Towards a Comparable Cross-Sector Risk Analysis: RAMCAP Revisited

Richard White, Aaron Burkhart, Terrance Boult, Edward Chow

Chapter 13

TOWARDS A COMPARABLE CROSS-SECTOR RISK ANALYSIS: RAMCAP REVISITED

Richard White, Aaron Burkhart, Terrance Boult and Edward Chow

Abstract The search for a uniform risk analysis approach for critical infrastructures has prompted a reexamination of the Risk Analysis and Management for Critical Asset Protection (RAMCAP) methodology to see if it can accommodate emerging threats from climate change, aging infrastructure and cyber attacks. This chapter examines the challenges involved in taking a site-specific formulation and turning it into a general model capable of analyzing performance under a full range of simulated conditions. The AWWA J100-10 standard provides the blueprint for a basic RAMCAP model that calculates risk as an attenuation of consequences via probability estimates of vulnerability, threat, resilience and countermeasures. The RAMCAP model was subjected to varying scenario loads in deterministic simulations that examined all hypothetical conditions and probabilistic simulations that examined likely conditions. RAMCAP performance was measured by the average net benefit and represented by the distribution of component values. Contrary to expectations, RAMCAP performance did not improve as the number of scenarios increased in the simulations. The methods and results of this study may hold implications for other critical infrastructure risk methodologies that are based on consequence, threat and vulnerability.

Keywords: Lifeline infrastructures, risk analysis, RAMCAP methodology

1. Introduction

Concerns about the threats to the water and wastewater infrastructure posed by climate change, aging infrastructure and cyber attacks prompted the Science and Technology Directorate of the Department of Homeland Security to undertake the development of a new risk analysis standard that uniformly measures risk across all the lifeline infrastructures. According to the 2013 National

Infrastructure Protection Plan (NIPP) [23], the lifeline infrastructures include water, energy, transportation and communications, four of the sixteen sectors identified in Presidential Policy Directive 21 (PPD-21). Uniform risk analysis, the ability to compare risk analysis results across infrastructure assets and sectors, facilitates cost-benefit analysis and strategic planning that are critical to optimizing homeland security investments and safeguarding the nation from catastrophic incidents, both natural and human initiated. A uniform risk analysis can also help the Department of Homeland Security achieve its goal of measuring resilience and quantifying the efficacy of countermeasures – in other words, inform the President and Congress where we are, where we are going and at what cost.

The importance of a uniform risk analysis approach for critical infrastructures was recognized by the White House when it requested the American Society of Mechanical Engineers (ASME) to develop a methodology shortly after the terrorist attacks of September 11, 2001 [2]. In 2006, ASME released the final specifications of the Risk Analysis and Management for Critical Asset Protection (RAMCAP) methodology. RAMCAP is a seven-step process that assesses the risk to an asset as a product of threat, vulnerability, consequence, resilience and applied countermeasures. RAMCAP incorporates a reference set of 41 threat and hazard scenarios to guide estimates of its terms and render the methodology uniformly applicable across the infrastructure sectors, The 2006 National Infrastructure Protection Plan [22] recommended RAMCAP for conducting risk analyses, but the methodology was not mentioned in the 2009 and 2013 revisions of the national plan. No RAMCAP implementations are known to be employed today. However, RAMCAP continues to serve as the basis for the American Water Works Association (AWWA) J100-10 standard for Risk and Resilience Management of Water and Wastewater Systems [2].

In October 2014, the University of Colorado at Colorado Springs launched a RAMCAP needs assessment to develop the requirements for uniform risk analyses of lifeline infrastructures. The project involved three tasks: (i) analysis of emerging threat and hazard scenarios; (ii) analysis of RAMCAP performance; and (iii) analysis of RAMCAP requirements. Task 1, completed on December 31, 2014, identified 38 candidate scenarios with catastrophic potential for the water, electricity, aviation and Internet subsectors due to emerging threats from climate change, aging infrastructure and cyber attacks. After combining the similarities and eliminating redundancies, the candidate scenarios were reduced to thirteen nominee scenarios. Based on the Task 1 results, the question put before Task 2 was whether or not RAMCAP would perform better with 54 reference scenarios instead of its current 41 scenarios. This project was the first attempt to evaluate RAMCAP performance in general terms. This chapter discusses the RAMCAP methodology and its characteristics, and the unexpected results that ensued.

Table 1. Lifeline infrastructure risk analysis methodologies.

Sector/Sector Specific Plan	**Subsector**	**Sector Specific Agency**	**Risk Analysis Methodology**
Water/Wastewater	Water	EPA	VSAT/SEMS
Energy	Electricity	DoE	SAV
Transportation	Aviation	FAA	AMRA
Communications	Internet	DHS	CARMA

2. Background

The Homeland Security Act of 2002 prescribed a risk management approach for protecting the national critical infrastructure. Accordingly, the 2013 National Infrastructure Protection Plan specifies a risk management framework (RMF) to: (i) set goals; (ii) identify assets; (iii) prioritize risk; (iv) implement countermeasures; and (v) measure results [23]. The risk management framework is implemented with voluntary participation by industry through Sector Coordinating Councils that represent the sixteen infrastructure sectors identified in PPD-21. Every four years, the Sector Specific Agency (SSA) federal representative compiles a Sector Specific Plan (SSP) that summarizes the risk management efforts for the assigned sectors [15]. In 2010, the water, electricity, aviation and Internet subsectors identified the risk analysis methodologies used in support of Step 3 of the risk management framework (Table 1). For example, the VSAT methodology, which is employed by the water subsector, has been certified by the American Water Works Association to be RAMCAP compliant [2].

