IT.06

Software for Optimizing Protection of Constructed Facilities

Amy S. Rushing, Chi J. Leng, Dr. Robert E. Chapman, and Dr. Harold E. Marshall

The September 11, 2001, attacks and the subsequent dispersion of anthrax through the U.S. postal system have changed the way many in the United States approach security and safety in constructed facilities. These events, in addition to the losses from recent hurricanes, wildfires, and high winds, have prompted owners and managers of constructed facilities to seek better protection of occupants, property, and building functions from natural and man-made hazards. Future disasters put us at risk for harm to occupants, physical damage to buildings and infrastructure, business interruptions, and financial losses.

These realities have led to changes in the way key decision-makers respond to the risk of hazards. Among these changes are the way owners and managers think about the design, location, construction, management, and renovation of their buildings. The range of responses available to decision-makers is extensive, as is the potential expense. Coupled with the reality of these risks are budgetary constraints. The two objectives—safeguarding constructed facilities while satisfying limitations—must be balanced through a cost-effective response to the risk of natural and man-made hazards.

To address these objectives, an economic tool that includes evaluation methods and software for implementing them is needed. A recent National Institute of Standards and Technology (NIST) report [4] describes a three-step protocol for optimizing protection against disasters. This paper takes the next step by describing a cost-effectiveness software tool being developed at NIST. The software provides the means for implementing several ASTM standardized economic evaluation methods and helps its users choose cost-effective strategies to reduce personal injuries, financial losses, and damage to constructed facilities. It also helps key decision-makers produce a risk mitigation plan that responds to the natural and man-made hazards in a financially responsible manner. By using standardized economic evaluation methods to promote more informed decisions, key decision-makers and other stakeholders will benefit from reduced exposure to losses from hazards.

OPTIMIZATION

Risk Mitigation Plan

Underlying the software is a three-step protocol for producing a risk-mitigation plan. Step 1 is to assess the risk of uncertain, costly, natural and man-made hazards, including floods, earthquakes, fire, and terrorism. Because resources are too limited to allow for full protection of all facilities against every possible hazard, economic efficiency dictates that the level of protection be a function of the likelihood of a disaster occurring, the expected value of damages, and the cost of protection. Through step 1, decision-makers can determine if a facility merits some degree of protection. For a comprehensive discussion of risk assessment aids, including descriptions of software and other tools for assessing facility risk, see Chapter 3 of Chapman and Leng [4].

Step 2 is to identify engineering, management, and financial strategies to abate the risk of damages. To protect a property, decision-makers tend to think first of physical barriers or heightened security regarding access. Yet there are numerous alternatives for protection against losses, such as increased setbacks, that are often overlooked. Some strategies will lower the probability of the disaster occurring, while others will lower the damages incurred once the disaster happens.

Step 3 uses economic analysis to select the optimum package of risk mitigation strategies. Note that all economic measures used in the software are consistent with ASTM standard measures of economic merit.

The majority of existing software focuses on step 1-risk assessment. The software discussed in this paper, however, focuses on step 3-helping users evaluate the life-cycle economic effectiveness of selected mitigation strategies.

Mitigation Strategies

Mitigation strategies reduce expected damages from a hazard. A strategy may be aimed at preventing the hazardous event, such as apprehending a terrorist before a bomb can be detonated. A strategy might also be designed to prevent or limit property damages and injuries from a realized hazardous event. An example would be investing in barriers to keep water away from property when flooding occurs. Finally, strategies can be used as policy instruments to encourage or discourage behaviors or investments to make facilities safer. Federal cost sharing of large U.S. water projects, for example, encourages local communities to construct facilities for flood control.

Mitigation strategies can be used singly or in combination to protect against a given hazard. A barrier to unauthorized entry might be used in combination with surveillance cameras and an HVAC system with enhanced filtration, for example, to protect against anthrax contamination of a building.

A single strategy might generate benefits aside from disaster mitigation objectives. An improved security system for protection against terrorists, for example, also protects the organization from theft. An improved egress system for evacuation during a terrorist event would also result in benefits from fewer injuries during a non-terrorist-related emergency.

Note that identification of strategies and measures of their likely performance are required inputs of the software program. Better information about the mitigation strategies will lead to better optimization solutions when using the software.

Most mitigation strategies can be classified as one of the following three types: engineering, management, and financial. The following three sections provide an overview of the strategies. For a more detailed description of the strategies, see Chapman and Leng [4].

Engineering Alternatives

Engineering alternatives for increased facility protection include structural/material changes, barriers, and mechanical system changes. Dams, levees, and channels are structures that protect facilities from flooding. Walls, fences, boulders, and large planters are some of the many types of structural barriers that are being used to protect facilities against terrorist attacks.

Other changes include alterations to HVAC systems, people-moving systems, and cyber security hardware and software. HVAC systems with high-technology sensors, sophisticated air controls, and specialized filters can detect terrorist-delivered chemical and biological contaminants, separate and contain the affected air, and filter out the contaminants. Technologies for verifying identities accurately and quickly help protect facilities from terrorist encroachment. Centrally administered hardware and software controls prevent cyber attacks and reduce the high costs of virus-infected computers.

