Risk Analysis, Vol. 27, No. 4, 2007 DOI: 10.1111/j.1539-6924.2007.00911.x

Critical Asset and Portfolio Risk Analysis: An All-Hazards Framework

Bilal M. Ayyub,[1]* William L. McGill,[1] and Mark Kaminskiy[1]

NOTE: This article should have appeared in Volume 27, Issue 3, as part of the Special Issue on Terrorism.

This article develops a quantitative all-hazards framework for critical asset and portfolio risk analysis (CAPRA) that considers both natural and human-caused hazards. Following a discussion on the nature of security threats, the need for actionable risk assessments, and the distinction between asset and portfolio-level analysis, a general formula for all-hazards risk analysis is obtained that resembles the traditional model based on the notional product of consequence, vulnerability, and threat, though with clear meanings assigned to each parameter. Furthermore, a simple portfolio consequence model is presented that yields first-order estimates of interdependency effects following a successful attack on an asset. Moreover, depending on the needs of the decisions being made and available analytical resources, values for the parameters in this model can be obtained at a high level or through detailed systems analysis. Several illustrative examples of the CAPRA methodology are provided.

KEY WORDS: All hazards; consequence; critical asset protection; decision; homeland security; risk analysis; security; terrorism; threat; vulnerability

1. INTRODUCTION

According to the Department of Homeland Security National Infrastructure Protection Plan, benefit-cost analysis is the hallmark of homeland security decision making.(1) Benefit-cost analysis provides a means of comparing the net reduction in risk with the associated price of achieving this reduction to determine the cost effectiveness of alternative risk reduction strategies.(2) Defensible benefit-cost analysis requires quantification of the risks before and after implementation of a risk reduction strategy using clearly defined metrics that capture all relevant uncertainties. In practice, however, the extreme uncertainties associated with potential hazards and the complexity of the parameters and decision variables characterizing risk often deter many from quantification due to a combination of insufficient resources to invest in data collection and analysis, and skepticism over the use of probabilistic techniques for scenarios lacking actuarial data. While a contribution to the debate on this issue is not within the scope of this article, we take the position that quantification is necessary to conduct defensible and meaningful benefit-cost analysis, and that credible expert opinion can compensate for the lack of actuarial data to support quantitative risk assessments.(3)

Decisions to enhance the protection of critical infrastructure and key resources require choosing from among a variety of protective, response, and recovery

[1] Center for Technology and Systems Management, University of Maryland, College Park, MD 20742, USA.
* Address correspondence to Bilal M. Ayyub, Center for Technology and Systems Management, Department of Civil and Environmental Engineering, University of Maryland, College Park, MD 20742, USA; tel: 301-405-1956; ba@umd.edu.

strategies to meet risk reduction objectives given finite available resources. Risk management strategies are of two general types—strategies to reduce the frequency of adverse events and strategies for mitigating the ensuing consequences given their occurrence.[4] While both natural and human-caused hazards are within the scope of homeland security, particularly troublesome are those intentional hazards initiated by an adversary that has motivation (e.g., political, economic, and religious), possesses variable and broad capabilities (e.g., weapons, manpower, and education), and is adaptive by being responsive to countermeasures.[5–7] To the decisionmaker's benefit, there are many more options available for mitigating security risks than those arising from natural hazards given that both probability and consequence can be affected through risk reduction strategies, such as through a combination of enhanced security at critical sites and measures to maintain continuity of lifeline services before, during, and following a malicious attack. Moreover, many of these options have a collateral effect of reducing risks associated with natural hazards. To quantitatively evaluate the effectiveness of risk mitigation strategies across all hazards, however, a common analytical framework is needed that accommodates all-hazards risk analysis.

To provide a defensible risk analysis that facilitates benefit-cost analysis, a quantitative framework for risk assessment and management is required. This article develops a general process for quantitatively assessing risks to critical assets and portfolios considering both natural and human-caused hazards that builds on previously published ideas on security effectiveness assessment,[8,9] terrorism risk analysis,[10–13] natural hazards risk analysis,[14–16] infrastructure risk analysis and interdependency analysis,[17,18] and systems risk and reliability analysis.[2,19] While other work in this area has produced a quantitative risk analysis methodology that supports asset-level analysis for security threats,[20] the primary objectives of this article are to develop a general equation for all-hazards risk assessment, develop a simple model for portfolio interdependency analysis, and demonstrate the application of both with a few simple illustrative examples.

2. BACKGROUND

2.1. Challenges with Human-Caused Threats

In recent years, decisionmakers charged with protecting critical assets have taken an all-hazards approach to risk management that focuses on both natural and human-caused hazards,[21] where each individual hazard type is physically unique and presents its own set of challenges with its characterization and assessment.[22] However, in contrast to natural hazards that are indiscriminate and without malicious intent, a unique challenge with assessing risks due to the deliberate actions of intelligent human adversaries is their ability to innovate and adapt to a changing environment. While one can rely on historical data to estimate annual occurrence rates for natural hazards affecting a region given that the timescale of geological and meteorological change is much greater than the planning horizon for most homeland security decisions,[14] assets in this same region are always plausible targets for adversaries despite a lack of past incidents.

The uncertainty associated with adversary intentions is largely epistemic, and in principle can be reduced given more knowledge about their intentions, motivations, preferences, and capabilities. In general, the threat component of the security risk problem is the most uncertain owing to the fact that defenders are often unaware of the adversary's identity and objectives. Less uncertain is the security vulnerability component of the risk equation, since countermeasures to defeat adversaries are relatively static in the absence of heightened alert. However, since the effectiveness of a security system depends on the capabilities and objectives of the attacker (which is uncertain), the performance of a security system under stress is more uncertain than the consequences following a successful attack. Thus, it seems that to build a security risk profile for an asset, it is prudent to start with those aspects of the risk problem that are most certain (i.e., consequence), and proceed with the less certain aspects (i.e., vulnerability then threat) as necessary to support resource allocation decisions.

With regard to critical asset protection, the process of assessing risks in this manner begins by identifying all relevant hazard scenarios based on the inherent susceptibilities of an asset's mission-critical elements. In this context, a *hazard scenario* is the combination of a hazard type (such as explosive attack or hurricane) and susceptible key element, and a *key element* is one that is essential for continuity of operations. Given these hazard scenarios, the loss given success for various threat intensities (e.g., size of explosive or wind speed) can be assessed. Without proceeding further, knowledge of loss as a function of hazard intensity can serve as the basis for risk mitigation decisions independent of hazard probability, such as if the decisionmaker prefers a precautionary approach. If a more complete picture of risk is needed to support

decision making or if other aspects of the risk problem are of greater concern, the analysis can postulate a set of alternative representative attack profiles (i.e., delivery system and intrusion path) for each hazard scenario, and thus in turn assess probability of adversary success, asset attractiveness, and annual rate of hazard. The choice of process steps and the level of detail pursued for each should be tuned to the needs of the decisionmaker.

