1

The Art and Science of Systems and Risk Analysis

1.1 INTRODUCTION

Risk-based decisionmaking and *risk-based approaches in decisionmaking* are terms frequently used to indicate that some systemic process that deals with uncertainties is being used to formulate policy options and assess their various distributional impacts and ramifications. Today, an ever-increasing number of professionals and managers in industry, government, and academia are devoting a large portion of their time and resources to the task of improving their understanding and approach to risk-based decisionmaking. In this pursuit, they invariably rediscover (often with considerable frustration) the truism: The more you know about a complex subject, the more you realize how much still remains unknown. There are three fundamental reasons for the complexity of this subject. One is that decisionmaking under uncertainty literally encompasses every facet, dimension, and aspect of our lives. It affects us at the personal, corporate, and governmental levels, and it also affects us during the planning, development, design, operation, and management phases. Uncertainty colors the decisionmaking process regardless of whether it (i) involves one or more parties, (ii) is constrained by economic or environmental considerations, (iii) is driven by sociopolitical or geographical forces, (iv) is directed by scientific or technological know-how, or (v) is influenced by various power brokers and stakeholders. Uncertainty is inherent when the process attempts to answer the set of questions posed by William W. Lowrance: "Who should decide on the acceptability of what risk, for whom, in what terms, and why?" [Lowrance, 1976]. The second reason why risk-based decisionmaking is complex is that it is cross-disciplinary. The subject has been further complicated by the development of diverse approaches of varying reliability. Some methods, which on occasion produce fallacious results and conclusions, have become entrenched and would be hard to eradicate. The third reason is grounded on the need to make trade-offs among all relevant and important costs, benefits, and risks in a multiobjective framework, without assigning weights with which to commensurate risks, costs, and benefits.

In his book *Powershift*, Alvin Toffler [1991] states:

> As we advance into the Terra Incognito of tomorrow, it is better to have a general and incomplete map,

Risk Modeling, Assessment, and Management, Fourth Edition. Yacov Y. Haimes.

> subject to revision and correction, than to have no map at all.

Translating Toffler's vision into the risk assessment process implies that a limited database is no excuse for not conducting sound risk assessment. On the contrary, with less knowledge of a system, the need for risk assessment and management becomes more imperative.

Consider, for example, the risks associated with natural hazards. Causes for major natural hazards are many and diverse, and the risks associated with these natural hazards affect human lives, the environment, the economy, and the country's social well-being. Hurricane Katrina, which struck New Orleans in the United States on August 29, 2005, killing a thousand people and destroying properties, levees, and other physical infrastructures worth billions of dollars, is a classic example of a natural hazard with catastrophic effects [McQuaid and Schleifstein, 2006]. The medium within which many of these risks manifest themselves, however, is engineering-based physical infrastructure—dams, levees, water distribution systems, wastewater treatment plants, transportation systems (roads, bridges, freeways, and ports), communication systems, and hospitals, to cite a few. Thus, when addressing the risks associated with natural hazards, such as earthquakes and major floods, or willful hazards, that is, acts of terrorism, one must also account for the impact of these hazards on the integrity, reliability, and performance of engineering-based physical and human-based societal infrastructures. The next step is to assess the consequences—the impact on human and non-human populations and on the socioeconomic fabric of large and small communities.

Thus, risk assessment and management must be an integral part of the decisionmaking process, rather than a gratuitous add-on technical analysis. Figure 1.1 depicts this concept and indicates the ultimate need to balance all the uncertain benefits and costs.

For the purpose of this book, *risk* is defined as *a measure of the probability and severity of adverse effects* [Lowrance, 1976]. Lowrance also makes the distinction between risk and safety: Measuring risk is an empirical, quantitative, scientific activity (e.g., measuring the probability and severity of harm). Judging safety is judging the acceptability of risks—a normative, qualitative, political activity. Indeed, those private and public organizations that can successfully address the risks inherent in their business—whether in environmental protection, resource availability, natural forces, the reliability of man–machine systems, or future use of new technology—will dominate the technological and service-based market.

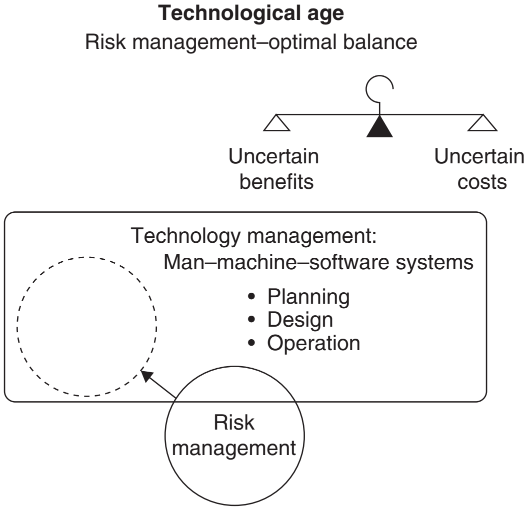

Figure 1.1 *Risk management as an integral part of overall management.*

The premise that risk assessment and management must be an integral part of the overall decisionmaking process necessitates following a systemic, holistic approach to dealing with risk. Such a holistic approach builds on the principles and philosophy upon which systems analysis and systems engineering are grounded.

1.2 SYSTEMS ENGINEERING

1.2.1 What Is a System?

The human body and each organ within it, electric power grids and all large-scale physical infrastructures, educational systems from preschool to higher education, and myriad other human, organizational, hardware, and software systems are large-scale, complex, multiscale interconnected and interdependent systems with life cycles that are characterized by risk and uncertainty along with emergent behavior. But exactly what is a system? *Webster's Third New*

International Dictionary offers several insightful definitions:

> A complex unity formed of many often diverse parts subject to a common plan or serving a common purpose; an aggregation or assemblage of objects joined in regular interaction or interdependence; a set of units combined by nature or art to form an integral, organic, or organizational whole.

Almost every living entity, all infrastructures, both the natural and constructed environment, and the entire households of tools and equipment are complex systems often composed of myriad subsystems that in their essence constitute *systems of systems* (*SoS*). Each is characterized by a hierarchy of interacting and networked components with multiple functions, operations, efficiencies, and costs; the component systems are selected and coordinated according to some existing trade-offs between multiple objectives and operational perspectives. Clearly, no single model can ever attempt to capture the essence of such systems—their multiple dimensions and perspectives.

1.2.2 What Is Systems Engineering?

Even after over half a century of systems engineering as a discipline, many engineers find themselves perplexed about the following question: What is systems engineering?

Systems engineering is distinguished by its practical philosophy that advocates holism in cognition and in decisionmaking. This philosophy is grounded on the arts, natural and behavioral sciences, and engineering and is supported by a complement of modeling methodologies, state-space theory, optimization and simulation techniques, data management procedures, and decisionmaking approaches. The ultimate purpose is to (i) build an understanding of the dynamic system's nature, functional behavior, and interaction with its environment, (ii) improve the decisionmaking process (e.g., in planning, design, development, operation, management), and (iii) identify, quantify, and evaluate risks, and epistemic and aleatory uncertainties for a guided and actionable decisionmaking process.

One way of gaining greater understanding of systems engineering is to build on the well-publicized ideas of Stephen R. Covey in his best-selling book, *The Seven Habits of Highly Effective People* [Covey, 1989], and to relate these seven habits to various steps that constitute systems thinking or the systems approach to problem solving. Indeed, Covey's journey for personal development as detailed in his book has much in common with the holistic systems concept that constitutes the foundation of the field of systems engineering. Even the transformation that Covey espouses, from thinking in terms of you to me to we, is similar to moving from the perception of interactions as reactive or linear to a holistic view of connected relationships. Viewed in parallel, the two philosophies—Covey's and the systems approach—have a lot in common. The question is: How are they related, and what can they gain from each other?

Analyzing a system cannot be a selective process, subject to the single perspective of an analyst who is responsible for deciphering the maze of disparate and other knowledge. Rather, a holistic approach encompasses the multiple visions and perspectives inherent in any vast pool of data and information. Such a systemic process is imperative in order to successfully understand and address the complexity of an SoS [NRC, 2002].

1.2.3 Historical Perspectives of Systems Engineering

1.2.3.1 Classical philosophers who practiced holistic systems thinking

The *systems* concept has a long history. The art and science of systems engineering as a natural philosophy can be traced to Greek philosophers. Although the term *system* itself was not emphasized in earlier writings, the history of this concept includes many illustrious names, including *Plato* (428–348 B.C.) [Hutchins, 1952] and *Aristotle* (384–322 B.C.). The writings of *Baron von Leibniz* (1646–1716), a mathematician and philosopher, are directed by holism and systems thinking. He shares with *Isaac Newton* (1642–1727) the distinction of developing the theory of differential and integral calculus. By quantifying the causal relationships among the interplanetary SoS, Newton represents the epitome of a systems philosopher and modeler. In their seminal book, *Isaac Newton,* *The Principia*, Cohen and Whitman [1999] write (p. 20):

> Newton's discovery of interplanetary forces as a special instance of universal gravity enables us to specify two goals of the Principia. The first is to show the conditions under which Kepler's laws of planetary motion are exactly or accurately true; the second is to explore how these laws must be modified in the world of observed nature by perturbations in the motions of planets and their moons.

Johann Gottlieb Fichte (1762–1814) introduced the idea of synthesis—one of the fundamental concepts of systems thinking. For example, he argued that *freedom* can never be understood unless one loses it. Thus, the *thesis* is that a man is born free, the loss of freedom is the *antithesis*, and the ability to enjoy freedom and do good works with it is the *synthesis*. In other words, to develop an understanding of a system as a whole (synthesis), one must appreciate and understand the roles and perspectives of its subsystems (thesis and antithesis). *Georg Hegel* (1770–1831), a contemporary of Fichte, was one of the most influential thinkers of his time. Like Aristotle before him, Hegel tried to develop a system of philosophy in which all the contributions of his major predecessors would be integrated. His *Encyclopedia of the Philosophical Sciences* (1817), which contains his comprehensive thoughts in a condensed form, provides important foundations for the concept of holism and the overall systems approach [Hegel, 1952].

Around 1912, *Max Wertheimer*, *Kurt Koffka*, and *Wolfgang Kohler* founded the Gestalt psychology, which emphasizes the study of experience as a *unified whole*. The German word *gestalt* means pattern, form, or shape [World Book, Inc., 1980]:

> Gestalt psychologists believe that pattern, or form, is the most important part of experience. The whole pattern gives meaning to each individual element of experience. In other words, the whole is more important than the sum of its parts. Gestalt psychology greatly influenced the study of human perception, and psychologists used Gestalt ideas in developing several principles—for example, the principle of closure (people tend to see incomplete patterns as complete or unified wholes).

1.2.3.2 Modern systems foundations

During his distinguished career, *Albert Einstein* attempted to develop a unified theory that embraces all forces of nature as a system. Feynman et al. [1963] describe a hierarchy or continuum of physical laws as distinct systems or disciplines that are cooperating and interdependent. Modern systems foundations are attributed to select scholars. Among them is *Norbert Wiener*, who in 1948 published his seminal book *Cybernetics*. Wiener's work was the outgrowth and development of computer technology, information theory, self-regulating machines, and feedback control. In the second edition of *Cybernetics* [1961], Wiener commented on the work of Leibniz:

> At this point there enters an element which occurs repeatedly in the history of cybernetics—the influence of mathematical logic. If I were to choose a patron saint for cybernetics out of the history of science, I should have to choose Leibniz. The philosophy of Leibniz centers about two closely related concepts—that of a universal symbolism and that of a calculus of reasoning. From these are descended the mathematical notation and the symbolic logic of the present day.

Ludwig von Bertalanffy coined the term *general systems theory* around 1950; it is documented in his seminal book, *General Systems Theory: Foundations, Development, Applications* [Bertalanffy, 1968/1976]. The following quotes from pages 9 to 11 are of particular interest:

> In the last two decades we have witnessed the emergence of the "system" as a key concept in scientific research. Systems, of course, have been studied for centuries, but something new has been added.... The tendency to study systems as an entity rather than as a conglomeration of parts is consistent with the tendency in contemporary science no longer to isolate phenomena in narrowly confined contexts, but rather to open interactions for examination and to examine larger and larger slices of nature. Under the banner of systems research (and its many synonyms) we have witnessed a convergence of many more specialized contemporary scientific developments. So far as can be ascertained, the idea of a "general systems theory" was first introduced by the present author prior to cybernetics, systems engineering and the emergence of related fields.

> Although the term "systems" itself was not emphasized, the history of this concept includes many illustrious names.

Kenneth Boulding, an economist, published work in 1953 on *General Empirical Theory* [Boulding, 1953] and claimed that it was the same as the general systems theory advocated by Bertalanffy.

The Society for General Systems Research was organized in 1954 by the American Association for the Advancement of Science. The society's mission was to develop theoretical systems applicable to more than one traditional department of knowledge.

The major functions of the society were to (i) investigate the isomorphy of concepts, laws, and models in various fields, as well as help in useful transfers from one field to another, (ii) encourage the development of adequate theoretical models in the fields that lack them, (iii) minimize the duplication of theoretical effect in different fields, and (iv) promote the unity of science by improving communication among specialists.

Several modeling philosophies and methods have been developed over the last three decades to address the intricacy of modeling complex large-scale systems and to offer various modeling schema. They are included in the following volumes: *New Directions in General Theory of Systems* [Mesarović, 1965], *General Systems Theory* [Macko, 1967], *Systems Theory and Biology* [Mesarović, 1968], *Advances in Control Systems* [Leondes, 1969], *Theory of Hierarchical Multilevel Systems* [Mesarović et al., 1970], *Methodology for Large-Scale Systems* [Sage, 1977], *Systems Theory: Philosophical and Methodological Problems* [Blauberg et al., 1977], *Hierarchical Analyses of Water Resources Systems: Modeling and Optimization of Large-Scale Systems* [Haimes, 1977], and *Multifaceted Modeling and Discrete Event Simulation* [Zigler, 1984].

In *Synectics: The Development of Creative Capacity*, Gordon [1968] introduced an approach that uses metaphoric thinking as a means to solve complex problems. In the same era, Lowrance [1976] published an influential work considering the science of measuring the likelihood and consequence of uncertain adverse effects that emerge from complex systems. He outlined critical considerations for engineering complex systems that are characterized by uncertainty. Gheorghe [1982] presented the philosophy of systems engineering as it is applied to real-world systems. In his book *Metasystems Methodology*, Hall [1989] developed a theoretical framework to capture the multiple dimensions and perspectives of a system. Other works include Sage [1992, 1995] and Sage and Rouse [1999]. Sage and Cuppan [2001] provide a definition of emergent behavior in the context of an SoS. Slovic [2000], among his many far-reaching works, presents the capabilities of decisionmakers to understand and make *optimal* decisions in uncertain environments. Other books on systems include Fang et al. [1993], Gharajedaghi [2005], Rasmussen et al. [1994], Rouse [1991], Adelman [1991], Zeleny [2005], Blanchard and Fabrycky [1998], Kossiakoff and Sweet [2002], Maier and Rechtin [2000], Buede [1999], Blanchard [2003], Blanchard and Fabrycky [2005], Sage and Armstrong [2003], and Hatley et al. [2000].