Management Practices

Building owners and managers can also use management practices to reduce their risk from natural and man-made hazards. Management practices can be procedural or technical. Some relate to security, training, communications, and emergency response. Others relate to location of and access to the building and systems within the building. Some practices complement engineering alternatives, and others substitute for them. Examples of management practices include using security personnel to perform identification checks at building entrances, training on sheltering procedures to improve survival during emergencies, and developing communications strategies to coordinate with security staff and emergency personnel responding to an incident.

Financial Mechanisms

Building owners and managers can use the two financial mechanisms of insurance and financial incentives to reduce the risk of losses.

Insurance reduces the financial exposure of owners of constructed facilities to natural and man-made hazards by transferring the costs to other parties. For example, owners and managers can purchase insurance for workers' compensation, property damage, business interruptions, and liability.

Financial incentives encourage decision-makers to make certain protective choices over others. These incentives for risk mitigation are policies or measures that provide further motivation for building owners and facility managers to implement risk mitigation measures. Financial incentives fall into two categories: government policy-based incentives and market-based incentives.

The government can institute direct incentives that reduce the relative price that building owners and managers pay to protect their buildings. These incentives include subsidies, tax write-offs, cost sharing, or loan guarantees for investments in protective measures.

Financial incentives may also be market based, through a building owner's transactions with tenants, insurers, employees, potential buyers, lenders, and other parties who benefit from a reduction in building vulnerability. Building owners who lease commercial space may find that tenants value a building's safety features and are willing to pay a leasing premium. Insurers may reduce premiums or deductibles or write more desirable policies for buildings that have protective measures. Owners of leveraged buildings may also receive incentives from their lenders to protect their assets by receiving preferential financing terms on the building loan.

Economic Evaluation

The decisions about how much to spend on protecting constructed facilities and their occupants from natural and man-made hazards and what types of measures are appropriate are two issues facing building owners and managers. The life-cycle cost approach and its software implementation provide tangible support for this decision-making process. The question of how much to spend, however, merits theoretical treatment [4]. The theoretical approach takes the decision within the life-cycle cost framework used in the software and breaks the expenditure decision down to its components. It illustrates how the different factors link choices to the lowest life-cycle cost. The approach also incorporates the annual capital and operating budget constraints that face decision-makers in each period.

The model includes, for time periods between 0 and T, the three types of risk mitigation measures described above; engineering alternatives, management practices, and financial mechanisms. The objective is for building owners and managers to choose the combination of these three measures that minimizes life-cycle costs (including expected losses from natural and man-made hazards). Not all measures are available in every period: in period 0, owners and managers choose how much to invest in engineering alternatives and a subsidy is offered. In all periods, they choose how much to spend on management practices. Equation 2.1 is the objective function for the model:

$$\min_{\{I_0; M_0, \ldots, M_T\}} \left\{ (1-\alpha)I_0 + \sum_{t=0}^{T} \frac{OM_t + O_t + E(L_t) + M_t}{(1+d)^t} \right\}$$

(equation 1)

subject to the following constraints:

$$K_{-1} \geq 0$$

(equation 2)

$$K_0 - K_{-1} = I_0$$

(equation 3)

$$(1-\alpha)I_0 \leq B_0^C$$

(equation 4)

$$M_t \leq B_t^{Op} \quad \text{for } t = 0,\ldots,T.$$

(equation 5)

The variables decision-makers choose are:

- I_0 the investment in engineering alternatives in period 0; the price of each unit of protection, P_I, is normalized to one dollar, so I_0 represents the gross flow (in dollars) of engineering alternatives in period 0.
- M_t the level of expenditure (in dollars) to implement management practices to reduce losses in period t, for $t = 0,\ldots,T$.

The other variables of the model are:

- α the proportion of the investment in protective measures borne by the government through an investment subsidy: $\alpha \in [0, 1]$.
- OM_t the dollar cost of operations and maintenance (O&M) in period t for all building components.
- O_t other dollar costs in period t for all building components. This variable captures the direct costs of the investment other than initial investment and O&M costs, such as disposal cost.
- $E(L_t)$ the expected loss due to all hazards in each period, measured in dollars. It is assumed that the probability of natural hazards and terrorist events and losses from each type of event are independent.
- d the discount rate, where $d \in [0,1]$.
- K_{-1} the value of preexisting stock of investment in engineering alternatives in the building measured in dollars.
- K_0 the dollar value of cumulative investments in engineering alternatives up to time 0: $K_0 = I_0 + K_{-1}$. There is no investment in engineering alternatives beyond period 0 and no physical depreciation of capital, so for all periods after time 0, the level of the building protection capital stock equals K_0: $K_t = K_0$ for $t = 1,\ldots,T$.
- B_0^C the period 0 budget allocation, in dollars, for discretionary investment in engineering alternatives.
- B_t^{Op} the discretionary operating budget in dollars, in each period $t = 0,\ldots,T$.

Equation 2 is the non-negativity condition for the inherited stock of protective capital. Equation 3 shows that the change in the stock of protective capital during period 0 equals the level of protective investment made during period 0. Equations 2 and 3 together describe the stock of capital invested in engineering alternatives during period 0. Equation 4 is the period 0 capital budget constraint, and Equation 5 is the operating budget constraint for all periods.

Expected loss from natural and man-made hazards is determined by two components: the probability of an event and the probability distribution of losses if an event occurs. It is assumed that the effectiveness of protective measures increases with the level of investment in these measures. These improvements in effectiveness are captured in the model as reductions in expected losses.