By one estimate, there are more than 250 critical infrastructure risk analysis methods [12]. The question is why are there so many methods? One answer may be that critical infrastructure risk analysis is beset by tradeoffs. Each method represents a different set of tradeoffs, determining both the type and the terms of the analysis, as shown in Figure 1.

Tradeoffs that determine the type of critical infrastructure risk analysis begin with the question of completeness: Does one analyze the asset or the network? Some researchers [3, 17] argue that an analysis is incomplete without considering interdependencies. Pederson et al. [18] identify 30 models that specialize in interdependency analysis. According to Creese et al. [7], interdependency models must be highly detailed to yield reasonable results. Since assets are part of the network detail, they must be assessed individually at some level. Thus, it is reasonable to begin risk analysis with an asset, but understand that the analysis is incomplete without including the network.

The next tradeoff involves qualitative risk analysis versus quantitative risk analysis. Qualitative risk analysis simplifies risk assessments by reducing inputs to a manageable set of judgments [6]. The risk and vulnerability analysis (RVA)

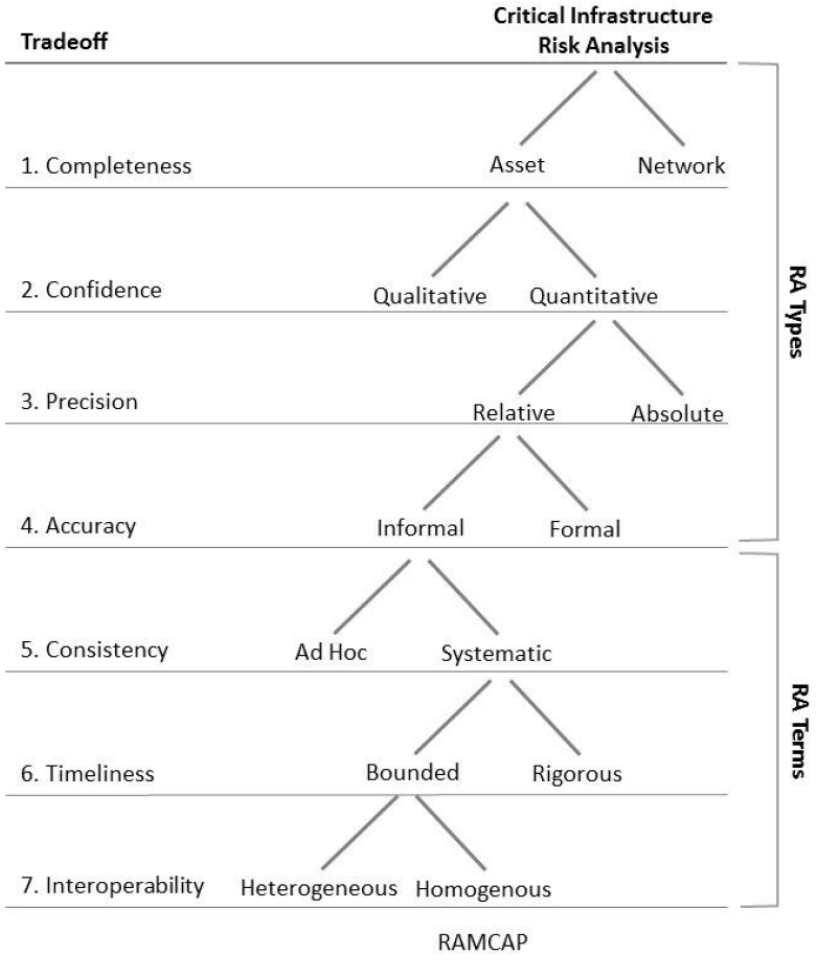

Figure 1. Critical infrastructure risk analysis tradeoffs.

methodology is one example of a qualitative approach [10]. A general criticism of qualitative methods, however, is that poor resolution of input data can lead to erroneous or misleading results [5, 6].

In contrast, quantitative methods promote confidence in results by reducing subjectivity [25]. However, quantitative risk analyses of critical infrastructures are tempered by precision. Unlike a disease, whose risk can be assessed in absolute terms [20], safety is not absolute and can only be assessed in a relative manner. This does not preclude the accuracy of results. Bayesian networks, conditional linear Gaussian networks, stochastic models and other formal quantitative methods have proven records of performance in diverse fields such as engineering, finance, healthcare and meteorology [1, 9, 11, 19]. What trips them up is the paucity of data for statistical analysis of catastrophic incidents, par-

ticularly those involving malicious human intent [16]. The attempts to work around this obstacle often lead to formulations that are neither transparent nor repeatable [16], rendering their consistent application problematic. The need for consistency has fueled the development of informal quantitative methods, many of which formulate risk as a function of threat, vulnerability and consequence. What distinguishes similar formulations [8] and even the U.S. Department of Homeland Security formulation itself [23] are the tradeoffs that are made in developing their terms.

Tradeoffs in developing terms for critical infrastructure risk analysis can take similar formulations and render them completely different from each other. Whereas the U.S. Department of Homeland Security has applied specific forms of the threat, vulnerability, consequence formulation [13], the National Infrastructure Protection Plan [23] does not specify any particular application. Therefore, it is not unreasonable for asset owners and operators to employ *ad hoc* methods for internal risk analyses and to assign threat, vulnerability and consequence values based on the best estimates of onsite personnel. To be sure, expert elicitation is an acceptable form of value estimation [16], but the consistency required for effective comparisons will not be realized without employing a formal system.