2.2. Actionable Risk Assessment

From the point of view of a homeland security decisionmaker, guidance on where to focus attention on reducing risk is at least as important as the risk results themselves. For example, conveying insight into which risk contributors (variables) should be targeted for risk reduction is as important as the magnitude of risk. Borrowing on the concept of actionable intelligence,[23] *actionable risk assessments* produce actionable information that has practical and relevant use to the decisionmaker for the purposes of identifying viable options for risk reduction. One strategy for producing actionable risk assessments is to provide estimates of risk accompanied by the relative sensitivity of the risk results to small changes in the decision variables, such as through the use of importance measures.[19,24,25] The sensitivity values can be used to direct risk management efforts supported by benefit-cost analysis.

2.3. Levels of Analysis

Risk assessment and management for critical infrastructure and key resource protection can be performed at a variety of levels. At the *asset level*, a survey of an asset's mission-critical elements coupled with knowledge of the consequences of disruption, physical and security vulnerabilities to a wide range of hazards and threats, and asset attractiveness provides insight into actions an asset owner can take to reduce an asset's overall risk exposure. An *asset* in this context is anything of value to its owner, such as a monument, vehicle, or facility. At the *portfolio or system* level, the total risk associated with a portfolio or system of assets (such as those associated with a region, jurisdiction, or infrastructure sector) can be assessed to compare investment alternatives that aim to reduce overall portfolio risk. A *portfolio* in this sense is a collection of assets with common attributes or linkages. Regional analysis, for example, would define a portfolio from the top down by first identifying the critical functions and services of the region, and then assigning membership to regional assets that contribute directly to these mission areas. In contrast, a portfolio can be built from the bottom up by first defining a set of assets, then examining how they relate with one another. In both cases, knowledge of the physical, geographic, cyber, and logical interdependencies among portfolio assets is important for assessing the potential for cascading consequences initiated by a hazard event.[18]

To facilitate comparison of risk across sectors and aggregation of risk to higher levels of abstraction, risk analysis for critical infrastructure protection at all levels should share a common analytical framework that supports decision making by all stakeholders; this quality enables information collected at the asset level to support decisions made at the portfolio-level and vice-versa.

3. ASSET ANALYSIS

This section develops an all-hazards risk analysis framework that supports resource allocation decision making at the asset level. A five-phase process for asset-level analysis is adopted as shown in Fig. 1. Since all portfolios, whether defined by a particular function or composed of otherwise unrelated elements, are defined by their assets, asset-level analysis provides the basic information needed to assess risk at higher levels of abstraction.

3.1. Scenario Identification

Let E be the set of all key elements ε associated with a certain asset. Let H be the set of possible hazard types h. A *hazard* is a source of danger or harm,[2] and in the homeland security context refers to a wide range of natural and human-caused hazards such as those listed in Table I compiled from a variety of sources.[10–17,22,26,27] Defining a *hazard scenario* as the pairing of hazard type to key element, the set of all conceivable hazard scenarios is given as $H \times E$. Defining *susceptibility* as the function s: $H \times E \rightarrow \{0,1\}$, where a value $s(h, \varepsilon) = 1$ indicates that ε is inherently susceptible to the damage mechanisms caused by h, the crisp set $X = \{(h, \varepsilon) \mid s(h, \varepsilon) = 1\}$ consists of all relevant hazard scenarios x for the asset. Specification of element susceptibility can be achieved *via* a *target susceptibility matrix* such as that shown in Table II.[20] Furthermore, if any hazard scenario is deemed to be insignificant from the decision-maker's point of view, it would be screened out from further analysis, and thus removed from X.

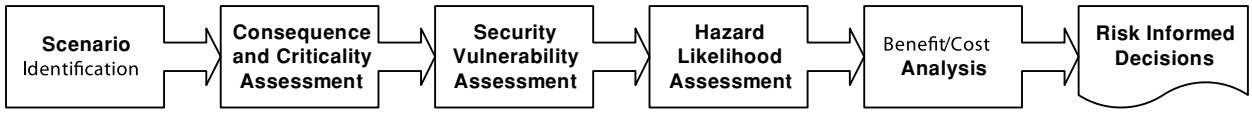

Fig. 1. Framework for critical asset and portfolio risk analysis.

Table I. Selected Hazard Types for Critical Asset Risk Analysis

Hazard Types	
Natural Hazards	Human-Caused (Unintentional)
• Earthquake	• Industrial accident
• Tropical storm/hurricane	Human-Caused (Intentional)
• Blizzard/winter storm	• Explosive
• Tornado	• Projectile/ballistic
• Tsunami	• Incendiary
• Volcano eruption	• Chemical
• Landslide	• Biological
• Flooding	• Radiological
• Wildfire	• Nuclear
• High wind/windstorms	• Radiofrequency/electromagnetic pulse
• Extreme temperature	
• Disease outbreak	• Sabotage
• Drought	• Cyber
• Meteorite/asteroid	• Laser

3.2. Consequence and Criticality Assessment

Consequence and criticality assessment estimates the losses associated with each hazard scenario x as a function of intensity q. Four loss dimensions are considered, as described in Table III. The sequence of events leading to loss given adversary success is as follows: first a successful attacker imparts a loading of a prescribed intensity on the target element, which results in damage according to the fragility of the target. The damage from attack maps to a percentage of maximum credible loss for number of fatalities, economic damage, and lost productivity or capability based on the system definition for the asset, and considering measures to mitigate potential losses. This loss is called the *potential loss*, and in general is represented by a probability distribution. The existence of emergency response and recovery measures, if available, would lessen the potential loss following the occurrence of the event.