The probability of natural hazards does not depend on any of these strategies. The probability of man-made events in each time period may depend on the stock of protective capital in each period, K_0. Protective measures may deter terrorists from targeting a particular building if the terrorists are aware of these measures. The likelihood of an attack and the severity of loss may fall due to improved detection of security breaches. The deterrent and detection effects of protection are captured as a negative relationship between the total level of protection and the probability of an attack. Because K_0 is the sum of inherited protective capital and investment during period 0, there is a negative relationship between the level of investment in protection and the probability of an attack.

The model provides for a government subsidy for investment in engineering alternatives. A government may decide to provide a subsidy if it judges that the marketplace does not adequately value the social benefits of disaster mitigation measures for constructed facilities. Differences between the private and social benefits and costs of risk mitigation may be due to effects of the measures on neighboring buildings or on the building's tenants that are not borne by the decision-maker. The fixed subsidy, α, represents the percentage of the total amount of investment in engineering alternatives that the government will bear.

The Lagrangian for this life-cycle cost minimization is given in Equation 6:

$$\begin{aligned} L &= (1-\alpha)I_0 + \sum_{t=0}^{T} \frac{OM_t + O_t + E(L_t) + M_t}{(1+d)^t} + \lambda_1 K_{-1} \\ &\quad + \lambda_2[K_0 - K_{-1} - I_0] \\ &\quad + \lambda_3[B_0^C - (1-\alpha)I_0] \\ &\quad + \sum_{t=0}^{T} \lambda_{4t}[B_t^{Op} - M_t], \end{aligned}$$

(equation 6)

The Lagrangian is used to derive the optimal conditions for choosing investment in engineering alternatives and expenditures to implement management practices. These conditions are written as Equations 7 and 8, respectively:

$$-\sum_{t=0}^{T}\left\{\frac{\partial OM_t/\partial I_0 + \partial O_t/\partial I_0 + \partial E(L_t)/\partial I_0}{(1+d)^t}\right\} + \lambda_2 + (1-\alpha)\lambda_3 = 1-\alpha$$

(equation 7)

$$-\left\{\frac{\partial OM_t/\partial M_t + \partial O_t/\partial M_t + \partial E(L_t)/\partial M_t}{(1+d)^t}\right\} + \lambda_{4t} = \frac{1}{(1+d)^t} \text{ for } t = 0,\ldots,T.$$

(equation 8)

The allocation of the period 0 budget for investment in engineering alternatives must satisfy Equation 7. The left-hand side of Equation 7 is the marginal benefit of each additional dollar of investment in engineering alternatives over the life cycle. With the negative sign, this benefit is written as the marginal reduction in cost. The reduction in cost could be in the form of lower O&M costs, lower other costs, or lower expected losses from an attack.

λ_3 is the shadow value of each unit increase in the budget. The right-hand side of the equation is the cost of each dollar of investment in period 0. $1 - \alpha$ represents the cost of each unit of investment in engineering alternatives paid for by the building owner, since government cost-sharing defrays a fixed proportion, α, of the investment. The life-cycle cost minimizing level of investment must satisfy this equality.

Equation 8 is the condition for optimal expenditure on management practices in each period from $t = 0,\ldots,T$. It shows that the present discounted value of the reduction of marginal cost in each period plus the shadow price of each additional dollar the operating budget is increased must equal the present discounted value of one dollar, which is the price per unit of expenditure on management practices.

SOFTWARE

Overview

The software product helps users make straightforward and consistent comparisons of risk mitigation strategies based on established economic evaluation practices. The uncertainty about natural and man-made hazards, in particular the multitude of imaginable terrorist attack scenarios, complicates the task of building owners and managers to identify and choose which hazards to guard against. The wide range of potential remediation measures, the permanence of investment-based solutions, and the expense of their implementation, installation, and maintenance necessitate a tool to systematically and consistently evaluate possible alternatives.

The software developed at NIST performs such evaluations by incorporating life-cycle cost analysis based on an industry consensus standard, ASTM E 917 [2]. The software allows building owners and managers to define hazard scenarios, identify possible consequences of those scenarios, and compare combinations of alternative strategies to mitigate those consequences. The software's standardized measures allow life-cycle comparisons of alternative strategies based on user-defined scenarios.

The Cost-Accounting Framework

The mitigation strategies and their associated costs described above provide the basis for calculating life-cycle costs. The flexibility of the life-cycle cost method, however, enables us to go beyond these generic costs. The result is a more focused representation of costs, referred to as the detailed cost-accounting framework.

Costs are classified along four dimensions within the cost-accounting framework: Bearer of Costs, Budget Category, Building/Facility Component, and Mitigation Strategy. A schematic representation of the cost-accounting framework is given in Figure 1.

The first dimension, Bearer of Costs, covers all stakeholder groups. A stakeholder group is defined as any collection of organizations or individuals directly affected by the project. Bearer of Costs has three cost types: Owner/Manager, Occupant/User, and Third Party. Owner/Manager costs are all costs incurred by the project's owner or agent. Occupant/User costs accrue to the direct users of the project. Third-Party costs are all costs incurred by entities who are neither the project's owner or agent nor direct users of the project.