Rigorous systems for estimating threat, vulnerability and consequence values encompass various means of elicitation and modeling. The Delphi method is, perhaps, the best known rigorous system among the various elicitation methods [4]. Fault trees, event trees, reliability block diagrams and other causal analysis methods are well respected in the reliability and safety engineering discipline [16, 21, 24]. However, rigorous methods require substantial investments in time and resources that make them impractical for large-scale applications. Alternatively, a bounded system could elicit threat, vulnerability and consequence values with respect to a set number of scenarios as proposed in [14]. The approach may be less rigorous, but it is also less resource intensive and, thus, practical for large-scale applications.

RAMCAP takes the bounding process one step further by stipulating a homogenous set of reference scenarios. The same reference scenarios are used in each analysis to facilitate comparisons across assets. An important component of Task 2 of the RAMCAP needs assessment project was to determine if additional reference scenarios would improve RAMCAP performance.

3. Problem Formulation

The chosen method of analysis for Task 2 was to develop a basic RAMCAP model and evaluate its performance under varying load scenarios. According to the AWWA J100-10 specification, RAMCAP calculates a net benefit value and a benefit-cost ratio [2].

The gross benefit Gb is the amount of risk-resilience gained by implementing a particular countermeasure for a given threat-asset pair:

$$Gb = Rs - Rs' \tag{1}$$

Table 2. Seven-step RAMCAP process.

Step	Description
Step 1	Asset Characterization
Step 2	Threat Characterization
Step 3	Consequence Analysis
Step 4	Vulnerability Analysis
Step 5	Threat Analysis
Step 6	Risk and Resilience Analysis
Step 7	Risk and Resilience Management

where Rs and Rs' correspond to the risk-resilience values with and without a countermeasure, respectively.

The net benefit Nb is the sum of gross benefits for all the threat-asset pairs associated with a particular countermeasure:

$$Nb = \sum Gb \tag{2}$$

Note that the higher the net benefit Nb, the greater the reduction in risk.

The selection of the countermeasure to be implemented is determined by the benefit-cost ratio BCR, which is computed by dividing the net benefit Nb by the cost of the countermeasure. The higher the benefit-cost ratio BCR, the greater the return on investment. Because the task was to compare performance, the benefit-cost ratio BCR was not computed. Thus, RAMCAP model performance was based on the computed net benefit Nb.

RAMCAP calculates the net benefit Nb using the seven-step process shown in Table 2. The process is very site-specific, especially when characterizing assets and countermeasures, and assessing consequences, vulnerabilities, threats and resilience. About the only independent component is Step 2 (threat characterization), which is based on the 41 RAMCAP reference scenarios. The challenge was to apply this specific approach to a general situation and evaluate RAMCAP performance against every conceivable threat-asset pairing under a number of scenarios for every possible combination of consequence, vulnerability, threat, resilience and countermeasure.

A basic RAMCAP model was developed by following the AWWA J100-10 seven-step process beginning with Step 1 (asset characterization). In RAMCAP, an asset is part of a system comprising some component of a critical infrastructure [2]. For example, a generator is part of a power plant, which is a component of the electricity infrastructure. RAMCAP Step 1 identifies assets whose disruption or destruction could result in "worst reasonable consequences" [2]. RAMCAP leaves it to the user to decide what constitutes the worst reasonable consequences.

RAMCAP Step 1 is conceptualized by assuming some combination of assets A whose disruption or destruction have consequences C that are some fraction of the worst reasonable consequences WRC:

$$C = WRC \cdot A \tag{3}$$

where A takes values from the unit interval [0,1].

RAMCAP Step 2 (threat characterization) aligns the identified assets with the 41 reference scenarios to form threat-asset pairs [2]. The purpose of this step is to set up subsequent value estimations and risk calculations for each threat-asset pair. Because A represents a combination of assets, not individual assets, the effect of this step is to control the number of value estimations and risk calculations based on the number of reference scenarios. Accordingly, this is the step in the model where the number of reference scenarios is varied to evaluate RAMCAP performance under different loads.

RAMCAP Step 3 (consequence analysis) assigns a magnitude to the worst reasonable consequences WRC. The magnitude is the sum of the individual estimates of fatalities, injuries and financial and economic losses converted to point values using the provided charts [2]. RAMCAP calculates the worst reasonable consequences WRC for each threat-asset pair. Again, because A represents a combination of assets, WRC can be assigned a value of 1.0 and Equation (3) reduces to:

$$C = A \tag{4}$$

Note that this assignment avoids controversial conversions between personal injury and property damage. Also, it implicitly accounts for disruptive incidents as well as destructive incidents.

RAMCAP Steps 4 through 6 address the risk and resilience calculations. RAMCAP calculates the risk for each threat-asset pair as the product of consequence, threat and vulnerability. Step 4 estimates the probability that a given asset will be disrupted or destroyed by a given scenario for each threat-asset pair [2]. Step 5 estimates the probability that a given asset will be subjected to a given scenario for each threat-asset pair [2].

In Step 6.1, RAMCAP calculates the risk as [2]:

$$R = C \cdot T \cdot V \tag{5}$$

Upon substituting Equation (4) into Equation (5), the following risk formulation R is obtained:

$$R = A \cdot T \cdot V \tag{6}$$

RAMCAP Step 6.2 calculates the resilience [2]. According to the AWWA J100-10 standard, perfect resilience is the ability to withstand a threatened incident [2]. Since vulnerability accounts for the inherent ability of a system to withstand a threatened incident, resilience presumably accounts for external mitigating factors such as first responders, National Guard and other such capabilities from outside the fence.

