Risk Analysis, Vol. 29, No. 12, 2009 DOI: 10.1111/j.1539-6924.2009.01310.x

On the Complex Definition of Risk: A Systems-Based Approach

Yacov Y. Haimes*

The premise of this article is that risk to a system, as well as its vulnerability and resilience, can be understood, defined, and quantified most effectively through a systems-based philosophical and methodological approach, and by recognizing the central role of the system states in this process. A universally agreed-upon definition of risk has been difficult to develop; one reason is that the concept is multidimensional and nuanced. It requires an understanding that risk to a system is inherently and fundamentally a function of the initiating event, the states of the system and of its environment, and the time frame. In defining risk, this article posits that: (a) the *performance capabilities* of a system are a function of its state vector; (b) a system's *vulnerability* and *resilience vectors* are each a function of the input (e.g., initiating event), its time of occurrence, and the states of the system; (c) the *consequences* are a function of the specificity and time of the event, the vector of the states, the vulnerability, and the resilience of the system; (d) the *states* of a system are time-dependent and commonly fraught with variability uncertainties and knowledge uncertainties; and (e) *risk* is a measure of the probability and severity of consequences. The above implies that modeling must evaluate consequences for each risk scenario as functions of the threat (initiating event), the vulnerability and resilience of the system, and the time of the event. This fundamentally complex modeling and analysis process cannot be performed correctly and effectively without relying on the states of the system being studied.

KEY WORDS: Definition of risk; resilience; state variables; systems approach; threat; time frame; vulnerability

1. INTRODUCTION

The premise of this article is that risk to a system, as well as its vulnerability and resilience, can be understood, defined, and possibly quantified most effectively through a systems-based philosophical and methodological approach, and by recognizing the central role of the states of a system in this process. This is important because after the 9/11 attack on the United States, a variety of confusing and often erroneous extensions were added to the *seemingly* simple and clear definition of risk by Lowrance:[1] "Risk is a measure of the probability and severity of adverse effects." This is not surprising given the large set of definitions and interpretations of risk that have been accepted and published in the literature. For example, the Risk Definition Committee of the Society for Risk Analysis (SRA)[2] printed 13 definitions of risk on the program jacket of its first meeting in 1981. The definitions of risk continue to multiply as "risk" becomes a household term.

Over time, increasing fuzziness has also led to varied conceptual and sometimes erroneous quantitative definitions and interpretations. A universally agreed-upon succinct definition of risk has been

*Address correspondence to Yacov Y. Haimes, Quarles Professor of Systems and Information Engineering, and Founding Director, Center for Risk Management of Engineering Systems, University of Virginia, PO Box 400736, Charlottesville, VA 22904, USA; tel: 434-924-3803; fax: 434-924-0865; haimes@virginia.edu.

difficult to develop; one reason is that the concept is multidimensional and nuanced. It requires an understanding that risk to a system is inherently and fundamentally a function of the states of the system and of its environment (and of course of the initiating event). (See References 3–8 for other definitions.)

While risk practitioners have legitimate reasons to define risk from their perspectives, these definitions can lead to confusion. This article posits that the composite meaning and implications of risk is best understood from the theory, perspectives, and methodology of systems engineering/analysis. The building blocks of systems modeling and the centrality of state variables are the keys to this understanding. This article will first discuss the elements of risk and then introduce the centrality of state variables in the definitions of risk to a system, as well as its vulnerability and resilience.

2. THE ELEMENTS OF RISK

In a seminal paper, Kaplan and Garrick introduced the theory of scenario structuring (TSS) and within it the triplet questions in the risk assessment process: "What can go wrong? What is the likelihood? What are the consequences?"[9]

There is ambiguity in defining risk as "a measure of the probability and severity of adverse effects."[1] What do we mean by the terms *probability (*or *likelihood)* and *adverse effects?* Consider the interpretation of the term *likelihood* in isolation (for now) of its probable consequences: Is it the likelihood of the occurrence of any kind of threat (or other initiating event), at any level or magnitude, and when, and of what duration? Or, is it the likelihood of the level and magnitude of the consequences (for every element of the vector of consequences)? Thus, the phrase "*probability and severity of adverse effects"* can be interpreted in two ways at the same time: (1) in terms of the probability of the *occurrence* of adverse effects, and (2) in terms of the probability of the *severity* of adverse effects, given their occurrence. Both interpretations are valid; however, each represents varied conceptual and theoretical challenges.