The second dimension, Budget Category, has three cost types: Capital Investment, O&M, and Other. All acquisition costs, residual values, and capital replacement costs fall under Capital Investment. Costs falling under O&M include energy costs and insurance premiums paid to reduce risk exposure. Other costs are non-capital costs that cannot be attributed to the O&M cost type.

The third dimension, Building/Facility Component, has three cost types: Building/Facility Elements, Building/Facility Site Work, and Non-Elemental. The first two costs are associated with the ASTM elemental building classification UNIFORMAT II [1]. Non-Elemental costs are all costs that cannot be attributed to specific functional elements of the project.

The fourth dimension, Mitigation Strategy, has three cost types: Engineering Alternatives, Management Practices, and Financial Mechanisms as described above.

The software uses the cost-accounting framework to illustrate how costs affect stakeholders in different ways. The framework and software promote a detailed, consistent breakdown of life-cycle costs so that a clear picture emerges of the cost differences between competing alternatives. In the sections that follow, use of the framework is demonstrated in both the input and output screens of the software.

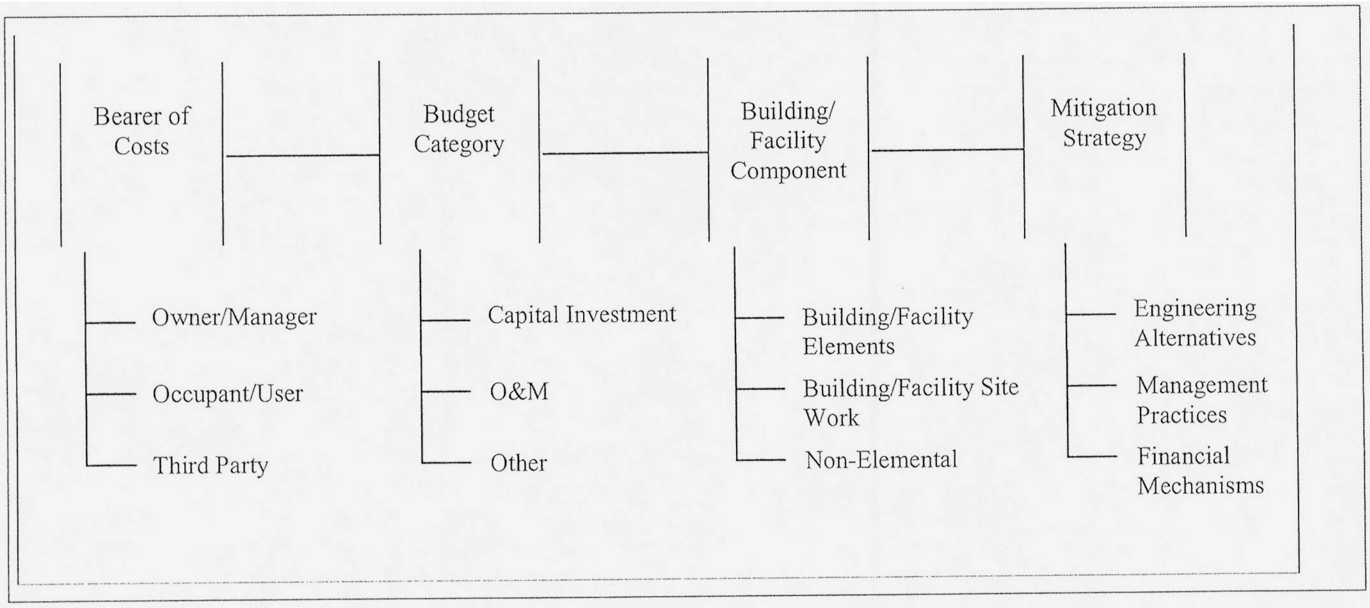

Figure 1—Overview of the Cost-Accounting Framework: Dimensions and Cost Types

Cost Summary Window

The Cost Summary window, shown in Figure 2 for a building renovation project, is the main screen of the software. This window is displayed when a new project is started or an existing project file is opened. Each dimension in the cost-accounting framework is listed on the window along with the life-cycle cost attributed to it. Note that each dimension captures the full spectrum of costs (i.e., all costs summed within each dimension add up to the same total). When a project is created, these values are all zero. As the user enters data into the software, these values automatically update, displaying the current values for life-cycle costs for each dimension.

A tree on the left-hand side of the Cost Summary window serves as the software's main menu. The tree contains three top-level nodes: Project, Analysis, and Reports. The items listed under the Project node allow users to enter project information, define alternatives, and manage cost and event information. The items under Analysis give users access to a baseline analysis and a sensitivity analysis. The items under Reports give users access to output reports.

Project Data

Clicking the Description option on the main menu tree opens the Project Description window (shown in Figure 3). Here a user can enter project information such as name, description, base year, length of study period, and discount rate. The Alternatives option allows the addition and deletion of project alternatives as well as entry of information about the alternatives. The software will analyze up to four alternatives.

Cost-related information inputted into the software consists of two types: input costs and event-related costs. Input costs represent all costs tied to the building or facility under analysis that are not associated with an event. They include initial investment costs, future renovation costs, and any salvage value for plant and equipment. Event modeling is used to evaluate natural and man-made risks. Events, such as earthquakes, high winds, or cyber attacks, can be entered into the software to model the hazards associated with these risks. Annual outcomes, with a specified probability of occurrence, are associated with each event. Event-related costs are associated with each outcome.