Accordingly, RAMCAP calculates resilience as a fraction of risk by attenuating the duration D and severity S as follows [2]:

$$Rs = D \cdot S \cdot A \cdot T \cdot V \tag{7}$$

This computation is generalized by combining D and S into a single mitigating factor F ($F \in [0, 1]$) representing a percent reduction in expected consequences brought about by external agents.

A risk reduction multiplier M is then computed as:

$$M = 1 - F \tag{8}$$

and the resilience Rs is computed as:

$$Rs = M \cdot A \cdot T \cdot V \tag{9}$$

Substituting the risk R in Equation (6) into Equation (9) yields:

$$Rs = M \cdot R \tag{10}$$

RAMCAP Step 7 adds the effects of countermeasures to the risk and resilience calculations, and takes the difference before and after countermeasures are applied to calculate the gross benefit Gb, net benefit Nb and benefit-cost ratio BCR. RAMCAP Step 7.2 calculates the effect of countermeasures on risk and resilience [2]. Because countermeasures attenuate risk similar to resilience, a mitigating factor F' ($F' \in [0, 1]$) is used to compute a risk reduction multiplier M':

$$M' = 1 - F' \tag{11}$$

Next, a reduced risk profile after applying a given countermeasure R' is computed as:

$$R' = M' \cdot R \tag{12}$$

Applying the same countermeasure to resilience yields the increased resilience after applying a given countermeasure Rs':

$$Rs' = M \cdot R' \tag{13}$$

RAMCAP Step 7.6 calculates Gb, Nb and BCR [2]. For the purposes of this model, it is assumed that all evaluated countermeasures result in risk reduction, therefore $R > R'$ and $Rs > Rs'$. Gb is computed according to Equation (1) for all threat-asset pairs. Nb is computed according to Equation (2) as the sum of Gb for all threat-asset pairs.

The preceding formulations make it possible to construct a general model for evaluating RAMCAP performance across every conceivable threat-asset pairing under a varying number of scenarios for every possible combination of consequence, vulnerability, threat, resilience and countermeasure.

Algorithm 1 : Basic RAMCAP model.

Inputs: Number of scenarios n, resolution of simulation r, number of bins b
Output: Overall average net benefit $Nbavg$

```
1: x = 0
2: Nbsum = 0
3: Nbavg = 0
4: for A = r to 1 step r do
5:     for S = 1 to n step 1 do
6:         for V = r to 1 step r do
7:             for T = r to 1 step r do
8:                 R = A · T · V
9:                 for F = r to 1 step r do
10:                    M = 1 − F
11:                    Rs = M · R
12:                    Nb = 0
13:                    for F′ = r to 1 step r do
14:                        M′ = 1 − F′
15:                        R′ = M′ · R
16:                        Rs′ = M · R′
17:                        Gb = Rs − Rs′
18:                        Nb = Nb + Gb
19:                    end for (various countermeasures)
20:                    x = x + 1
21:                    Nbsum = Nbsum + Nb
22:                    Bin(Nb) = Bin(Nb) + 1
23:                end for (various resilience)
24:            end for (various threat probabilities)
25:        end for (various vulnerability probabilities)
26:    end for (various scenarios)
27: end for (various asset-WRC combinations)
28: Nbavg = Nbsum/x
```

Algorithm 1 specifies the basic RAMCAP model computations. The RAMCAP model has three inputs: (i) number of scenarios n; (ii) resolution of the simulation r; and (iii) number of bins b for tabulating the calculated net benefits. The reference scenarios are reduced to a set of threat and vulnerability values as determined by the simulation resolution r. Because the generated threat and vulnerability values span the entire range of combinations, they can represent any type of natural hazard or human initiated threat at any geographical location.

The simulation resolution r directly determines the magnitude of the generated values and number of loop iterations. By the same token, the resolution r indirectly determines the time required to execute the simulation. For each combination of assets A, the RAMCAP model computes the net benefit Nb for varying combinations of vulnerability, threat, resilience and countermeasure for the given number of scenarios. The calculated Nb values are tabulated in b bins in order to graph the resulting distribution. The calculated Nb values are

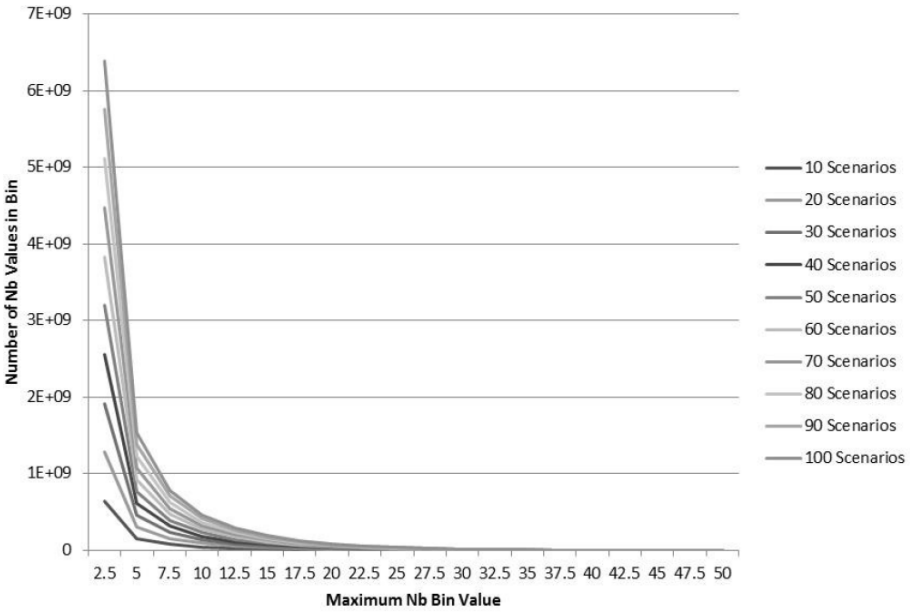

Figure 2. SIM1b $Nbavg$ value distributions for 10 to 100 scenarios.

