Risk Assessment & Control

Is your system safety program wasting resources?

By Pat Clemens and Tom Pfitzer

Abstract: *The familiar risk assessment matrix supports subjective hazard-by-hazard risk evaluations. For those hazards found to pose risk above the tolerance limit, countermeasures must be implemented—often at great expense for hazards presenting risk just above the acceptable threshold. Often, greater reduction of whole-system risk may be obtained by applying the same or lesser resources to hazards with already acceptable risk.*

A HAZARD may be viewed as a threat of harm posed to an asset (often called a "target") that one wishes to protect. System safety analytical approaches such as preliminary hazard analysis, fault hazard analysis and failure modes and effects analysis are available to help identify hazards within a system (Stephans and Talso). These "hazard inventory" methods identify and catalog individual hazards as though they exist as line items in an inventory of all system hazards. Hazards H_1 to H_n in Figure 1 represent such an inventory.

Risk is an attribute of a hazard/target combination. It is a measure of the degree of threat that a hazard poses to a target. Risk for an individual hazard/target combination is characterized by the severity (S) of the harm threatened and the probability (P) that the harm will occur. When considered quantitatively, risk has long been recognized as the simple arithmetic product of its severity and probability components (Arnauld and Nicole). To assess risk for a particular hazard/target ensemble, these two components can be introduced numerically—for example, using actuarial data or handbook values—or subjectively, by applying judgment-based estimation.

In system safety practices based on the hazard inventory methods, subjective methods are predominant. These methods are customarily based on application of a risk assessment matrix such as that shown in Figure 2. Such matrixes are found throughout the literature and relevant standards (e.g., DOD; NASA). The matrix shown in Figure 2 is based on one found in MIL-STD-882D, modified to conform to findings on user preferences (Clemens). Descriptive phrases (not shown in the matrix) guide interpretations of severity and probability levels of the matrix. The matrix supports risk assessment and through its zoning guides risk acceptance/rejection decisions.

Applying the Matrix

The line-item inventory (Figure 1) models results that are obtained by applying the matrix to hazards H_1 to H_n. For each hazard, the analyst judges the severity of harm (S_1 to S_n) that might be inflicted on the target of concern. The probability of that harm is also calculated for each (P_1 to P_n). Entering the matrix axes of Figure 2 with these data provides an indication of the level of risk posed (R_1 to R_n). Matrix zoning indicates risk acceptability. In this example, risk in the zone labeled "3" is acceptable. Risk in zone 1 is wholly unacceptable, while that in zone 2 is acceptable by management-approved waiver, but only for nonpersonnel targets.

Nature of the Problem

Viewing & Applying Analysis Results

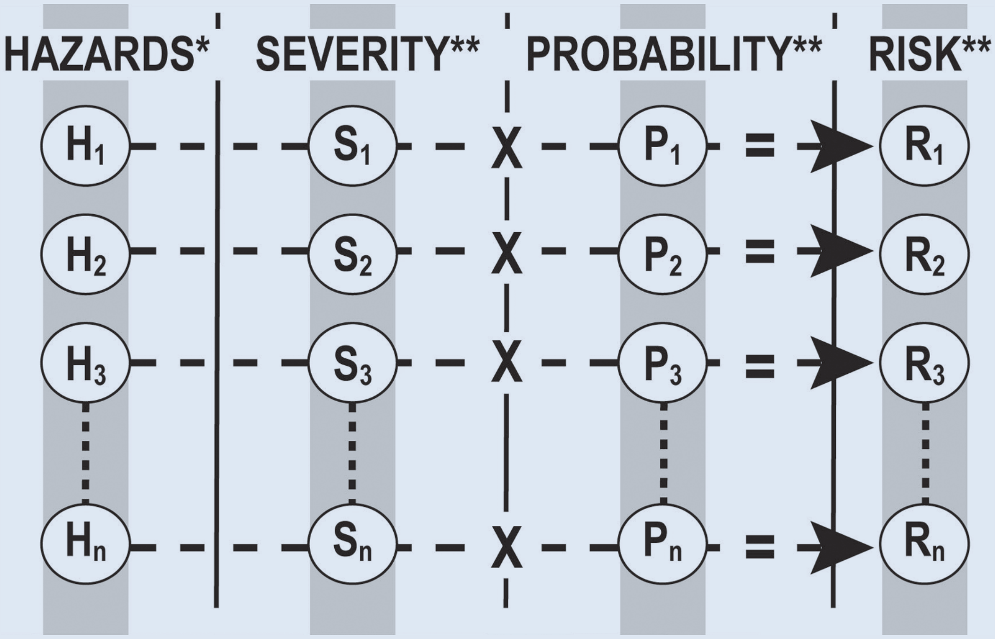
A bar chart paradigm (Figure 3) models results of the hazard-by-hazard, matrix-guided risk assess-