On the basis of the above narrative, the expression for loss, L, as a function of hazard intensity attributed to a hazard scenario x is given by:

$$L_x = F_{\varepsilon|h}\,(1 - E_{M,\varepsilon})\,L_{MC,h}\,(1 - E_R)\,, \qquad (1)$$

where $F_{\varepsilon|h}$ is the fragility of the target element ε due to hazard type h as a function of hazard intensity, E_M measures the resistance of the asset's mission(s) to loss as a function of element damage, $L_{MC,h}$ is the maximum credible (or possible) loss associated with hazard h, and E_R measures the effectiveness of response and recovery capabilities (which is hazard independent). Note that Equation (1) is used to separately assess the loss for each loss dimension from the asset owner's part of view.

3.3. Security Vulnerability Assessment

Security vulnerability assessment investigates the ability of a determined adversary to successfully defeat security countermeasures put in place to protect an asset and execute an attack. Since hazard scenarios are broadly defined as a combination of key element and hazard type, a representative set of hazard

	Key Element					
Hazard Type	HAZMAT Storage	Building	Pipeline	Rail Car	People	Computer Network
Explosive	×	×	×	×	×	×
Projectile/impact	×	×	×	×	×	–
Incendiary	×	×	–	–	×	×
Chemical	–	–	–	–	×	–
Biological	–	–	–	–	×	–
Radiological	–	–	–	–	×	×
Laser	–	–	–	–	×	–
Radiofrequency	–	–	–	–	–	×
Cyber	–	–	–	–	–	×
Sabotage	×	–	×	×	–	×

Table II. Target Susceptibility Matrix for a Notional Asset[20]

Table III. Loss Dimensions and Associated Units of Measure

Loss Dimension	Description	Unit of Measure
Casualty	Measures the number of people injured or killed	Number of fatality equivalents[2]
Economic	Measures direct economic damage including property loss, repair and cleanup costs, environmental losses, and loss due to interdependency effect for the case of portfolio analysis	Current year dollars
Mission disruption	Measures degree of mission disruption for each relevant mission	Percentage reduction in available production capacity
Recuperation time	Measures the time to reconstitute lost functionality and production capacity	Time (days or years as appropriate)

delivery systems and intrusion paths is necessary to evaluate the probability of adversary success. Let D_h denote the set of possible delivery systems d for a given hazard h and let M_ε denote the set of representative intrusion paths m from the asset perimeter to key element ε. Defining an *attack profile* as the pairing of a delivery system d with a specific intrusion path m, the set of all conceivable attack profiles for a hazard scenario is given as $D_h \times M_\varepsilon$. Defining the relevance of an attack profile as the function r: $D_h \times M_\varepsilon \rightarrow \{0, 1\}$, where a value of one indicates that the given hazard can be delivered with delivery system d via intrusion path m, the crisp set $Y_x = \{(d, m) \mid r(d, m) = 1\}$ consists of all relevant attack profiles y for a given hazard scenario x. Specification of the attack profile relevance can be achieved via an *attack profile compatibility matrix* such as that shown in Table IV.

Building on the expression and techniques for security system effectiveness presented in References 1, 8–10, the probability of adversary success, P_S, as a function of hazard intensity for a specified attack profile y is given as:

$$P_{S,y} = (1 - E_{S,y})\, P_K Q, \tag{2}$$

where $E_{S,y}$ is the security system effectiveness with respect to the characteristics of attack profile y (e.g., detection, delay, and response measures[8]), P_K is the probability that the adversary will successfully execute its attack on the target given failure of the security system (i.e., probability of kill), and Q is the probability distribution for hazard intensity imparted on the target, which is a function of the characteristics of the delivery system. Note that $P_S = Q$ for natural hazards, which essentially gives the probability distribution on hazard intensity.

Table IV. Attack Profile Matrix for a Notional Human-Caused Hazard Scenario

	Intrusion Path				
Delivery System A: Autonomous; H: Human Driver	Via Back Road	Via Main Access Road	Via Forest	Via Water	Via Air
On person	×	×	×	×	–
Ground vehicle (H)	×	×	–	–	–
Ground vehicle (A)	×	×	–	–	–
Waterborne vehicle (H)	–	–	–	×	–
Waterborne vehicle (A)					
Aerial vehicle (H)	–	–	–	–	×
Aerial vehicle (A)	–	–	–	–	×

3.4. Hazard Likelihood Assessment

Hazard likelihood assessment determines the annual rate of occurrence for each attack profile and hazard scenario. Within a probabilistic framework, hazard likelihood is defined as the product of the estimated annual rate of occurrence for a given hazard type, and for deliberate human-caused hazards, the probability that the adversary will pursue a specified attack profile. The annual rate of occurrence, λ, associated with a given attack profile y associated with hazard scenario x and hazard h can be expressed as:

$$\lambda_y = A_{P,y} A_{S,x} A_{A,h} \lambda_{0,h}, \tag{3}$$

where $A_{P,y}$ is the relative attractiveness of attack profile y, $A_{S,x}$ is the relative attractiveness of hazard scenario x, $A_{A,h}$ is the relative attractiveness of the asset with respect to hazard type h, and $\lambda_{0,h}$ is a baseline annual rate of occurrence. Values for the attractiveness terms in Equation (3) can be determined based on the perceived utilities from the adversary perspective, such as those suggested in References 1 and 11. For natural hazards, all attractiveness terms are set equal to one.

3.5. Risk Assessment

The total risk associated with an attack profile is the combination of rate of attack, probability of adversary success given attack, and the loss given adversary success. From Equations (1)–(3), the annual risk, R_y, associated with an attack profile y, hazard scenario x and hazard type h is thus:

$$R_y = \int_0^\infty \{F_{\varepsilon\,|\,q}(1 - E_{M,\varepsilon})L_{MC,h}(1 - E_R)(1 - E_{S,y}) \times QA_{P,y}A_{S,x}A_{A,h}\lambda_{0,h}\}\,dq, \quad (4)$$

where the integration is taken over all hazard intensities q.

Noting that the maximum credible loss $L_{MC,h}$, baseline annual rate of hazard occurrence $\lambda_{0,h}$, and assuming that all attractiveness terms are independent of q, the total hazard risk, R_h, across all hazard scenarios and profiles for a given hazard type can be expressed as:

$$R_h = L_{MC,h}V_h\lambda_{A,h}, \quad (5)$$

where $\lambda_{A,h} = A_{A,h}\lambda_{0,h}$ is the annual rate of occurrence for a given hazard affecting the asset, and the overall vulnerability $V_h \in [0, 1]$ is given by:

$$V_h = \sum_{x \in X_h} A_{S,x}\left(\sum_{y \in Y_x} A_{P,y}\left[\int_0^\infty \{F_{\varepsilon\,|\,h}(1 - E_{M,\varepsilon}) \times (1 - E_R)(1 - E_{S,y})Q\}\,dq\right]\right), \quad (6)$$

where the summations are taken over all hazard scenarios X_h and corresponding attack profiles Y_x for a given hazard type h. The vulnerability parameter can be interpreted as the degree of maximum credible (or possible) loss following a hazard event that captures both the inherent physical and security weaknesses associated with different system states (e.g., damage, functionality, etc.) of an asset and its key elements. In this sense, this parameter provides a measure for overall vulnerability that is in agreement with the definition of vulnerability provided in Reference 28.

