risk-INFORMED DECISION MAKING

Knowing where you are most likely to fail can help set the stage for reducing the chances of failure.

By Bilal M. Ayyub, Peter G. Prassinos, and John Etherton

A journey of a thousand miles, the old saying goes, starts with a single step. And even the most complex project or industry-changing product begins with a single idea. But just as a traveler would be foolish to set out on a journey without packing provisions and studying a map to find the optimal route, a good idea isn't enough to make a successful business venture. Among the many measures a company or organization should take before setting off on a new project, one of the most important is an assessment of the inherent risks. Risk is associated with all projects and business ventures taken by individuals and organizations regardless of their sizes, their natures, and the time and place of execution and utilization.

Risk is present in various forms and levels—even in small domestic projects such as adding a deck to a residential house—but it becomes most apparent in large multi-billion-dollar projects, such as developing and producing a space shuttle or building a new hydroelectric dam. Large-scale endeavors can result in significant budget overruns, delivery delays, failures, financial losses, environmental damages, and even injuries and loss of life. But while they can lead to devastating consequences, such endeavors are taken because of potential societal benefits, personal rewards, survival, and future return on investment.

Not everyone is involved in such monumental undertakings. Even in developing a new product, say a drug delivery device or a child's stroller, understanding risk and how to reduce or mitigate it can make the difference between reaching your goal and losing your bearings.

The stroller is an interesting example: recently, a manufacturer had to recall a line of strollers that, when a child sticks a finger in the hinge during unfolding, could cause a serious injury. The product was by most accounts very successful, popular with parents and children alike. And the stroller was quite easily modified to be safe, through the addition of a tough fabric sleeve over the dangerous joint. But because this one potential failure was overlooked by the product designers, the company has had to endure a great deal of bad publicity and has opened itself to possible litigation.

It's just that sort of product failure that risk-informed decision making is designed to reduce.

Bilal M. Ayyub, an ASME Fellow, is a professor and the director of the Center for Technology Systems and Systems Management at the University of Maryland. Peter G. Prassinos is an aerospace engineer in the Office of Safety and Mission Assurance at NASA headquarters. John Etherton is director of the Center for Safer Solutions in Morgantown, W.Va.

[RISK ANALYSIS]

The concept of risk can be linked to uncertainties associated with events. Within the context of a project, risk is commonly associated with an uncertain event or condition that, if it occurs, has a positive or a negative effect on the project's objectives or results in unwanted consequences.

These questions are commonly called the "risk triplet."

In answering the first question—"What can go wrong?"—the analysis identifies a single event or a sequence of events that can lead to an undesired consequence. These single events or sequences of events are called scenarios. The event or scenario can be viewed as a cause that, if it occurs, results in an adverse consequence of some degree of severity. One example of such an event could be the shortage of trained personnel needed to perform a task that's critical for the project. The personnel shortage is an event that will lead to consequences: higher costs for the project, or a delay in the schedule, or a reduction in the quality of the results.

Risk originates from the Latin term *risicum* meaning the challenge presented by a barrier reef to a sailor. The term is conventionally defined as the chance of hazard, bad consequence, loss, and so on. Risk is the chance of a negative outcome.

Formally, risk can be defined as the potential of losses for a system resulting from an uncertain exposure to a hazard or as a result of uncertain events. The analysis of risk attempts to identify and quantify the potential outcomes from a certain set of events. In essence, risk analysis boils down to answering such questions as: What can go wrong? How likely is it? What are the outcomes or consequences if it occurs?

Events can reside in a project environment that may contribute to project success or failure, such as project management practices, or external partners or subcontractors.

To complete the analysis of risk, the probability of each scenario is determined along with the magnitude or severity of the consequences involved. Additionally,