also summed to compute an overall average net benefit $Nbavg$ for the entire simulation. Thus, RAMCAP performance for the n scenarios is characterized by the computed average net benefit $Nbavg$ and the corresponding distribution curve. The average net benefit $Nbavg$ was expected to increase as the number of scenarios increases; interestingly, this did not occur.

4. Results

The basic RAMCAP model specified in Algorithm 1 is designated as SIM1. SIM1 was almost immediately upgraded to SIM1b, which replaces the average net benefit $Nbavg$ calculation in Line 28 with the running average calculation:

$$Nbavg = Nbavg + (Nb - Nbavg)/x \tag{14}$$

in Line 21.

SIM1b was executed ten times while varying the number of scenarios n from 10 to 100 in increments of 10. For each execution, the simulation resolution r was set to 0.01 and the number of bins n was set to 20. Figure 2 presents the results. As expected, the distributions are proportional; the curves have the same shape, but the magnitudes are larger as the number of scenarios increases.

However, the SIM1b results in Figure 3 are surprising – $Nbavg$ decreases as the number of scenarios increases. The results may be explained by observing that, in Figure 2, the smaller Nb values on the left-hand side of the graph increase more than the larger Nb values on the right-hand side of the graph

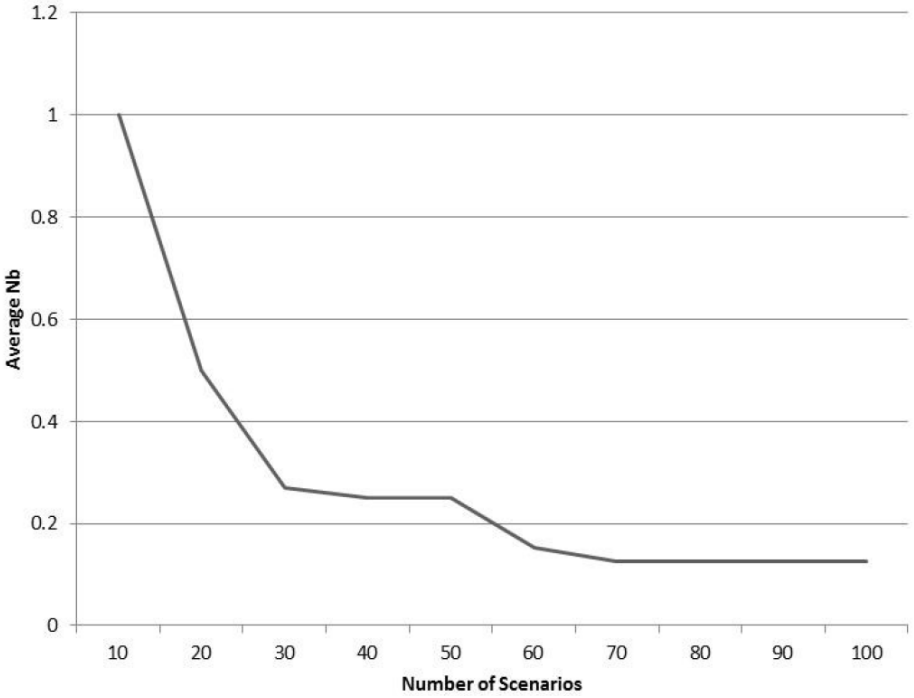

Figure 3. SIM1b *Nbavg* values over 10 to 100 scenarios.

as the number of scenarios increases. *Nbavg* is lower because the number of smaller *Nb* values outstrip the number of larger *Nb* values as the number of scenarios increases. Still, the counterintuitive implication is that adding more reference scenarios does not improve RAMCAP performance.

The curious results produced by SIM1b necessitated another look. SIM1b is a deterministic model that helps examine the hypothetical limits of RAMCAP performance. On the other hand, RAMCAP was specifically developed to analyze low-frequency, high-consequence events that are homeland security concerns. SIM2 was developed as a probabilistic model that generates random Gaussian values between 0 and 1 for A, T, V, M and M'. The calculated average net benefit *Nbavg* would be different for each execution. Consequently, SIM2 required multiple executions to calculate the average net benefit *Nbavg*.

Figure 4 plots the average net benefit *Nbavg* for 1,000 SIM2 executions for 40 scenarios at 0.05 simulation resolution with 20 bins. As shown in Figure 4, the average net benefit computed by SIM2 for 1,000 executions appears to be well behaved, clustering fairly tightly in the range between 0.2904 and 0.6954. The average of all these averages is 0.485125, which is considerably lower than the *Nbavg* value of 0.7199 computed by SIM1c. In fact, none of the SIM2 results approach the *Nbavg* values computed by SIM1c.

