized according to Performance Index to include the malicious acts, since the frequency of attack is not available. Sensitivity analysis is performed to show how the risk ranking changes due to the uncertainties. In addition, a deliberative process is used to scrutinize the results.

Another contribution of the research is that it provides a framework for the development of a risk-informed decision strategy. Compared to the risk-based approach which relies heavily on technical expertise, this approach includes not only a formal, quantitative, and replicable analysis, but also a deliberative process to capture the factors that could not be addressed in the analysis. Furthermore, the methodology enables the stakeholders to provide additional input. It also provides a platform for the stakeholders to discuss and communicate during the decision process.

By implementing this framework in a test-bed (the MIT campus), it has been demonstrated that this framework is reasonable, practical, transparent, and can be used by other similar communities. For example, the delineation of Macro-Groups allows for the often decentralized elements of a university's infrastructure and key assets to be aggregated into clusters that are readily recognizable from one university to another. Furthermore, these Macro-Groups are defined with sufficient granularity that the concept can be transferred to perform multi-hazard vulnerability assessments at other decentralized entities such as research and teaching hospitals, government research laboratories, and similarly sized municipalities.

The limitations of the study are the following:

- This study focuses on high-level risk assessment. Only significant scenarios are captured in the scenario development. As a starting point of continuous risk management, it has provided satisfactory results in this phase. It is anticipated that once the decision has been made to manage some risks, more detailed scenarios should be developed for the selected risks.
- In terms of utilities (infrastructures), only the risks for the utility end-users and the utility sources (generators) were analyzed. For the infrastructure network, like our test-bed, the analysis has provided an overview of the risks across the utility network. However, for a larger and more complex infrastructure network, rigorous network analyses should be implemented to analyze the critical locations (nodes) in the network. It is anticipated the ideas generated from this study will help to assess the risks due to multiple hazards for these critical locations.
- The existence of incompleteness and uncertainties may weaken the results of the model. In this study, the potential uncertainties are: the possibly incomplete

scenarios, the probabilities of the scenarios, the elements in the value tree (for example, constructed scales are used instead of continuous disutility functions), and the conservative estimation of the physical consequences. It is also assumed that the occurrence of failures is homogeneously distributed across the campus, and that the locations with similar operations and activities have the same consequences in terms of the same scenario. These assumptions may also lead to uncertainties. The sensitivity analysis has demonstrated that the frequency of occurrence is the top uncertainty parameter. It is anticipated the uncertainties will decrease through further analysis in future work.

8 Future Research

The ultimate goal of risk assessment and ranking is risk management. The preliminary strategy to mitigate the risks is to reduce the probabilities of the scenarios, reduce the consequences of the risks, or use a combination of these two ways. The risk ranking and explanation in this study has provided support for the stakeholders to generate preliminary alternatives to manage the risks, as is shown in Chapter 6. Detail risk management is called for future study.

A major future challenge is the management of risks from malicious acts. The lack of probability of attack makes it difficult to compare these risks with risks from random events for which probabilities can be estimated. Although Garrick (Garrick, Hall et al., 2004) has brought out ideas to use expert judgment to estimate this probability, it is still a technical challenge.

Another challenge is how to handle the rare but catastrophic risks. It may be inappropriate to ignore them because of their low probabilities. This study has demonstrated that purely ranking the risks according to the expected consequences (the expected disutility value) may not work for the low probability high consequence risks. To handle this challenge, the precautionary principle and defense-in-depth principle may be pursued in future research.

In risk management, how to make the stakeholders achieve consensus may be a potential challenge as well. Although disagreement does not appear in this test-bed (the MIT campus) study, it is a necessary consideration. The limitation of MAUT is that it works only for a single decision maker. In most cases, there is no satisfactory way to combine the utility functions for group. Many researchers have done much work to overcome this limitation. Karydas and Gifun (Karydas and Gifun, 2006) developed a method based on MAUT in which the stakeholders made consensus on all the quantities of the decision model through deliberative process. Mangin and de Neufville (Mangin, de Neufville et al., 1995) found that it is possible to build a group utility function when the group people share the same vision (e.g., in the same organization or company). In that case, their single dimensional utility functions can be considered to be positive linear transformations of each other, that is, statistically equivalent within a sufficient degree of confidence (e.g., 95%). Koonce and Apostolakis (Koonce, Apostolakis et al., 2006) developed various MAUT value trees for various decision makers, and found the alternative ranking changes little. The point is that decision analysis provides a framework for the stakeholders to discuss and communicate, thus it enhances the chances that the stakeholders will reach consensus, or help them think hard and create new alternatives to better satisfy the stakeholders' preferences (Apostolakis and Pickett, 1998).