TABLE 1. RISK ASSESSMENT METHODS (AYYUB 2003)	
Method	*Scope*
Safety/Review Audit	Identifies equipment conditions or operating procedures that could lead to a casualty or result in property damage or environmental impacts.
Checklist	Ensures that organizations are complying with standard practices.
What-If	Identifies hazards, hazardous situations, or specific accident events that could result in undesirable consequences.
Hazard and Operability Study (HAZOP)	Identifies system deviations and their causes that can lead to undesirable consequences and determine recommended actions to reduce the frequency and/or consequences of the deviations.
Preliminary Hazard Analysis (PrHA)	Identifies and prioritizes hazards leading to undesirable consequences early in the life of a system. It determines recommended actions to reduce the frequency and/or consequences of the prioritized hazards. This is an inductive modeling approach.
Probabilistic Risk Analysis (PRA)	Quantifies risk, and was developed by the nuclear engineering community for risk assessment. This comprehensive process may use a combination of risk assessment methods.
Failure Modes and Effects Analysis (FMEA)	Identifies the equipment failure modes and the impacts on the surrounding components and the system. This is an inductive modeling approach.
Fault Tree Analysis (FTA)	Identifies combinations of equipment failures and human errors that can result in an accident. This is an deductive modeling approach.
Event Tree Analysis (ETA)	Identifies various sequences of events, both failures and successes that can lead to an accident. This is an inductive modeling approach.
The Delphi Technique	Assists experts to reach consensus on a subject such as project risk while maintaining anonymity by soliciting ideas about the important project risks that are collected and circulated to the experts for further comment. Consensus on the main project risks may be reached in a few rounds of this process. (Ayyub, 2001)
Interviewing	Identifies risk events by interviews of experienced project managers or subject-matter experts. The interviewees identify risk events based on experience and project information.
Experience-Based Identification	Identifies risk events based on experience including implicit assumptions.
Brain Storming	Identifies risk events using facilitated sessions with stakeholders, project team members, and infrastructure support staff.

there is uncertainty associated with each of these parameters that must also be evaluated. A common representation of risk is in the form of an exceedance probability function of consequences, where risk ($R(x)$) is the sum of the probability (p_i) over all scenarios ($i \rightarrow n$) for which the consequence (x_i) is equal to or greater than consequence x:

$$R(x) = \sum_{x_i \geq x}^{n} p_i$$

Risk estimation is a technical and scientific process by which the risks of a given situation for a system are modeled and quantified. Risk assessment can require as well as provide both qualitative and quantitative data to decision makers for use in risk management. Risk analysis is the comprehensive and systematic process of breaking down risk into its underlying elements. Risk assessment provides the process for identifying scenarios, determining event-probabilities, and assessing potential consequences. (For a summary of selected methods for conducting and providing input to risk analysis, see chart on this page.)

A typical scenario-based risk analysis and management methodology can have the following primary steps:

- Defining the objective(s) of the analysis, including the consequence measures of importance to the decisions.
- System definition and familiarization based on its criteria for success.
- Identification of hazards and potential initiating events.
- Modeling and identification of the accident scenarios.
- Evaluation of the failure of each event in the accident scenarios.
- Conducting qualitative and quantitative risk assessment.

• Data and uncertainty analysis.
• Managing system risk through the application of controls, countermeasures, failure prevention and consequence mitigation using risk-based decision making.

For instance, in an accident scenario, *consequences* can be defined as the degree of damage or loss from some failure or sequences of failures. Each failure of a system has one or more consequences. A failure could lead to economic or environmental damage, injury or loss of human life, or some other possible undesired outcome. Consequences need to be quantified in terms of failure-consequence severities using either relative or absolute measures for various consequence types to facilitate risk analysis.

The occurrence probability (p) of an outcome (o) can be decomposed into an occurrence probability of an event or sequence of events (the scenario) involving a hazard (h), and the outcome-occurrence probability given the occurrence of the scenario ($o|h$). The occurrence probability of an outcome can be expressed as follows using conditional probability concepts:

$$p(o) = p(h)\ p(o|h)$$

The probability $p(o|h)$ can be decomposed further into additional components that are dependent on their number and the definitions of the characteristics of the underlying system. Risk can be viewed to be a multi-dimensional quantity that includes scenario-occurrence probability, event-occurrence consequences, consequence significance, and the population at risk. In practice, however, risk is commonly measured as a pair: the probability of occurrence of a scenario, and the outcomes or consequences associated with the scenario's occurrence. This pairing can be represented by the following equation:

$$Risk \ldots [(p_1,c_1),(p_2,c_2),\ldots,(p_i,c_i),\ldots,(p_n,c_n)]$$

where p_i is the occurrence probability of an outcome or scenario i out of n possible scenarios, and c_i is the occurrence of consequences or outcomes of each scenario.