To manage the creation, deletion, and editing of input costs, the user clicks Costs on the tree or Edit in the Edit Costs/Events group box in the top right corner of Figure 2. To manage the creation, deletion, and editing of events, the user clicks Events on the tree or Edit in the Edit Costs/Events group box.

Output

The software's output reports are designed to help the user examine how costs are distributed across Bearer, Budget Category, Building/Facility Component, and Mitigation Strategy. This approach gives users a snapshot of all costs entering into the analysis, expressed in present value terms, which "roll up" into the life-cycle costs recorded in the Cost Summary window. The user will also have the option to obtain additional reports for economic measures other than life-cycle cost.

Case Study Example

The following case study, developed by NIST [3], describes a renovation project for an actual building. The study focuses exclusively on two of the three mitigation strategies—engineering solutions and management practices—for protection against terrorism. In this section, we illustrate the software using the case study as an example project.

The building is a single-story data center undergoing renovation in a suburban community. The renovation has been planned for some time to upgrade the data center's HVAC, telecommunications, and data processing systems and to address a number of generic security concerns. Specific risks evaluated in the case study are associated with the vulnerability of information technol-

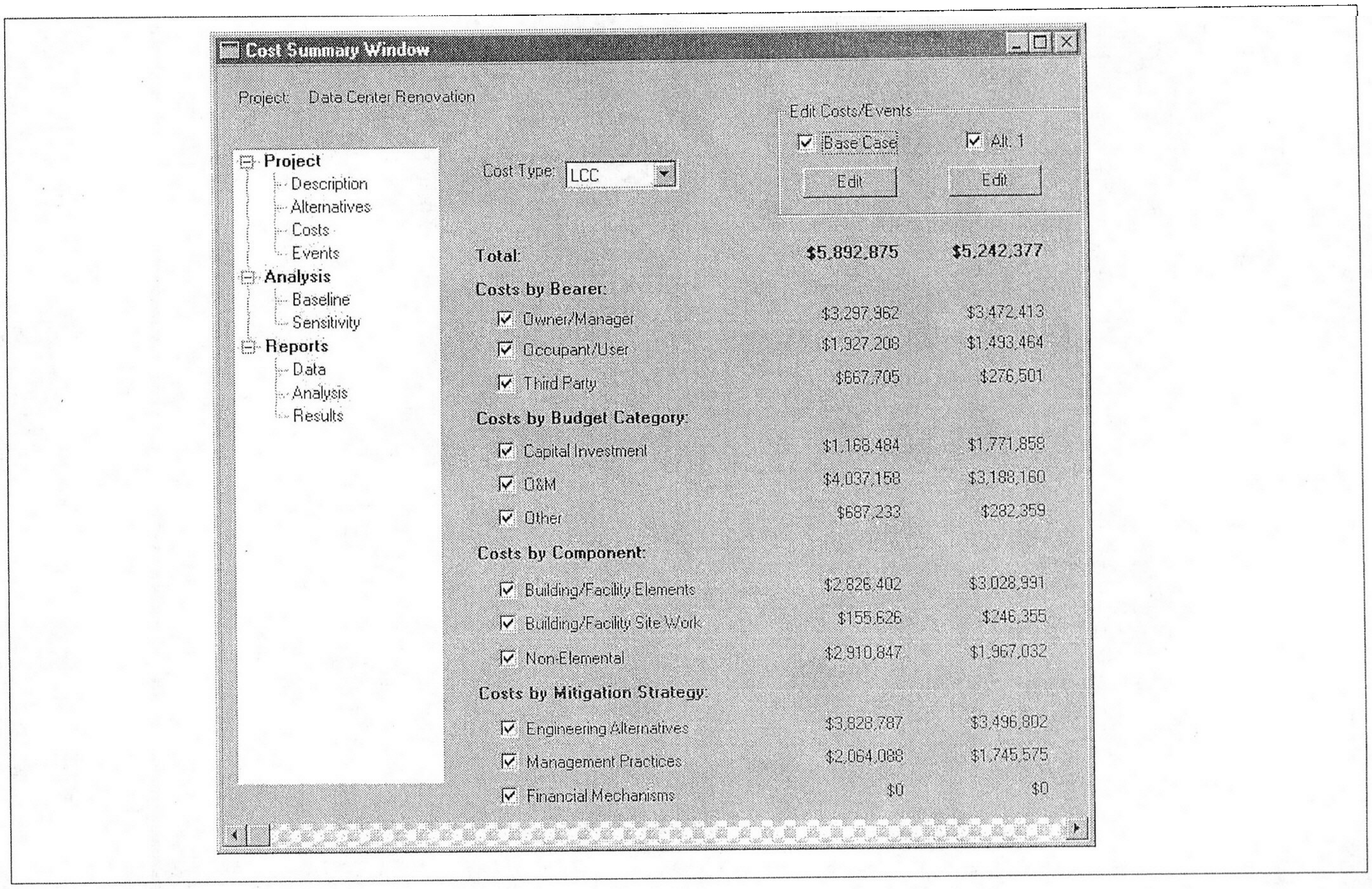

Figure 2—Cost Summary Window

ogy resources and the potential for damage to the facility and its contents from chemical, biological, radiological, and explosive (CBRE) hazards.