In any case, the scenario-based risk assessment approach and decision analysis are strong tools for enabling us to do the future work. The scenario-based approach tells us where and how much the risks are, and therefore helps us to generate mitigation alternatives to handle the risks. It can also tell us the risk reduction if a decision alternative is acted. The decision analysis allows capturing the stakeholders' preferences into the analysis, and provides a measure to evaluate the alternatives.

Finally, risk assessment, risk ranking and risk management is a continuous process. There should be continuous work for this task. It is anticipated that this study will help the decision makers develop insights on understanding the risks, and help them engender risk awareness.

References

Accorsi, R., Zio, E. and Apostolakis, G. E. (1999) Developing Utility Functions for Environmental Decision Making. *Progress in Nuclear Energy,* 34, pp 387-411.

Andrews, C. J., Hassenzahl, D. and Johnson, B. (2003) Legitimizing Uncertain Risk Information. *http://radburn.rutgers.edu/andrews/projects/njcrp/ACSP03.pdf.*

Apostolakis, G. (1990) The Concept of Probability in Safety Assessments of Technological Systems. *Science,* 250, pp 1359-1364.

Apostolakis, G. E. (2004) How Useful is Quantitative Risk Assessment. *Risk Analysis,* 24, pp 515-520.

Apostolakis, G. E. and Lemon, D. M. (2005) A Screening Methodology for the Identification and Ranking of Infrastructure Vulnerabilities Due to Terrorism. *Risk Analysis,* 25, pp 361-376.

Apostolakis, G. E. and Pickett, S. E. (1998) Deliberation: Integrating Analytical Results into Environmental Decisions Involving Multiple Stakeholders. *Risk Analysis,* 18, pp 621-634.

Ayscue, J. K. (1996) Hurricane Damage to Residential Structures: Risk and Mitigation. *Natural Hazards Research Working Paper #94, http://www.colorado.edu/hazards/publications/wp/wp94/wp94.html.*

Ayyub, B. M., McGill, W. L. and Kaminskiy, M. (2007) Critical Asset and Portfolio Risk Analysis: An All-Hazards Framework. *Risk Analysis,* 27, pp 789-801.

Borcherding, K., Eppel, T. and von Winterfeldt, D. (1991) Comparison of Weighting Judgments in Multiattribute Utility Measurement. *Management Science,* 37, pp 1603-1619.

Bühne, S., Halmans, G. and Pohl, K. (2003) Modeling Dependencies between Variations Points in Use Case Diagrams. *Proceeding of 9th Intl. Workshop on Requirements Engineering - Foundations for Software Quality (REFSQ'03),* Klagenfurt/Velden, Austria.

Bukowski, R. W., Budnick, E. K. and Schemel, C. F. (1999) Estimates of the Operational Reliability of Fire Protection Systems. *International Conference on Fire Research and Engineering (ICFRE3), Third (3rd). Proceedings. Society of Fire Protection Engineers (SFPE), National Institute of Standards and Technology (NIST) and International Association of Fire Safety Science (IAFSS),* October 4-8, 1999, Chicago, IL, Society of Fire Protection Engineers, Boston, MA, pp 87-98.

Clemen, R. (1995) *Making Hard Decisions: An Introduction to Decision Analysis,* Belmont, California: Duxbury Press.

Comerio, M. C., Bertero, V. and Quigley, J. M. (2000) The Economic Benefits of a Disaster Resistant University: Earthquake Loss Estimation for UC Berkeley. *Working Paper 2000-02,* Berkeley, CA: Institute of Urban & Regional Development, University of California.

Comerio, M. C., Stallmeyer, J. C., Kim, Y. I., Hung, K., Lau, S., Dooley, R., Smith, R. and Kim, J. I. (2003) Seismic Protection of Laboratory Contents: The UC Berkeley Science Building Case Study. *Working Paper 2003-02,* Berkeley, CA: Institute of Urban & Regional Development, University of California.