Combined, Equations (5) and (6) represent the general formula for all-hazards risk analysis for critical asset protection. The total all-hazards risk associated with an asset can be obtained by summing the risks calculated in Equation (5) over all hazards. Note that the simple expression in Equation (6) has roughly the same form as the common expression for security risk:[26]

$$\text{Risk} = \text{Consequence} \times \text{Vulnerability} \times \text{Threat}, \quad (7)$$

where consequence is specified as the maximum credible (or possible) loss, vulnerability is characterized by the expression for overall vulnerability in Equation (6), and threat is the annual rate of hazard occurrence for the asset. The advantage of Equation (5) over Equation (7) is the clear meaning associated with each parameter; this quality facilitates the data collection process.[3] Depending on the resources available to conduct analysis, Equation (5) can be used to calculate risk either through detailed analysis of each parameter in Equation (6) or through direct elicitation of V_h from experts.

As noted in Section 2, to provide actionable risk information means to provide both a measure of risk and suggestions on what to do about it. A simple expression for determining the sensitivity, S, of the total expected risk, R, with respect to a small improvement in the mean value of each risk contributor (parameter) is given by:

$$S_i = \frac{1}{p}\frac{\Delta_p R_i}{R}, \quad (8)$$

where $\Delta_p R_i$ is the change in risk due to a favorable fractional change p in the value of the ith risk contributor. Equation (8) yields the ratio of fractional reduction in risk due to a small uniform favorable percentage change in the value of each risk contributor, which is similar in concept to the risk reduction worth importance measure described in Reference 19.

Combined with the risk profiles determined for each hazard, sensitivity and importance measures provide insight into which risk contributors should be targeted for cost-effective risk reduction, and thus communicate actionable risk information. In addition to Equation (8), other importance measures can also be used, such as variance based on moment-independent uncertainty importance methods described in Reference 24.

3.6. Benefit-Cost Analysis

Benefit-cost analysis determines the cost effectiveness of proposed countermeasures and consequence mitigation strategies for reducing the risk associated with an asset or portfolio of assets. The benefit-to-cost ratio for a given investment alternative can be calculated as:[2]

$$\text{Benefit-to-Cost Ratio } (B/C) = \frac{B}{C}, \quad (9)$$

where the benefit B is the difference between the risk before and after implementation expressed in dollars

per year, and the cost C is the equivalent annual cost to implement and sustain the risk mitigation action over a specified time horizon. The probability that a target benefit-to-cost ratio, α, will be realized can be determined as:[2]

$$\Pr\left(\frac{B}{C} \geq \alpha\right) = 1 - \Pr\left(B - \alpha C \leq 0\right). \tag{10}$$

The selection of a best risk reduction alternative from a cost-effectiveness standpoint seeks to maximize the probability of realizing the target benefit-cost ratio. Alternatively, risk reduction strategies can be ranked according to the benefit cost ratio α^p that yields a probability of exceedence equal to p. Moreover, Equations (9) and (10) can be used to set limits on costs to achieve risk reduction objectives.

4. PORTFOLIO-LEVEL ANALYSIS

The overall process for portfolio-level risk assessment is similar to the asset-level analysis described in the previous section and shown in Fig. 1, the main differences being that multiple assets are considered according to the definition of the portfolio and that all losses are assessed from a portfolio perspective. Several cases can be identified that fall under the domain of portfolio-level analysis such as: (1) a set of assets, (2) a particular sector that extends over a geographic area, such as electric generation and distribution, and (3) a region, such as a jurisdiction or a city.

4.1. Portfolio Consequence and Criticality Assessment

The primary difference between asset and portfolio-level analysis risk analysis concerns the assessment of loss. While asset-level analysis estimates loss with respect to the asset, in general portfolio-level analysis considers both direct asset losses and indirect portfolio or system losses arising from physical geographic, cyber, and logical interdependencies.[18] Furthermore, interdependencies can be internal to the portfolio, or arise from external interactions between portfolio assets in the external world.

Let A be a portfolio of assets a, where $a \in A$. The expression for total portfolio economic loss, L_A, for a given hazard scenario afflicting asset $b \in A$ can be written as:

$$L_A = L_D + L_I, \tag{11}$$

where L_D is the direct economic loss (or aggregate loss as appropriate) to the asset calculated from Equation (1) assuming a portfolio perspective, and L_I gives the loss due to interdependency effects:

$$L_I = \sum_{\substack{a \in A \\ a \neq b}} L_{I,a}, \tag{12}$$

where L_I expresses the contribution to total interdependency loss for each portfolio asset.

While Equation (11) may appear simple, calculating portfolio losses in Equation (12) considering the full scope of interdependency effects is a significant challenge, particularly due to the highly nonlinear nature of interdependencies, substitution effects, and so forth.[18] By making some assumptions, however, a relatively simple expression for estimating first-order losses due to interdependency effects can be obtained as:

$$L_I = \left(\mathrm{c}_A^T \mathbf{K}_A \mathrm{u}_b\right) \cdot L_{T,b}, \tag{13}$$

where c_A^T is a vector that assigns a cost per unit time of disruption for each asset in the portfolio, $\mathbf{K}_A$ is the portfolio interdependency matrix where elements k_{ij} give the percentage degree of disruption to asset a_i due to complete loss of asset a_j ($a_i, a_j \in A$), $\mathbf{u}_b$ is a disruption vector with elements u_i that take on the value of the percentage service disruption for i corresponding to asset b (zero otherwise), and $L_{T,b}$ is the time to recover lost functionality of asset b (i.e., recuperation time determined from Equation (1) for the asset). The following assumptions were made to justify the form of Equation (13).