Furthermore, when likelihood is translated into *probability,* it introduces an important conceptual and cognitive hurdle. By its very nature, probability is an abstract term often used as a model of variability and frequency, or to quantify the *level of confidence that we have in the information*. In other words, probability really does not exist as a physical entity *per se* (although the wave functions of quantum particles may be as real as anything).

Kolmogorov[10] builds his widely recognized definition of probability on three basic axioms. Gnedenko[10] provides a succinct presentation of Kolmogorov's theory of probability:

> Kolmogorov starts with a set U consisting of *elementary events*. What constitutes the elements of this set **is** immaterial for the logical development of probability theory. He then considers a certain family F of subsets of the set U; the elements of the family F are called *random events*. The following three conditions are imposed on the structure of the family F: (1) F is contained in the set U as one of its elements. (2) If the subsets A and B of the set U are elements of F, then the sets $A + B$, AB, $\bar{A}$ and $\bar{B}$ are also elements of F. (3) If the subsets $A_1, A_2, \ldots, A_n, \ldots$ of the set U are elements of the set F, then the sum $A_1 + A_2 + \cdots + A_n + \cdots$ of these subsets and the product $A_1, A_2, \ldots A_n \ldots$ of these subsets are also elements of F. Thus:
>
> Axiom 1: With each random event A in a field of events F, there is associated a nonnegative number $\mathbf{P}(A)$, called its probability.
>
> Axiom 2: $\mathbf{P}(U) = 1$.
>
> Axiom 3 (Addition Axiom): If the events $A_1, A_2, \ldots, A_n$ are pair-wise mutually exclusive, then $\mathbf{P}(A_1 + A_2 + \cdots + A_n) = \mathbf{P}(A_1) + \mathbf{P}(A_2) + \cdots + \mathbf{P}(A_n)$.

Kolmogorov's theory of probability has become the gold standard in the field because it is built on a holistic systems philosophy. He considers entire states of the system as subsets of the universe of event space U. In this sense, Komolgorov's theory establishes a requirement to understand probability holistically, and since probability is a central component of risk, then risk itself also espouses holism.

3. THE CENTRALITY OF STATE VARIABLES IN THE DEFINITIONS OF RISK, VULNERABILITY, AND RESILIENCE

The systems modeling process relies on the fundamental building blocks of mathematical models: *input, output, state variables, decision (control) variables, exogenous variables, uncertain variables,* and *random variables.* Identifying, understanding, and quantifying the building blocks of a mathematical model of any system are fundamental steps in modeling. This is because at any instant the levels of the state variables are affected by the other building blocks and these levels determine the outputs of the system.

All state variables are subject to continuous natural, desired, or forced changes (positive and negative). This does not mean that all models must have time-dependent state variables. This is where

the art of modeling comes into play. Models are built to answer specific questions and to represent the relevant essence of the system under consideration. Thus, if small or insignificant changes in a state variable have no important effect on the answers sought from the model, then that state variable may be assumed static—not time-dependent. Deciding whether a state variable should be modeled as static (not changing with time) or dynamic (changing with time) is similar to the modeler selecting only those state variables that represent the essence of the system. In fact, the art and science of systems modeling is characterized by a continuous process of tradeoffs, made by modelers with respect to complexity and accuracy. *Any model should be as simple as possible and as complex as needed to answer the expected questions.*

Vulnerability and resilience are key concepts in risk analysis. Their systems-based definitions improve our understanding of risk and help make them operational for modeling. For example, in a *Risk Analysis* paper, "On the Definition of Vulnerabilities in Measuring Risks to Infrastructures," Haimes[11] introduced the following systems-based definition: *vulnerability is the manifestation of the inherent states of the system (e.g., physical, technical, organizational, and cultural) that can be subjected to a natural hazard or be exploited to adversely affect (cause harm or damage to) that system*. The vulnerability of a system is multidimensional, a *vector* in mathematical terms. Suppose we first consider the risk of terrorism to a military base. The states of the base (as a system) that represent vulnerabilities (to natural hazards or to malevolent acts) are: functionality/availability of telecommunications, electric power, water supply, soldiers' quarters, officers' quarters, perimeter security, and others, all of which are critical to the overall functionality of the base. Furthermore, each of these state variables is not static in its operations and functionality—its levels of functionality change and evolve continuously. In addition, each is a system of its own and has its own substate variables.