Several modeling philosophies and methods have been developed over the years to address the complexity of modeling large-scale systems and to offer various modeling schema. In his book *Methodology for Large-Scale Systems*, Sage [1977] addressed the "need for value systems which are structurally repeatable and capable of articulation across interdisciplinary fields" with which to model the multiple dimensions of societal problems. Blauberg et al. [1977] pointed out that, for the understanding and analysis of a large-scale system, the fundamental principles of *wholeness* (representing the integrity of the system) and *hierarchy* (representing the internal structure of the system) must be supplemented by the principle of *the multiplicity of description for any system*. To capture the multiple dimensions and perspectives of a system, Haimes [1981] introduced hierarchical holographic modeling (HHM) (see Chapter 3) and asserted: "To clarify and document not only the multiple components, objectives, and constraints of a system but also its welter of societal aspects (functional, temporal, geographical, economic, political, legal, environmental, sectoral, institutional, etc.) is quite impossible with a single model analysis and interpretation." Recognizing that a system "may be subject to a multiplicity of management, control and design objectives," Zigler [1984] addressed such modeling complexity in his book *Multifaceted Modeling and Discrete Event*

Simulation. Zigler (p. 8) introduced the term *multifaceted* "to denote an approach to modeling which recognizes the existence of multiplicities of objectives and models as a fact of life." In his book *Synectics: The Development of Creative Capacity*, Gordon [1968] introduced an approach that uses metaphoric thinking as a means to solve complex problems. Hall [1989] developed a theoretical framework, which he termed *Metasystems Methodology*, to capture the multiple dimensions and perspectives of a system. Other early seminal works in this area include the book on societal systems and complexity by Warfield [1976] and the book *Systems Engineering* [Sage, 1992]. Sage identified several phases of the systems engineering life cycle; embedded in such analyses are the multiple perspectives—the structural definition, the functional definition, and the purposeful definition. Finally, the multiple volumes of the *Systems and Control Encyclopedia: Theory, Technology, Applications* [Singh, 1987] offer a plethora of theory and methodology on modeling large-scale and complex systems. Thus, multifaceted modeling, metasystems, HHM, and other contributions in the field of large-scale systems constitute the fundamental philosophy upon which systems engineering is built.

Reflecting on the origins of modern systems theory since the introduction of the Gestalt psychology in 1912, we cannot underestimate the intellectual power of the holistic philosophy that has sustained systems engineering. This multidisciplinary field transcends the arts, humanities, natural and physical sciences, engineering, medicine, and law, among others. The fact that systems engineering, systems analysis, and risk analysis have continued to grow and infiltrate other fields of study over the years can be attributed to the fundamental premise that a system can be understood only if all the intra- and interdependencies among its parts and its environment are also understood. For more than a century, mathematical models constituted the foundations upon which systems-based theory and methodologies were developed, including their use and deployment on the myriad large-scale projects in the natural and constructed environment. If we were to identify a single idea that has dominated systems thinking and modeling, it would be the state concept. Indeed, the centrality of state variables in this context is so dominant that no meaningful mathematical model of a real system can be built without identifying the critical states of that system and relating all other building blocks of the model to them (including decision, random, and exogenous variables, and inputs and outputs). In this respect, system modeling—the cornerstone of this book—has served, in many ways, as the medium with which to infuse and instill the holistic systems philosophy into the practice of risk analysis as well as of engineering and other fields.

1.2.4 Systems Engineering and Covey's Seven Habits

The concepts that Covey introduces can be compared with the systems approach as applied to the entire life cycle of a system. Through this comparison, a joint model is developed that demonstrates how the ideas from the two approaches overlap and how an understanding of this view can benefit personal development as well as systems design and development [Haimes and Schneiter, 1996].

Covey's philosophy is used in the following discussion as a vehicle with which to explain the holistic systems engineering philosophy.

1.2.4.1 Paradigm: The systems concept

From the outset, Covey stresses the understanding of paradigms—the lenses through which we see the universe. Furthermore, according to Covey, it is not what happens to us that affects our behavior; rather, it is our interpretation of what happens. Since our interpretation of the world we live in determines how we create new and innovative solutions to the problems we face, it is essential that we understand the elemental interrelationships in the world that surrounds us. Thus, both understanding the systemic nature of the universe and defining the system that we need to address are imperative requirements for our ability to solve problems.

In his book *The Fifth Discipline*, Peter Senge [1990] gives a good example of how to understand the systems concept. To illustrate the rudiments of the *new language* of systems thinking, he considers a very simple system—filling a glass of water:

> From a linear viewpoint, we say, "I am filling a glass of water." But in fact, as we fill the glass, we are

> watching the water level rise. We monitor the gap between the level and our goal, the desired water level. As the water approaches the desired level, we adjust the faucet position to slow the flow of water, until it is turned off when the glass is full. In fact, when we fill a glass of water we operate a water-regulation system.

The routine of filling a glass of water is so basic to us that we can do it successfully without thinking about it. But when the system becomes more complex, such as building a dam across a river, it is essential to see the systemic nature of the problem to avoid adverse consequences.

Sage [1992] defines systems engineering as “the design, production, and maintenance of trustworthy systems within cost and time constraints.” Sage [1990] also argues that systems engineering may be viewed as a philosophy that looks at the broader picture; it is a holistic approach to problem solving that relates interacting components to one another. Blanchard and Fabrycky [1990] define a system as all the components, attributes, and relationships needed to accomplish an objective. Understanding the systemic nature of problems is inherent in problem definition.

Understanding both the systemic nature of the world and the elements of the systems under question enables the shift to the paradigm of systems thinking. Just as the shift to Covey’s Principle-Centered Paradigm [Covey, 1989] enables the adoption of his Seven Habits, the shift to systems thinking enables the successful implementation of the systems approach. This change of perspective alone, however, is not enough to make either concept or approach successful. One must carry out the steps to ensure that success.

1.2.4.2 The Seven Habits of highly effective people

The Seven Habits introduced by Covey [1989] are as follows:

Habit 1: Be proactive.
Habit 2: Begin with the end in mind.
Habit 3: Put first things first.
Habit 4: Think win–win.
Habit 5: Seek first to understand, then to be understood.
Habit 6: Synergize.
Habit 7: Sharpen the saw.

The first three of the Seven Habits are the steps toward what Covey calls *Private Victory*, and Habits 4–6 are the steps toward *Public Victory*. These habits will be examined in terms of their relationships to the systems approach as represented by its guiding universal principles and by the 13 steps that manifest it. The guiding principles are as follows:

- Adhere to the systemic philosophy of holism.
- Recognize the hierarchical decisionmaking structure (multiple decisionmakers, constituencies, power brokers, etc.).
- Appreciate the multiple-objective nature:
  - There is no single solution.
  - There are choices and trade-offs.
- Respond to the temporal domain: past, present, and future.
- Incorporate the culture, vision, mentality, and interpersonal relationships—to build an informal network of trust.
- Address the uncertain world (taxonomy of uncertainty).
- Strive for continuous improvement of quality.
- Honor the cross-disciplinary nature of quality problem solving.
- Focus on the centrality of human and interpersonal relationships.

The following is a set of 13 logical steps with which to address problems [Haimes and Schneiter, 1996]:

1. Define and generalize the client’s needs. Consider the total problem environment. Clearly identify the problem.
2. Help the client determine his or her objectives, goals, performance criteria, and purpose.
3. Similar to step 1: consider the total problem’s environment. Evaluate the situation, the constraints, the problem’s limitations, and all available resources.
4. Study and understand the interactions among the environment, the technology, the system, and the people involved.

5. Incorporate multiple models and synthesize. Evaluate the effectiveness, and check the validity of the models.
6. Solve the models through simulation and/or optimization.
7. Evaluate various feasible solutions, options, and policies. How does the solution fulfill the client's needs? What are the costs, benefits, and risk trade-offs for each solution (policy option)?
8. Evaluate the proposed solution for the long term as well as the short term. In other words, what is the sustainability of the solution?
9. Communicate the proposed solution to the client in a convincing manner.
10. Evaluate the impact of current decisions on future options.
11. Once the client has accepted the solution, work on its implementation. If the solution is rejected, return to any of the above steps to correct it so that the client's desires are fulfilled.
12. Postaudit your study.
13. Iterate at all times.

1.2.4.3 Relating the Seven Habits to the systems approach

Covey's Seven Habits are not straightforward steps. The first three progress from dependence toward independence. Viewed in a problem-solving light, they make an essential contribution to the solution: The first habit frames the problem, the second determines the desired outcome, and the third organizes time and effort toward eventual solution. From this point, Habits 4–6 are guiding principles that enable personal growth toward interdependence. They stress communication and understanding in relationships and stress teamwork and creativity in the problem-solving process. Thus, they help *direct* the efforts mobilized in the first three habits. Habit 7 stresses constant reevaluation and improvement. This combination of elements is very similar to those necessary for successful systems engineering.

Habit 1: Be proactive

The first habit deals with how to view the problem and where to focus one's energies. Covey's primary tool for this habit is the set of concentric circles, the *circle of concern* and the *circle of influence*. The circle of concern includes all things that concern us. The circle of influence includes elements that are under our control. From a systems standpoint, this perspective can relate to the definition of a system and its elements, indeed an SoS. The system's boundary defines the context within which the problem will be addressed—a subset within the circle of concern that is to be studied. (It is also possible that elements in the system lie outside the circle of concern—e.g., externalities.) The state variables, which are central to system modeling, are our primary concern; however, we do not have absolute control over them. The only variables within our circle of influence are the decision variables. Random and exogenous variables and constraints are beyond our control, although we must be cognizant of them (these terms will be defined and explained in Chapter 2).

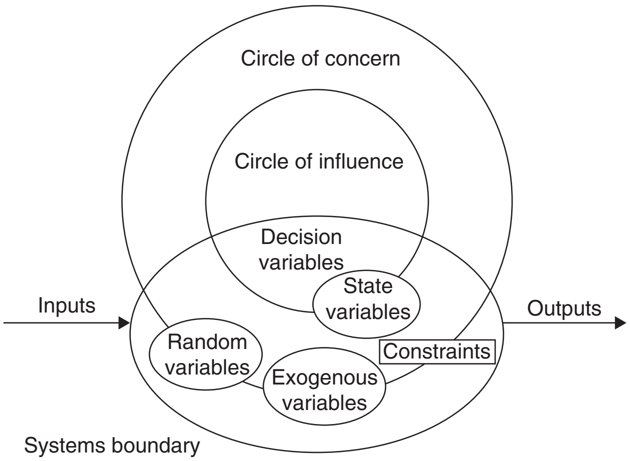

Figure 1.2 *Systemic view of concentric circles. From Haimes and Schneiter [1996]; © 1996 IEEE.*

Figure 1.2 combines Covey's key proactive circles with the elements that fully describe a system and its interrelationships.

Successful decisionmaking or problem solving requires understanding the elements within both the circle of influence and the circle of concern, that is, the elements of the SoS and its interacting environment.

Habit 2: Begin with the end in mind

In Covey's context, this habit involves mentally creating a solution to problems or developing a mission statement. Beginning with the end in mind is one of the cornerstones of systems thinking. Often referred to as the *top-down approach* to problem solving, this involves determining the overall goals for a system before beginning the design. In the filling the glass with water example, this means determining whether the goal is to fill one glass of water or many glasses or to design a useful faucet or sink. From a mathematical modeling perspective, the goal for a problem could be to minimize or maximize some function, f, of the state variables, S—for example, minimize $f(S)$. For example, we may want to minimize the distance from water level to the top of the glass, S_1, while minimizing the amount of water spilled, S_2. This can be represented as minimize $f(S_1, S_2)$.

Begin with the end in mind is also termed the leadership habit. One means of applying this is in the form of a mission statement—everything should follow from the mission statement that the leader provides. Likewise, the preliminary steps of systems engineering provide a mission for the project by determining goals, requirements, specifications, or criteria by which eventual proposed solutions will be evaluated.

In our basic example, the mental picture (goal) is a full glass of water. However, the situation is not always this simple. A more complex situation is the American effort to put a man on the moon. This is perhaps the best example of the importance of holding fast to the mental creation of an outcome. Throughout the project, the leaders kept their strong belief in this goal. This was essential because much of the necessary technology did not even exist at the outset of the project. Reliance on status quo technology or knowledge would have doomed the project—much as failure to *begin with the end in mind* would keep one from reaching personal goals.

Habit 3: Put first things first

This habit is designed to help concentrate efforts toward *more important* activities in a *less urgent* atmosphere.

Instead of trying to address the myriad problems that the first two habits may bring to the light, Covey places the emphasis on time management, leaving the eventual solution of the problem to the individual. The extensive set of actions available to help solve problems in the journey of personal growth is analogous to the array of problem-solving approaches in engineering. No specific approach is appropriate in every situation. The plethora of systems and risk-based methodologies and tools introduced in this book attest to this fact. It should be left to the individual problem solver to use the best method in a particular application. The key step is following the goal-oriented systems approach and using the most appropriate tools for the specific problem.

Time management tools commonly used in systems engineering that are analogous to Covey's time management matrix include the project evaluation and review technique (PERT) and the critical path method (CPM). Other tools such as failure mode and effects analysis (FMEA) and failure mode, effects, and criticality analysis (FMECA) are discussed in Chapter 13. In addition, Chapter 15 is devoted to project management, where time management is at the heart of project management. These help organize the order of events and assist in time management by indicating those activities whose completion times directly affect the total project time.

Habit 4: Think win–win (or no deal)

This habit illustrates the importance of the abundance mentality, a guiding principle in applying the ideas incorporated in the first three habits. Instead of focusing on outsmarting or outmaneuvering the opponent, it stresses that both parties should work together to find a mutually beneficial outcome.

This concept can come into play in the systems engineering process in several different places: in creating alternative solutions or in the working relationships of group members. Problem solving always involves trade-offs among conflicting objectives. In such situations, win–lose alternatives are abundant, but more can be gained by thinking win–win. On a more personal level, constructive cooperation between group members is essential for the eventual success of a group effort. The informal network of trust that is the foundation of successful group interaction will be eroded by win–lose thinking. A culture that embodies win–win cooperation has much greater chances for success.

Habit 5: Seek first to understand, then to be understood

This habit concerns different perspectives, implying that ordinarily adversarial roles must be overcome. This habit can be viewed on multiple levels. It is especially important in any arena where there are numerous constituencies. With the advent of cross-functional deployment, many distinct working groups are called together for a common cause. Unlike previous processes where a design group would throw plans *over the wall* to manufacturing, representatives from manufacturing are included in the design process from the start. The importance of developing a shared understanding from both perspectives is obvious.

Seek first to understand, then to be understood also highlights the importance of communication and of viewing every process from the perspective of the customer. The customer must always be satisfied, whether it is a consumer or the next workstation in an assembly process. Again, understanding the customer's perspective is essential. The application of this habit to interpersonal communication is obvious as well. Covey calls this *empathic listening*; experts in business may call this knowledge management.

Brooks [2000] offers the following succinct definition of knowledge management, which is adapted from the American Productivity and Quality Center:

> Knowledge management: Strategies and processes to create, identify, capture, organize, and leverage vital skills, information, and knowledge to enable people to best accomplish the organization mission.

In his book *Emotional Intelligence*, Goleman [1997] offers another perspective of Habit 5: "The roles for work are changing. We're being judged by a new yardstick: not just how smart we are or our expertise, but also how well we handle ourselves and each other." Relating successful individuals to personal emotional intelligence, Goleman (p. 39) quotes Gardner and Hatch [1989]: "Successful salespeople, politicians, teachers, clinicians, and religious leaders are all likely to be individuals with [a] high degree of interpersonal intelligence." Explicit in this orientation is the holistic vision that the goals of a system or a decisionmaker can be achieved by addressing and managing them as integral parts of the larger system. A central tenet of the vision of successful organizations is building and codifying trust that transcends institutions, organizations, decisionmakers, professionals, and the public at large. Their leadership has to imbue trust as the enabling landmark for knowledge management in order to lower, if not eliminate, the high *walls* and other barriers among the multiple partners of the organization. Undoubtedly, achieving this laudable goal will be a challenge in the quest to manage change.

Davenport and Prusak [1998] advocate three tenets for the establishment of trust: Trust must be visible, trust must be ubiquitous, and trustworthiness must start at the top.

Building on these three foundations of trust to realize the goals of a system means the following [Longstaff and Haimes, 2002]:

- Successful sharing of information must be built on sustained trust.
- Trust in the system is a prerequisite for its viability (e.g., a banking system that loses the trust of its customers ceases its viability).
- Trustworthiness in systems depends on their ability to be adaptable and responsive to the dynamics of people's changing expectations.
- Organizational trust cannot be achieved if the various internal and external boundaries dominate and thus stifle communication and collaboration.
- Trust in the validity of the organization's mission and agenda is a requisite for its sustained effectiveness and for the intellectual productivity of its employees; otherwise, the trust can be transient and have no problems.