Pat Clemens, P.E., CSP, *performs system safety engineering work for A-P-T Research Inc., Huntsville, AL. He is a past president of the Board of Certified Safety Professionals. During his career, Clemens has developed and implemented system safety programs in both government contracting and in the private sector. He teaches system-safety-related courses for various private corporations, ASSE, NASA and universities. Clemens is a professional member of ASSE's Middle Tennessee Chapter and is a member of the Society's Engineering Practice Specialty.*

Tom Pfitzer *is founder and president of A-P-T Research Inc. He holds an M.S. in Industrial Engineering (system safety option) from Texas A&M University. Pfitzer is a graduate of the U.S. Army Intern Program in Safety Engineering and has 19 years' service in the safety career field for the U.S. Army. He has been recognized by the System Safety Society as National Manager of the Year for his efforts to bring common practices to the areas of system safety, range safety and explosives safety.*

Figure 1

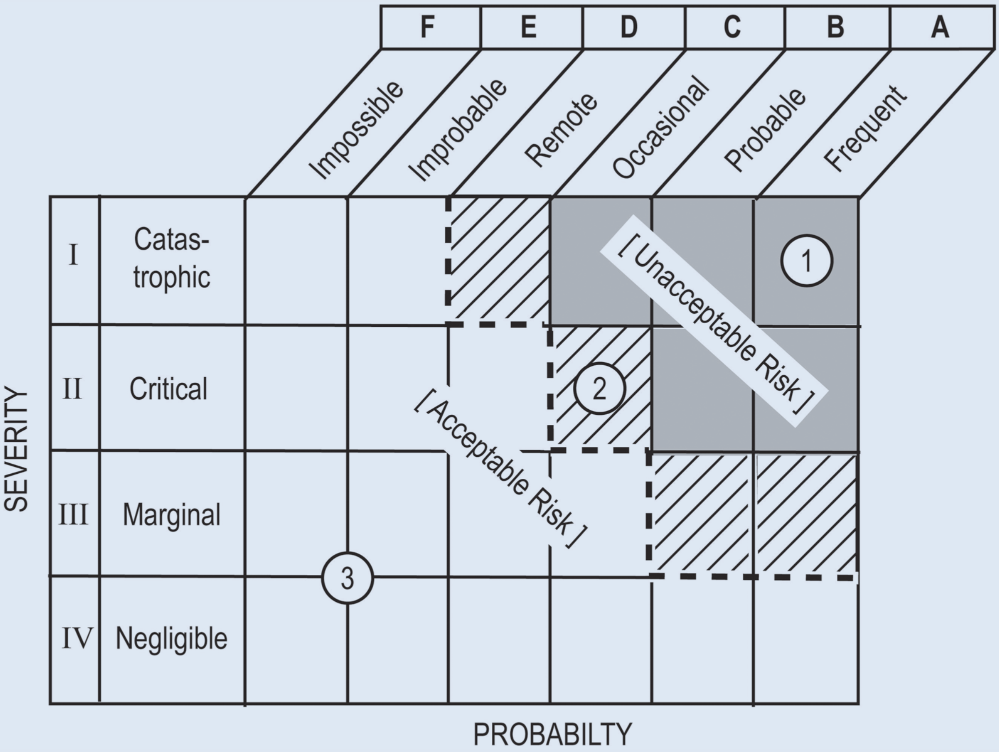
The Hazard Inventory Result



*From PHA, FMEA, etc.
**From Risk Assessment Matrix.