Senior management is considering two alternative renovation strategies. The basic renovation has the lowest initial investment cost; it is designated as the Base Case. The enhanced renovation is designated as the Proposed Alternative. The renovation strategy that results in the lowest life-cycle cost will be the recommended alternative for use in the risk mitigation plan.

The first step in using the software for this case study is to input information in the Project Description window. The project information is shown in Figure 3. The alternatives under consideration are then added to the project via the Alternatives window. In this case we have two alternatives, the Base Case and the Proposed Alternative.

Next, input costs need be added to each alternative. Figure 4 shows an example of an input cost for the Proposed Alternative. This cost is in the amount of $50,000. It occurs in the first and second year of the study period so the Periodic radio button is selected and the proper year information is entered in the First Occurrence, Last Occurrence, and Occurs Every fields. The Classification Information group box at the bottom of the screen reflects how this cost is classified. In this case, the bearer is Third Party, the component is Non-Elemental, and the mitigation strategy is Management Practices. The remaining input costs for each alternative are entered in a similar fashion.

The next step is to enter event and outcome information for each alternative. In this example, we have events for cyber and CBRE attacks. Each event can result in several outcomes. For example, the CBRE attack outcomes are: no breaches, minor damage, and major damage.

After the event and outcome information is entered, event-related costs can be added to the outcomes. Figure 5 shows the event-related cost screen. The top of the screen provides information about the cost and shows what event, alternative, and outcome correspond to it. For example, we see the associated event is CBRE attack, the Alternative is the Base Case, and the associated outcome is Major Damage. We also learn the cost type is Capital Investment. The remainder of the screen asks for input about the cost. This cost item covers Damage to the Data Center in the amount of $3,000,000. In the Classification Information group box, we specify the bearer as Owner/Manager, the component as Building/Facility Elements, and the mitigation strategy as Engineering Alternatives. The remaining event-related costs for each alternative are entered in a similar fashion.

Once all input and event-related costs are entered, the results of the baseline analysis are ready to be examined. Referring back to Figure 2, we see from the Cost Summary window that the life-cycle cost of the Base Case is $5,892,875 and the Proposed Alternative is $5,242,377. Since the Proposed Alternative results in lower life-cycle costs, it is the more cost-effective choice. Note that Occupant/User and Third Party costs are higher for the Base

