MANY HAZARD ANALYSES *Conceal* WHOLE-SYSTEM RISK

By P.L. CLEMENS

Many system safety analytical techniques produce line-item inventories of individual hazards, along with subjective assessments of risks posed by each. Because these hazards tend to be independent, stand-alone entities, their risks sum to approximate total risk for the system. Via this process, the analyst may be deceived into believing that because risk is acceptable when viewed hazard-by-hazard, overall system risk is also acceptable. This same principle is responsible for the often-erroneous assumption that a system with many identified hazards carries more risk than one with fewer. It may also lead to misguided deployment of resources to reduce whole-system risk.

Many definitions have been proposed for the term "hazard." At its simplest, a hazard may be thought of as a threat of harm to a resource of value—for example, a threat of harm to personnel, equipment, the environment, productivity or the product of an enterprise. A typical hazard description contains three elements that express the threat:

- **source:** activity and/or condition that serves as the root of the hazard;
- **mechanism:** means by which the source can produce the harm;
- **outcome:** harm that might be suffered as a consequence of the hazard.

These three elements express what is often called a "hazard scenario"—a brief narrative description of a potential mishap attributable to the hazard. For example: inert gas (source) leaking to displace oxygen (mechanism) from an occupied confined space, resulting in asphyxia (outcome). The scenario need not specifically address each of the three aspects, nor need it express them in the sequence shown. However, it should be possible to infer all three from the hazard description.

DISJOINT HAZARDS

Many subjective hazard analysis and risk assessment techniques—including preliminary hazard analysis, failure modes and effects analysis (FMEA) and their many derivatives—produce hazard-by-hazard lists of discrete hazards. These hazards are largely disjoint—that is, they are independent of one another. In FMEA parlance, each individual system element becomes a hazard source, each failure mode becomes a mechanism, and the effects are the outcomes, which are judged as to the severity of potential harm. (See Stephans and Talso for an anthology of such techniques. Raheja and Goldberg, et al describe their use and provide examples of their application.)

Figure 1 models the progression of a typical subjective analysis. System hazards (H) are identified one-by-one via methods such as inspections, checklists, reviews of near-miss reports and operational walk-throughs. By long-standing convention, the worst credible outcome is evaluated to reflect the severity component (S) of risk. [This convention can, however, mislead the analyst to declare risk at an erroneously low level (Clemens).]

The likelihood of that outcome is then

Some analytical techniques can deceive the analyst into believing that because risk is acceptable when viewed hazard-by-hazard, overall system risk is also acceptable.

FIGURE 1 Hazard Analysis Process

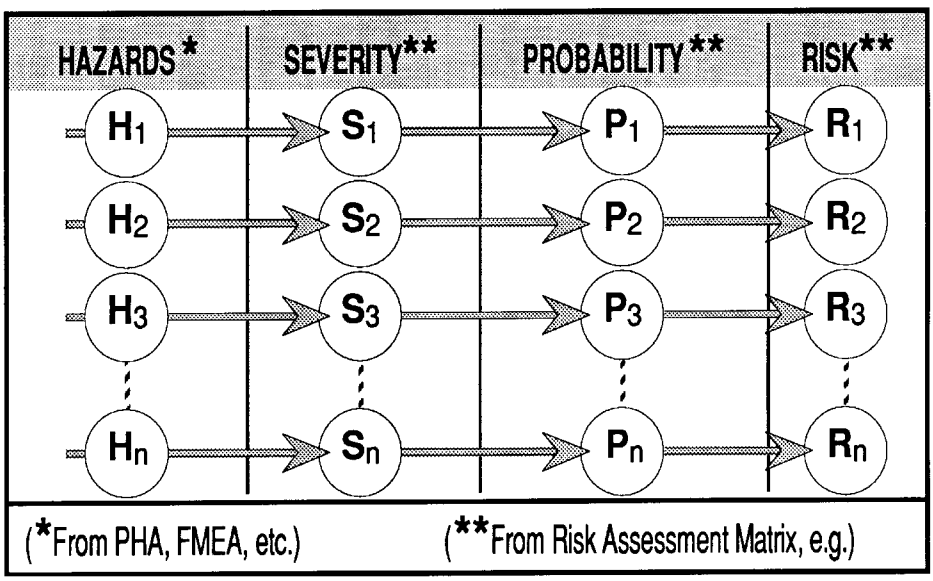
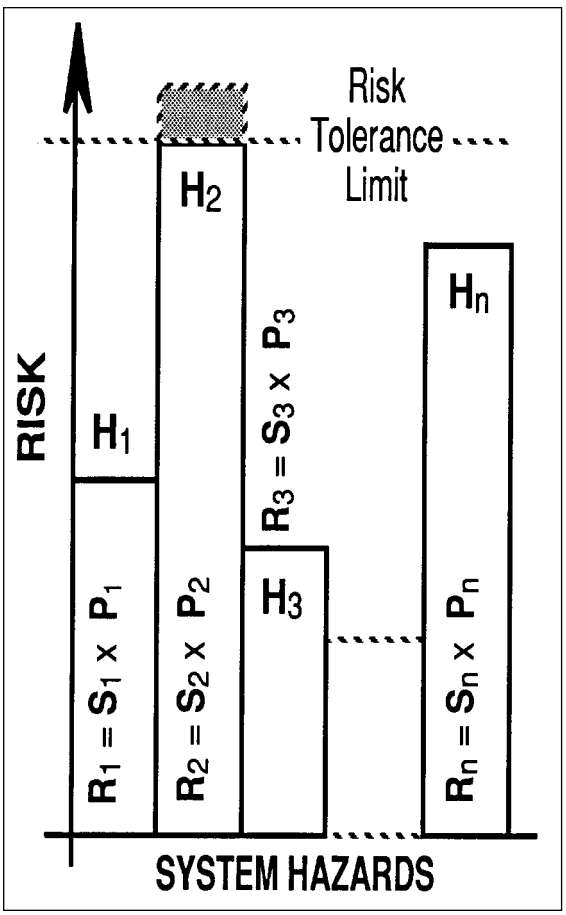