Department of Defense (1999) DOD Directive 2000. *http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB55/2000.12.pdf.*

Dudenhoeffer, D. D., Permann, M. R. and Boring, R. L. (2006a) Decision Consequence in Complex Environments: Visualizing Decision Impact. *In Proceeding of Sharing Solutions for Emergencies and Hazardous Environments,* American Nuclear Society Joint Topical Meeting: 9th Emergency Preparedness and Response/11th Robotics and Remote Systems for Hazardous Environments, pp 211-218.

Dudenhoeffer, D. D., Permann, M. R. and Manic, M. (2006b) CIMS: A Framework for Infrastructure Interdependency Modeling and Analysis. *Proceedings of the 2006 Winter Simulation Conference,* December 3-6, Portola Plaza Hotel, Monterey, CA USA.

Ellis, J., Fisher, D., Longstaff, T., Pesante, L. and Pethia, R. (1997) Report to the President's Commission on Critical Infrastructure Protection. *http://www.cert.org/archive/pdf/2-97sr003.pdf.*

Fischer, G. W. (1995) Range Sensitivity of Attribute Weights in Multiattribute Value Models. *Organizational Behavior and Human Decision Processes,* 62, pp 252-266.

Florig, H. K., Morgan, M. G., Morgan, K. M., Jenni, K. E., Fischhoff, B., Fischbeck, P. S. and DeKay, M. L. (2001) A Deliberative Method for Ranking Risks (I): Overview and Test Bed Development. *Risk Analysis,* 21, pp 913-921.

Forester, J., Bley, D., Cooper, S., Lois, E., Siu, N., Kolaczkowski, A. and Wreathall, J. (2004) Expert Elicitation Approach for Performing ATHEANA Quantification. *Reliability Engineering and System Safety,* 83, pp 207-220.

Garrick, J., Hall, J. E., Kilger, M., McDonald, J. C., O'Toole, T., Probst, P. S., Parker, E. R., Rosenthal, R., Trivelpiece, A. W., Arsdale, L. A. V. and Zebroski, E. L. (2004) Confronting the Risks of Terrorism: Making the Right Decisions. *Reliability Engineering & System Safety,* 86, pp 129-176

Garrison, L. and Grand, M. (2001) Cyberterrorism: An Evolving Concept. *NIPC Highlights, http://www.nipc.gov/publications/highlights/2001/highlight-01-06.htm.*

Hughes, W. R. (1986) Deriving Utilities Using the Analytic Hierarchy Process. *Socio-Economic Planning Sciences,* 20, pp 393-395.

Kaplan, S. and Garrick, B. J. (1981) On the Quantitative Definition of Risk. *Risk Analysis,* 1, pp 11-27.

Karydas, D. M. (2002) A Comprehensive Approach for Property Conservation and Loss Prevention in Power Generation Stations. *Personal correspondence.*

Karydas, D. M. and Gifun, J. F. (2006) A Method for the Efficient Prioritization of Infrastructure Renewal Projects. *Reliability Engineering and System Safety,* 91, pp 84-99.

Keeney, R. L. (1981) Analysis of Preference Dependencies Among Objectives. *Operations Research,* 29, pp 1105-1120.

Keeney, R. L. (1982) Decision Analysis: An Overview. *Operations Research,* 30, pp 803-838.

Keeney, R. L. (1994) Using Values in Operations Research. *Operations Research,* 42, pp 793-813.

Keeney, R. L. and Gregory, R. S. (2005) Selecting Attributes to Measure the Achievement of Objectives. *Operations Research,* 53, pp 1-11.

Keeney, R. L. and Raiffa, H. (1993) *Decisions with Multiple Objectives: Preferences and Value Tradeoffs,* Cambridge, United Kingdom: Cambridge University Press.

Keeney, R. L. and von Winterfeldt, D. (1991) Eliciting Probabilities from Experts in Complex Technical Problems. *IEEE Transactions on Engineering Management,* 38, pp 191-201.

Kleindorfer, P. R., Kunreuther, H. C. and Schoemaker, P. J. H. (1993) *Decision Sciences: An Integrative Perspective,* New York: Cambridge University Press.