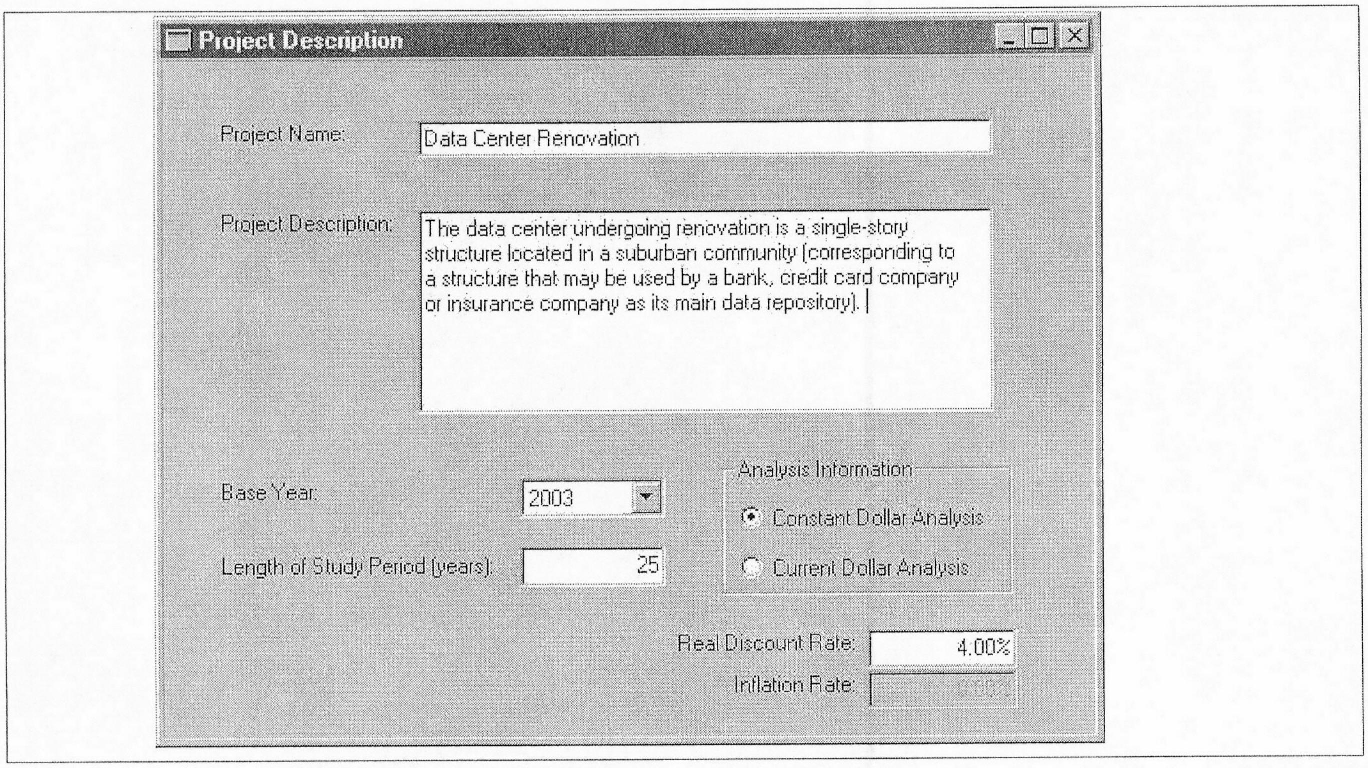

Figure 3—Project Description Window

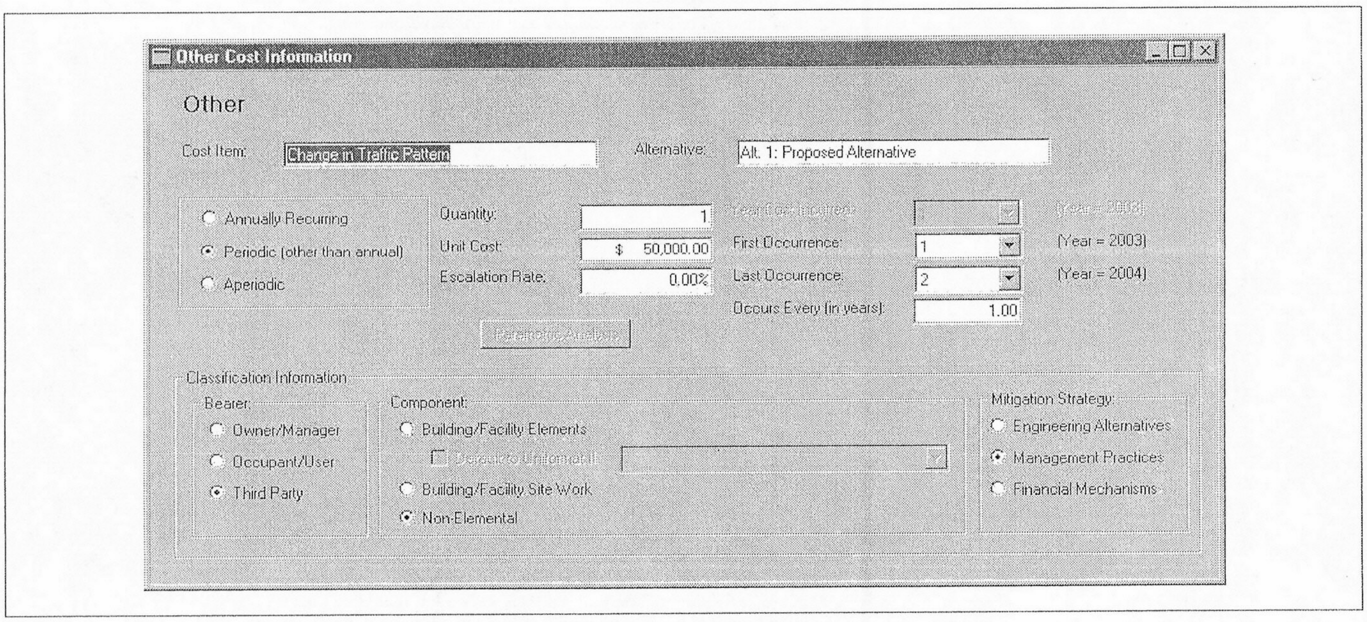

Figure 4—Sample Cost Information Window

Case, whereas Owner/Manager costs are higher for the Proposed Alternative. Understanding who bears which costs is an essential component of the risk mitigation plan.

After reviewing the Cost Summary window, the user can generate output reports by clicking the options under Reports in the main menu tree. These reports provide a summary of inputted background information, alternative descriptive information, and input and event-related cost summaries. The reports will also present a tabular and graphical representation of the information found on the Cost Summary window.