1. Only first-order interdependencies are considered. While second- and third-order interdependencies are by no means unimportant, their complexity and unpredictability make them difficult to manage using a model that looks at the connection between individual assets.
2. Substitution of services is not considered. The model makes the conservative assumption that the interdependent assets will not make any nonimmediate substitutions beyond what is nominally available in the market relating to the asset.
3. The degree of degradation of an asset function is linearly proportional to the degree of degradation in its dependencies. This assumption justifies the use of the interdependency matrix $\mathbf{K}_A$ with elements k_{ij} that linearly map disruption of the initiating asset to percentage disruption of interdependent assets.

4. The loss associated attributed to disruption of an asset is proportional to the degree of disruption and the time to reconstitute its function. This assumption justifies the use of the cost vector c_A^T to map percent damage to economic loss, and use of the recuperation time L_{T0} of the initiating asset to scale it according to time. This assumption is conservative in the sense that with increasing time, portfolios such as a region or infrastructure sector will tend to compensate for the loss via substitution.

5. DISCUSSION AND NOTIONAL EXAMPLES

This section discusses applications and practical implementation of the proposed model presented in Sections 3 and 4 through several examples: (1) an example demonstrating a detailed asset analysis of a single hazard scenario and attack profile, (2) an example demonstrating the methodology for high-level risk analysis, and (3) an example demonstrating portfolio interdependency analysis.

5.1. Example 1: Detailed Asset Risk Assessment

This example considers an asset consisting of a single key element protected by two concentric rings of protection as shown in Fig. 2. This example represents the simplest case of asset-level analysis since there is no potential for collateral damage at other key elements, and the security model has only one primary intrusion path. The objective of this example is to assess consequence, probability of adversary success, and hazard likelihood in turn to determine whether the risks are significant from the perspective of the decisionmaker.

Assuming the asset to be a building and focusing strictly on human-caused hazards, the scenario identification phase identified three relevant hazard scenarios (see Table II): "explosive attack against the building," "projectile attack against the building," and "incendiary attack against the building." For the purposes of illustrating the methodology, this example will only consider the explosive attack scenario.

Proceeding to the consequence and criticality assessment phase, the maximum credible loss for each of the four loss dimensions described in Table III is given as shown in Table V. Expressed in matrix form, the fragility of the building to explosive effects is provided in Table VI assuming detonation at the boundary of the vehicle barrier, which is conservative since detonation any place farther away from this boundary results in a lesser intensity imparted to the building. The mitigation effectiveness for each loss dimension as a function of damage state is provided in Table VII as a matrix, where for simplicity the degree of loss for each damage level is assumed to be normally distributed with mean and coefficient of variation specified. Assuming that little information is available to form a credible judgment on the effectiveness of emergency response, a conservative value of zero is assumed for this parameter ($E_R = 0$). Also, the number of casualties is assumed to be a function of building damage; however, in most practical applications the damage to people and adjacent elements would be included in the analysis.

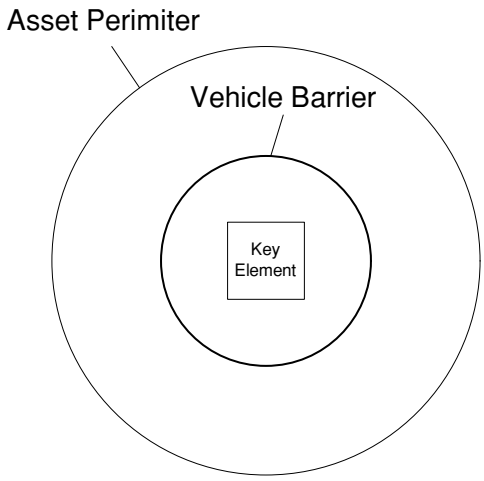

Fig. 2. Notional asset with one key element and concentric rings of protection.

Table V. Maximum Credible Loss for the Hazard Scenario

Loss Dimension	Maximum Credible Loss, L_{MC}
Casualty	500 Fatality equivalents
Economic	$10,000,000
Mission disruption	100%
Recuperation time	One year

Table VI. Fragility Matrix for the Key Element

	Hazard Intensity, q (pounds TNT) Ranges			
Damage Level	1–10	10–100	100–1000	>1000
No damage	0.9	0.4	0.0	0.0
Partial damage	0.1	0.5	0.5	0.0
Complete damage	0.0	0.1	0.5	1.0

Table VII. Mitigation Effectiveness Matrix for the Hazard Scenario

	Mitigation Effectiveness for Each Loss Dimension, E_M			
Damage Level	Casualty	Economic	Service Disruption	Recuperation Time
No damage	0.02 (0.25)	0.002 (0.25)	0.20 (0.25)	0.10 (0.30)
Partial damage	0.40 (0.25)	0.20 (0.25)	0.95 (0.01)	0.25 (0.30)
Complete damage	0.90 (0.25)	1.00 (0)	1.00 (0)	1.00 (0)

Note: Coefficient of variation (COV) for entries shown in parentheses.

At this point, the decisionmaker might be unsure of whether to proceed with additional analysis. Say, for example, that the decisionmaker only wants to pay attention to those scenarios that would exceed 50 or more fatalities or equivalent economic damages of $7,500,000 with probability 0.5. From Equation (1), the loss distribution as a function of intensity for casualty, economic, and aggregate loss is determined as shown in Table VIII assuming a $5,000,000 statistical value of life and $250,000/year per percent lost productivity. The probability of exceeding the threshold values is given in Table IX for each hazard intensity. These results indicate that a 10 to 100 lb-TNT explosive or larger may result in losses that exceed the decisionmaker's threshold. If the decisionmaker were to take a precautionary position, he or she could decide at this point to mitigate this potential loss through such options as hardening, adding redundancy, or enhancing response capabilities. For the purposes of this example, however, the decisionmaker will continue through the entire risk analysis process to obtain a risk profile for the explosive hazard scenario.

According to the security vulnerability phase, there is only one representative intrusion path from the asset perimeter given that security measures are symmetric with respect to the key element. Furthermore, assume that the decisionmaker is concerned about vehicle-borne explosive devices. The attack profile defined by the combination of intrusion path and delivery system (i.e., vehicle bomb) provides the basis to evaluate the effectiveness of the security system considering all protective measures to detect, delay, respond to, and neutralize the adversary. Assume that a security systems analysis such as that described in References 8 and 9 yielded a value of $E_S = 0.8$ for security system effectiveness. Furthermore, assume that the probability of successful execution $P_K = 1$ and the discrete distribution of hazard intensity $Q(q)$ for the vehicle-borne delivery system is $Q(0\text{–}10) = 0.0$, $Q(10\text{–}100) = 0.1$, $Q(100\text{–}1000) = 0.7$, and $Q(>1000) = 0.2$, where the values in parentheses denote the hazard intensity in pounds TNT. From Equation (2), E_S, P_K, and Q yield the probability of adversary success as a function of hazard intensity as shown in Table X. Combined, the probability of adversary success in Table X and loss given success in Table VIII yields a *conditional risk* of 266 fatalities per occurrence with a coefficient of variation of 0.15 (for casualties), and $18-million per occurrence with a coefficient of variation of 0.08 (for economic loss). The conditional risk could be used as the basis for investment decisions or for the purpose of screening attack profiles.