As another example, to treat a patient, a physician must first know the temperature, blood pressure, and other states of the patient's physical health. The human body is vulnerable to infectious diseases. Different organs and parts of the body are continuously bombarded by a variety of bacteria, viruses, and other pathogens. However, only a subset of the human body is vulnerable to the threats from a subset of the would-be attackers, and due to our immune system, only a smaller subset of the body would experience adverse effects. (This multifaceted characteristic can also be observed for the state variables representing a terrorist network, such as its organization, doctrine, technology, resources, and sophistication.)

The resilience of a system is also *a manifestation of the states of the system and it is a vector that is time- and threat (initiating event)-dependent*.[12] More specifically, *resilience* represents *the ability of the system to withstand a major disruption within acceptable degradation parameters and to recover within an acceptable cost and time*. In other words, resilience is a vector state of the system that is neither abstract or static, nor deterministic. Moreover, resilience is similar to vulnerability in that it cannot simply be measured in a single unit metric; its importance lies in the ultimate multidimensional outputs of the system (the consequences) for any specific inputs (threats).

Consider a cyberinfrastructure system (a complex, large-scale cyber network encompassing hardware, software, policies, and procedures, including critical connections to the Internet). In any such complex system, the question, "What is the resilience of cyberinfrastructure X?" is unanswerable. This is because the answer implicitly depends upon knowing whether it would recover following any attack y within an acceptable time, taking into account the associated costs and other risks. Thus, such a question can be answerable only when the threat (initiating event) scenario (or a set of scenarios) is specifically identified. Resilience is not merely an abstract concept; it is a state of the system (composed of a vector of substates) that may have different responses to different inputs (threat scenarios) from any specific substate within the hardware, software, policies and procedures, or connections to the Internet.

4. SCENARIO STRUCTURING AND SYSTEMS ENGINEERING

To perform effective risk assessment and management, the analyst must understand the system and its interactions with its environment, and this understanding is requisite to modeling the behavior of the states of the system under varied probabilistic conditions. For example, government agencies, the military, the private sector, major corporations, nongovernmental think-tank organizations, and futuristic scholars—all are interested in better understanding the trends and preventing or preparing for not-unlikely sources of risk. Forced changes affect the states of the system (e.g., the 9/11 attack on the United States was a forced change that affected the states of the economy, homeland security, and international relationships, to cite a few). Thus, tracking

emergent forced changes to a system through observations, precursors, intelligence and data collection, and most importantly through modeling, constitutes the essence of the risk assessment and management process. *The term emergent forced changes connotes external or internal sources of risk that may adversely affect the states of the system*, and thus the system as a whole.

The theory of scenario structuring (TSS) was first presented in 1981 by Kaplan and Garrick.[9] The ultimate purpose and efficacy of TSS are to envision, foresee, and predict emergent forced changes based on the capability of the human imagination, the availability of evidence, and the predictions of modeling tools. Emergent forced changes, whether they originate from within or from outside the system—and when they are unanticipated, their precursors undetected or ignored, or are altogether misunderstood—are likely to affect the states of the system with adverse consequences. From a broader perspective, the risk assessment process, and to a limited extent the risk management process, are supported by envisioning, discovering, and tracking emergent forced changes through the TSS.