Koonce, A. M., Apostolakis, G. E. and Cook, B. K. (2006) Bulk Power Grid Risk Analysis: Ranking Infrastructure Elements According to their Risk Significance. http://esd.mit.edu/WPS/esd-wp-2006-19.pdf

Mangin, C. G. E., de Neufville, R., III, F. F. and Clark, J. (1995) Defining Markets for New Materials. *Resources Policy,* 21, pp 169-178.

McCord, M. and de Neufville, R. (1983) Fundamental Deficiency of Expected Utility Decision Analysis. *Multiobjective Decision-Making, S. French, R. Hartley, L.C. Thomas and D. J. White, eds.,* London and New York: Academic Press, pp 279-305.

McCord, M. and de Neufville, R. (1986) "Lottery Equivalents": Reduction of the Certainty Effect Problem in Utility Assessment. *Management Science,* 32, pp 56-60.

National Research Council (1994) *Building Consensus Through Risk Assessment and Management of the Department of Energy's Environmental Remediation Program,* Washington, D.C.: National Academy Press.

National Research Council (1996) *Understanding Risk: Informing Decisions in a Democratic Society,* Washington, DC: National Academy Press.

Office of the Vice Provost and Disaster-Resistant University Steering Committee (2000) Strategic Plan for Loss Reduction and Risk Management: University of California, Berkeley. *Working Paper 2000-03,* Berkeley, CA: Institute of Urban & Regional Development, University of California.

Patterson, S. A. and Apostolakis, G. E. (2007) Identification of Critical Locations across Multiple Infrastructures for Terrorist Actions. *Reliability Engineering and System Safety,* 92, pp 1183-1203.

Pillay, A. and Wang, J. (2003) Modified Failure Mode and Effects Analysis Using Approximate Reasoning. *Reliability Engineering and System Safety,* 79, pp 69-85.

Rausand, M. and Hoyland, A. (2004) *System Reliability Theory: Models, Statistical Methods, and Applications,* Hoboken, New Jersey: John Wiley & Sons Press.

Rinaldi, S. M., Peerenboom, J. P. and Kelly, T. K. (2001) Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies. *IEEE Control Systems Magazine,* 21, pp 11-25.

Saaty, T. L. (2000) *Fundamentals of Decision Making and Priority Theory with the Analytic Hierarchy Process,* Pittsburgh PA: University of Pittsburgh.

The White House (November 2002) The Homeland Security Act of 2002. *http://www.whitehouse.gov/deptofhomeland/bill/.*

Triantaphyllou, E. and Sanchez, A. (1997) A Sensitivity Analysis Approach for Some Deterministic Multi-Criteria Decision-Making Methods. *Decision Sciences,* 28, pp 151-194.

U.S. Office of Homeland Security (July 2002) National Strategy for Homeland Security. *http://www.whitehouse.gov/homeland/book/.*

UNCW (2003) *The University of North Carolina at Wilmington Hazard Assessment,* University of North Carolina, NC.

von Nitzsch, R. and Weber, M. (1993) The Effect of Attribute Ranges on Weights in Multiattribute Utility Measurements. *Management Science,* 39, pp 937-943.

Weil, R. and Apostolakis, G. (2001) A Methodology for the Prioritization of Operating Experience in Nuclear Power Plants. *Reliability Engineering and System Safety,* 74, pp 23-42.

Appendix 1: Definitions

Risk

Quantitative or probabilistic risk assessment (QRA or PRA) is an analytical process designed to answer three basic questions about risks from a system point of view (Kaplan and Garrick, 1981; Garrick, Hall et al., 2004):

> *What can go wrong?*
> *How likely is it to happen?*
> *What are the consequences if it does happen?*

These questions, known in the risk sciences as the "triplet definition of risk", provide a general framework for all types of risk assessment.