A useful exercise at this point is to back-calculate the minimum annual rate of occurrence for the attack profile needed to yield an unacceptable risk profile based on the conditional risk and Equations (3) and (4). Assuming that the decisionmaker desires to mitigate any risk that exceeds 5 fatalities per year or $500,000 in property damage with a probability of 0.5 or greater, the annual frequency must not exceed

Table VIII. Loss Distribution for the Hazard Scenario

	Loss Distribution, L (from Equation (2))		
Hazard Intensity, q (Pounds TNT)	Casualty Loss (Fatalities per Event)	Economic Loss ($-Million per Event)	Aggregate Loss ($-Million per Event)
0–10	29 (0.19)	1.0 (0.25)	146 (0.19)
10–100	149 (0.18)	6.3 (0.19)	751 (0.18)
100–1000	325 (0.19)	21 (0.11)	1,646 (0.19)
>1000	450 (0.25)	35 (0.00)	2,285 (0.24)

Note: Coefficient of variation (COV) for entries shown in parentheses. Uncertainties propagated using the techniques in Reference 31.

Table IX. Probability of Exceeding Threshold Values

Hazard Intensity, q (Pounds TNT)	Probability of Exceeding Threshold	
	Casualty Loss (35 Fatalities)	Economic Loss ($7,500,000)
0–10	0.14	0.00
10–100	1.00	0.17
100–1000	1.00	1.00
>1000	1.00	1.00

Note: Threshold values given in parentheses under each loss heading.

Table X. Probability of Adversary Success as a Function of Intensity

Hazard Intensity, q (Pounds TNT)	Probability of Adversary Success, p_S (Equation (3))
0–10	0.00
10–100	0.08
100–1000	0.56
>1000	0.16

0.019 events per year (assuming this parameter is normally distributed). Assuming that the baseline annual rate of occurrence for an explosive attack was estimated to be $\lambda_0 = 0.05$ per year with a coefficient of variation of 0.3, and that the profile attractiveness, scenario attractiveness, and asset attractiveness were assessed as $A_P = 1.0$, $A_S = 1.0$, and $A_A = 0.35$ from hazard likelihood assessment, the estimated annual attack profile rate of occurrence is 0.018 with coefficient of variation of 0.3 according to Equation (3). Moreover, combining these values with the loss distribution from Table VIII and probability of adversary success from Table X yields an expected risk of 4.7 fatalities per year with a coefficient of variation of 0.33 (casualty) and $314,983 per year with a coefficient of variation of 0.41 (economic). Clearly, these risk results do not exceed the decisionmaker's threshold.

5.2. Example 2: High-Level Regional Risk Assessment

This example demonstrates the application of the risk formula in Equation (5) for the case of a high-level portfolio risk analysis for a region. This situation would be encountered if a decisionmaker desires a rapid assessment of regional all-hazards risk, such as could be the case given limited time and analytical resources to conduct a hazard identification and risk analysis (HIRA) as part of the risk assessment requirements of the U.S. government's Hazard Mitigation Grant Program.[29] Despite the apparent simplicity of this equation and its assessment, it offers a more defensible way to go about assessing risks as compared to traditional qualitative risk-rating systems.[30]

Following the procedures in the scenario identification phase for portfolio analysis, a set of relevant hazard scenarios for the region can be established from those hazard types listed in Table I by screening out those scenarios that are deemed unlikely or inconsequential. For the purposes of this example, only a subset of the hazards in Table I is considered, as shown in Table XI. Further assume that only casualty risks are of concern to the decisionmaker. Following each step of the proposed methodology in turn, data for maximum credible loss, vulnerability, and annual hazard frequency to support risk assessment for each hazard would be elicited from subject matter experts drawing on previous studies, available data, intelligence reports, and reasonable assumptions to obtain risk results such as those shown in Table XI. Based on these risk estimates, the hazard risk profiles

Hazard	Maximum Credible Loss (Fatalities)	Vulnerability	Annual Rate of Occurrence in Region	Casualty Risk	Sensitivity
Major hurricane	10,000	0.2 (0.25)	0.2 (0.2)	400 (0.32)	0.80
Tornado	100	0.3 (0.25)	2 (0.2)	60 (0.32)	0.12
Drought	0	0.2 (0.25)	0.1 (0.2)	0 (0.32)	0.00
Winter storm	100	0.01 (0.25)	3 (0.2)	3 (0.32)	0.01
Nuclear attack	500,000	0.8 (0.25)	1.00E-06 (0.3)	0.4 (0.39)	0.00
Explosive attack	300	0.3 (0.25)	0.05 (0.3)	4.5 (0.39)	0.01
Airplane as projectile	5,000	0.1 (0.25)	0.01 (0.3)	5 (0.39)	0.01
Biological attack	100,000	0.2 (0.25)	1.00E-03 (0.3)	20 (0.39)	0.04
Industrial accident	2,500	0.01 (0.25)	0.2 (0.3)	5 (0.39)	0.01

Note: Coefficient of variation (COV) for entries shown in parentheses.