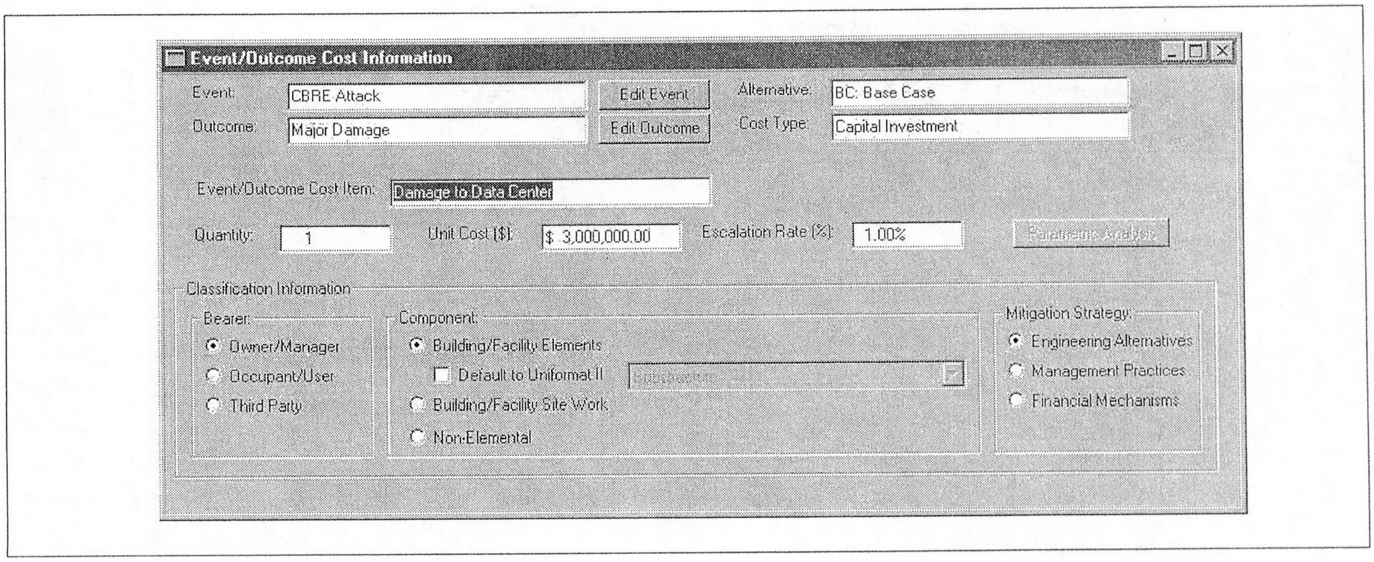

Figure 5—Event/Outcome Cost Information Window

FUTURE PLANS

Software Rollout

The development of the software is a multi-year process. The design of the software will build on the expertise NIST has developed through past software products as well as input from a Steering Committee composed of a cross-section of external subject matter experts.

In 2004, NIST will produce two preliminary versions of the software. The first is an alpha version that includes all features needed to perform a baseline analysis. The alpha version will be tested as part of a collaborative effort between NIST and the Wharton Risk Management and Decision Processes Center. A beta version that includes the capability of performing a deterministic sensitivity analysis will be completed in September. This version of the software will be field-tested with a team of potential customers drawn from industry and governmental partners.

In 2005, NIST will develop and distribute Version 1.0. It will produce the types of analysis results that provide decision-makers with the basis for generating a risk mitigation plan and will include help files to assist users.

In 2006, NIST will develop and distribute Version 2.0, expanded to include a financial risk module which makes use of Monte Carlo techniques. This will enable users to conduct a rigorous, probabilistic financial risk assessment of alternative mitigation strategies. Version 2.0 will include a users manual. NIST will also develop a training module for the software.

A software development web site has been established at http://www.bfrl.nist.gov/oae/software/cet.html. Information detailing the software's progress and downloadable testing versions of the software can be obtained from this site. We encourage readers to visit the site and download the current version.

Economic Standards for Security-Related Issues in Constructed Facilities

To support the cost-effectiveness software, NIST will work through the Building Economics Subcommittee of ASTM to produce a revised and expanded version of the life-cycle cost standard practice, E 917, and a new standard guide on how to use the three-step protocol outlined in Section 2.1 to produce a cost-effective risk mitigation plan.

The life-cycle cost standard practice is the core component of the software product. ASTM E 917 does not currently address, however, the analysis of low-probability, high-consequence events. Such events are at the heart of any analyses of natural and man-made hazards. Thus, NIST has proposed to the Building Economics Subcommittee and gained approval to submit modifications to E 917 to incorporate discussions of how to analyze such events and a technical appendix illustrating how such an analysis would be performed.

The proposed standard guide will present the protocol for developing a risk mitigation plan, direct users to the relevant ASTM standard practices, explain when and how to employ these practices, and demonstrate how use of the software product enables them to implement these practices.

REFERENCES

1. ASTM International. 2003. *Standard Classification for Building Elements and Related Site Work-UNIFORMAT II*. E 1557. **Annual Book of ASTM Standards**: 2003. Vol. 04.11. West Conshohocken, PA: ASTM International.
2. ASTM International. 2003. *Standard Practice for Measuring Life-Cycle Costs of Buildings and Building Systems*. E 917. **Annual Book of ASTM Standards**: 2003. Vol. 04.11. West Conshohocken, PA: ASTM International.

3. Chapman, Robert E. **Applications of Life-Cycle Cost Analysis to Homeland Security Issues in Constructed Facilities: A Case Study**, NISTIR 7025 (Gaithersburg, MD: National Institute of Standards and Technology, October 2003).
4. Chapman, Robert E., and Leng, Chi J. **Cost-Effective Responses to Terrorist Risks in Constructed Facilities**, NISTIR 7073 (Gaithersburg, MD: National Institute of Standards and Technology, February 2004).

Amy S. Rushing
National Institute of Standards and Technology
100 Bureau Drive, MS 8603
Gaithersburg, MD 20899-8603
E-mail: amy.rushing@nist.gov

Chi J. Leng
National Institute of Standards and Technology
100 Bureau Drive, MS 8603
Gaithersburg, MD 20899-8603
E-mail: chi.leng@nist.org

Dr. Robert E. Chapman
National Institute of Standards and Technology
Building and Fire Research Laboratory
100 Bureau Drive, MS 8603
Gaithersburg, MD 20899-8603
E-mail: robert.chapman@nist.gov

Dr. Harold E. Marshall
National Institute of Standards and Technology
100 Bureau Drive, MS 8603
Gaithersburg, MD 20899-8603
E-mail: harold.marshall@nist.gov