Infrastructures and Assets

In the Homeland Security Act of 2002 (The White House, November 2002) establishing the Department of Homeland Security (DHS), the "critical infrastructure" is defined as:

> *"Systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."*

The President's *National Strategy for Homeland Security* (NSHS) (U.S. Office of Homeland Security, July 2002)defines "key assets" as:

> "*Individual targets whose destruction would not endanger vital systems, but could create local disaster or profoundly damage our Nation's morale or confidence. Key assets include symbols or historical attractions, such as prominent national, state, or local monuments and icons. In some cases, these include quasi-public symbols that are identified strongly with the United States as a Nation...... Key assets also include individual or localized facilities that deserve special protection because of their destructive potential or their value to the local community."*

Hazard

"A source of potential harm or damage, or a situation with potential for harm or damage." (http://www.peercenter.net/glossary/)

Initiating Event

"The first significant deviation from the normal situation that may lead to a system failure or an accident." (Rausand and Hoyland, 2004)

End State

"An end state is the set of conditions at the end of an event sequence that characterizes the impact of the sequence."
(http://www.nuce.boun.edu.tr/psa/psaglossary.html)

Vulnerability

*"A characteristic of a critical infrastructure's design, impleme*ntation, or operation that renders it susceptible to destruction or incapacitation by a threat." (Ellis, Fisher et al., 1997)