Table XI. Regional Risk Assessment Results

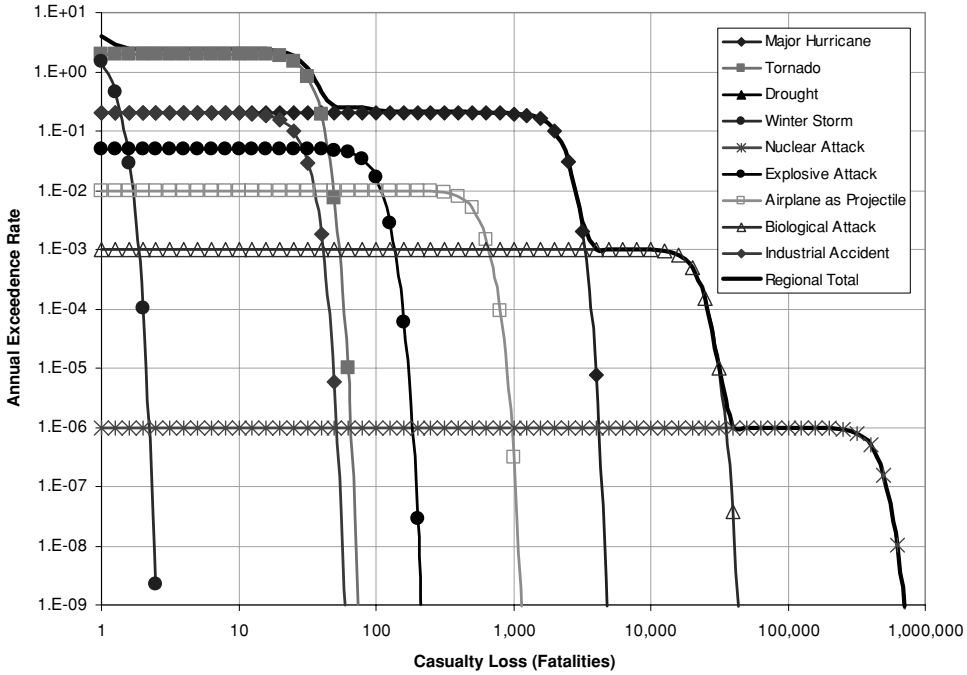

Fig. 3. Loss exceedence curve for each regional hazard.

for the region can be expressed in the form of loss-exceedence curves[2] as shown in Fig. 3. Combined, the total expected all-hazards risk for the region is 498 fatalities per year.

To turn the above risk assessment into an actionable risk assessment product, the sensitivity of the results to small favorable changes in each risk contributor must be included so as to identify areas for cost-effective risk reduction. Using the results in Table XI with Equation (8), a rank-ordered list of hazards based on the sensitivity of expected risk attributed to the changes in the vulnerability was obtained as shown in the last column of Table XI. These results suggest that hurricanes are the greatest contributor to all-hazards risk in the region.

The next question a decisionmaker might ask is how much should be invested to reduce the region's vulnerability to hurricanes by a factor of 4 (assuming a $5,000,000 statistical value of life) given that a benefit-to-cost ratio of 1.5 is desired with a probability of 0.75. Assuming that the cost of a proposed mitigation action is modeled with a random variable, tradeoffs need to be made between expected value (in dollars per year) and its uncertainty. Following the procedures in Section 3.6, Fig. 4 graphically shows the tradeoff between expected value and coefficient of variation that achieves the target benefit-cost ratio. From this figure, the decisionmaker can evaluate whether a proposed mitigation option is cost effective and the value of data collection efforts to reduce the coefficient of variation.

5.3. Example 3: Portfolio Interdependency Analysis

This example illustrates the assessment of interdependency losses associated with portfolio-level consequence and criticality assessment. Consider a portfolio of three assets—Asset A, Asset B, and Asset C—with interdependency matrix $\mathbf{K}_A$ and loss vector $\mathbf{c}_A$, as shown in Table XII. Furthermore, consider a single hazard type affecting this portfolio, and assume point estimates for the degree of functional degradation and recuperation time for each asset following each hazard event (i.e., hazard afflicting an asset) are given in Table XIII. From Equation (13) and the data from Tables XII and XIII, the total interdependency loss for each hazard event was calculated as shown in last column of Table XIII.

6. CONCLUSIONS

This article proposes a quantitative all-hazards framework for critical asset and portfolio risk analysis

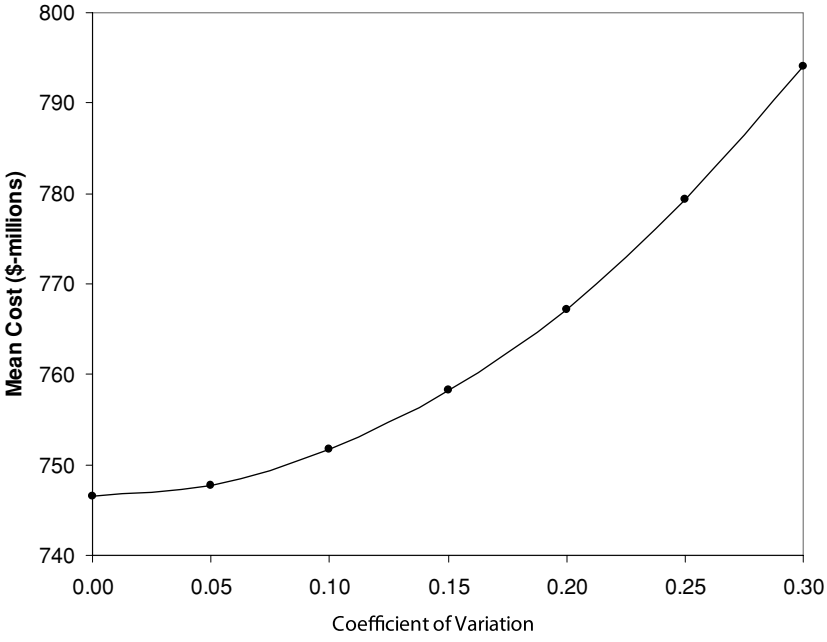

Fig. 4. Trade-off curve between expected cost and uncertainty for a cost-effective investment alternative.

Table XII. Portfolio Interdependency Matrix and Daily Cost of Disruption

Asset	Percent Disruption Due to Loss of Asset			Cost per Day of Disruption (Dollars)
	A	B	C	
Asset A	NA	1.0	0.1	2,000,000
Asset B	0.3	NA	0.4	1,000,000
Asset C	0.8	0.6	NA	5,000,000

Table XIII. Data from Asset-Level Analysis of Each Asset and Resulting Interdependency Loss

Affected Asset	Service Disruption (%/Event)	Recuperation Time (Days/Event)	Interdependency Loss (Dollars/Event)
Asset A	0.4	5	8,600,000
Asset B	0.2	10	10,000,000
Asset C	0.9	15	8,100,000

(CAPRA). Following a high-level development of the quantitative details underlying each phase, a general formula for all-hazards risk analysis was obtained that resembles the traditional security risk model where risk is the product of consequence, vulnerability, and threat, though with clear meanings assigned to each parameter. Furthermore, a simple first-order technique for capturing the consequences resulting from portfolio interdependencies was provided. The details of how to perform the assessment are dependent on the asset type, portfolio characteristics, and hazard types, and may vary based on the needs of the decisionmaker and time and analytical resources available to support analysis.