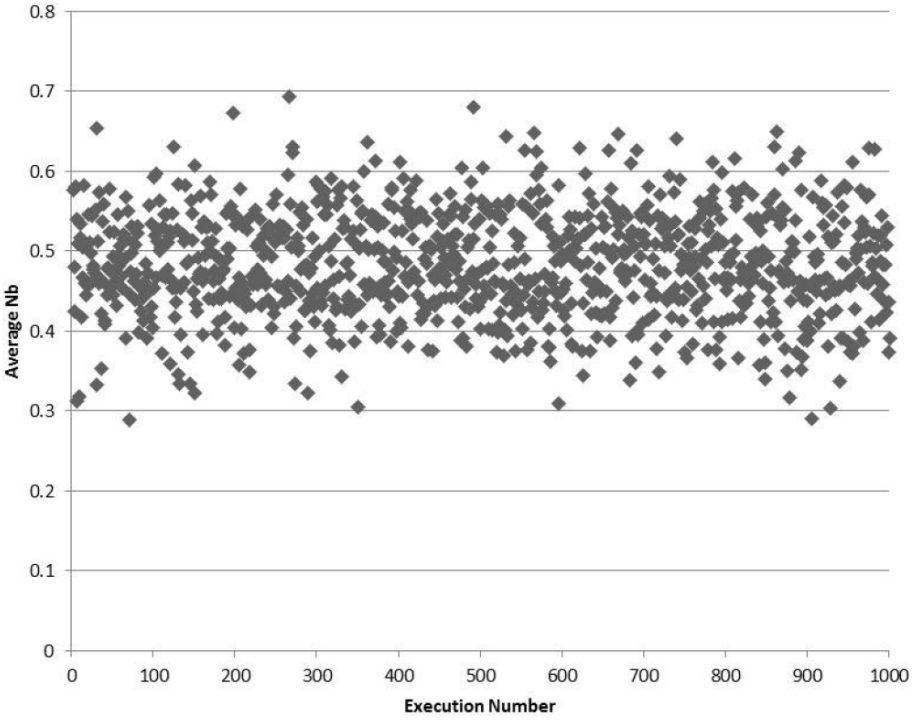

Figure 4. SIM2 *Nbavg* values for 1,000 executions.

Figure 5 may help explain the difference between the SIM2 and SIM1c results. As seen in Figure 5, the curve representing the SIM2 *Nbavg* distributions rises much higher in Bin 1 than that for SIM1c, pulling down the SIM2 *Nbavg* results as seen previously. SIM1c has an additional advantage because it has a larger number of higher values than SIM2; this is because the SIM1c curve cuts across and rises above the SIM2 curve in Figure 5. Given these observations, it is expected that the SIM2 *Nbavg* values would be generally lower, albeit no less valid, than the SIM1c *Nbavg* calculations.

Hence, the SIM1b experiment was repeated using SIM2. In particular, SIM2 was executed 100 times each for 10 to 100 scenarios. More iterations were possible, but 100 iterations required 29 hours even at a reduced simulation resolution of 0.05. Figure 6 presents the SIM2 results.

The SIM2 results in Figure 6 are somewhat misleading, suggesting a large fluctuation with no clear trend. In reality, a 0.024556 difference exists between the largest value of 0.495424 and the smallest value of 0.470868. A trend is apparent in Figure 7, when the SIM2 results are compared against the results obtained for the same execution using SIM1c.

Note that the simulation resolution was reduced from 0.01 for SIM1b to 0.05 for both SIM1c and SIM2, so the same downward trend seen in Figure 3 is not seen in Figure 7. However, the expected clear upward trend is also not seen in

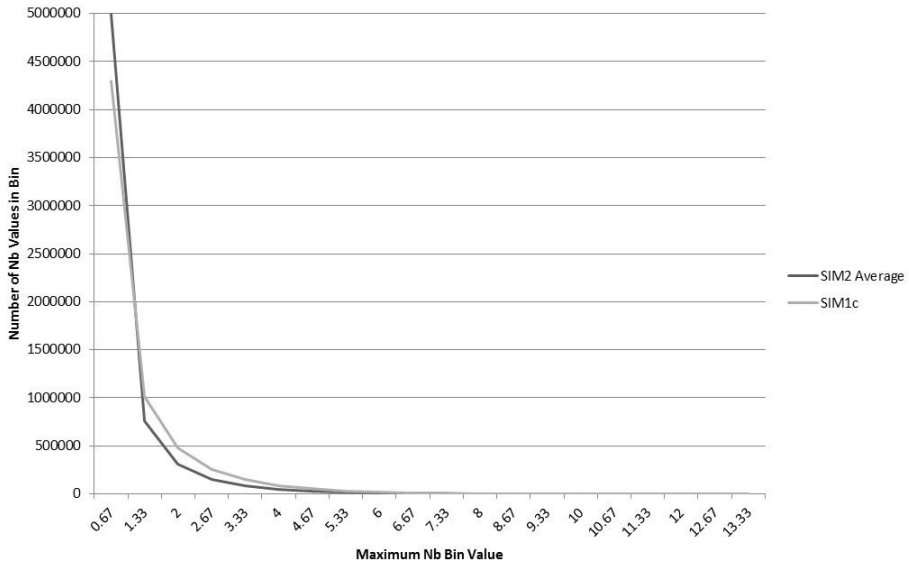

Figure 5. *Nb* value distributions for SIM2 and SIM1c.