Appendix 2: Event Trees

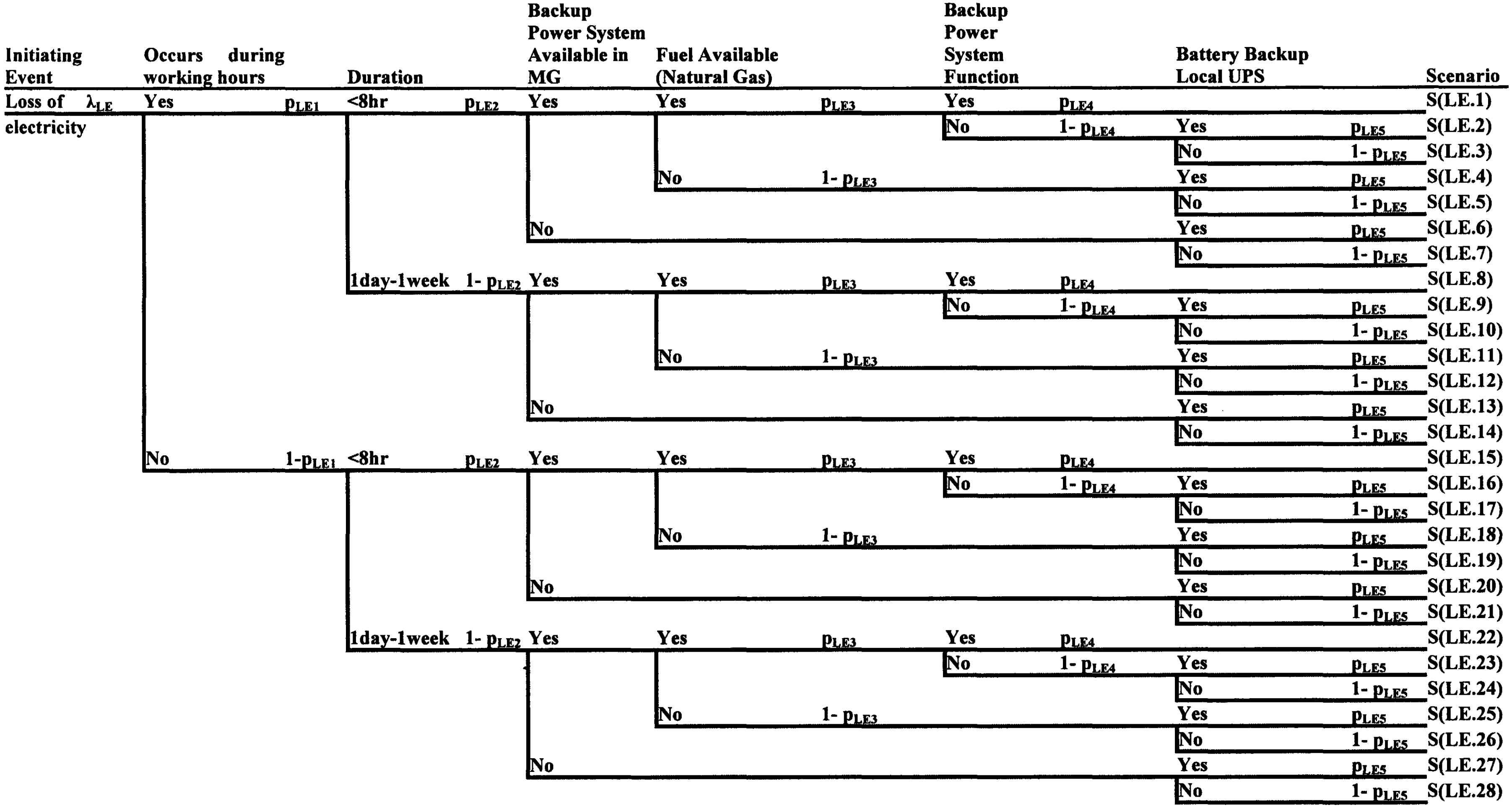

Figure 27: Loss of Electricity Event Tree

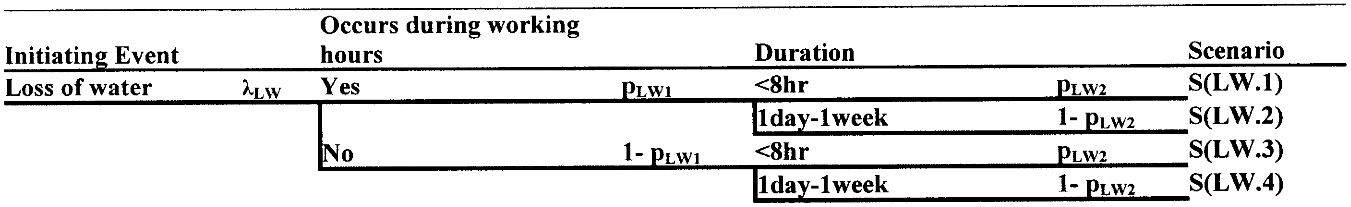

Figure 28: Loss of Water Event Tree

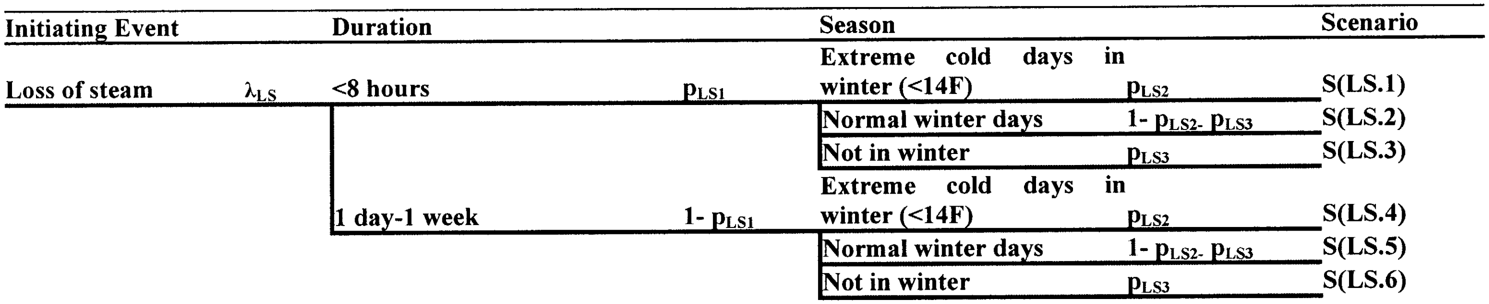

Figure 29: Loss of Steam Event Tree

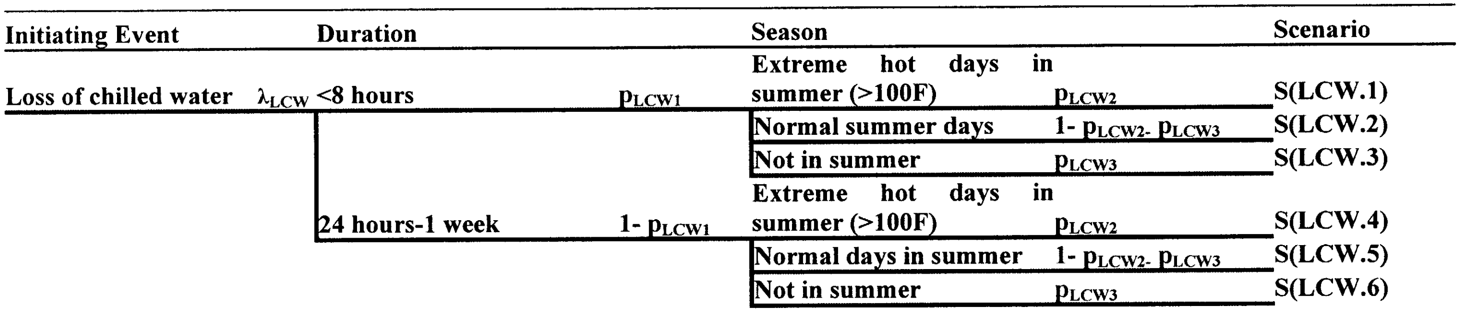

Figure 30: Loss of Chilled Water Event Tree

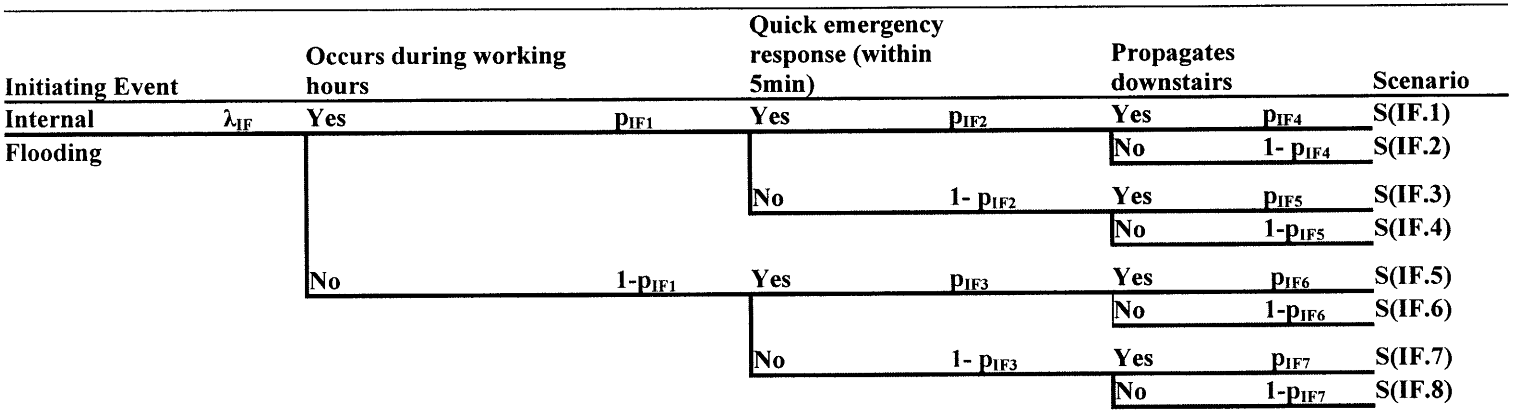

Figure 31: Internal Flooding Event Tree

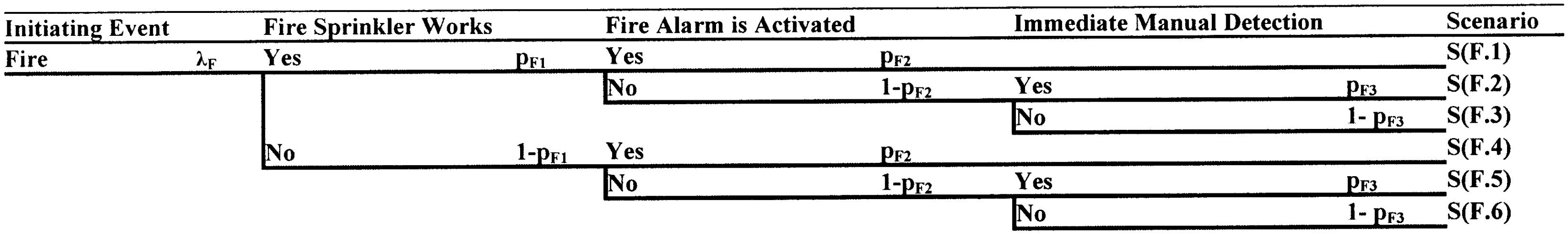

Figure 32: Fire Event Tree

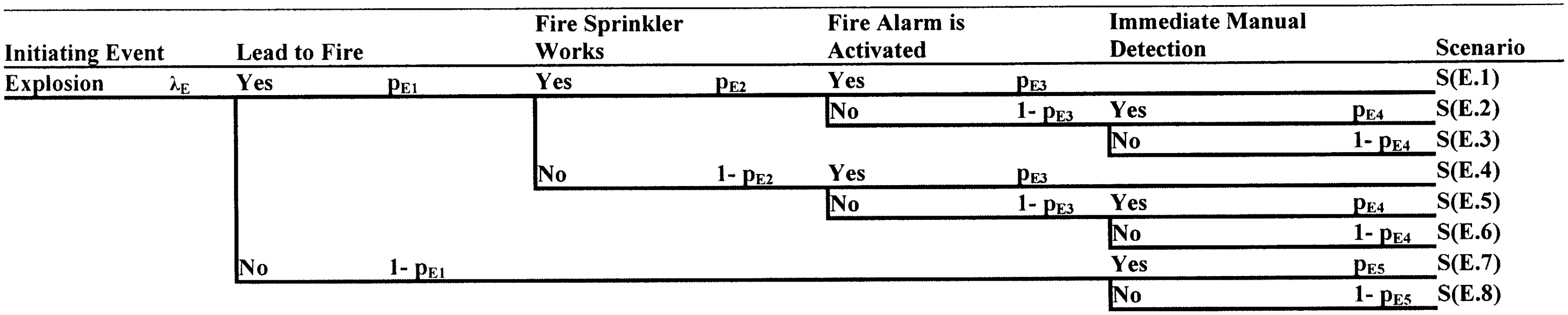

Figure 33: Explosion Event Tree

Appendix 3: Stakeholder List

Title	Department
Associate Professor	Biological Engineering Division
Dept Head & Director of Campus Activities Complex	Campus Activities Complex
Professor & Director	Center for Material Science & Engineering
Research Specialist	Center for Materials Science and Engineering
Technical Associate	Center for Materials Science and Engineering
Research Specialist	Center for Materials Science and Engineering
Research Scientist	Center for Materials Science and Engineering
Project Technician	Center for Materials Science and Engineering
Principal Research Scientist	Center for Materials Science and Engineering
Manager of Finance and Administration	Controller's Accounting Office