Habit 6: Synergize

Habit 6 builds on the two preceding habits. With the ability to communicate openly and maturely, creative cooperation and problem solving become possible. The role of synergy in the systems approach is particularly important. According to Covey, synergy means not only that the whole is greater than the sum of the parts, but that the relationship between the parts is an element in itself. By its nature, systems engineering commonly views systems or processes as the aggregation of multiple interconnected and interdependent components. It is often helpful or instructive to understand a system by analyzing its parts, but this does not necessarily ensure a comprehensive understanding of the entire process. Only through study of the relationships among components can the true nature of the system be grasped.

Covey's discussion of synergy primarily deals with relationships among people. This, of course, is applicable to systems engineering because people with different backgrounds and positions are commonly teamed to solve a particular problem. The more successful teams will exhibit synergistic traits: They will approach the problem with open minds, they will communicate in a manner that encourages creative interaction, and they will value the differences in each other's approaches to the problem. This will enable them to recognize and assess all possible approaches as candidate solution options. Only by the inspection of all possibilities can an *optimal* solution be determined. Indeed, a basic premise of the holistic systems philosophy is that the total system is better than the sum of its parts. Chapter 3, which is devoted to modeling the multiple perspectives and dimensions of a system, highlights the imperativeness of group synergy in system modeling and thus in decisionmaking.

Habit 7: Sharpen the saw

By concluding with this habit, Covey hopes that people will continually reevaluate their personal progress, reshape their goals, and strive to improve. These issues have become quite common in engineering environment—often referred to as *kaizen*, the Japanese word for continuous improvement [Imai, 1986]. An application of this habit is also seen in the Shewhart cycle [Deming, 1986]. Iteration also plays a primary role in systems engineering. In a relationship with a client, it is necessary to receive constant feedback to ensure correct understanding, building on emotional intelligence. As our knowledge about a system develops throughout the problem-solving process, it is necessary to reevaluate the original goals. The centrality of humans in the life cycle of systems calls for individuals who can perform under pressure by continuously rejuvenating and recharging themselves.

1.2.4.4 The Seven Habits compared to the systems approach

The relationship between Covey's philosophy for personal change and the systems approach is further illustrated by a pairwise comparison of the two, as shown in Figure 1.3. The fact that Habit 1 corresponds to Steps 1, 3, and 4 indicates that these problem-definition steps could be grouped together. They should all be completed before the goals are determined. When these three steps are grouped together, Covey's first three habits correspond to the order of problem solving following the systems approach. First, the problem is defined, then the desired outcome is envisioned, and time and effort are organized to achieve this desired outcome. The general reference to problem solution in Habit 3, *Put first things first*, corresponds to many steps in this systems approach. Figure 1.3 indicates that these, too, could be integrated into a single category.

Habits 4–6 are more difficult to apply to specific steps. Analogous to the overriding principles enumerated in Figure 1.3, these habits are applicable throughout the problem-solving process. To the extent that these steps promote communication, the habits *think win–win* and *seek first to understand…* apply to almost every situation that involves group interaction. More specifically, *think win–win* can apply to creative problem solving and idea generation, and *seek first to understand…* directs the interaction between a systems engineer and a client. *Synergize* can also be applied on numerous levels. Finally, *sharpen the saw* directly corresponds to the constant iteration that is stressed throughout the systems engineering approach.

In sum, the side-by-side comparison of the seven habits and the steps in the systems approach serves to show how the elements of both not only correspond to, but also complement, each other. Both philosophies stress problem definition, early determination of the desired outcome, and an organized effort to determine a solution. They also promote similar overriding principles to better enable the problem-solving process. This similarity is remarkable given that the seven habits are a guide to personal development, whereas the systems approach is geared for systems design, development, and management. Most important, comparing Covey's philosophy as described earlier can help improve the understanding of systems engineering and thus better relate the process of risk assessment and management to the systems approach.

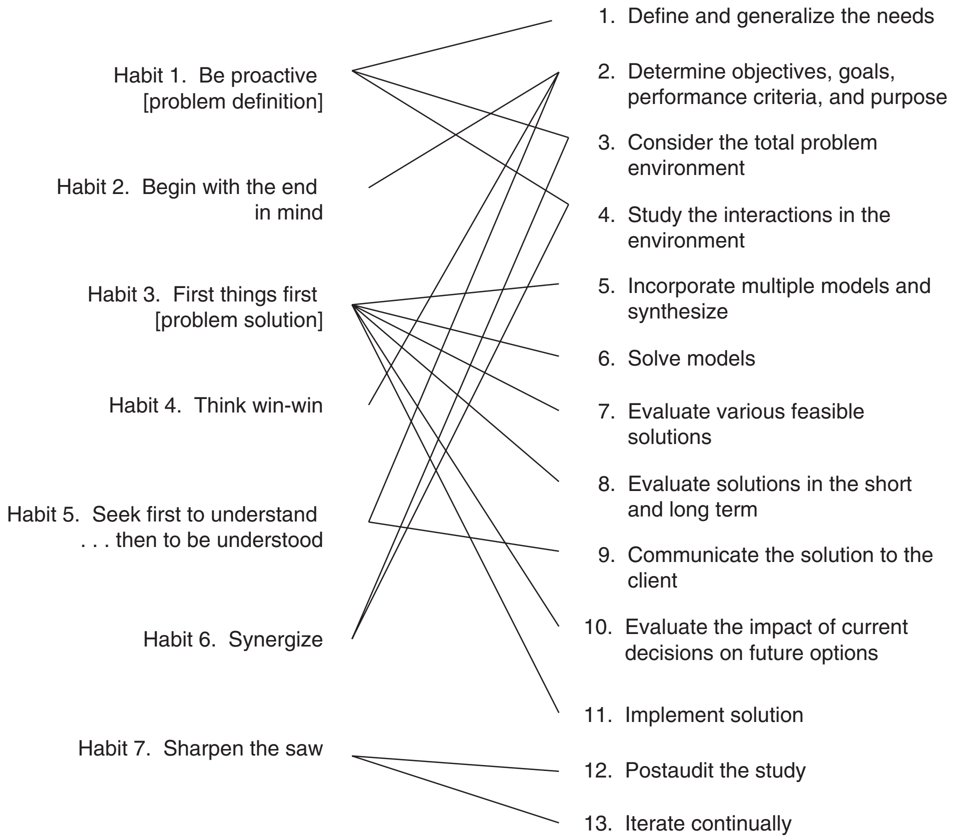

Figure 1.3 *Juxtaposition of the seven habits [Covey, 1989] with the systems approach. From Haimes and Schneiter [1996]; © 1996 IEEE.*

1.3 RISK ASSESSMENT AND MANAGEMENT

1.3.1 Holistic Approach

Good management of both technological and nontechnological systems must address the holistic nature of the system in terms of its hierarchical, organizational, and fundamental decisionmaking structure. Also to be considered are the multiple noncommensurate objectives, subobjectives, and sub-subobjectives, including all types of important and relevant risks; the various time horizons; the multiple decisionmakers, constituencies, power brokers, stakeholders, and users of the system; as well as a host of institutional legal and other socioeconomic conditions. Thus, risk management raises several fundamental philosophical and methodological questions [Fischhoff et al., 1983; Hall, 1989; Krimsky and Golding, 1992; Lewis, 1992; Burke et al., 1993; Wernick, 1995; Bernstein, 1996; Kunreuther and Slovic, 1996; Kaplan et al., 2001; NRC, 2002].

Engineering systems are almost always designed, constructed, integrated, and operated under unavoidable conditions of risk and uncertainty and are often expected to achieve multiple and conflicting objectives. Identifying, quantifying, evaluating, and trading off risks, benefits, and costs should constitute an integral and explicit component of the overall managerial decisionmaking process and should not be a separate, cosmetic afterthought. The body of knowledge in risk assessment and management has gained significant attention during the last three decades (and especially since the September 11, 2001, attack on the United States); it spans many disciplines and encompasses empirical and quantitative as well as normative, judgmental aspects of decisionmaking. Does this constitute a new discipline that is separate, say, from systems engineering and systems analysis? Or has systems engineering and systems analysis been too narrowly defined? When risk and uncertainty are addressed in a practical decisionmaking framework, has it been properly perceived that the body of knowledge known as risk assessment and management markedly fills a critical void that supplements and complements the theories and methodologies of systems engineering and systems analysis? Reflecting on these and other similar questions on the nature, role, and place of risk assessment and management in managing technological and nontechnological systems and in the overall managerial decisionmaking process should stem not from intellectual curiosity only. Rather, considering such questions should provide a way to bridge the gaps and remove some of the barriers that exist between the various disciplines [Haimes, 1989].

As will be discussed in more detail in this book, integrating and incorporating risk assessment and management of technological and nontechnological systems within the broader holistic approach to technology management also require the reexamination of the expected-value concept when it is used as the sole representation of risk. Many agree that in the expectation operation, commensurating high-frequency/low-damage and low-frequency/catastrophic-damage events markedly distorts their relative importance and consequences as they are viewed, perceived, assessed, evaluated, and traded off by managers, decisionmakers, and the public. Some are becoming more and more convinced of the grave limitations of the traditional and commonly used expected-value concept; and they are complementing and supplementing the concept with conditional expectation, where decisions about extreme and catastrophic events are not averaged out with more commonly occurring events. In Chapter 8 and throughout this book, risk of extreme and catastrophic events will be explicitly addressed and quantified, and the common expected-value metric for risk will be supplemented and complemented with the conditional expected value of risk.

1.3.2 The Evolution of Risk Analysis

In March 1961, Norbert Wiener, who is considered by many to be one of the fathers of what is known today as systems engineering, wrote the following in the Preface of the second edition of his book *Cybernetics* [Wiener, 1961]:

> If a new scientific subject has real vitality, the center of interest in it must and should shift in the course of years…. The role of information and the technique of measuring and transmitting information constitute a whole discipline for the engineer, for the physiologist, for the psychologist, and for the sociologist…. Thus it behooves the cyberneticist to move on to new fields and to transfer a large part of his attention to ideas which have arisen….

If one accepts the premise that good and appropriate technology management must be grounded in a holistic approach and based on Wiener's philosophical and almost prophetic statements, then it is possible that what we are witnessing today is a shift of the center of interest, an evolution toward a more holistic approach to management. Is knowledge from diverse disciplines converging into a more coherent, albeit still heterogeneous, aggregate of theory, methodologies, tools, and heuristics? To highlight this evolutionary process, let us consider Wiener's *shift* from single-objective modeling and optimization to multiple-objective modeling and optimization. The 1970s saw the emphasis shift from the dominance of single-objective modeling and optimization toward an emphasis on multiple objectives. During the past three decades, the consideration of multiple objectives in modeling and decisionmaking has grown by leaps and bounds. This has led to the emergence of a new field that has come to be known as *multiple criteria decisionmaking* (MCDM). MCDM has emerged as a philosophy that integrates common sense with empirical, quantitative, normative, descriptive, and value-judgment-based analysis. MCDM, as a subset of systems engineering, is also a philosophy that is supported by advanced systems concepts (e.g., data management procedures, modeling methodologies, optimization and simulation techniques, and decisionmaking approaches) that are grounded in both the arts and sciences for the ultimate purpose of improving the decisionmaking process. Multiple objectives are incorporated into most modeling and optimization of technological systems today.

1.3.3 Risk Communication

The risk assessment and management process is aimed at answering specific questions in order to make better decisions under uncertain conditions. In system modeling, the saying is that a model must be as simple as possible and as complex as desired and required. Similarly, the process of risk assessment and management must follow these same basic principles. These seemingly conflicting simultaneous attributes—simplicity and complexity—can be best explained and justified through effective risk communication. Invariably, the questions raised during the risk assessment and management process originate from decisionmakers at various levels of responsibilities, including managers, designers, stakeholders, journalists and other media professionals, politicians, proprietors, and government or other officials. Although the issues under consideration and their associated questions may be complex and require similarly complex sets of answers, it is imperative that their meanings and ramifications be understood by the decisionmakers. Inversely, for the risk assessment and management process to be effective and complete, decisionmakers, who originate the risk-based questions for the analysts, must be able to communicate openly, honestly, and comprehensively the multidimensional perspectives of the challenges facing them and for which they desire better understanding and possible answers. In turn, risk analysts must be able to translate complex technical analysis and results into a language to which decisionmakers can relate, understand, and incorporate into actionable decisions.

This intricate mental and intellectual dance between risk analysts and decisionmakers was comprehensively addressed in three seminal books with diverse titles: *Good to Great*, *Working with Emotional Intelligence*, and *Working Knowledge*. In his book *Good to Great*, Collins [2001] addresses the importance of the culture of discipline, transcending disciplined people, disciplined thought, and disciplined actions. He explains [p. 200]: "When you have a culture of discipline, you can give people more freedom to experiment and find their own best path to results." On the same page, Collins juxtaposes clock building with time telling: "Operating through sheer force of personality as a disciplinarian is time telling; building an enduring culture of discipline is clock building." These are important requisite traits for effective working relationships between decisionmakers and risk analysts. Goleman [1998, p. 211], in *Working with Emotional Intelligence*, identifies the following elements of competence when people collaborate and cooperate with others toward shared goals: "Balance a focus on task with attention to relationships; collaborate, sharing plans, information, and resources; promote a friendly, cooperative climate; and spot and nurture opportunities for collaboration." Goleman states on page 317 that "emotional intelligence refers to the capacity for recognizing our own feelings and those of others, for motivating ourselves, and for managing emotions well in ourselves and in our relationships." Indeed, these fundamentals are the sine qua non for effective risk communication among all parties involved in the entire process of risk assessment and management.

Invariably, complex problems cannot be solved without addressing their multiple perspectives, scales of complexity, time dependencies, and multiple interdependencies, among others. Among the many parties commonly involved in the process of risk assessment and risk management are the professionals supporting the decisionmakers, the risk analysts, and the decisionmakers themselves. Knowledge management, which builds on embracing trust, exchange of information, and collaboration within and among organization, parties, and individuals, has become essential to performing and successfully deploying the results and fruits of risk assessment and management. Moreover, knowledge management may be viewed, in many ways, as synonymous to effective risk communication. In their book *Working Knowledge*, Davenport and Prusak [1998, p. 62] identify the following five knowledge management principles that can help make the above fusion among the parties work effectively:

1. Foster awareness of the value of the knowledge sought and a willingness to invest in the process of generating it.
2. Identify key knowledge workers who can be effectively brought together in a fusion effort.
3. Emphasize the creative potential inherent in the complexity and diversity of ideas, seeing differences as positive, rather than sources of

conflict, and avoiding simple answers to complex questions.

4. Make the need for knowledge generation clear so as to encourage, reward, and direct it toward a common goal.
5. Introduce measures and milestones of success that reflect the true value of knowledge more completely than simple balance-sheet accounting.

In sum, embracing the principles advocated by these three books provides an important road map for risk communication and thus for a complete and successful risk assessment, risk management, and risk communication process (see Figure 1.5). The philosopher Peter F. Drucker [2004, p. 9] eloquently sums up his message to organizations: "Attract and hold the highest-producing knowledge workers by treating them and their knowledge as the organization's most valuable assets."

1.3.4 Sources of Failure, Risk Assessment, and Risk Management

In the management of technological systems, the failure of a system can be caused by failure of the *hardware*, the *software*, the *organization*, or the *humans* involved. Of course, the initiating events may also be natural occurrences, acts of terrorism, or other incidents.

The term *management* may vary in meaning according to the discipline involved and/or the context. *Risk* is often defined as a measure of the probability and severity of adverse effects. *Risk management* is commonly distinguished from *risk assessment*, even though some may use the term *risk management* to connote the entire process of risk assessment and management. In risk assessment, the analyst often attempts to answer the following set of triplet questions [Kaplan and Garrick, 1981]:

- What can go wrong?
- What is the likelihood that it would go wrong?
- What are the consequences?
- Here we add a fourth question: What is the time frame?