Kaplan and Garrick[9] introduced the following mathematical "set of triplets" definition of risk, R: $R = \{<s_i, l_i, x_i >\}$, where s_i denotes the ith *risk scenario,* l_i denotes the *likelihood* of that scenario, and x_i the "damage vector" or resulting *consequences*. Since then, this definition has served the field of risk analysis well. As stated, much debate has continued to challenge the professional community about how to quantify the l_i and x_i, and the meanings of "probability," "frequency," and "probability of frequency" in this connection.[13–16]

In Kaplan and Garrick, the scenarios S_i were defined, somewhat informally, as answers to the question, "What can go wrong?" with the system or process being analyzed. Subsequently, a subscript "c" was added to the set of triplets by Kaplan: $R = \{<s_i, l_i, x_i >\}_c$ to denote that the set of scenarios, $\{s_i\}$, should be *complete,* meaning it should include "all the possible scenarios, or at least all the important ones."[14,16]

Kolmogorov's theory of probability, discussed in Section 2, can be related to the TSS developed by Kaplan and Garrick. *Fundamentally, the process of risk assessment (and TSS within it) is a systemic exercise that attempts to "discover" potential future risk-based events, to watch for precursors*[17] *of forced changes, and thus to prepare for and respond to possible adverse events through risk management and risk communication.* The TSS attempts to develop risk-based scenarios systemically and methodologically. Ultimately, the completeness of the scenarios developed by the TSS, claimed in the original paper,[9] was modified[18] (as discussed later). In many ways, the TSS is a foundation for assuring that we understand the scope of risk assessment with respect to the system being evaluated. It also contributes to the measurement of risk by providing a tool for interpreting the output of the analysis. In extending the TSS, Kaplan *et al.* [18] refined the original "set of triplets" definition of risk so that in itself it did not assume or imply that the set of risk scenarios is finite or denumerable. Rather, this refined definition allows the set of risk scenarios to be a continuum, i.e., nonenumerable. This continuous set of scenarios constitutes the "true" risk and is independent of the method used to identify them.

5. SYSTEMS ENGINEERING AND RISK

Risk analysis and systems engineering/analysis have a common philosophical approach to problem solving, but they differ in their historical evolution and technical maturity. Both aspire to the *gestalt*-holistic philosophy in their problem-solving methodologies. Systems modeling frameworks build on a plethora of theories, methods, tools, and techniques to provide the instruments with which problems are studied, assessed, understood, managed, and solved, to the extent possible. Thus, the previous sections of this article provided the systems-based foundations for our understanding of the complex definition of risk to a system as well as its measurement.

Risk analysis is similar to the systems engineering/systems analysis approach, which is predicated on the centrality of the *states of the system* and their roles in determining for each input (threat) the resulting outputs (consequences). In particular, note that:

(a) The *performance capabilities* of a system are a function of its state vector;
(b) A system's *vulnerability* and *resilience vectors* are each a function of the input (threat), its time of occurrence, and (the vector of) the states of the system;
(c) The *consequences* are functions of the time of the event, the vector of the states, the vulnerability, and the resilience of the system;

(d) The *states* of a system are time-dependent and commonly fraught with variability and knowledge uncertainties; and
(e) *Risk* is a measure of the probability and severity of adverse effects[1] (i.e., consequences).

These five premises imply that "risk" is a vector of the same units (dimensions) as the consequences, and is a function of:

(i) *time*,
(ii) *the probability of the threat (initiating event) and its specificity (input)*,
(iii) *the probability of the consequences, given the threat*,
(iv) *the vector of the states of the system (including its performance capability, vulnerability, and resilience), and*
(v) *the vector of the resulting consequences.*

Based on the above discussion, it is appropriate to make the time domain explicit in the questions of the risk assessment process developed by Kaplan and Garrick.[9] To the three original questions: "What can go wrong? What is the likelihood? What are the consequences?" we add a fourth one: "*Over what time frame?"*

Consider a sample of the multidimensional vector of consequences from Hurricane Katrina: loss of lives, displaced population, loss of property, opportunities, and jobs, and the erosion of confidence in government and technology, among others. If we were to develop a risk scenario for a future hurricane with an unusually high surge of water, a similar vector of risk components would necessarily emerge from the risk assessment process. Since consequences are measured through a natural vector of noncommensurate attributes, the units of each element of the risk vector ought to correspond, respectively, to the same units of the vector of consequences.

The above discussion implies that significant modeling efforts are required to first evaluate the vector of consequences for each threat scenario (as functions of the threat (initiating event), the vulnerability and resilience of the system, and the time of the event). Then each element of this vector must be paired with (i) the probability of the scenario's occurrence, or (ii) by the probability of the severity of the consequences. This fundamentally complex modeling and analysis process cannot be performed correctly and effectively without relying on the states of the system being studied.