Figure 2

A Typical Risk Assessment Matrix



ments. (Note: In Figures 3 and 4, risk bars bear linear scale relationships to one another to more simply portray the concept presented. The authors recognize and prefer use of logarithmic scales in risk quantifications.) Bar heights, as gauged against the linearly scaled risk axis, represent the values of risk provided by the matrix. The risk tolerance boundary from the matrix now appears as a horizontal limit.

Here, risk is found to be acceptable for hazards H_1, H_3 and H_4, but not for hazard H_2, which exceeds the risk tolerance limit by the amount indicated by the shaded portion of the bar. Standards-based system safety program plans customarily require that abatement measures be imposed to reduce the risk of hazard H_2 and of any other hazard with risk exceeding the tolerance limit. Risk tolerance limits set by such standards almost universally apply to individual hazards, not to risk for the overall system.

Misguided Direction

A particular shortcoming of this seemingly logical and orderly treatment of system risk arises out of the characteristics of the approach—that is, the use of the hazard inventory methods coupled with applying the matrix guidance found in most standards and system safety program plans.

- Hazards are identified and cataloged singly as results of hazard inventory methods (e.g., preliminary hazard analyses, failure modes and effects analyses, fault hazard analyses). These hazards can be viewed as individual entries in a line-item inventory.
- Risks of the hazards are assessed singly, item-by-item and their acceptability is judged individually.
- Risks of the individual hazards sum to a collective value of total system risk that is not seen by the analyst. (Simple risk summation expresses a near-exact value for total system risk. Cases in which this is

not true are relatively rare and are considered beyond the purposes of this article.)

•Standards and program plans prescribe a risk tolerance limit only for individual hazards; for hazards with risk that exceeds the prescribed level of tolerance, risk must be reduced to an acceptable level.

This leads to an insidious outcome: Because whole-system risk is the summation of the partial risks, the portrayal of risk for the system becomes that modeled in Figure 4. Here, the bars of Figure 3 have been stacked end-to-end to produce a representation of total summed risk for the system. (Although total summed system risk is often overlooked in system safety guidance documents, it is gaining widespread recognition as a parameter of importance in the risk-acceptance decision process.)

$$R_{Total} \approx \sum_{i=R_1}^{i=R_n} (R_i) = R_1 + R_2 + R_3 + \cdots + R_n$$

The expression is presented here as an approximation to accommodate rare instances in which simple summation may be insufficiently exact. One can now appreciate that one may be misled to believe that because the partial system risks are seen as individually acceptable, whole-system risk is, therefore, tolerable. For a large, complex system, this may be untrue.

An Example Case: An Uncomplicated Scenario

Surprisingly, many SH&E professionals may not recognize that the risks of independent hazards to a system do indeed sum in the manner shown in Figure 4. An example illustrates this principle.

Consider a system that must operate full time. A dollar value has been assigned to the loss outcome caused by any unplanned system outage. Thus, the severity penalty from a system outage is well known. System safety analysis has identified four hazards that would cause an outage—utility power interruption, flooding, operator error and fire—and the probabilities of each have been evaluated. The risk for each hazard has been assessed using a risk assessment matrix (if done subjectively) or by simple multiplication of the severity of each by its associated probability (if done quantitatively).