The data requirements for CAPRA include both historical information and expert opinions, and uncertainty is accommodated as appropriate using standard techniques for uncertainty propagation and representation.[31] Recent work suggests data from previous risk and vulnerability assessments, assessments of similar facilities or regions, and expert opinion to construct parameter distributions can be aggregated using evidence-theory-based techniques.[32]

ACKNOWLEDGMENTS

Funding for the study described in this article was provided by the Maryland Emergency Management Agency (MEMA) and the Maryland Governor's Office for Homeland Security. The arrangement between the University of Maryland (UMD) and MEMA does not require UMD to obtain approval from MEMA prior to submission of a manuscript to an academic journal. The opinions stated in this article

are those of the authors and do not necessarily reflect the opinions of MEMA, the Maryland Governor's Office of Homeland Security, or the state of Maryland.

The authors wish to thank MEMA and its representatives, including Mr. Daniel Green, Mr. Mel Blizzard, Mr. Adam Trister, Mr. Christopher Geldart, and Mr. Michael Beland, for their support. We also thank the anonymous reviewers for their helpful comments and suggestions.

REFERENCES

1. Department of Homeland Security. (2006). *National Infrastructure Protection Plan*. Available at: http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf. Last accessed 27 November 2006.
2. Ayyub, B. M. (2003). *Risk Analysis in Engineering and Economics*. FL: Chapman & Hall/CRC Press.
3. Ayyub, B. M. (2001). *Elicitation of Expert Opinions for Uncertainty and Risks*. FL: CRC Press.
4. Pate-Cornell, M. E. (1986). Warning systems and risk management. *Risk Analysis*, *6*(2), 223–234.
5. Hoffman, B. (1998). *Inside Terrorism*. New York: Columbia University Press.
6. Jackson, B. A. (2001). Technology acquisition by terrorist groups: Threat assessment informed by lessons from private sector technology adoption. *Studies in Conflict and Terrorism*, *24*, 183–213.
7. Sandler, T., & Lapan, H. E. (1988). The calculus of dissent: An analysis of terrorist's choice of targets. *Synthese*, *76*, 245–261.
8. Hicks, M. J., Snell, M. S., Sandoval, J. S., & Potter, C. S. (1999). Physical protection systems—Cost and performance analysis: A case study. *IEEE AES Systems Magazine*, April.
9. Dessent, G. H. (1987). Prison perimeter cost effectiveness. *Journal of the Operational Research Society*, *10*, 975–980.
10. Martz, H. F., & Johnson, M. E. (1987). Risk analysis of terrorist attacks. *Risk Analysis*, *7*(1), 35–47.
11. Pate-Cornell, M. E., & Guikema, S. (2002). Probabilistic modeling of terrorist threats: A systems analysis approach to setting priorities among countermeasures. *Military Operations Research*, *7*(4), 5–23.
12. Garrick, B. J., Hall, J. E., Kilger, M., McDonald, J. C., O'Toole, T., Probst, P. S., Parker, E. R., Rosenthal, R., Trivelpiece, A. W., Van Arsdale, L. A., & Zebroski, E. L. (2004). Confronting the risks of terrorism: Making the right decisions. *Reliability Engineering and System Safety*, *86*(2), 129–176.
13. Kowalski, W. J. (2003). *Immune Building Systems Technology*. New York: McGraw-Hill.
14. Woo, G. (1999). *The Mathematics of Natural Catastrophes*. UK: Imperial College Press.
15. Cornell, C. A. (1968). Engineering seismic risk analysis. *Bulletin of the Seismological Society of America*, *58*(5), 1583–1606.
16. Augusti, G., Borri, C., & Niemann, H.-J. (2001). Is Aeolian risk as significant as other environmental risks? *Reliability Engineering and System Safety*, *74*, 227–237.
17. Ezell, B. C., Farr, J. V., & Wiese, I. (2000). Infrastructure risk analysis model. *Journal of Infrastructure Systems*, *6*(3), 114–117.
18. Rinaldi, S. M., Peerenboom, J. P., & Kelly, T. K. (2001). Complex networks: Identifying, understanding, and analyzing critical infrastructure interdependencies. *IEEE Control Systems Magazine*, December.
19. Modarres, M. M., Kaminskiy, M., & Krivstov, V. (1999). *Reliability Engineering and Risk Analysis: A Practical Guide*. New York: Marcel Deckker.
20. McGill, W. L., Ayyub, B. M., & Kaminskiy, M. (2007). Risk analysis for critical asset protection. *Risk Analysis*, forthcoming.
21. Waugh, W. L. (2005). Terrorism and the all-hazards model. *Journal of Emergency Management*, *3*(2), 8–10.
22. Tobin, G. A., & Montz, B. E. (1997). *Natural Hazards: Explanation and Integration*. Guilford Press.
23. Kipfer, B. A. (Ed.). (2005). *Webster's New Millennium Dictionary of English* (preview edition v. 0.9.6). Long Beach, CA: Lexico Publishing Group.
24. Borgonovo, E. (2006). Measuring uncertainty importance: Investigation and comparison of alternative approaches. *Risk Analysis*, *26*(5), 1349–1361.
25. Andsten, R. S., & Vaurio, J. K. (1992). Sensitivity, uncertainty, and importance analysis of a risk assessment. *Nuclear Technology*, *98*, 160–170.
26. Broder, J. F. (1984). *Risk Analysis and the Security Survey*. MA: Butterworth Publishers.
27. Radasky, W. A., Baum, C. E., & Wik, M. W. (2004). Introduction to the special issue on high-power electromagnetics (HPEM) and intentional electromagnetic interference. *IEEE Transactions on Electromagnetic Compatibility*, *46*(3), 314–321.
28. Haimes, Y. Y. (2006). On the definition of vulnerabilities in measuring risks to infrastructures. *Risk Analysis*, *26*(2), 293–296.
29. 44 C.F.R. Parts 201 and 206. Available at http://www.fema.gov/txt/help/fr02-4321.txt.
30. Cox, L. A., Babayev, D., & Huber, W. (2005). Some limitations of qualitative risk rating systems. *Risk Analysis*, *25*(3), 651–662.
31. Ayyub, B. M., & Klir, G. J. (2006). *Uncertainty Modeling and Analysis in Engineering and the Sciences*. FL: Chapman & Hall/CRC Press.