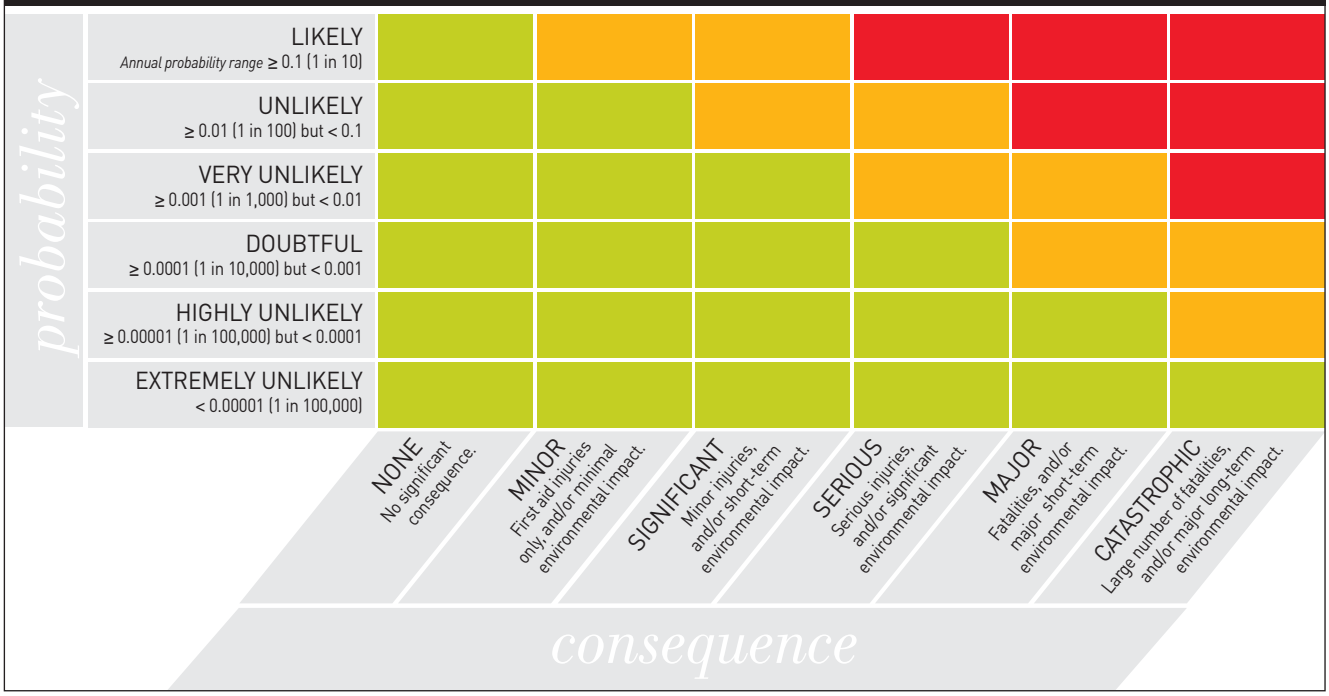
A generalized definition of risk can be expressed as

$$Risk \ldots [(l_1,o_1,u_1,cs_1,po_1),(l_2,o_2,u_2,cs_2,po_2),\ldots,(l_n,o_n,u_n,cs_n,po_n)]$$

where l is likelihood, o is outcome, u is utility (or significance of the outcome), cs is causal scenario, po is population affected by the outcome, and n is the number of outcomes. The definition according to that equation covers all attributes measured in risk assessment described in this article, and offers a complete description of risk, from the causing event to the affected population and consequences.

Indeed, the population-size effect should be considered in risk studies since society responds differently for risks associated with a large population in comparison to a small population. For example, a fatality rate of 1 in 100,000 per event for an affected population of 10 results in an expected fatality of 10^{-4} per event whereas the same fatality rate per event for an affected population of 10,000,000 results in an expected fatality of 100 per event. Although, the impact of the two scenarios might be the same on the society (same risk value), the total

TABLE 2. RISK MATRIX



number of fatalities per event or accident is a factor in risk acceptance. Plane travel may be "safer" than, for example, recreational boating, but 200 to 300 injuries per accident are less acceptable to society. Therefore, the size of the population at risk and the number of fatalities per event should be considered as factors in setting acceptable risk.

Risk-based technologies are tools and processes used to assess and manage the risks of a component—or even of an entire system. One RBT method is *risk assessment*, which consists of hazard identification, scenario-probability assessment, and consequence assessment. Another method is risk control, which uses failure prevention and consequence mitigation, and risk communication. Risk control requires the definition of acceptable risk and the comparative evaluation of options and alternatives through monitoring and decision analysis. Risk control also includes failure prevention and consequence mitigation.