Answers to these questions help risk analysts identify, measure, quantify, and evaluate risks and their consequences and impacts. Risk management builds on the risk assessment process by seeking answers to a second set of three questions [Haimes, 1991]:

- What can be done and what options are available?
- What are the associated trade-offs in terms of all relevant costs, benefits, and risks?
- What are the impacts of current management decisions on future options?

Note that the last question is a most critical one for any managerial decisionmaking. This is so because unless the negative and positive impacts of current decisions on future options are assessed and evaluated (to the extent possible), these policy decisions cannot be deemed to be *optimal* in any sense of the word. Indeed, the assessment and management of risk is essentially a synthesis and amalgamation of the empirical and normative, the quantitative and qualitative, and the objective and subjective effort. Only when these questions are addressed in the broader context of management, where all options and their associated trade-offs are considered within the hierarchical organizational structure, can a total risk management (TRM) be realized. (The term TRM will be formally defined later.) Indeed, evaluating the total trade-offs among all important and relative system objectives in terms of costs, benefits, and risks cannot be done seriously and meaningfully in isolation from the modeling of the system and the broader resource allocation perspectives of the overall organization.

Good management must thus incorporate and address risk management within a holistic and all-encompassing framework that incorporates and addresses all relevant resource allocation and other related management issues. A TRM approach that harmonizes risk management with the overall system management must address the following four sources of failure (see Figure 1.4):

- Hardware failure
- Software failure
- Organizational failure
- Human failure

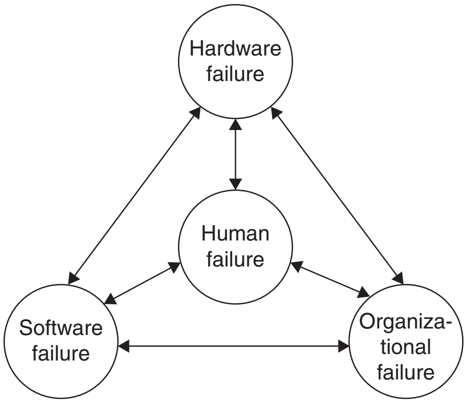

Figure 1.4 System failure.

The above set of sources of failure is intended to be internally comprehensive (i.e., comprehensive within the system's own internal environment). (External sources of failures are not discussed here because they are commonly system dependent.) These four elements are not necessarily independent of each other, however. The distinction between software and hardware is not always straightforward, and separating human and organizational failure is often not an easy task. Nevertheless, these four categories provide a meaningful foundation upon which to build a TRM framework. In his premier book on quality control, *Kaizen*, Imai [1986] states: "The three building blocks of business are hardware, software, and 'humanware.'" He further states that total quality control "means that quality control effects must involve people, organization, hardware, and software." Effective knowledge management within an organization, is instrumental in reducing the rates of these sources of failure.

Organizational errors are often at the root of failures of critical engineering systems. Yet, when searching for risk management strategies, engineers often tend to focus on technical solutions, in part because of the way risks and failures have been analyzed in the past. In her study of offshore drilling rigs, Paté-Cornell [1990] found that over 90% of the failures documented were caused by organizational errors. The following is a list of common organizational errors:

- Overlooking and/or ignoring defects
- Tardiness in correcting defects
- Breakdown in communication
- Missing signals or valuable data due to inadequate inspection or maintenance policy
- Unresolved conflict(s) between management and staff
- Covering up mistakes due to competitive pressure
- Lack of incentives to find problems
- The *kill the messenger* syndrome instead of *reward the messenger*
- Screening information, followed by denial
- Tendency to accept the most favorable hypothesis
- Ignoring long-term effects of decisions
- Loss of institutional memory
- Loss of flexibility and innovation

The importance of considering the four sources of failure is twofold. First, they are comprehensive, involving all aspects of the system's life cycle (e.g., planning, design, construction, integration, operation, and management). Second, they require the total involvement in the risk assessment and management process of everyone concerned—blue- and white-collar workers and managers at all levels of the organizational hierarchy.

1.3.5 TRM

TRM can be defined as a systematic, statistically based, holistic process that builds on quantitative risk modeling, assessment, and management. It answers the previously introduced two sets of questions for risk assessment and risk management, and it addresses the set of four sources of failures within a hierarchical–multiobjective framework. Figure 1.5 depicts the TRM paradigm (the time dimension is implicit in Figure 1.5).

The term *hierarchical–multiobjective framework* can be explained in the context of TRM. Most, if not all, organizations are hierarchical in their structure and, consequently, in the decisionmaking process that they follow. Furthermore, at each level of the organizational hierarchy, multiple, conflicting, competing, and noncommensurate objectives drive the decisionmaking process. At the heart of good management decisions is the *optimal* allocation of the organization's resources among its various hierarchical levels and subsystems. The *optimal*

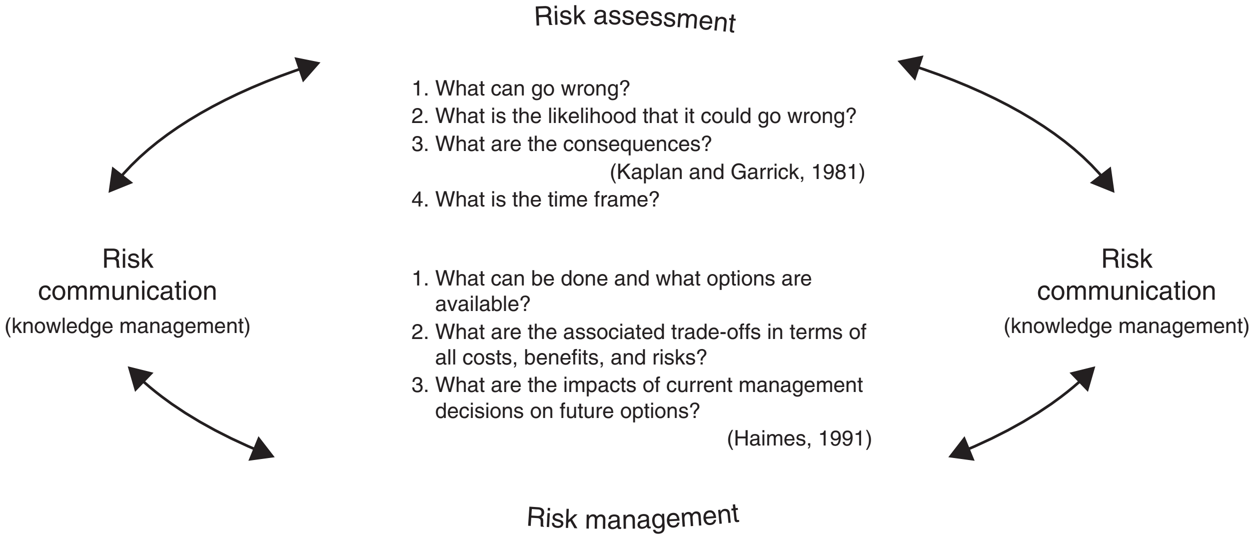

Figure 1.5 *Total risk management.*

allocation is meant in the Pareto-optimal sense, where trade-offs among all costs, benefits, and risks are evaluated in terms of hierarchical objectives (and subobjectives) and in terms of their temporal impacts on future options. Methodological approaches for such hierarchical frameworks are discussed in Haimes et al. [1990].

1.3.6 Multiple Objectives: The Student's Dilemma

The trade-offs among multiple noncommensurate and often conflicting and competing objectives are at the heart of risk management (Chapter 5 is devoted in its entirety to multiobjective analysis). Lowrance [1976] defines safety as the level of risk that is deemed acceptable, and one is invariably faced with deciding the level of safety and the acceptable cost associated with that safety [Chankong and Haimes, 1983, 2008]. The following student dilemma is used to demonstrate the fundamental concepts of Pareto-optimality and trade-offs in a multiobjective framework.

A student working part time to support her college education is faced with the following dilemma that is familiar to all of us:

$$\text{Maximize}\begin{cases}\text{income from part-time work}\\ \text{grade-point average}\\ \text{leisure time}\end{cases}$$

In order to use the two-dimensional plane for graphic purposes, we will restrict our discussion to two objectives: maximize income and maximize grade-point average (GPA). We will assume that a total of 70 h/week are allocated for studying and working. The remaining 98 h/week are available for *leisure time*, covering all other activities. Figure 1.6 depicts the income generated per week as a function of hours of work. Figure 1.7 depicts the relationship between studying and GPA. Figure 1.8 is a dual plotting of both functions (income and GPA) versus working time and studying time, respectively.

The concept of optimality in multiple objectives differs in a fundamental way from that of a single-objective optimization. *Pareto-optimality* in a multiobjective framework is that solution, policy, or option for which one objective function can be improved only at the expense of degrading another. A Pareto-optimal solution is also known as a noninferior, nondominated, or efficient solution (see Chapter 5). In Figure 1.6, for example, studying up to 60 h/week (and correspondingly working 10 h/week) is Pareto-optimal, since in this range income is sacrificed for a higher GPA. On the other hand, studying over 60 h/week (or working <10 h/week) is a non-Pareto-optimal policy, since in this range both income and GPA are diminishing. Similarly, a non-Pareto-optimal solution is also known as an inferior, dominated, or nonefficient solution. Figure 1.9 further distinguishes between Pareto- and

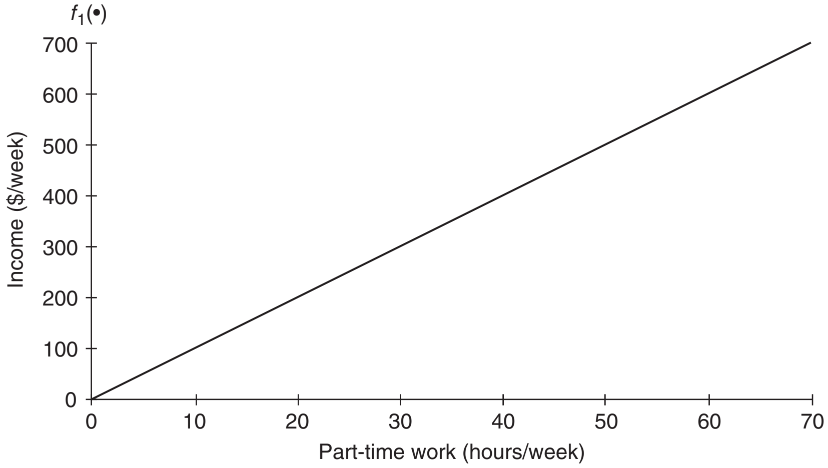

Figure 1.6 *Income from part-time work.*

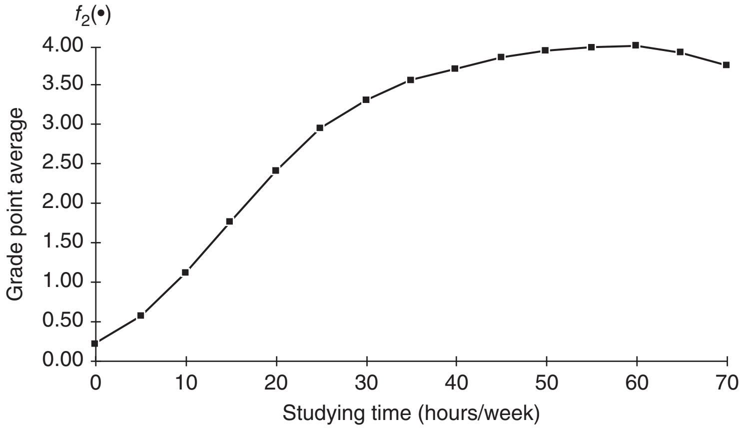

Figure 1.7 *GPA as a function of studying time.*

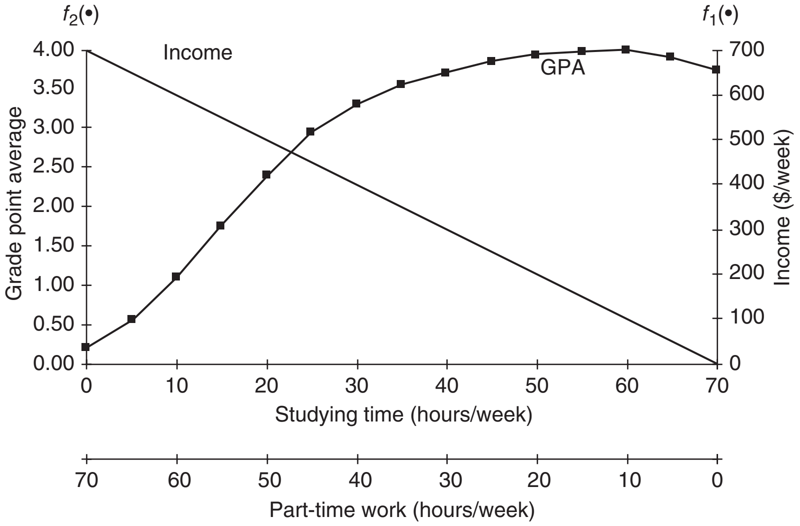

Figure 1.8 *GPA versus income.*

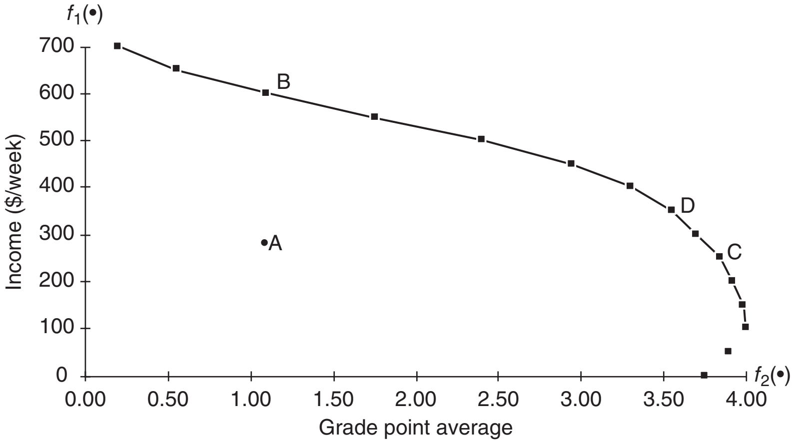

Figure 1.9 *Pareto-optimal frontier.*

non-Pareto-optimal solutions by plotting income versus GPA. The line connecting all the square points is called the Pareto-optimal frontier. Note that any point interior to this frontier is non-Pareto-optimal. Consider, for example, policy option A. At this point, the student makes $300 per week at a GPA of just above one, whereas at point B, she makes $600 per week at the same GPA level. One can easily show that all points (policy options) interior to the Pareto-optimal frontier are inferior points.

Consider the risk of groundwater contamination as another example. We can generate the Pareto-optimal frontier for this risk-based decisionmaking. Minimizing the cost of contamination prevention and the risk of contamination is similar in many ways to generating the Pareto-optimal frontier for the student dilemma problem. Determining the best work–study policy for the student can be compared to determining (at least implicitly) the level of safety—that is, the level of acceptability of risk of contamination and the cost associated with preventing such contamination. To arrive at this level of acceptable risk, we will again refer to the student dilemma problem illustrated in Figure 1.9. At point B, the student is making about $600 per week at a GPA of just above 1. Note that the slope at this point is about $100 per week for each 1 GPA. Thus, the student will opt to study more. At point C, the student can achieve a GPA of about 3.6 and a weekly income of about $250. The trade-off (slope) at this point is very large: By sacrificing about 0.2 GPA, the student can increase her income by about $200 per week. Obviously, the student may choose neither policy B nor C; rather she may settle for something like policy D, with an acceptable level of income and GPA. In a similar way, and short of strict regulatory requirements, a decisionmaker may determine the level of resources to allocate for preventing groundwater contamination at an acceptable level of risk of contamination.

In summary, the question is: Why should we expect environmental or other technologically based problems involving risk–cost–benefit trade-offs to be any easier than solving the student dilemma?