Facilities Manager, EHS Coordinator and Chemical Hygiene Officer	Department of Biology
Director, Department of Chemistry Instrumentation Facility (DCIF)	Department of Chemistry
Administrative Officer	Department of Chemistry
Operations Manager, Department of Chemistry Instrumentation Facility	Department of Chemistry
Operations/Facilities Manager	Departments of Chemistry and Earth, Atmospheric and Planetary Science
Manager, Sustainability Engineering & Utility Planning	Department of Facilities
Deputy Director	Department of Facilities
Director of Operations	Department of Facilities
Supervisor, Repair and Maintenance	Department of Facilities
Project Associate	Office of the Dean for Student Life-Housing
Assistant Director, Evening Operations	Office of the Dean for Student Life-Housing
Professor & Director	Division of Comparative Medicine
Associate Director	Division of Comparative Medicine
Director	Environment, Health and Safety Office
EHS Coordinator and Chemical Hygiene Officer	Department of Chemistry
Deputy Director, Biosafety Program	Environment, Health and Safety Office
Professor	Engineering Systems Division

Title	**Department**
Associate Director	Office of the Dean for Student Life-Housing
Senior Information Technology Consultant	Human Resources Department
Senior Human Resources Officer	Human Resources Department
Administrative Officer	Human Resources Department
Manager of Health and Welfare Benefits	Human Resources Department
MIT Affiliate	Human Resources Department
Senior Telephony Analyst	Information Services & Technology
MIT Network Manager	Information Services & Technology
Director, Telephony & IS&T Shared Services	Information Services & Technology
Manager, 5ESS Operations	Information Services & Technology
Senior Project Manager, Network Strategies	Information Services & Technology
Director, Operations & Infrastructure Services	Information Services & Technology
Facilities Manager/Safety Officer	Medical Department
Superintendent of Reactor Operations	Nuclear Reactor Laboratory
Quality Assurance Supervisor	Nuclear Reactor Laboratory
Associate Dean and Director of Housing	Office of the Dean for Student Life
Senior Associate Dean for Students, House Master	Office of the Dean for Student Life
MIT Affiliate	Office of the Dean for Student Life
Associate Dean for Student Life Programs	Office of the Dean for Student Life
Captain	Security and Campus Police Services
Lieutenant	Security and Campus Police Services
Director	Security and Campus Police Services