Risk can be quantified by estimating probabilities and consequences in a qualitative manner using expert opinion and communicated using matrices for preliminary screening. A risk matrix is a two-dimensional presentation of likelihood and consequences using qualitative metrics for both dimensions, with each (probability and consequence) assessed as high, medium, and low.

There are several other important concepts to consider. *Safety* is not, as in common usage, the absence of risk, but rather a judgment of risk tolerance (or acceptability in the case of decision making) for the system.

Safety is a relative term since the decision of risk acceptance may vary depending on the individual making the judgment. Different people are willing to accept different risks as demonstrated by different factors such as location, method or system type, occupation, and lifestyle. The selection of these different activities demonstrates an individual's safety preference despite a wide range of risk values. It should be noted that *risk perceptions* of safety may not reflect the actual level of risk in some activity.

Risk communication involves an interactive process of exchange of information and opinion among stakeholders such as individuals, groups, and institutions. It often involves multiple messages about the nature of risk or expressing concerns, opinions, or reactions to risk managers or to legal and institutional stakeholders for risk management. Risk communication greatly affects risk acceptance and helps define the acceptance criteria for safety.

All this comes together under the concept of *risk management*, which entails decision analysis for cost-effective risk reduction within available resources. The benefit of risk prevention and mitigation actions can be assessed as follows:

$$Benefit = unmitigated\ risk - mitigated\ risk$$

The ratio of the benefit to the cost of mitigation can be used to justify the allocation of resources. The benefit-to-cost ratio can be computed, and may also be helpful in decision-making. The benefit-to-cost ratio can be computed as:

$$Benefit\text{-}to\text{-}Cost\ Ratio\ (B/C) = \frac{Benefit}{Cost} = \frac{Unmitigated\ Risk - Mitigated\ Risk}{Cost}$$

There are four primary ways available to deal with risk within the context of a risk management strategy: Risk reduction or elimination, risk transfer (that is, to some other party), risk avoidance, and risk absorbance or pooling.

There's one last major concept to consider—performance probabilities. Performance can be broadly defined as the execution, accomplishment, fulfillment, and operation or functioning of a system. For example, the reliability of a system is defined as its ability to fulfill its design purposes defined as performance requirements for some time period and environmental conditions.

Performance as a notion of the ability to meet or exceed expectations or objectives can be measured based on recognizing two primary components: the capacity provided by the system and the demand defined by the expectations or objectives. Both capacity and demand involve uncertainties that require the use a probabilistic framework for quantification and aggregation. The quantifiable measure of performance can be facilitated by defining a performance (Z) as capacity (C) minus demand (D). Thus, nonperformance probability can be computed as the probability of Z being less than zero.

[REDUCING FAILURE]

How would an engineer apply these concepts when developing a new product? Products are designed to succeed—to perform their function to the satisfaction of the customer. But risk analysis requires the engineer and manager to step back and look at the product (system) in so-called failure space: that is, all the ways that a product can let down the customer.

When conducting a risk analysis on a new product, everything from a new airliner to a small medical device, engineers have to look at the intersection of potential failures and the hardware in the product. For instance, from a stable, steady state system, something perturbs the system leading to a failure. Is there something about the design that could be changed that would reduce the likelihood of that failure?

In an airliner, say, one way to reduce the likelihood of a catastrophic failure when a landing gear tire is punctured is through changing the design to have multiple wheels on each gear. For a stroller, the use of slightly heavier metal struts would reduce the likelihood that the strut would become bent and inoperative.

Another aspect of the product or system to look at is operations. Generally, this is a consideration of the ways a human operator can induce failure, often through acci-

dental or unintentional misuse. So an engineer must find ways to keep such misuse from occurring or to reduce the consequences once it does occur.

For instance, a knob can be redesigned so that it doesn't turn past the point where it would break or cause some other damage to the product. The nozzles on gasoline pumps have automatic shut-offs to reduce the potential for fuel spills. Even familiar software provides a prompt to ask if the user is sure he wants to delete a file. All these methods reduce the likelihood that human error leads to product failure of some sort.