A single decisionmaker as in the student dilemma problem is not common, especially when dealing with public policy; rather, the existence of multiple decisionmakers is more prevalent. Indeed, policy options on important and encompassing issues are rarely formulated, traded off, evaluated, and finally decided upon at one single level in the hierarchical decisionmaking process. Rather, a hierarchy that represents various constituencies, stakeholders, power brokers, advisers, administrators, and a host of shakers and movers constitutes the true players in the complex decisionmaking process. For more on multiobjective analysis, see Chapter 5, Haimes and Hall [1974], Chankong and Haimes [2008], and Haimes et al. [1994].

1.3.7 The Perception of Risk

The enormous discrepancies and monumental gaps in the dollars spent by various federal agencies in their quest to save human lives can no longer be justified under austere budgetary constraints. These expenditures vary within five to six orders of magnitude. For example, according to Morrall [2003], the cost per life saved by regulating oil and gas well service is $100,000 (1984 dollars); for formaldehyde, it is $72 billion, and for asbestos, it is $7.4 million (see Table 1.1).

A natural and logical set of questions arises: What are the sources of these gaps and discrepancies? Why do they persist? And what can be done to synchronize federal agency policies on the value of human life? A somewhat simplistic, albeit pointed, explanation may be found in the lexicon of litigation, intimidation, fear, and public pressure in the media and by special interest groups as well as in the electoral and political processes. Larsen [2007] offers interesting views on government spending and on the perception of risk. Keeping the threat of terrorism in perspective, he writes on page 22:

> Nearly 2,000 Americans died on 9/11. It was a human tragedy on a scale that was difficult for most of us to comprehend. However, during a four-year period from January 2002 to December 31, 2005, not a single American died in our homeland from international terrorism. During the same period, 20,000 Americans died from food poisoning, 160,000 died in automobile accidents, and nearly 400,000 died from medical mistakes.

US companies have ample statistical information on the costs of improved product safety but are most careful to keep their analyses secretive and confidential [Stern and Fineberg, 1996]. Our litigious society has effectively prevented industry and government from both explicitly developing and publicly sharing such analyses [Fischhoff et al., 1983; Douglas, 1990; Sage, 1990; The Royal Society, 1992; NRC, 1996].

What is needed is at least a temporary moratorium on litigation in this area. We should extend immunity and indemnification to all analysts and public officials engaged in quantifying the cost-effectiveness of all expenditures aimed at saving human lives and/or preventing sickness or injury. In sum, we ought to generate a public atmosphere that is conducive to open dialogue and reason and to a holistic process of risk assessment and management.

1.3.8 The Central Tendency Measure of Risk and Risk of Extreme Events

The expected value of risk is an operation that essentially multiplies the consequences of each event by its probability of occurrence and sums (or integrates) all these products over the entire universe of events. This operation literally commensurates adverse events of high consequences and low probabilities with events of low consequences and high probabilities. In the classic expected-value approach, extreme events with low probability of occurrence are each given the same proportional importance regardless of their potential catastrophic and irreversible impact. This mathematical operation is similar to the precommensuration of multiple objectives through the weighting approach (see Chapter 5).

The major problem for the decisionmaker remains one of information overload: For every policy, action, or measure adopted, there will be a vast array of potential consequences as well as benefits and costs with their associated probabilities. It is at this stage that most analysts are caught in the pitfalls of the unqualified expected-value analysis. In their quest to protect the decisionmaker from information overload, analysts precommensurate catastrophic damages that have a low probability of occurrence with minor damages that have a high probability. From the perspective of public policy, it is obvious that a catastrophic dam failure or major flood that has a very low probability of happening cannot be viewed by decisionmakers in the same vein as minor flooding that has a high probability of happening. This is exactly what the expected-value function would ultimately generate. Yet, it is clear to any practitioner or public official involved in flood management that the two cases are far from being commensurate or equal. Most important, the analyst's precommensuration of these low-probability, high-damage events with high-probability, low-damage events into one expectation function (indeed some kind of a utility function) markedly distorts the relative importance of these events and consequences as they are viewed, assessed, and evaluated by the decisionmakers. This is similar to the dilemma that used to face theorists and practitioners in the field of MCDM [Haimes et al., 1990; Chankong and Haimes, 2008] (see Chapter 5 for discussion on MCDM and multiobjective analysis).

TABLE 1.1 Comparative Costs of Safety and Health Regulations

Regulation	Year	Agency	Status[a]	Initial Annual Risk Estimate[b]	Lives Saved Annually	Cost per Life Saved ($ Thousand, 1984)
Steering column protection	1967	NHTSA	F	7.7 in 10^5	1,300,000	100
Unvented space heaters	1980	CPSC	F	2.7 in 10^5	63,000	100
Oil and gas well service	1983	OSHA-S	P	1.1 in 10^3	50,000	100
Cabin fire protection	1985	FAA	F	6.5 in 10^8	15,000	200
Passive restraints/belts	1984	NHTSA	F	9.1 in 10^5	1,850,000	300
Fuel system integrity	1975	NHTSA	F	4.9 in 10^6	400,000	300
Trihalomethanes	1979	EPA	F	6.0 in 10^6	322,000	300
Underground construction	1983	OSHA-S	P	1.6 in 10^3	8,100	300
Alcohol and drug control	1985	FRA	F	1.8 in 10^6	4,200	500
Servicing wheel rims	1984	OSHA-S	F	1.4 in 10^5	2,300	500
Seat cushion flammability	1984	FAA	F	1.6 in 10^7	37,000	600
Floor emergency lighting	1984	FAA	F	2.2 in 10^8	5,000	700
Crane suspended personnel platform	1984	OSHA-S	P	1.8 in 10^3	5,000	900
Children's sleepwear flammability	1973	CPSC	F	2.4 in 10^6	106,000	1,300
Side doors	1970	NHTSA	F	3.6 in 10^5	480,000	1,300
Concrete and masonry construction	1985	OSHA-S	P	1.4 in 10^5	6,500	1,400
Hazard communication	1983	OSHA-S	F	4.0 in 10^5	200,000	1,800
Grain dust	1984	OSHA-S	P	2.1 in 10^4	4,000	2,800
Benzene/fugitive emissions	1984	EPA	F	2.1 in 10^5	0,310	2,800
Radionuclides/uranium mines	1984	EPA	F	1.4 in 10^4	1,100	6,900
Asbestos	1972	OSHA-H	F	3.9 in 10^4	396,000	7,400
Benzene	1985	OSHA-H	P	8.8 in 10^4	3,800	17,100
Arsenic/glass paint	1986	EPA	F	8.0 in 10^4	0,110	19,200
Ethylene oxide	1984	OSHA-H	F	4.4 in 10^5	2,800	25,600
Arsenic/copper smelter	1986	EPA	F	9.0 in 10^4	0,060	26,500
Uranium mill tailings/inactive	1983	EPA	F	4.3 in 10^4	2,100	27,600
Acrylonitrile	1978	OSHA-H	F	9.4 in 10^4	6,900	37,600
Uranium mill tailings/active	1983	EPA	F	4.3 in 10^4	2,100	53,000
Coke ovens	1976	OSHA-H	F	1.6 in 10^4	31,000	61,800
Asbestos	1986	OSHA-H	F	6.7 in 10^5	74,700	89,300
Arsenic	1978	OSHA-H	F	1.8 in 10^3	11,700	92,500
Asbestos	1986	EPA	P	2.9 in 10^5	10,000	104,200
DES (cattle feed)	1979	FDA	F	3.1 in 10^7	68,000	132,000
Arsenic/glass manufacturing	1986	EPA	R	3.8 in 10^5	0,250	142,000
Benzene/storage	1984	EPA	R	6.0 in 10^7	0,043	202,000
Radionuclides/DOE facilities	1984	EPA	R	4.3 in 10^6	0,001	210,000
Radionuclides/elemental phosphorus	1984	EPA	R	1.4 in 10^5	0,046	270,000
Acrylonitrile	1978	OSHA-H	R	9.4 in 10^4	0,600	308,000
Benzene/ethylbenzenol styrene	1984	EPA	R	2.0 in 10^8	0,006	483,000
Arsenic/low-arsenic copper	1986	EPA	R	2.6 in 10^4	0,090	764,000
Benzene/maleic anhydride	1984	EPA	R	1.1 in 10^6	0,029	820,000
Land disposal	1986	EPA	P	2.3 in 10^8	2,520	3,500,000
EDB	1983	OSHA-H	P	2.5 in 10^4	0,002	15,600,000
Formaldehyde	1985	OSHA-H	P	6.8 in 10^7	0,010	72,000,000

From Morrall [2003].

CPSC, Consumer Product Safety Commission; EPA, Environment Protection Agency; FAA, Federal Aviation Administration; FDA, Food and Drug Administration; NHTSA, National Highway Traffic Safety Administration; OSHA-H, Occupational Safety and Health Administration.

[a] Proposed, rejected, or final rule.

[b] Annual deaths per exposed population.

This act of commensurating the expected-value operation is analogous in some sense to the commensuration of all benefits and costs into one monetary unit. Indeed, few today would consider benefit–cost analysis, where all benefits, costs, and risks are commensurated into monetary units, as an adequate and acceptable measure for decisionmaking when it is used as the sole criterion for excellence. Close to four decades ago, multiple-objective analysis was demonstrated as a superior approach to benefit–cost analysis [Haimes, 1970; Haimes et al., 1971; Haimes and Hall, 1974]. In many respects, the expected value of risk is similar in its theoretical–mathematical construct to the commensuration of all costs, benefits, and risks into monetary units.

One of the most important steps in the risk assessment process is the quantification of risk. Yet the validity of the approach most commonly used to quantify risk—its expected value—has received neither the broad professional scrutiny it deserves nor the hoped-for wider mathematical challenge that it mandates. One of the few exceptions is the conditional expected value of the risk of extreme events (among other conditional expected values of risks) generated by the *partitioned multiobjective risk method* (PMRM) [Asbeck and Haimes, 1984] (see Chapters 8 and 11).

1.3.9 Software Risk Management

Computers have become pervasive in our society. They are integral to everything from VCRs and video games to power plants and control systems for aircraft. Computers enhance satellite communications systems that provide television nationwide; they enabled the governments (as well as CNN) to communicate during wars and other major national and international events. Computers touch the lives of most people daily.

Computers are composed of two major components. One is hardware: the power supply, printed circuit boards, and CRT screens. The other is software, sometimes thought of as the computer's intelligence.

Software engineering, unlike traditional forms of engineering, has no foundation in physical laws. The source of the structure for software engineering is in standards and policies that are defined by teams of experts. Because software is founded only in mathematics and logic and not in physical laws (except that the software logic must comply with physical laws), the risk of introducing uncertainty and other sources of failure into a software system is greater than in any other field.

Effective control of uncertainties introduced during the software development cycle should be through very stringent management. This has not been the case; to date, there has not been a well-defined process for supervising software development [Chittister and Haimes, 1994; Boehm, 2006; Jackson, 2006; Post et al., 2006]. Chapter 17 offers additional discussion on risks associated with software engineering.

The increasing dominance of computers in the design, manufacture, operation, maintenance, and management of most small- and all large-scale engineering systems has made possible the resolution of many complex technological problems. At the same time, the increased influence of software in decisionmaking has introduced a new dimension to the way business is done in engineering quarters; many former engineering decisions have been or soon will be transferred to software, albeit in a limited and controlled manner. This power shift in software functionality (from the centrality of hardware in system control and operations to software), the explicit responsibility and accountability of software engineers, and the expertise required of technical professionals on the job have interesting manifestations and implications, and they offer challenges to the professional community to adapt to new realities. All of these affect the assessment and management of risk associated with software development and use. Perhaps one of the most striking manifestations of this power shift relates to real-time control systems. Consequently, the impact of software on the reliability and performance of monitoring and warning systems for natural hazards is becoming increasingly more significant. Furthermore, the advances in hardware technology and reliability and the seemingly unlimited capabilities of computers render the reliability of most systems heavily dependent on the integrity of the software used. Thus, software failure must be scrutinized with respect to its contribution to overall system failure, along with the same diligence and tenacity that have been devoted to hardware failure.

1.3.10 Risk Characteristics of Engineering-Based Systems

In spite of some commonalities, there are inherent differences between natural systems (e.g., environmental, biological, and ecological systems) and man-made, engineering-based systems. In this section, it is constructive to focus on the characteristics of risk associated with engineering-based systems.

The following 12 risk characteristics are endemic to most engineering-based systems:

1. *Organizational failures of engineering-based systems are likely to have dire consequences*. Risk management of technological systems must be an integral part of overall systems management. Organizational failures often constitute a major source of risk of overall system failure.
2. *Risk of extreme and rare events is misrepresented when it is solely measured by the expected value of risk*. The precommensuration of rare but catastrophic events of low probability with much less adverse events of high probability in the expected-value measure of risk can lead to misrepresentation and mismanagement of catastrophic risk.
3. *Risk of project cost overrun and schedule delay*. Projects involving engineering-based systems have been experiencing major cost overruns and delays in schedule completion, particularly for software-intensive systems. The process of risk assessment and management is also the sine qua non requirement for ensuring against unwarranted delay in a project's completion schedule, cost overrun, and failure to meet performance criteria.
4. *Risk management as a requisite for engineering-based systems integration*. Effective systems integration necessitates that all functions, aspects, and components of the system must be accounted for along with an assessment of the associated risks. Furthermore, for engineering-based systems, systems integration is not only the integration of components but also an understanding of the functionality that emerges as a by-product from the integration.
5. *Rehabilitation and maintenance of physical infrastructure*. Maintaining and rehabilitating physical infrastructures, such as water distribution networks, have become an important issue as nations address the risk of their infrastructure failure. Accurate assessment of the risks of failure of deteriorating physical infrastructures is a prerequisite for the optimal allocation of limited resources.
6. *Multiple failure modes and multiple reliability measures for engineering-based systems*. Engineering-based systems often have any number of paths to failure. Evaluating the interconnected consequences of multiple modes of failure is central to risk assessment and management of engineering systems.
7. *Risk in software engineering development*. The development of software engineering—an intellectual, labor-intensive activity—has been marred by software that does not meet performance criteria while experiencing cost overruns and time and delivery delays. An integrated and holistic approach to software risk management is imperative.
8. *Risk to emergent and safety-critical systems*. Assessing and managing risk to emergent and safety-critical systems is not sufficient without building resilience in such systems. This means ensuring that even in the remote likelihood of a system failure, there will be a safe shutdown without catastrophic consequences to people or facilities. Examples of such critical systems include transportation systems, space projects, the nuclear industry, and chemical plants.
9. *Cross-disciplinary nature of engineering-based systems*. All engineering-based systems are built to serve the well-being of people. The incorporation of knowledge-based expertise from other disciplines is essential. The risk of system failures increases without incorporation of outside knowledge.

10. *Risk management: A requisite for sustainable development*. Sustainable development ensures long-term protection of the ecology and the environment, in harmony with economic development. This cannot be realized without a systemic process of risk assessment and management.
11. *Evidence-based risk assessment*. Sparse databases and limited information often characterize most large-scale engineering systems, especially during the conception, planning, design, and construction phases. The reliability of specific evidence, including the evidence upon which expert judgment is based, is essential for effective risk management of these systems.
12. *Impact analysis*. Good technology management necessarily incorporates good risk management practices. Determining the impacts of current decisions on future options is imperative in decisionmaking.

1.3.11 Guiding Principles for Risk Analysis

Numerous studies have attempted to develop criteria for what might be considered *good* risk analyses, the most prominent of which is the Oak Ridge Study [Fischhoff et al., 1980]. Good risk studies may be judged against the following list of 10 criteria. The study must be:

- Comprehensive
- Adherent to evidence
- Logically sound
- Practical, by balancing risk with opportunity
- Open to evaluation
- Based on explicit assumptions and premises
- Compatible with institutions (except when change in institutional structure is deemed necessary)
- Conducive to learning
- Attuned to risk communication
- Innovative

Chapter 12 introduces the systems-based guiding principles for risk modeling, planning, assessment, management, and communication.