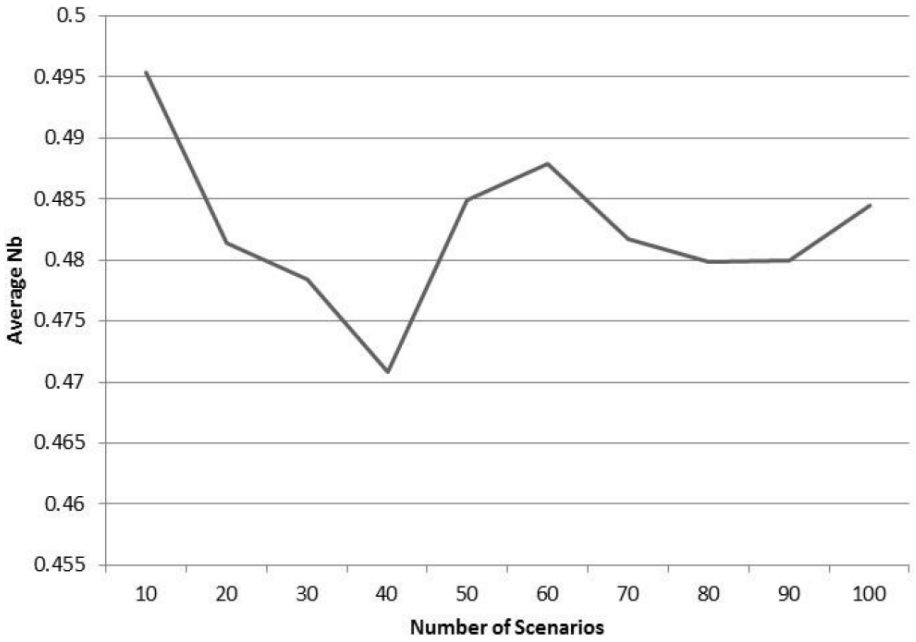

Figure 6. SIM2 *Nbavg* values for 100 executions of 10 to 100 scenarios.

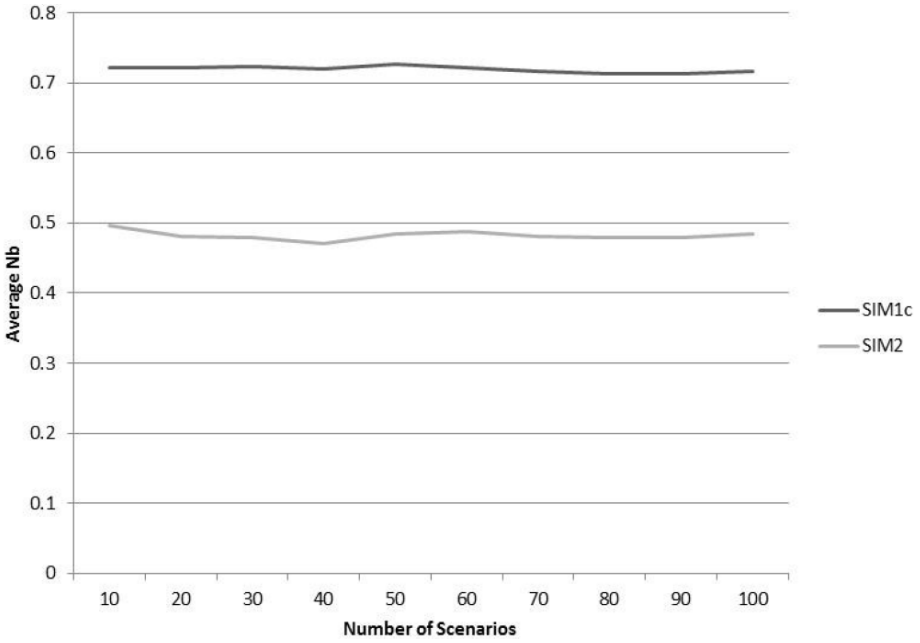

Figure 7. SIM2 and SIM1c results.

Figure 7. The results in Figure 7 support the previous observation that adding more reference scenarios does not improve RAMCAP performance.

5. Conclusions

The search for a uniform risk analysis methodology for critical infrastructures prompted a re-evaluation of RAMCAP to determine if it can accommodate emerging threats posed by climate change, aging infrastructure and cyber attacks. This research has examined the challenges of taking a site-specific formulation and turning it into a general model capable of analyzing performance under a full range of simulated conditions.

A basic RAMCAP model with a systematic attenuation of consequences based on estimations of probabilities for threat, vulnerability, resilience and countermeasures was developed. The model was made possible by formalizing the relationship between consequences, worst reasonable consequences and assets, and then normalizing the worst reasonable consequences. This insight eliminates the problems associated with defining consequences in terms of injury, death and damage; additionally, it implicitly covers disruptive as well as destructive catastrophes.

The model also considers resilience and countermeasures as risk mitigating factors. This insight simplifies the estimation of both terms and enables them to be incorporated as individual risk reduction multipliers. Simulations involving

10 to 100 scenarios quantified RAMCAP performance in terms of an average net benefit and net benefit distribution – the higher the net benefit, the better the performance. Since the scenario parameter only controls the number of internal iterations, it was expected that more scenarios would result in a higher average net benefit. However, this did not occur – as the number of scenarios increases, RAMCAP performance and the net benefit metric decrease.