6. RELEVANCE OF THE MULTIDIMENSIONAL RISK MEASURE TO RISK MANAGEMENT

Each risk scenario must address the risk assessment questions: "What can go wrong? What is the likelihood? What are the consequences?" and "What is the time frame?" The risk management process asks:[19,20] "What can be done and what options are available? What are the tradeoffs in terms of all relevant costs, benefits, and risks?" and "What are the impacts of current decisions on future options?" Risk management addresses each important element of the vector of consequences, noting that different mitigation policy options may address and impact different consequences more effectively. A one-dimensional instrument is unlikely to address the entire vector of risk elements. Rather, a portfolio of risk management policies is required so that their integrative effects are capable of addressing all important and critical risk elements. This process leads to the well-established multiple-criteria decisionmaking (MCDM), where multiple competing, conflicting, and noncommensurate objectives are traded off. [21,22]

Consider a future hurricane scenario similar to Katrina making a landfall at New Orleans. The challenges associated with both the perception[23] of risk and the quantification and management of the risk vector are: loss of lives, number of people displaced, damage to infrastructures, and other varied costs. Each of these consequences is a function of the *threat* (e.g., the time of the landfall, its wind speed, and its expected water surge), the *vulnerability* of the community (e.g., those in the area below sea level, the states of the levee system, the canals, etc.), the *resilience* of the levee system (the reliability of the water pumps, preparedness, first responders, etc.), and the *time* of the hurricane. All these factors and many others must be included in any modeling efforts to assess and quantify the likely consequences associated with this scenario. Similarly, the risk management process must also address each element of the risk vector individually and the entire set as a whole. Clearly, the assessment and quantification of risk cannot be any better than the quality of the efforts devoted to quantifying the consequences.

To sum up, *the questions in the risk management process address the policy options, their tradeoffs, the future dynamics of the system and its environment, and the emergent forced changes. These cannot be*

addressed correctly and effectively without adhering to and tracking the evolution of the states of the system as functions of the risk management decisions and time.

7. RISK OF LOW PROBABILITY WITH EXTREME CONSEQUENCES

This section discusses one of the most prevalent sources of complexity in the quantification of risk; namely, the use, and often misuse, of the expected value of risk metric as the sole measurement of risk. The concerns of the public and most decisionmakers focus on events with dire consequences, even with low probabilities. In the face of calamities as bridges falling, dams bursting, and airplanes crashing, we must acknowledge the importance of studying "extreme" events. Yet, models have been helping to *mask* the criticality of catastrophic events by adhering to the expected value of risk, which intrinsically can equate a low probability of high-consequence events with a high probability of low-consequence events. The reliance on this commonly used metric, when it is used as the *sole measure of risk*, can confuse the decisionmakers, leading to bad choices. The problem is that the expected value of risk is an operation that essentially multiplies the consequences of each event by its probability of occurrence and adds all these products over the entire probability range.

For example, imagine a catastrophic dam failure that might cause flooding of 10^6 acres of land with associated loss of human life and damage to the environment, but it has a very low probability, e.g., a probable maximum flood (10^{-6}) of happening. Obviously, this cannot be viewed by decisionmakers in the same vein as minor flooding of 10^2 acres of land, which has a high probability of 10^{-2} of happening. Yet this is exactly what the expected value function would ultimately generate. (Note that the products $10^6 \times 10^{-6} = 10^2 \times 10^{-2} = 1$.) Most important, equating these events into one expectation function distorts the relative importance of both the events and consequences. Instead of using the traditional expected value of risk as the *sole measure of risk*, other methods, such as the partitioned multiobjective risk method,[20] supplement and complement the expected value of risk by generating a number of conditional expected value of risk functions. The risk of extreme and catastrophic events literature, which spans social and behavioral scientists, natural scientists and engineers, and economists, to cite a few, defies the reliance on the expected value of risk.