FIGURE 2
System Risk
As Viewed by the Analyst



judged to represent risk's probability component (P). A risk assessment matrix customarily guides the subjective evaluations of both severity and probability and leads to a declaration of risk (R) (Raheja; Goldberg, et al). These data become entries in the hazard analysis for the line-item hazard under consideration.

Figure 2 offers a view of the resulting whole-system risk. Taken as a function of its severity and probability components, risk is seen as a separate entity for each hazard (e.g., H_1, H_2, H_3). These hazard-by-hazard risks are expressed in terms of the severity and probability coordinates that characterize each in the risk assessment matrix. Alternatively, each risk may be expressed quantitatively as the product of its severity and probability components; numerical data to support this time-consuming method are often not available, however, so it is rarely used. In either case, the analyst's attention is focused on risk as viewed at the elemental level of individual hazards within the system.

When these techniques are used, risk for an occasional hazard may be found to exceed a declared level of tolerance. For example, as indicated by the shading, risk for hazard H_2 in Figure 2 may initially have exceeded the tolerance limit. When this occurs, mitigating countermeasures are applied to reduce risk by lowering either its severity or probability component (or both). Risk is then reassessed to ensure that it falls within acceptable bounds.

In most cases, codes, standards and regulations prescribe specific countermeasures to be applied against individual hazards. That is, risk is controlled by requiring particular mitigation features for each hazard taken singly. For example, standards dictate that an elevated open-sided platform must have guardrails and toeboards to protect against falls and dropped objects; high-intensity sound pressure levels require hearing conservation measures. In other words, standards typically address whole-system risk on a hazard-by-hazard basis.

TRUTH ABOUT WHOLE-SYSTEM RISK

Individual hazards are largely disjoint as they are recognized and described. Therefore, they are largely independent of one another. (Two items are statistically independent if neither can cause nor be caused by the other.) In reality, however, the risks of disjoint hazards sum. Thus, nature views a system's total risk to be approximately equal to the sum of partial risks for individual hazards (Figure 3).

Figure 4 depicts this relationship; the risk bars of Figure 2 now appear end-to-end. This view of whole-system risk goes unseen by the analyst who uses subjective hazard inventory methods. Nor is it seen by the manager who must decide whether to accept risk. And, of course, it is rarely addressed by codes or standards.

This creates an obvious pitfall. Both analyst and manager may believe that, because risk for each system hazard is acceptable when viewed individually, whole-system risk is, therefore, also acceptable. As Figure 4 shows, this may not be the case.

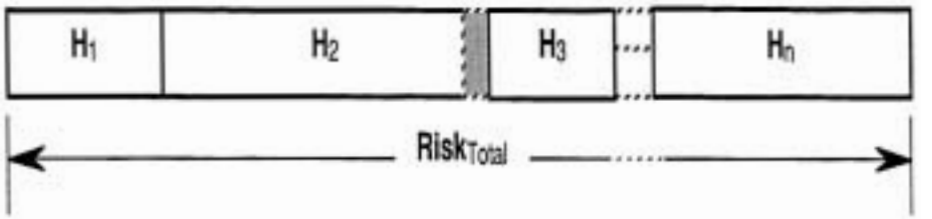
These same principles create another, less-obvious trap. One might conclude that whole-system risk is great for a system with a long list of hazards and that risk is comparatively less for a system with a short list of hazards. For two reasons, this may be a faulty conclusion:

1) Such a conclusion presumes that all hazards pose equal risks. This may not be so, and it is the *risks* of hazards that sum in the expression (Figure 3), not the hazards

FIGURE 3
Expression of Risk

$$\text{Risk}_{\text{Total}} \approx \sum_{i=1}^{i=n} S_i \times P_i = (S_1 \times P_1) + (S_2 \times P_2) + (S_3 \times P_3) + \cdots (S_n \times P_n)$$

FIGURE 4 System Risk As Viewed by Nature



themselves. The long list may include many hazards with trivial risk, while the short list may contain hazards with risks that have a high collective magnitude.