1.4 CONCEPT ROAD MAP

1.4.1 Overview of the Risk Assessment and Management Process (Chapter 1)

The importance, impact on decisionmaking at all levels, and complexity of the risk assessment and management process call for iterative learning, unlearning, and relearning [Toffler, 1980]. This chapter, which provides an overview of the book, highlights the strong commonalities and interdependencies between a holistic systems engineering philosophy and a systemic quantitative risk assessment and management, where both are grounded on the arts and the sciences. Some key ideas advanced in this chapter include:

1. Risk assessment and management is a process that must answer the following set of questions [Kaplan and Garrick, 1981; Haimes, 1991]:
   What can go wrong?
   What is the likelihood?
   What are the consequences?
   (And at what time frame?)
   What can be done and what options are available?
   What are the associated trade-offs in terms of all costs, benefits, and risks?
   What are the impacts of current decisions on future options?
2. Organizational failures are major sources of risk.
3. The perception of risk and its importance in decisionmaking should not be overlooked.
4. Risk management should be an integral part of technology management, leading to multiple-objective trade-off analysis.
5. The expected value of risk leads to erroneous results when used as the sole criterion for risk measurement. Also, risk of extreme and catastrophic events should not be commensurate with high-probability/low-consequence events.

1.4.2 The Role of Modeling in the Risk Assessment Process (Chapter 2)

To provide a unified road map for this book and to relate the 19 chapters of this fourth edition to the processes of modeling, assessment, and management of risk, Chapter 2 introduces a systems-based approach to the complex definitions of risk, vulnerability, and resilience. Consider the following oversimplified farmer's dilemma that is formulated and solved in Appendix A.3.

A farmer who owns 100 acres of agricultural land is considering two crops for next season—corn and sorghum. Due to a large demand for these crops, he (the term *he* is used here generically to denote either gender) can safely assume that he can sell his entire yield. From past experience, the farmer knows that the climate in his region requires (i) an irrigation of 3.9 acre-ft of water per acre of corn and 3 acre-ft of water per acre of sorghum at a subsidized cost of $40 per acre-ft and (ii) nitrogen-based fertilizer of 200 lb/acre of corn and 150 lb/acre of sorghum at a cost of $25/100 lb of fertilizer (an acre-ft of water is a measure of one acre of area covered by one foot of water).

The farmer believes that his land will yield 125 bushels of corn per acre and 100 bushels of sorghum per acre. He expects to sell his crops at $2.80 per bushel of corn and $2.70 per bushel of sorghum.

The farmer has inherited his land and is very concerned about the loss of topsoil due to erosion resulting from flood irrigation—the method used in his farm. A local soil conservation expert has determined that the farmer's land loses about 2.2 tons of topsoil per acre of irrigated corn and about 2 tons of topsoil per acre of irrigated sorghum. The farmer is interested in limiting the total topsoil loss from his 100 acre land to no more than 210 tons per season.

The farmer has a limited allocation of 320 acre-ft of water available for the growing season, but he can draw all the credit needed for the purchasing of fertilizer. He would like to determine his optimal planting policy in order to maximize his income. He considers his labor to be equally needed for both crops, and he is not concerned about crop rotation. Note that at this stage in the case, water quality (e.g., salinity and other contamination), impact on groundwater quality and quantity, and other issues (objectives) are not addressed.

This seemingly simple farmer's dilemma includes most of the ingredients that constitute a complex, risk-based decisionmaking problem. To explore the elements of risk and uncertainty addressed in this book, in Appendix A.3, we will first model the problem with a deterministic model, focusing on the role of modeling in the risk assessment process. We will subsequently explore more realistic assumptions and situations that lend themselves to probabilistic and dynamic modeling and treatment.

Even this oversimplified version of the problem has many interesting characteristics. The following are some of the most important modeling elements:

1. There are multiple conflicting and competing objectives: Maximize crop yield and minimize soil erosion.
2. There are resource constraints: water, land, and capital.
3. These resources manifest themselves in a major modeling building block—the state variables—a concept that will be extensively explored in subsequent discussions. Examples of state variables include the state of soil erosion and soil moisture.

Note that the role of the decision variables is to bring the states of the system to the appropriate levels that ultimately optimize the objective functions. (For the farmer, it means what crops to grow, when to irrigate, etc.) To know when to irrigate and fertilize a farm, a farmer must assess the states of the soil—its moisture and level of nutrients. Although an objective function can be a state variable, the role of the decision variables is not to directly optimize the objective functions. Identifying and quantifying (to the extent possible) the building blocks of a mathematical model of any system constitutes a fundamental step in modeling, where one building block—state variables—is the sine qua non in modeling.

Although the deterministic version of the farmer's dilemma is formulated and solved in Appendix A.3, no one would expect the farmer to predict all model parameters accurately—except, of course, for the availability of 100 acres of land that he owns. All other entries are merely average estimates predicated on past experience. For example, the amount of water needed to irrigate corn and sorghum is dependent on one state variable—soil moisture, which in turn depends on the amount of irrigation or precipitation for the season. The same argument applies to prices, which fluctuate according to market supply and demand. In particular, the level of soil erosion is heavily dependent on the climate and land use. Dry seasons are likely to increase soil erosion; irrigation patterns such as flood or sprinkles irrigation combined with the type of crops being grown and climate conditions can markedly vary the rate of soil erosion.

1.4.3 Identifying Risk through HHM (Chapter 3)

To effectively model, assess, and manage risk, one must be able to identify (to the extent possible) all important and relevant sources of that risk. Clearly, the root causes of most risks are many and diverse. Farmers face numerous risks at every stage of the farming life cycle. Other examples may include the risk of project cost overrun, time delay in its completion, the risk of not meeting performance criteria, and environmental and health risks. In Chapter 3, we introduce HHM, a systemic modeling philosophy/methodology that captures the multiple aspects, dimensions, and perspectives of a system. This systemic methodology serves as an excellent medium with which to answer the first question in risk assessment (What can go wrong?) and the first question in risk management (What can be done and what options are available?). Several visions or perspectives of risk are investigated in the HHM methodology, which includes the adaptive multiplayer HHM game.

1.4.4 Decision Analysis and the Construction of Evidence-Based Probabilities (Chapter 4)

Facing numerous natural and man-made challenges, the farmer can markedly benefit from the assorted decisionmaking tools and techniques assembled under the umbrella of decision analysis. For example, the farmer may wonder whether the market for his crops will be good, fair, or poor. If he could know the market condition in advance, he would direct his crop-growing decisions accordingly. Not wanting to rely on past statistical data to make future projections, the farmer may desire to minimize his maximum loss, maximize his minimum gain, or maximize his maximum gain. Here, the minimax (or maximin) principle can be very helpful. Furthermore, the Hurwitz rule, which bridges between maximizing his maximum gain and minimizing his maximum loss, can further enhance his decision-making process under conditions of uncertainty.

Chapter 4 will review some of these risk-based decisionmaking tools. For example, much of the farmer's dilemma can be posed in terms of a decision tree. Although decision-tree analysis will be introduced in Chapter 4 at its rudimentary level, an extensive treatment of decision trees with multiple objectives will be presented in Chapter 9. Indeed, one may argue that since most, if not all, problems lend themselves to multiple objectives, then extending decision trees to incorporate multiple objectives is an important step forward. The reader will note that the entire concept of optimality has to be modified and extended to encompass Pareto-optimality (see Chapter 5) in multiobjective decision-tree (MODT) analysis (as discussed in Chapter 9).

Chapter 4 also will introduce two approaches for the construction of probabilities on the basis of evidence from experts, due to the lack of statistical data. These approaches are the fractile method and triangular distribution. Modeling population dynamics is important, not only to farmers (to forecast the age distribution of their livestock over time) but also for the planning of schools and hospitals, among other installations, by communities and government agencies. For this purpose, the Leslie model [Meyer, 1984] will be introduced in Chapter 4.

Finally, Chapter 4 also will introduce the Phantom System Model (PSM). This enables system modelers to effectively study, understand, and analyze major forced changes in the characteristics and performance of multiscale assured systems. One example would be the physical infrastructure of a bridge SoS and the associated major interdependent socioeconomic systems [Haimes, 2007]. (Note that the term PSM will connote the overall modeling philosophy, while PSMs will connote the modeling components.) The PSM builds on and incorporates input from HHM discussed in Chapter 3. HHM is a holistic philosophy/methodology aimed at capturing and representing the essences of the inherent diverse characteristics and attributes of a system—its multiple aspects, perspectives, facets, views, dimensions, and hierarchies.

1.4.5 Multiobjective Trade-Off Analysis (Chapter 5)

The farmer knows that the finer the soil from cultivation, the higher the expected crop yield. However, this land use management practice is likely to lead to higher soil erosion. This dilemma is at the heart of multiobjective trade-off analysis—the subject of Chapter 5. This is the expertise domain of numerous scholars around the world, most of whom have devoted their entire professional career to this subject. Indeed, the International Society on Multiple Criteria Decision Making meets about every 2 years, and experts on MCDM share their experience and knowledge.

An important component of Chapter 5 is the discussion of the surrogate worth trade-off (SWT) method [Haimes and Hall, 1974; Chankong and Haimes, 2008]. Two basic principles upon which the SWT method is grounded are as follows: (i) the premise that sound decisions cannot be made merely on the basis of the absolute values of each objective function—rather, these absolute values must be supplemented and complemented with associated trade-offs at specific levels of attainment of these objectives—and (ii) the Epsilon-constraint method [Haimes, 1970; Haimes et al., 1971; Chankong and Haimes, 2008].

In particular, multiobjective trade-off analysis (within the SWT method) avoids the need to commensurate all objectives in, say, monetary terms. The trade-offs enable the analyst and decisionmaker(s) to determine the preferred policy on the basis of the values of these objective functions and their associated trade-offs.

The farmer may make use of multiobjective trade-off analysis in many other ways. For example, he may desire to change different pieces of equipment, each with specific cost and reliability. In this case, his trade-offs are his investments in farming equipment versus reliability and performance. These types of decisions are best handled via multiobjective trade-off analysis.

Chapter 5 presents an extensive discussion on this subject with ample example problems.

1.4.6 Defining Uncertainty and Sensitivity Analysis (Chapter 6)

The farmer, having lived and worked on his farm for many years, where several past generations have passed on valuable knowledge and wisdom, is rightfully skeptical of the modeling efforts by his systems analyst. He is very well aware of the following Arabic proverb [Finkel, 1990]:

> He who knows and knows he knows,
>   He is wise—follow him;
> He who knows not and knows he knows not,
>   He is a child—teach him;
> He who knows and knows not he knows,
>   He is asleep—wake him;
> He who knows not and knows not he knows not,
>   He is a fool—shun him.

It is here that the uncertainty taxonomy presented in Chapter 6 is helpful in diffusing some of the farmer's concerns about the uncertainty and variability associated with model assumptions, databases, causal relationships, and other factors affecting his ultimate decisions. Chapter 6 is devoted to exploring and categorizing the sources of uncertainty and variability in modeling and decisionmaking under risk and uncertainty.

One of the major concerns of our farmer is the risk of bankruptcy due to one or a sequence of disastrous growing seasons. In many respects, such disasters are tantamount to a calamity with irreversible consequences. The need to assess the sensitivity, response, and stability of a system (the farm in our case) to unexpected, unplanned, or catastrophic changes is imperative for good management and prudent decisionmaking. Risk of extreme and catastrophic events is discussed in Chapters 8 and 11.

The uncertain world within which we live continuously presents surprises and unexpected events with potential dire consequences. Planning for such eventualities and assessing the impacts of current decisions on future options are at the heart of good risk assessment and management. Furthermore, the use of models in decisionmaking has markedly increased during the last four decades. Decisions involving air traffic control, nuclear reactors, petroleum refineries, manufacturing, airline reservations, and thousands of other enterprises all make extensive use of models. For example, the farm may use a simple linear programming model (see Chapter 2 and the Appendix) to determine the optimal mix of growing corn and sorghum while balancing two conflicting objectives: maximizing income from crop yields and minimizing soil erosion. Some farmers use linear models to help them determine the optimal mix of feed ingredients for their livestock as the prices fluctuate in the marketplace.

Of course, models are constructed on the basis of certain assumptions and premises, and they are composed of variables and parameters of many dimensions and characteristics (they will be discussed in detail in Chapter 2). Clearly, when making decisions on the basis of mathematical models, one must be cognizant of at least the following four eventualities:

1. Most systems are dynamic in nature, and previously assumed values for model parameters may not be representative under new conditions.
2. Model topology (e.g., its structure, dimension, and other characteristics) may not constitute a good representation of the system.
3. Model parameters may not be representative in the first place.
4. Model output may be very sensitive to certain parameters.

The uncertainty sensitivity index method (USIM) [Haimes and Hall, 1977] and its extensions [Li and Haimes, 1988] provide a methodological framework with which to evaluate the sensitivity of the model output, the objective functions, or the constraints to changes in model parameters. Furthermore, the USIM and its extension enable the analysts or decisionmaker to trade off a decrease in the sensitivity of model output with a reduction in some performance functions. (Section 18.11 presents further discussion on the USIM.)

The farmer may make use of the USIM in many ways. He may, for example, want to minimize the sensitivity of soil erosion to an assumed nominal value of the model parameter that represents soil permeability, while being willing to forgo an increased crop yield. Chapter 6 will introduce the USIM and its extensions and offer a large number of examples.

1.4.7 Risk Filtering, Ranking, and Management (RFRM) (Chapter 7)

Most people and organizations tend to rank risks by asserting that *Risk A is higher than Risk B*. Such ranking, however, is invariably made on an ad hoc basis and with no systemic or quantifiable metric. Indeed, one of the major challenges facing the risk analysis community is to develop a more universal risk-ranking method (without relying on numerical order) capable of taking into account the myriad number of attributes that deem one risk higher or lower than others.

Chapter 7 discusses one such ranking method [Haimes et al., 2002]. The farmer, for example, may desire to rank the perceived or actual risks facing his farming enterprise (to the crops, livestock, water supply, long-term investment, etc.). The application of the RFRM to a variety of studies is discussed throughout this book.

1.4.8 Risk of Extreme Events and the Fallacy of the Expected Value (Chapter 8)

Risk is a complex concept. It measures an amalgamation of two constructs: One, probability, is a mental, human-made construct that has no physical existence per se. The other is severity of adverse effects, such as contaminant concentration, loss of lives, property loss, and defects in manufactured products, among others. The correct measure of mixing probability and severity in a risk metric is the subject of Chapter 8.

The expected value (the mean or the central tendency), which does not adequately capture events of low probabilities and high consequences, is supplemented with the PMRM [Asbeck and Haimes, 1984]. In particular, risk associated with safety-critical systems cannot be assessed or managed by using the expected value as the sole metric.

The farmer, for example, may be concerned with more than one consecutive drought year. In this case, the PMRM can generate a conditional expected value of drought (e.g., rainfall of <20 in). Having this additional knowledge base, the farmer may adjust his farming policy to reduce his chance of bankruptcy. Several example problems, where extreme-event analysis is critical, are introduced and solved in this chapter.

1.4.9 MODT (Chapter 9)

Decision-tree analysis with a single-objective function was discussed in Chapter 4 as part of decision analysis. Chapter 9 extends the decision-tree methodology to incorporate multiobjective functions. Indeed, MODT [Haimes et al., 1994] adds much more realism and practicality to the power of decision trees [Raiffa, 1964].

The farmer, for example, may desire to use MODT in analyzing his policy options as to what crops to grow and at what level, what irrigation method to use and how much to irrigate, and what land use practices to follow in cultivating his land—all in order to maximize his income and reduce his soil erosion. MODT analysis is a very versatile tool in decisionmaking under risk and uncertainty. Chapter 9 is devoted in its entirety to this powerful method with many example problems.

1.4.10 Multiobjective Risk Impact Analysis Method (Chapter 10)

Chapter 10 addresses the question, *What is the impact of current decisions on future options?* This impact analysis is important whether the decisions are made under deterministic conditions or under conditions dominated by risk and uncertainty. Impact analysis is also important for emergent systems. These have features that are not designed in advance but evolve, based on sequences of events that create the motivations and responses for properties that ultimately emerge into system features. This is because our world is dynamic, and decisions thought to be optimal under current conditions may prove to be far from optimal or maybe even disastrous. In a sense, the multiobjective risk impact analysis method (MRIAM) [Leach and Haimes, 1987] combines two separately developed methodologies: the multiobjective impact analysis method (MIAM) [Gomide and Haimes, 1984] and the PMRM.