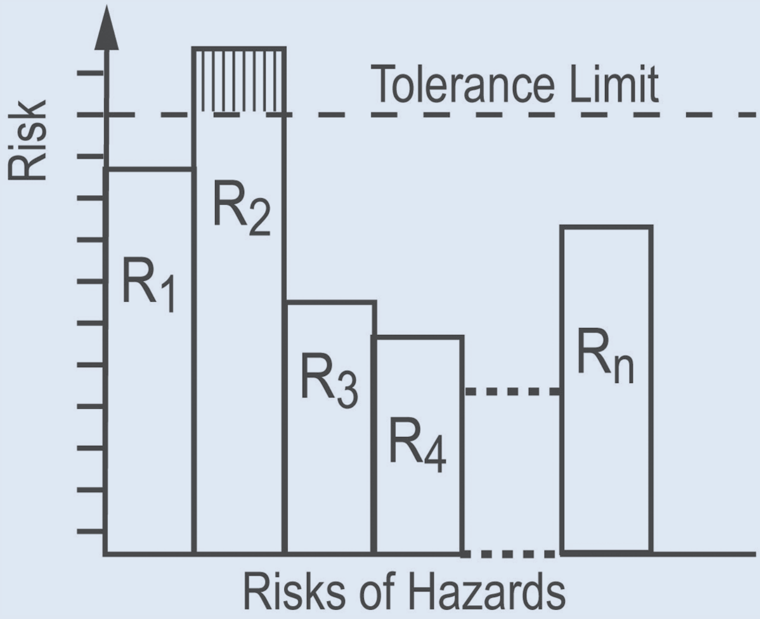
The result is as shown in Figure 3, where R_1 represents the system outage risk for the utility power interruption hazard, R_2 for flood, R_3 for operator error and R_4 for fire. Total risk is the simple arithmetic sum of these partial risks. An insurer providing coverage for these individual hazards will adjust the premium to a value determined chiefly by this sum.

A Resource Distribution Anomaly

Another important failing must be noted. Consider the cost of mitigation. Most system safety standards and program plans would require abating the flood hazard (R_2) because its risk exceeds the allowed threshold of tolerance for individual hazards. Mitigating this hazard can be accomplished only by moving the facility to a higher elevation at a cost of $473,000.

Figure 3

The Bar Chart Paradigm



However, an uninterruptible power supply can be installed at the far lower cost of $22,000, greatly reducing R_1. As shown in Figure 4, doing so will lower total system risk by an appreciably greater amount than is represented by the risk tolerance overage of R_2. The already acceptable risk R_1 is appreciably greater than is the unacceptable overage of R_2. Spending the lesser sum will result in a markedly greater overall system risk reduction than spending the greater sum.

As this example shows, blind pursuit of the guidance given for such cases can lead to misallocation of abatement resources if the purpose is to achieve the greatest reduction in whole-system risk that can be realized per abatement dollar committed.

Addressing the Problem

"Tailor" the Matrix

In MIL-STD-882D and NPR 8715.3, risk assessment matrixes appear as examples, not as mandatory system safety program requirements. It is expected that one will tailor such matrixes to satisfy the risk management needs of particular settings. Yet, such customizing is rare.

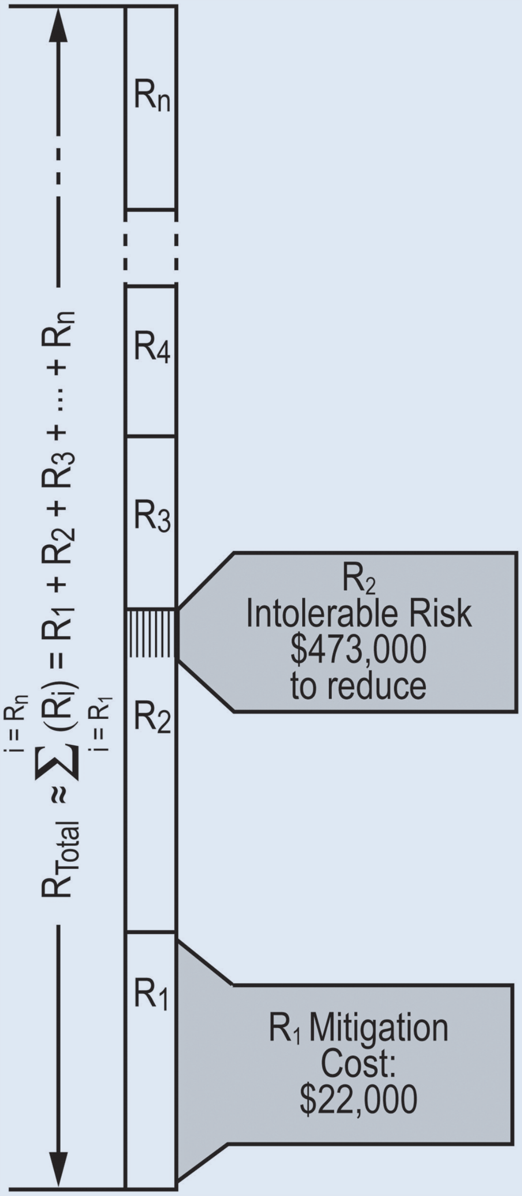
Tailoring can be accomplished in several ways. For example, the scales for the severity and probability axes can be adjusted, or the risk tolerance boundaries separating risk zones can be shifted. Such adjustments can provide an easily applied, practical solution to the problem highlighted here.