The counterintuitive results prompted a second experiment using a probabilistic model. Instead of calculating parameter values, parameters were assigned random Gaussian values. The second experiment resulted in no improvement in RAMCAP performance. An examination of the corresponding distribution curves reveals that the magnitudes of the curves increase as the number of scenarios increases. However, as the number of scenarios increases, the number of lower net benefit values is proportionally higher than the number of larger net benefit values; the smaller values tend to outstrip the higher values, contributing to the decrease in the average net benefit value as the number of scenarios increases. The immediate implication is that, contrary to intuition, adding more reference scenarios does not improve RAMCAP performance. These counterintuitive results may also apply to other critical infrastructure risk methodologies that, like RAMCAP, are based on consequence, threat and vulnerability formulations.

References

[1] E. Adar and A. Wuchner, Risk management for critical infrastructure protection challenges, best practices and tools, *Proceedings of the First IEEE International Workshop on Critical Infrastructure Protection*, pp. 90–100, 2005.

[2] American Water Works Association, Risk and Resilience Management of Water and Wastewater Systems, Denver, Colorado, 2010.

[3] B. Carreras, D. Newman, P. Gradney, V. Lynch and I. Dobson, Interdependent risk in interacting infrastructure systems, *Proceedings of the Fortieth Annual Hawaii International Conference on System Sciences*, 2007.

[4] R. Cooke and L. Goossens, Expert judgment elicitation for risk assessments of critical infrastructures, *Journal of Risk Research*, vol. 7(6), pp. 643–656, 2004.

[5] L. Cox, What's wrong with risk matrices? *Risk Analysis*, vol. 28(2), pp. 497–512, 2008.

[6] L. Cox, D. Babayev and W. Huber, Some limitations of qualitative risk rating systems, *Risk Analysis*, vol. 25(3), pp. 651–662, 2005.

[7] S. Creese, M. Goldsmith and A. Adetoye, A logical high-level framework for critical infrastructure resilience and risk assessment, *Proceedings of the Third Workshop on Cyberspace Safety and Security*, pp. 7–14, 2011.

[8] D. Daniels and B. Ware, State/local CIP risk analysis: First results and emerging trends in the data, *Proceedings of the IEEE Conference on Technologies for Homeland Security*, pp. 393–400, 2009.

[9] M. Ghazel, Using stochastic Petri nets for level-crossing collision risk assessment, *IEEE Transactions on Intelligent Transportation Systems*, vol. 10(4), pp. 668–677, 2009.

[10] G. Giannopoulos, R. Filippini and M. Schimmer, Risk Assessment Methodologies for Critical Infrastructure Protection, Part 1: A State of the Art, JRC 70046, European Commission Joint Research Centre, Ispra, Italy, 2012.

[11] S. Lee, Probabilistic risk assessment for security requirements: A preliminary study, *Proceedings of the Fifth International Conference on Secure Software Integration and Reliability Improvement*, pp. 11–20, 2011.

[12] T. Lewis, R. Darken, T. Mackin and D. Dudenhoeffer, Model-based risk analysis for critical infrastructures, *WIT Transactions on State-of-the-Art in Science and Engineering*, vol. 54, pp. 3–19, 2012.

[13] T. Masse, S. O'Neil and J. Rollins, The Department of Homeland Security's Risk Assessment Methodology: Evolution, Issues and Options for Congress, CRS Report for Congress, RL33858, Congressional Research Service, Washington, DC, 2007.

[14] W. McGill, B. Ayyub and M. Kaminskiy, Risk analysis for critical asset protection, *Risk Analysis*, vol. 27(5), pp. 1265–1281, 2007.

[15] J. Moteff, Critical Infrastructures: Background, Policy and Implementation, CRS Report for Congress, RL30153, Congressional Research Service, Washington, DC, 2015.

[16] National Research Council, *Review of the Department of Homeland Security's Approach to Risk Analysis*, National Academies Press, Washington, DC, 2010.

[17] D. Newman, B. Nkei, B. Carreras, I. Dobson, V. Lynch and P. Gradney, Risk assessment in complex interacting infrastructure systems, *Proceedings of the Thirty-Eighth Annual Hawaii International Conference on System Sciences*, 2005.

[18] P. Pederson, D. Dudenhoeffer, S. Hartley and M. Permann, Critical Infrastructure Interdependency Modeling: A Survey of U.S. and International Research, INL/EXT-06-11464, Idaho National Laboratory, Idaho Falls, Idaho, 2006.

[19] J. Resurreccion and J. Santos, Stochastic modeling of manufacturing-based interdependent inventory for formulating sector prioritization strategies in reinforcing disaster preparedness, *Proceedings of the IEEE Systems and Information Engineering Design Symposium*, pp. 134–139, 2012.

[20] E. Schechtman, Odds ratio, relative risk, absolute risk reduction and the number needed to treat – Which of these should we use? *Value in Health*, vol. 5(5), pp. 431–436, 2002.

[21] M. Stamatelatos, Probabilistic Risk Assessment: What is it and Why is it Worth Performing it? NASA Office of Safety and Mission Assurance, National Aeronautics and Space Administration, Washington, DC, 2000.

[22] U.S. Department of Homeland Security, National Infrastructure Protection Plan, Washington, DC, 2006.

[23] U.S. Department of Homeland Security, National Infrastructure Protection Plan: Partnering for Critical Infrastructure Security and Resilience, Washington, DC, 2013.

[24] A. Volkanovski, M. Cepin and B. Mavko, Application of fault tree analysis for assessment of power system reliability, *Reliability Engineering and System Safety*, vol. 94(6), pp. 1116–1127, 2009.

[25] G. Woo, The evolution of terrorism risk modeling, *Journal of Reinsurance*, vol. 10(3), pp. 1–9, 2003.