Talbeb[24] ascribes three attributes to an extreme event: (a) it is an outlier, as it lies outside the realm of regular expectation; nothing in the past can convincingly point to its possibility, (b) it carries an extreme impact, and (c) in spite of its outlier status, human nature makes us concoct explanations for its occurrence *after the fact*, making it explainable and predictable. Risk analysts and systems engineers are challenged by the need to go beyond the simple formulation to assess the role of extreme events.

8. THE CRITICAL ROLE OF THE TIME DOMAIN IN RISK MANAGEMENT

Risk management connotes actionable measures taken to reduce, curtail, or minimize future risks to a system at acceptable composite costs. The implicit and explicit purpose of an investment in risk management is to render the states of the system less vulnerable and more resilient. Preparedness is one important way with which risk managers change the states of natural and constructed environmental systems.

The time frame plays a central role in risk assessment, risk management, and risk communication. In *risk assessment*, the significance of the question "What can go wrong?" has everything to do with the timing of the adverse effect. When this source of risk is expected further in the future, risk managers have more flexibility. In the *risk management* process, the significance of the question "What are the impacts of current decisions on future options?" again lies in the flexibility and constraints that risk managers desire to have in the future, and with emergent forced changes with which they also must cope. In *risk communication*, the time frame plays a substantial role in the perception of risk and in the acceptance of risk management policy options deployed by decisionmakers in both the private and public sectors.[23] Typically, the efficacy of risk management decisions cannot be proved when they are made. There is a time lag between the decision and its impact, and public understanding of this inherent latency is paramount. Although risk management decisions are important, they may not suffice to make those at risk feel safer. The ultimate integrated steps in the risk analysis process are to explain how risk management policies and actions contribute to improved safety, and to communicate and justify the residual risk to the multiple stakeholders and the affected public (when removing the entire risk is neither economically nor technically feasible).[25]

In sum, *the fundamental public concerns about risk reside in the ever-lingering question: "What can go wrong in the future, and what might be the adverse consequences?" Since the present is deterministic and the future is not, there is an imperative need to assess the future states of the system as they might respond and evolve as a consequence of emergent forced changes. Thus the criticality of the time frame in risk analysis and in understanding and assessing the evolving states of the system over time*.

9. EPILOGUE: A LOGICAL INTEGRATION

Systems engineering/analysis is distinguished by its practical philosophy, which advocates holism in cognition and in decision-making. This philosophy is grounded on the arts, natural and behavioral sciences, and on engineering and is supported by a collection of modeling methodologies, optimization and simulation techniques, data management procedures, and decision-making approaches. The centrality of state variables in modeling, and thus in systems engineering/analysis and in risk analysis, are the *sine qua non* for any quest to model and understand the intricacy of any system, and of complex multi- and large-scale systems in particular. The holistic nature of systems engineering/analysis, and of risk analysis, leads to systems modeling through state variables with specified system boundaries, and the integration and analysis of the interdependencies and interconnectedness among all subsystems. Modeling the risk vector as an explicit function of the initiating event, its timing and level of intensity, and of the system's vulnerability and resilience (the latter two themselves being functions of the states of the system) constitutes a fundamental task in risk analysis.

From the viewpoint of systems modeling and systems engineering/analysis, it is reasonable to ask why the U.S. Department of Homeland Security (DHS) had to go through four stages of defining risk in eight years (2001–2009).[3] The answer is that the DHS followed a non-systems-based approach in defining the nontrivial notion of risk.[26]

The multifaceted composition of risk includes the levels of uncertainty and intensity of the initiating events or threats, the time frame, and the dynamic, probabilistic, and often nonlinear natures of the states of all natural and constructed environments on which the system's vulnerability and resilience depend. This intricacy cannot be modeled and understood on an *ad hoc* basis. In other words, *we must understand, model, and define the complexity of risk, vulnerability, and resilience in a systemic way and through a methodical, theoretically-based systems approach, where the states of the system constitute the essence of the analysis.*

In closing, by projecting Heisenberg's uncertainty principle and Einstein's advice on the complexity of theories to the field of risk analysis, we assert that:

To the extent that risk analysis is precise and simple, it is not real.

To the extent that risk analysis is real and complex, it is not precise.