Consider the earlier example. The critical need is for full-time operation. Four hazards that threaten such operation have been identified. The risk posed individually by each hazard is of less importance than is the risk of system outage. Thus, the apportionment of total system risk among the contributing hazards can be addressed as a risk management problem separately from the greater concern for system outage. Tailoring one matrix to represent risk tolerance for individual hazards and another to represent whole-system risk tolerance would allow one to apply this logic. Of course, because matrixes express risk tolerance intentions, they must have the approval of the system proprietor—that party ultimately responsible for risk acceptance.

One can be misled to believe that because the partial system risks are seen as individually acceptable, whole-system risk is, therefore, tolerable.

Figure 4

Total System Risk


R_n
R_4
R_3
R_2
R_1
$R_{Total} \approx \sum_{i=R_1}^{i=R_n} (R_i) = R_1 + R_2 + R_3 + \ldots + R_n$
R_2 Intolerable Risk \$473,000 to reduce
R_1 Mitigation Cost: \$22,000

The Practitioner's Obligation

The problem can be further resolved by the responsible system safety practitioner who:

- becomes acquainted with both the shortcomings and the strengths of the system safety techniques that result in line-item inventories of individual hazard risks;
- is alert to opportunities to apply his/her understanding of the individual analytical approaches to the best overall benefit of controlling whole-system risk;
- promotes, among risk managers and system owners, an improved understanding of the important distinction between partial risk and whole-system risk, to the advantage of achieving reduced overall system risk at the least cost.

Risk Managers & Standards Writers

Those who manage system risk and those who write standards and program plans would do well to:

- understand the distinction between partial risk and whole-system risk;
- be wary of wasting resources as a result of levying mandates that hinder abatement of whole-system risk;
- recognize that provisions should be made to accommodate the practical deployment of assets in ways that optimize overall system risk reduction. Maximizing risk reduction per dollar spent is best achieved by recognizing both partial risks and whole-system risk.

Conclusion

Although the principles described here are obvious and uncomplicated, the authors are surprised that system safety practitioners in the U.S. have been slow to recognize and adopt them. Such is not the case abroad. For example, Kummer describes application of these concepts to minimize risk at minimum cost in Swiss facilities.

It should also be noted that aspects of the need for codeworthiness have not been addressed in this article. System safety principles, no matter how diligently applied, do not substitute for the need to conform to applicable codes, standards and regulations. This is of great importance when considering personnel as assets to be protected by the system safety program plan. ■

References

Arnauld, A. and P. Nicole. *La logique, ou l'art de penser (Logic or the Art of Thinking).* Paris: 1668.

Clemens, P.L. "Preferences in Interpreting the Risk Assessment Matrix." *Professional Safety.* June 1995: 37-39.

Kummer, P.O. "Reducing Risk to the Max: Does It Cost a Fortune?" *Proceedings of the 31st DOD Explosives Safety Seminar,* San Antonio, TX; August 2004.

NASA. *NASA Safety Manual.* NPR 8715.3. Washington, DC: NASA, January 2000.

Stephans, R.A. and W.W. Talso, eds. *System Safety Analysis Handbook.* Unionville, VA: System Safety Society, 1997.

U.S. Dept. of Defense (DOD). Standard Practice for System Safety. MIL-STD-882D. Washington, DC: U.S. DOD, February 2000.