More recently, the software a system uses has been analyzed as a potential source of operational error. In some ways, software-induced failure is similar to that caused by a human operator. But it's a source of failure that risk assessment is still trying to get a firm handle on, since in spite of its machine-based nature, software can often perform unpredictably in circumstances beyond its design parameters.

A third consideration in risk analysis is the role of maintenance. Maintenance can be used to reduce the probability of failure in two ways. Periodic surveillance can be built into the routine operation of the product. Checking the oil level in a car engine is one example of this kind of surveillance, as is checking for cracks or wear in a critical part of a product. By turning up signs that a part might need to be repaired or replaced, simple surveillance can reduce the likelihood of a component loss that could lead to a more serious failure.

Of course, some components don't show obvious signs of wear before they fail. But if there is good statistical data on how long such a part can perform before failure, a system of preventive maintenance can be established. By replacing critical parts before they fail (according to a certain statistical probability of failure), one can drive down the likelihood of failure for the entire system.

Preventive maintenance, of course, is not without cost. By doing this, one is replacing a part that might have quite a bit of operating life left in it. And every time one conducts system maintenance, one introduces the possibility of human error, for example, if a part is incorrectly installed. These factors must also be considered when performing a full risk analysis.

Finally, there are so-called upset conditions that can occur no matter what an engineer or manager does to reduce risk. These are known as external conditions: natural phenomena, such as storm damage or earthquakes, or accidents from random human events outside the scope of the system.

Are there ways to plan for something as unlikely as a traffic accident that knocks out a transformer that feeds electricity to a factory? Yes; though not every possible random occurrence can be accounted for. A robust risk analysis will model a system in steady state, pulse it with some external events, and analyze how the system reacts. By building an event tree forward from selected potential random occurrences, one can look for places where hardware might falter or a human operator might make a mistake.

Risk analysis will tell you how, given an event, the system can fail. This information then gives a manager the data he needs to manage the risk in the system.

That doesn't mean reducing the probability to zero. There will always be an acceptable risk level that is set by a regulator or executive. And ultimately, final decisions on the system and its components will not be risk-based, but risk-*informed*, where decisions are made through a combination of analysis and deliberation. But the use of tools such as risk analysis helps enable decision-makers to be as informed on the risks involved with each choice as they are with other important parameters of the system such as strategic importance, schedule criticality, cost, and customer satisfaction. ■

Editor's Note: This article was prepared by the executive committee of ASME's Safety Engineering and Risk Analysis Division (SERAD) drawing on their expertise in academia, space missions, energy and fuel cells, manufacturing, infrastructure, and marine systems.

Selected Sources

Ayyub, B. M., 2001, *Elicitation of Expert Opinions for Uncertainty and Risks*, CRC Press, Boca Raton, Fla.

Ayyub, B. M., 2003, *Risk Analysis in Engineering and Economics*, Chapman and Hall/CRC Press, Boca Raton, Fla.

Ayyub, B.M., Gupta, A., Assakkaf, I., Shah, N., Kotwicki, P., Avrithi K., 2007. *Development of Reliability-Based Load and Resistance Factor Design (LRFD) Methods for Piping*, ASME Report CRTD-86, ASME Research Task Force on the Development of Reliability-Based Load and Resistance Factor Design (LRFD) Methods for Piping, ASME, Washington, DC.

Ayyub, B. M., and Klir, G. J., 2006, *Uncertainty Modeling and Analysis in Engineering and the Sciences*, Chapman and Hall/CRC Press, Boca Raton, Fla.

Balkey, K.R., Ayyub, B.M., Vic Chapman, O.J., Gore, B.F., Harris, D.O., Karydas, D., Simonen, F.A., Smith, H., 1991. *Risk-Based Inspection - Development of Guidelines, Volume 1 - General Document*, CRTD - Vol. 20-1, The American Society of Mechanical Engineers.

Haldar, A., and Mahadeva, S., 2000, *Probability, Reliability and Statistical Methods in Engineering Design*, John Wiley and Sons, New York.

Kumamoto, H., and Henley, E.J., 1996, *Probabilistic Risk Assessment and Management for Engineers and Scientists*, Second Edition, IEEE Press, New York.

NASA Procedural Requirement (NPR) 8715.3, NASA General Safety Program Requirements (March 27, 2006).

National Research Council, 1996, *Understanding Risk: Informing Decisions in a Democratic Society*, National Academy Press, Washington, D.C.