ACKNOWLEDGMENTS

I am grateful to Michael Greenberg, the Editor-in-Chief of the journal, who has markedly improved the cogency of this article through his constructive review and editorial work, to my fellow Area Editors—Warner North and Tony Cox—for their helpful comments, and to my technical editor, Grace Zisk, for her professional help.

REFERENCES

1. Lowrance WW. Of Acceptable Risk. Los Altos, CA: William Kaufmann, 1976.
2. Society for Risk Analysis. Risk Newsletter, 1987; 7(3):5.
3. U.S. Government Accountability Office (GAO), Homeland Security. Risk-Based Methodology is Reasonable, but Current Version's Measure of Vulnerability is Limited, GAO-08-852, Washington, DC: DHS, June 2008. Available at: http://www.gao.gov/new.items/d09168r.pdf, Accessed on May 27, 2009.
4. Sahinoglu M. Security meter: A practical decision-tree model to quantify risk. IEEE Security & Privacy, 2005, May:18–24.
5. Bell R, Glade T. Quantitative risk analysis for landslides—Examples from Bildudalur, NW Iceland. Natural Hazards and Earth System Sciences, 2004; 4(1):117–131.
6. Feather MS, Cornford SL. Quantitative risk-based requirements reasoning. Requirements Engineering, 2008; 8:248–265.
7. Apostolakis GE. How useful is quantitative risk assessment? Risk Analysis, 2004; 24(3):515–520.
8. Paté-Cornell EM. Uncertainties in risk analysis: Six levels of treatment. Reliability Engineering and Systems Safety, 1996; 54:95–111.
9. Kaplan S, Garrick BJ. On the quantitative definition of risk. Risk Analysis, 1981; 1(1):11–27.
10. Gnedenko BV. The Theory of Probability (translated from the Russian by BD Seckler). New York: Chelsea Publishing Company, 1963, p. 53.
11. Haimes YY. On the definition of vulnerabilities in measuring risks to infrastructures. Risk Analysis, 2006; 26(2):293–296.
12. Haimes YY. On the definition of resilience in systems. Risk Analysis, 2009; 29(4):498–501.
13. Kaplan S. The words of risk analysis. Risk Analysis, 1997; 7(4):407–417.
14. Kaplan S. The general theory of quantitative risk assessment in its role in the regulation of agricultural pests, International

approaches to pest risk analysis. North American Plant Protection Organization Bulletin, 1993; 11:19–30.
15. Kaplan S. An Introduction to TRIZ: The Russian Theory of Inventive Problem Solving. Southfield, MI: Ideation International Inc., 1996.
16. Kaplan S. The general theory of quantitative risk assessment. Pp. 11–39 in Haimes YY, Moser D, Stakhiv E (eds). Risk-Based Decision Making in Water Resources V. New York: American Society of Engineers, 1991.
17. Phimister JR, Bier VM, Kunreuther HC (eds). Accident Precursors Analysis and Management: Reducing Technological Risk Through Diligence. National Academy of Engineering, Washington, DC: National Academies Press, 2004.
18. Kaplan S, Haimes YY, Garrick BJ. Fitting hierarchical holographic modeling into the theory of scenario structuring and a resulting refinement of the quantitative definition of risk. Risk Analysis, 2001; 21(5):807–815.
19. Haimes YY. Total risk management. Risk Analysis, 1991; 11(2):169–171.
20. Haimes YY. Risk Modeling, Assessment, and Management, 2nd ed. New York: Wiley, 2009.
21. Keeney RL, Raiffa H. Decisions with Multiple Objectives. New York: Wiley, 1976.
22. Chankong V, Haimes YY. Multiobjective Decision Making: Theory and Methodology. New York: Dover, 2008.
23. Slovic P. The Perception of Risk. London and Sterling, VA: Earthscan Publications, Ltd., 2004.
24. Talbeb NN. The Black Swan: The Impact of the Highly Improbable. New York: Random House, 2007.
25. National Research Council of the National Academies. Science and Decisions: Advancing Risk Assessment. Washington, DC: National Academies Press, 2009.
26. National Research Council of the National Academies, Department of Homeland Security. Bioterrorism Risk Assessment. Washington, DC: National Academies Press, 2008.