Most decisionmaking situations address systems with transitory characteristics. For example, the farmer may desire to ascertain the impact of any of the following variations on his livelihood: crop market prices over the years, water availability in future years, changes in hydrological conditions, and others.

Chapter 10 will present a section that relates the MODT introduced in Chapter 9 to the MRIAM [Dicdican and Haimes, 2005], which will also be presented with example problems.

1.4.11 Statistics of Extremes: Extension of the PMRM (Chapter 11)

Very often, historical, statistical, or experimental data are sparse, especially on extreme events (the tail of the probability distribution function). The statistics of extremes is a body of statistical theory that attempts to overcome this shortage of data by classifying most probability distributions into three families on the basis of how fast their tails decay to zero. These three families are commonly known as Gumbel type I, type II, and type III.

Chapter 11 extends Chapter 8 and builds on the body of knowledge of the statistics of extremes, incorporates the statistics of extremes with the PMRM, and extends the theory and methodology of risk of extreme events. This chapter also relates the concepts of the return period to the conditional expected value of extreme events and to the statistics of extremes.

The farmer, for example, may desire to relate the return period of a sizable flood or drought to the expected value and conditional expected value of crop yield. He can do so using parts of the methodology discussed in this chapter.

1.4.12 Systems-Based Guiding Principles for Risk Modeling, Planning, Assessment, Management, and Communication (Chapter 12)

The 10 principles set forth in this chapter are intended to provide a broad framework for understanding and practicing risk analysis—regardless of the specific domain, problem, system, or discipline. These fundamental systems-based principles build on and encapsulate the theory and methodology presented throughout this book. They are designed to guide both quantitative- and qualitative-centered risk analyses. Although these principles may be applied to a range of disciplines, to retain focus, this chapter draws from and is guided by both risk analysis and systems engineering theory, methodology, and practice.

1.4.13 Fault Trees (Chapter 13)

Assessing the reliability of an engineering system or a system component is vital to its design, development, operations, maintenance, and replacement. In particular, an analyst or a decisionmaker would invariably want to know the trade-offs among different policy options in terms of their cost and associated reliability (or unreliability). Fault trees have been developed and extensively used in myriad engineering and nonengineering applications. Most notable among them is the nuclear industry [US Nuclear Regulatory Commission, 1981].

Chapter 13 extends fault-tree analysis to incorporate a variety of probability distribution functions into a new methodology termed distribution analyzer and risk evaluator (DARE) [Tulsiani et al., 1990]. FMEA and FMECA—two important tools with extensive use in the life cycle of engineering systems—are also discussed in Chapter 13.

The farmer, for example, may desire to ascertain the reliabilities of his farm equipment or irrigation system in order to make investment decisions. He can do so using fault-tree analysis.

1.4.14 Multiobjective Statistical Method (MSM) (Chapter 14)

The MSM is grounded on adherence to the following basic premises [Haimes et al., 1980]:

1. Most, if not all, systems have a multiobjective nature.
2. State variables, which represent the essence of a system at any time period, play a dominant role in modeling.
3. Sources of risk and uncertainty can be best modeled through probabilistic modeling methods.
4. The joint use of simulation and optimization is by far more effective than the use of each one alone.
5. A good database is invaluable to good systems analysis, and the improvement of the database can be accomplished through questionnaires, expert judgment, and other mechanisms for data collection.

Our challenge in the farmer's example problem is modeling soil erosion, which is an objective function and a state variable (i.e., minimizing one objective function, which is soil erosion, is the same as minimizing the state variable soil erosion). For the purpose of this discussion, denote soil erosion by S. This state variable depends on at least three other major variables:

- Random variables ($\mathbf{r}$), such as precipitation and climate conditions (e.g., temperature, wind)
- Decision variables ($\mathbf{x}$), such as land use and irrigation patterns
- Exogenous variables ($\mathbf{e}$), such as soil characteristics (e.g., permeability and porosity and other morphological conditions)

Note that some of the variables may fall into multiple categories—this is part of the nature of the modeling process.

Through simulation, one aims at determining the causal relationships between S and the other three variables; that is, $S = S(\mathbf{r},\mathbf{x},\mathbf{e})$. Note, however, that by their nature, the random variables (precipitation and climatic conditions) are characterized by an ensemble of values over their sample space. Here, one may make use of the expected value, which is the mean or average value of the realization of each random variable. Alternatively, one may supplement and complement the expected value of the random variable with the conditional expected value as derived through the use of the PMRM [Asbeck and Haimes, 1984]. The PMRM and its extensions are extensively discussed in Chapters 8 and 11.

An analyst who is helping the farmer with crop decisions may develop a set of questionnaires to be distributed to other farmers in the region and may obtain more scientific information from the literature at agriculture experiment stations to quantify $S = S(\mathbf{r},\mathbf{x},\mathbf{e})$.

The above analyses will yield a multiobjective optimization problem where the SWT method [Haimes and Hall, 1974] can be used. The SWT method is discussed in Chapter 5.

1.4.15 Principles and Guidelines for Project Risk Management (Chapter 15)

The life cycle management of systems—small and large—is an integral part of good systems engineering and good risk management. Indeed, the increasing size and complexity of acquisition and development projects in both the public and private sectors have begun to exceed the capabilities of traditional management techniques to control them. With every new technological development or engineering feat, human endeavors inevitably increase in their complexity and ambition. This trend has led to an explosion in the size and sophistication of projects by government and private industry to develop and acquire technology-based systems. These systems are characterized by the often unpredictable interaction of people, organizations, and hardware. In particular, the acquisition of software has been marred with significant cost overruns, time delay in delivery, and the lack of meeting performance criteria.

Although the farmer has markedly increased the use of computers and, of course, the use of various software packages in his enterprise, he may not concern himself with the risk associated with software development. Nevertheless, since the software component of modern, large-scale systems continues to assume an increasingly critical role in such systems, it is imperative that software risk management be discussed in this book. Software has a major effect on any system's quality, cost, and performance. Indeed, system quality is predicated, as never before, upon the quality of its software. System risk is increasingly being defined relative to the risk associated with its software component. Acquisition officials, who previously concentrated on the hardware components of a system, instead find themselves concentrating more of their energies, concerns, and resources on the embedded hardware–software components.

Chapter 15 will address project risk management and the characteristics of software risk management and offer tools and methodologies for the management of the risk of cost overrun, the risk of time delay in software delivery, and the risk of not meeting performance criteria.

1.4.16 Modeling Complex SoS with PSM (Chapter 16)

The fact that modeling is as much an art as a science—a tedious investigative trial-and-error, learn-as-you-go process—means that an equally imaginative approach is necessary to discover the inner functionality of complex systems through modeling. In this context, Chapter 16 (i) addresses system modeling, and the inverse problem, or the system identification problem, through the PSM; (ii) analyzes the contributions of PSM as a modeling mechanism through which to experiment with creative approaches to modeling complex SoS; and (iii) relates (at the metamodeling level) the intrinsic common/shared state variables among the subsystems of the SoS, thereby offering more insight into the intra- and interdependencies among the subsystems.

1.4.17 Adaptive Two-Player HHM Game for Counterterrorism Intelligence Analysis (Chapter 17)

Intelligence gathering and analysis for countering terrorism is a vital and costly venture; therefore, approaches need to be explored that can help determine the scope of collection and improve the efficacy of analysis efforts. The Adaptive Two-Player HHM Game introduced in Chapter 3 and discussed in detail in Chapter 17 is a repeatable, adaptive, and systemic process for tracking terrorism scenarios. It builds on fundamental principles of systems engineering, system modeling, and risk analysis. The game creates two opposing views of terrorism: one is developed by a Blue Team defending against acts of terrorism, and the other by a Red Team planning to carry out a terrorist act. The HHM process identifies the vulnerabilities of potential targets that could be exploited in attack plans. These vulnerabilities can be used by the Blue Team to identify corresponding surveillance capabilities that can help to provide warning of a possible attack. Vulnerability-based scenario structuring, comprehensive risk identification and the identification of surveillance capabilities that can support preemption are all achieved through the deployment of HHM.

State variables, which represent the essence of the system, play a pivotal role in the Adaptive Two-Player HHM Game, providing an enabling road map to intelligence analysts. Indeed, vulnerabilities are defined in terms of the system's state variables: Vulnerability is the manifestation of the inherent states of a system (e.g., physical, technical, organizational, cultural) that can be exploited by an adversary to cause harm or damage. Threat is a potential adversarial intent to cause harm or damage by adversely changing the states of the system. Threat to a vulnerable system may lead to risk, which is a measure of the probability and severity of adverse effects.

1.4.18 Inoperability Input–Output Model and Its Derivatives for Interdependent Infrastructure Sectors (Chapter 18)

In assessing a system's vulnerability, it is important to analyze both the intraconnectedness of the subsystems that compose it and its interconnectedness with other external systems. This chapter develops a methodology that quantifies the dysfunctionality or *inoperability* as it propagates throughout our critical infrastructure systems or industry sectors. The inoperability that may be caused by willful attacks, accidental events, or natural causes can set off a complex chain of cascading impacts on other interconnected systems. For example, telecommunications, power, transportation, banking, and others are marked by immense complexity, characterized predominantly by strong intra- and interdependencies as well as hierarchies. The Inoperability Input–Output Model (IIM) [Haimes and Jiang, 2001; Santos, 2003; Haimes et al., 2005a, b; Lian, 2006; Crowther, 2007] and its derivatives build on the work of Wassily Leontief, who received the 1973 Nobel Prize in Economics for developing what came to be known as the Leontief Input–Output Model (I/O) of the economy [Leontief, 1951a, b, 1986]. The economy consists of a number of subsystems, or individual economic sectors or industries, which are a framework for studying its equilibrium behavior. It enables understanding and evaluating the interconnectedness among the various sectors of an economy and forecasting the effect on one segment of a change in another. The IIM is extended in Chapter 18 to model multiregional, dynamic, and uncertainty factors.

1.4.19 Case Studies (Chapter 19)

Six case studies applying risk modeling, assessment, and management to real-world problems are introduced in Chapter 19. The first case study documents the application of the IIM and its derivatives (see Chapter 18) to measure the effects of the August 2003 northeast electric power blackout in North America [Anderson et al., 2007]. Systemic valuation of strategic preparedness through applying the IIM and its derivatives with lessons learned from Hurricane Katrina is the subject of the second case study [Crowther et al., 2007]. The third case study is an ex post analysis of the September 11, 2001, attack on the United States using the IIM and its derivatives [Santos, 2003]. The focus of the fourth case study is the 5770 foot Mount Pinatubo volcano that erupted in the Philippines. We analyze the risks associated with the huge amount of volcanic materials deposited on its slopes (about $1\,\text{mi}^3$). Several concepts and methodologies introduced in this book are applied. The fifth case study provides the perspectives of the risk of extreme events when considering the six-sigma capability in quality control. The PMRM introduced in Chapter 8 and the statistics of extremes introduced in Chapter 11 are related to and compared with the six-sigma capability metric. The sixth case study provides the reader a deeper insight into the propagation of sequential Pareto-optimal decisions made within emergent complex SoS, with an application to the FAA NextGen. In particular, this case study addresses the third question in risk management—*What are the impacts of current decisions on future options?*—that is critically important for emergent complex SoS, because their conception, the evolution of their requirements and specifications, their design and development, and their ultimate operation can span several years. Furthermore, the sequential decisions made during the development of each individual subsystem of any given complex SoS will most likely affect the development of other new subsystems of the SoS in the future—with the ultimate goal that, in their totality, all of the subsystems will operate as an integrated, harmonious whole. For example, decisions to achieve specific outcomes made on subsystem **A** of an emergent SoS can change the states of subsystem **A**, but they can also affect other interconnected and interdependent subsystems that share states with subsystem **A**.

1.5 EPILOGUE

The comprehensiveness of TRM makes the systemic assessment and management of risk tractable from many perspectives. Available theories and methodologies developed and practiced by various disciplines can be adopted and modified as appropriate for TRM. Fault-tree analysis, for example, which has been developed for the assessment and management of risk associated with hardware, is being modified and applied to assess and manage all four sources of failure: hardware, software, organizational, and human. Hierarchical/multiobjective trade-off analysis is being applied to risk associated with public works and the infrastructure. As the importance of risk is better understood and its analysis is incorporated within a broader and more holistic management framework, the following progress will be likely:

1. The field of risk analysis will lose some of its current mystique, gain wider recognition, and more closely merge with the fields of systems engineering, systems analysis, and operations research.
2. The various disciplines that conduct formal risk analysis will find more common ground in their assessment and management than ever before.
3. As a by-product of 1 and 2 above, the field of risk analysis will advance by leaps and bounds as the professional community benefits from the synergistic contributions made in the area of risk assessment and management by the various disciplines: engineering, environmental science, medical health care, social and behavioral sciences, finance, economics, and others.
4. New measures of risk will likely emerge either as a substitute for, or as a supplement and complement to, the expected-value-of-risk measure.
5. Probably most important, government officials, other professionals, and the public at large will have more appreciation of, and confidence in, the process of risk assessment and management.
6. The spread of international terrorism will likely engage the attention of more and more risk analysts.

Finally, it is important to keep in mind two things: (i) Heisenberg's uncertainty principle [Feynman et al., 1963], which states that the position and velocity of a particle in motion cannot simultaneously be measured with high precision, and (ii) Einstein's statement: "So far as the theorems of mathematics are about reality, they are not certain; so far as they are certain, they are not about reality." By projecting Heisenberg's principle and Einstein's statement to the field of risk assessment and management, we assert that:

> To the extent that risk assessment is precise, it is not real
> To the extent that risk assessment is real, it is not precise

REFERENCES

Adelman, L., 1991, *Evaluating Decision Support and Expert Systems*, John Wiley & Sons, Inc., New York.

Anderson, C.W., J.R. Santos, and Y.Y. Haimes, 2007, A risk-based input-output methodology for measuring the effects of the August 2003 Northeast Blackout, *Economics Systems Research* **19**(2): 183–204.

Asbeck, E.L., and Y.Y. Haimes, 1984, The partitioned multiobjective risk method (PMRM), *Large Scale Systems* **6**(1): 13–38.

Bernstein, P., 1996, *Against the Gods: The Remarkable Story of Risk*, John Wiley & Sons, Inc., New York.

Bertalanffy, L., 1968/1976, *General System Theory: Foundations, Development, Applications*, George Braziller, New York.

Blanchard, B.S., 2003, *Systems Engineering Management*, Third edition, John Wiley & Sons, Inc., Hoboken, NJ.

Blanchard, B.S., and W.J. Fabrycky, 1990, *Systems Engineering and Analysis*, Prentice-Hall, Englewood Cliffs, NJ.

Blanchard, B.S., and W.J. Fabrycky, 1998, *Systems Engineering and Analysis*, Third edition, Prentice-Hall, Englewood Cliffs, NJ.

Blanchard, B.S., and W.J. Fabrycky, 2005, *Systems Engineering and Analysis*, Fourth edition, Prentice-Hall, Englewood Cliffs, NJ, 816 pp.

Blauberg, I.V., V.N. Sadovsky, and E.G. Yudin, 1977, *Systems Theory: Philosophical and Methodological Problems*, Progress Publishers, New York.

Boehm, B., 2006, Some future trends and implications for systems and software engineering processes, *Systems Engineering* **9**(1): 1–19.

Boulding, K.E., 1953, *The Organizational Revolution*, Harper & Row, New York.

Brooks, C.C., 2000, Knowledge management and the intelligence community, *Defense Intelligence Journal* **9**(1): 15–24.

Buede, D.M., 1999, *The Engineering Design of Systems: Models and Methods*, John Wiley & Sons, Inc., New York, 488 pp.