2) The long list may have been produced by a thorough analyst, the short list by one performing only a superficial analysis. Ironically, the more-thorough analyst now has a system that appears to pose great risk simply as a result of that very thoroughness.

WHERE TO REDUCE WHOLE-SYSTEM RISK?

The practitioner concerned with lowering whole-system risk must decide which hazard(s) to attack. The natural inclination is to concentrate resources on those hazards with greater risks. However, in some cases, devoting those same resources to hazards with less risk may produce a greater overall reduction in whole-system risk.

According to Figure 4, system risk would be reduced as much by shortening one bar as by shortening any other by an equal amount. Thus, the best course of action is to select those hazards that will yield the greater risk decrements per dollar of outlay. For example, it may be less expensive to eliminate risk for hazards H_1 or H_3 altogether than to reduce the shaded area of hazard H_2. The shrewd practitioner strives to maximize reduction of overall risk. (This presumes, of course, that code compliance has been satisfied.)

OPPORTUNITY FOR DECEIT

Embedded within these principles is an opportunity for artful deceit. The analyst who finds that risk is unacceptably high for a particular hazard may be able to conceal this outcome simply by performing the analysis at a lower level of system indenture.

For example, consider this transportation hazard: "Spontaneous loss of front wheel at highway speed (source) leading to steering incapacity (mechanism) and fatal crash (outcome)."

Expressed in this manner, the hazard outcome and its corresponding probability evaluation must take into account all credible means whereby a front wheel might be lost. For a particular design configuration and an intended rough-duty application, probability and severity might, indeed, combine to produce an unacceptably high assessment of risk. As a result, a redesign or a change to light-duty service would be needed to mitigate the hazard.

However, if the analyst drops the level of the analysis to piece-parts within the system, the hazard may become subdivided into lesser elements such as "failure of wheel mounting stud threads to retain fastener." This leads only to a less-than-fatal transfer of mechanical stress to the surviving studs, which are designed to accept the extra load. By conducting the analysis in this manner, an important component of system risk may be concealed—a deceit facilitated by the fact that this approach often appears to reflect superior analytical thoroughness.

COMMENTS ON COPING

To avoid these problems, the system safety practitioner should:

1) Reject the offhand assumption that because risk is acceptable for each individual hazard identified, whole-system risk is, therefore, also acceptable.

2) Not conclude, without justification, that a short list of hazards necessarily represents a system with less overall risk than one which produces a long list.

3) Describe the methods used to identify hazards and assess their risks, and provide sufficient detail so an independent reviewer can appreciate the degree of thoroughness involved.

4) Consider first those hazards that will yield the greatest risk decrements per dollar of outlay. This presumes that individual hazards covered by codes have been addressed appropriately.

5) Reject the assumption that simply because a system is wholly codeworthy, the risk it poses is, therefore, acceptable.

Nature views a system's total risk to be approximately equal to the sum of partial risks for individual hazards.

6) Consider the level at which analysis has been performed in relation to the system's architecture. Analysis should be conducted at systemically appropriate levels to avoid blindly accepting a large collection of partial risks that may each be made to appear individually acceptable. ■

REFERENCES

Clemens, P.L. "Worst Credible Event: An Important But Flawed Convention." *Hazard Prevention.* 2nd Quarter, Vol. 35, 1999.

Goldberg, B.E., et al. "System Engineering 'Toolbox' for Design-Oriented Engineers." NASA Reference Publication 1358. Washington, DC: NASA, 1994.

Raheja, D.G. *Assurance Technologies: Principles and Practices.* New York: McGraw-Hill, 1991.

Stephans, R.A. and W. Talso, eds. *System Safety Analysis Handbook.* 2nd ed. Unionville, VA: System Safety Society, 1997.

P.L. Clemens, *P.E., CSP, performs system safety engineering work for Sverdrup Technology Inc., located in Tullahoma, TN. A past president of the Board of Certified Safety Professionals, he has developed and implemented many system safety programs in both government contracting and in the private sector. Clemens is a professional member of ASSE's Middle Tennessee Chapter and a member of the Engineering Practice Specialty Division.*