Burke, T., N. Tran, J. Roemer, and C. Henry, 1993, *Regulating Risk, the Science and Politics of Risk*, International Life Sciences Institute, Washington, DC.

Chankong, V., and Y.Y Haimes, 1983 *Multiobjective Decision Making: Theory and Methodology*, Elsevier-North Holland, New York.

Chankong, V., and Y.Y. Haimes, 2008, *Multiobjective Decision Making: Theory and Methodology*, Dover, Mineola, NY.

Chittister, C., and Y.Y. Haimes, 1994, Assessment and management of software technical risk, *IEEE Transactions on Systems, Man, and Cybernetics* **24**(4): 187–202.

Cohen, I.B., and A. Whitman, 1999, *Isaac Newton: The Principia*, University of California Press, Berkeley, CA.

Collins, J., 2001, *Good to Great*, HarperCollins Publishers, New York

Covey, S.R., 1989, *The Seven Habits of Highly Effective People*, Simon and Schuster, New York.

Crowther, K.G., 2007, *Development of a Multiregional Preparedness Framework and Demonstration of Its Feasibility for Strategic Preparedness of Interdependent Regions*, Ph.D. dissertation, University of Virginia, Charlottesville, VA.

Crowther, K.G., Y.Y. Haimes, and G. Taub, 2007, Systemic valuation of strategic preparedness through application of inoperability input–output model with lessons learned from hurricane Katrina, *Risk Analysis* **27**(5): 1345–1364.

Davenport, T.H., and L. Prusak, 1998, *Working Knowledge: How Organizations Manage What They Know*, Harvard Business Press, Boston, MA.

Deming, W.E., 1986, *Out of the Crisis, Center for Advanced Engineering Study*, Massachusetts Institute of Technology, Cambridge, MA.

Dicdican, R.Y., and Y.Y. Haimes, 2005, Relating multiobjective decision trees to the multiobjective risk impact analysis method, *Systems Engineering* **8**(2): 95–108.

Douglas, M., 1990, Risk as a forensic resource, *Daedalus* **119**(4): 1–16.

Drucker, P.F., 2004, *The Daily Drucker*, Harper Business, New York.

Fang, L., K.W. Hipel, and D.M. Kilgour, 1993, *Interactive Decision Making: The Graph Model for Conflict Resolution*, John Wiley & Sons, Inc., New York, 240 pp.

Feynman, R.P., R.B. Leighton, and M. Sands, 1963, *The Feynman Lectures on Physics*, Addison-Wesley, Reading, MA.

Finkel, A.M., 1990, *Confronting Uncertainty in Risk Management*, Center for Risk Management, Resources for the Future, Washington, DC.

Fischhoff, B., S. Lichtenstein, P. Slovic, R. Keeney, and S. Derby, 1980, *Approaches to Acceptable Risk: A Critical Guide*, ORNL Sub-7656, Oak Ridge National Laboratory, Eugene, OR.

Fischhoff, B., S. Lichtenstein, P. Slovic, S. Derby, and R. Keeney, 1983, *Acceptable Risk*, Cambridge University Press, Cambridge.

Gardner, H., and T. Hatch, 1989, Multiple intelligences go to school, *Educational Researcher* **18**(8): 4–10.

Gharajedaghi, J., 2005, *Systems Thinking: Managing Chaos and Complexity: A Platform for Designing Business Architecture*, Second edition, Butterworth-Heinemann, Boston, MA, 368 pp.

Gheorghe, A.V., 1982, *Applied Systems Engineering*, John Wiley & Sons, Inc., New York.

Goleman, D., 1997, *Emotional Intelligence: Why It Can Matter More than IQ*, Bantam Books, New York.

Goleman, D., 1998, *Working with Emotional Intelligence*, Bantam Books, New York.

Gomide, F., and Y.Y. Haimes, 1984, The multiobjective, multistage impact analysis method: Theoretical basis, *IEEE Transactions on Systems, Man, and Cybernetics* **14**: 89–98.

Gordon, W.J.J., 1968, *Synectics: The Development of Creative Capacity*, Collier Books, New York.

Haimes, Y.Y., 1970, *The Integration of System Identification and System Optimization*, Ph.D. dissertation, School of Engineering and Applied Science, University of California, Los Angeles, CA.

Haimes, Y.Y., 1977, *Hierarchical Analyses of Water Resources Systems: Modeling and Optimization of Large-Scale Systems*, McGraw-Hill, New York.

Haimes, Y.Y., 1981, Hierarchical holographic modeling, *IEEE Transactions on Systems, Man, and Cybernetics* **11**(9): 606–617.

Haimes, Y.Y., 1989, Toward a holistic approach to risk management (Guest Editorial), *Risk Analysis* **9**(2): 147–149.

Haimes, Y.Y., 1991, Total risk management, *Risk Analysis* **11**(2), 169–171.

Haimes, Y.Y., 2007, Phantom system models for emergent multiscale systems, *Journal of Infrastructure Systems* **13**(2): 81–87.

Haimes, Y.Y., and W.A. Hall, 1974, Multiobjectives in water resources systems analysis: the surrogate worth trade-off method, *Water Resources Research* **10**(4): 615–624.

Haimes, Y.Y., and W.A. Hall, 1977, Sensitivity, responsivity, stability, and irreversibility as multiobjectives in civil systems, *Advances in Water Resources* **1**: 71–81.

Haimes, Y.Y., and P. Jiang, 2001, Leontief-based model of risk in complex interconnected infrastructures, *ASCE Journal of Infrastructure Systems* **7**(1): 1–12, 111–117.

Haimes, Y.Y., and C. Schneiter, 1996, Covey's seven habits and the systems approach, *IEEE Transactions on Systems, Man, and Cybernetics* **26**(4): 483–487.

Haimes, Y.Y., L.S. Lasdon, and D.A. Wismer, 1971, On the bicriterion formulation of the integrated system identification and systems optimization, *IEEE Transactions on Systems, Man, and Cybernetics* **1**: 296–297.

Haimes, Y.Y., K.A. Loparo, S.C. Olenik, and S.K. Nanda, 1980, Multiobjective statistical method (MSM) for interior drainage systems, *Water Resources Research* **16**(3): 467–475.

Haimes, Y.Y., K. Tarvainen, T. Shima, and J. Thadathil, 1990, *Hierarchical Multiobjective Analysis of Large Scale Systems*, Hemisphere Publishing, New York.

Haimes, Y.Y., D.A. Moser, and E.Z. Stakhiv (Eds.), 1994, *Risk-Based Decision Making in Water Resources VI*, American Society of Civil Engineers, New York.

Haimes, Y.Y., S. Kaplan, and J.H. Lambert, 2002, Risk filtering, ranking, and management framework using hierarchical holographic modeling, *Risk Analysis* **22**(2): 383–397.

Haimes, Y.Y., B.M. Horowitz, J.H. Lambert, J.R. Santos, K.G. Crowther, and C. Lian, 2005a, Inoperability input–output model (IIM) for interdependent infrastructure sectors: case study, *Journal of Infrastructure Systems* **11**(2): 80–92.

Haimes, Y.Y., B.M. Horowitz, J.H. Lambert, J.R. Santos, C. Lian, K.G. Crowther, 2005b, Inoperability input-output model (IIM) for interdependent infrastructure sectors: theory and methodology, *Journal of Infrastructure Systems* **11**(2): 67–79.

Hall, A.D. III, 1989, *Metasystems Methodology: A New Synthesis and Unification*, Pergamon Press, New York.

Hatley, D.J., P. Hruschka, and I.A. Pirbhai, 2000, *Process for System Architecture and Requirements Engineering*, Dorset House Publishing Co., Inc., New York, 434 pp.

Hegel, G., 1952, *Great Books of the Western World*, Vol. **46**, Encyclopaedia Britannica, Inc., Chicago, IL.

Hutchins, R.M., Encyclopaedia Britannica, Inc., and University of Chicago, 1952, *Plato*, Vol. **7**. Great Books of the Western World. W. Benton, Chicago, IL.

Imai, M., 1986, *Kaizen: The Key to Japan's Competitive Success*, McGraw-Hill, New York.

Jackson, D., 2006, Dependable software by design, Scientific American June: 69–75.

Kaplan, S., and B.J. Garrick, 1981, On the quantitative definition of risk, *Risk Analysis* **1**(1): 11–27.

Kaplan, S., Y.Y. Haimes, and B.J. Garrick, 2001, Fitting hierarchical holographic modeling (HHM) into the theory of scenario structuring and a refinement to the quantitative definition of risk, *Risk Analysis* **21**(5): 807–819.

Kossiakoff, A., and W.N. Sweet, 2002, *Systems Engineering Principles and Practice*, John Wiley & Sons, Inc., Hoboken, NJ, 488 pp.

Krimsky, S., and D. Golding (Eds.), 1992, *Social Theories of Risk*, Praeger Publishers, Westport, CT.

Kunreuther, H., and P. Slovic (Eds.), 1996, *Challenges in Risk Assessment and Risk Management, the Annals of the American Academy of Political and Social Science*, Sage, Thousand Oaks, CA.

Larsen, R.J., 2007, *Our Own Worst Enemy: Asking the Right Questions about Security to Protect You, Your Family, and America*, Grand Central Publishing, New York.

Leach, M., and Y.Y. Haimes, 1987, Multiobjective risk-impact analysis method, *Risk Analysis* **7**: 225–241.

Leondes, C.T. (Ed.), 1969, *Advances in Control Systems*, Vol. **6**, Academic Press, New York.

Leontief, W.W., 1951a, Input/output economics, *Scientific American* **185**(4): 15–21.

Leontief, W.W., 1951b, *The Structure of the American Economy, 1919–1939*, Second edition, Oxford University Press, New York.

Leontief, W.W., 1986, Quantitative input–output relations in the economic system of the United States, *Review of Economics and Statistics* **18**(3): 105–125.

Lewis, H., 1992, *Technological Risk*, W. W. Norton, New York.

Li, D., and Y.Y. Haimes, 1988, The uncertainty sensitivity index method (USIM) and its extension, *Naval Research Logistics* **35**: 655–672.

Lian, C., 2006, *Extreme Risk Analysis of Dynamic Interdependent Infrastructures and Sectors of the Economy with Applications to Financial Modeling*, Ph.D. dissertation, University of Virginia, Charlottesville, VA.

Longstaff, T.A., and Y.Y. Haimes, 2002, A holistic roadmap for survivable infrastructure systems, *IEEE Transactions on Systems, Man, and Cybernetics* **32**(2): 260–268.

Lowrance, W.W., 1976, *Of Acceptable Risk*, William Kaufmann, Los Altos, CA.

Macko, D., 1967, *General System Theory Approach to Multilevel Systems*, Report SRC 106-A-67-44, Systems Research Center, Case Western Reserve University, Cleveland, OH.

Maier, M.W., and E. Rechtin, 2000, *The Art of Systems Architecting*, Second edition, CRC, Boca Raton, FL, 344 pp.

McQuaid, J., and M. Schleifstein, 2006, *Path of Destruction: The Devastation of New Orleans and the Coming of Age of Superstorms*, Little, Brown and Co., New York.

Mesarović, M.D., 1965, Multilevel concept of systems engineering, *Proceedings of the Systems Engineering Conference*, Chicago, IL.

Mesarović, M.D. (Ed.), 1968, *Systems Theory and Biology*, Springer-Verlag, New York.

Mesarović, M.D., D. Macko, and Y. Takahara, 1970, *Theory of Hierarchical, Multilevel Systems*, Academic Press, New York.

Meyer, W., 1984, *Concepts of Mathematical Modeling*, McGraw-Hill, New York.

Morrall, J.F. III, 2003, Saving lives: a review of the record, *Journal of Risk and Uncertainty* **27**(3): 221–237.

National Research Council (NRC), 1996, *Shopping for Safety: Providing Consumer Automotive Safety Information*, Special Report 248, Transportation Research Board, National Academy Press, Washington, DC.

National Research Council (NRC), 2002, *Making the Nation Safer: The Role of Science and Technology in Countering Terrorism*, The National Academy Press, Washington, DC.

Paté-Cornell, M.E., 1990, Organizational aspects of engineering system safety: the case of offshore platforms, *Science* **250**: 1210–1217.

Post, D.E., R.P. Kendall, and R.F. Lucas, 2006, The opportunities, challenges and risks of high performance computing in computational science and engineering, *Advances in Computers* **66**: 239–301, Marvin Zelkowitz, (Ed.), Elsevier Academic Press, New York.

Raiffa, H., 1964, *Decision Analysis: Introductory Lectures on Choices Under Uncertainty*, Random House, New York.

Rasmussen, J., A.M. Pejtersen, and L.P. Goodstein, 1994, *Cognitive Systems Engineering*, First edition, John Wiley & Sons, Inc., New York, 396 pp.

Rouse, W.B., 1991, *Design for Success: A Human-Centered Approach to Designing Successful Products and Systems*, First edition, John Wiley & Sons, Inc., New York, 304 pp.

Sage, A.P., 1977, *Methodology for Large Scale Systems*, McGraw-Hill, New York.

Sage, A.P. (Ed.), 1990, *Concise Encyclopedia on Information Processing in Systems and Organizations*, Pergamon Press, Oxford.

Sage, A.P., 1992, *Systems Engineering*, John Wiley & Sons, Inc., New York.

Sage, A.P., 1995, *Systems Management for Information Technology and Software Engineering*, John Wiley & Sons, Inc., New York.

Sage, A.P., and J.E. Armstrong, Jr., 2003, *Introduction to Systems Engineering*, John Wiley & Sons, Inc., Hoboken, NJ.

Sage, A.P., and C.D. Cuppan, 2001, On the systems engineering and management of systems of systems and federation of systems, *Information, Knowledge, Systems Management* **2**(4): 325–345.

Sage, A.P., and W.B. Rouse (Eds.), 1999, *Handbook on Systems Engineering and Management*, Second edition, John Wiley & Sons, Inc., New York.

Santos, J.R., 2003, *Interdependency Analysis: Extensions to Demand Reduction Inoperability Input–Output Modeling and Portfolio Selection*, Ph.D. dissertation, University of Virginia, Charlottesville, VA.

Senge, P.M., 1990, *The Fifth Discipline*, Doubleday, New York.

Singh, M.G., 1987, *Systems and Control Encyclopedia: Theory, Technology, Applications*, Pergamon Press, New York.

Slovic, P., 2000, *The Perception of Risk*, Earthscan Publications Ltd., Sterling, VA

Stern, P., and H. Fineberg (Eds.), 1996, *Understanding Risk: Informing Decisions in a Democratic Society*, National Research Council, National Academy Press, Washington, DC.

The Royal Society, 1992, *Risk: Analysis, Perception and Management: Report of a Royal Society Study Group*, The Royal Society, London.

Toffler, A., 1980, *The Third Wave: The Classic Study of Tomorrow*, Bantam Books, New York.

Toffler, A., 1991, *Powershift*, Bantam Books, New York.

Tulsiani, V., Y.Y. Haimes, and D. Li, 1990, Distribution analyzer and risk evaluator (DARE) using fault trees, *Risk Analysis* **10**(4): 521–538.

US Nuclear Regulatory Commission, 1981, *Fault Tree Handbook, NUREG-0492*, U.S. Government Printing Office, Washington, DC.

Warfield, J.N., 1976, *Social Systems—Planning and Complexity*, John Wiley & Sons, Inc., New York.

Wernick, I.K. (Ed.), 1995, *Community Risk Profiles*, Rockefeller University, New York.

Wiener, N., 1961, *Cybernetics*, Second edition, MIT Press, Cambridge, MA.

World Book, Inc., 1980, *The World Book Encyclopedia*, Vol. **8**, World Book—Childcraft International, Inc., Chicago, IL.

Zeleny, M., 2005, *Human Systems Management: Integrating Knowledge, Management and Systems*, First edition, World Scientific Publishing Company, Hackensack, NJ, 484 pp.

Zigler, B.P., 1984, *Multifaceted Modeling and Discrete Simulation*, Academic Press, New York.