Finding All the Hazards

How do we know we are done?

By Susan Cantrell and Pat Clemens

IN THE PRACTICE OF SYSTEM SAFETY, hazards are threats of harm to assets that one wants to protect. These assets may include life, limb, health, equipment, the environment or productivity. System safety practitioners seek to identify the hazards posed both by and to a system. Risk that each hazard poses to each asset is then assessed in terms of the severity and the probability of the potential harm. Risk at intolerable levels must then be abated or accepted (Ericson, 2005; Manuele, 2008).

The most fundamental step in practicing system safety is identifying the hazards. If not practiced well, then all that follows is crippled. Hazards remain unidentified and unmitigated, erroneous assumptions about safety of the system are made and used for future planning, and people and hardware are put at risk unawares. The adage is true, "If you can't find the hazards, you can't practice system safety."

In the system safety literature, much is made of the importance of identifying hazards. Authors in the field describe many independent methods for hazard discovery. Manuele (2008) presents a list of 10 basic methods. The fact that there are so many varied ways to identify hazards indicates that finding all of them is more than casually challenging.

Little has been reported in the literature concerning the thoroughness with which the analyst may expect to identify system hazards. Of 11 U.S.-published textbooks recently consulted for information on the topic, only one (Leveson, 1995) provided definitive information on the subject. Even the encyclopedic and well-indexed three-volume *Lees' Loss Prevention in the Process Industries* (Mannan, 2005) makes no mention of the matter of thoroughness in hazard discovery.

Can that first step in this system safety process, finding the hazards, be done exhaustively? Or can it be performed only with questionable thoroughness? Dare a system safety engineer ever claim to have found all hazards in a system? If one admits to finding fewer than all of them, what portion might have been missed? Is waiting for a loss event the only sure way to identify an additional hazard? SH&E professionals must be able to address fundamental but troubling questions such as these.

The Measurement Challenge: Do We Find All the Hazards?

The purpose is not to revisit the many ways of finding hazards, nor to stress the importance of doing so, as the literature already contains much on those subjects. Rather, the purpose is to address the questions, Do we ever really find all of the hazards? What must we do to at least optimize our process? Admitting to finding fewer than all of them requires both an understanding of that failure and a method for expressing this less-than-perfect degree of thoroughness.

To determine what proportion of all hazards within a system have been identified by any particular technique, one must first establish how many hazards actually exist within the system. Figure 1 helps illustrate this paradox. As shown, each of many analytical methods will identify some system hazards. Each may also find some that are found by others. But no single method will find them all.

To determine the effectiveness of a method for finding all hazards, the total hazard population must first be discovered. However, if a method for finding that population were available, it would be used universally, eliminating the need to evaluate others. On the basis of this logic, it can be concluded that either:

- It is possible to find all of the hazards in a system but there is no way to demonstrate this.
- It is impossible to learn what proportion of all of the hazards have been identified.

What remains is the query that haunts all who practice system safety: How do we know when we are done?

A Practical Measurement Approach: A Straightforward Procedure

By what practical method might one gauge the

Susan Cantrell *is a system safety engineer with experience in both the NASA and Department of Defense realms. She is currently working on the ground-based midcourse defense program, and is a member of the System Safety Society.*

Pat Clemens, P.E., CSP, *is a past president of BCSP. He has developed and implemented many system safety programs in both government contracting and the private sector. He has developed and taught system-safety-related courses for various private corporations, for NASA and on several university campuses. He has served for several years as a visiting professor at the von Kàrmàn Institute for Fluid Dynamics, Brussels, Belgium. Clemens is a professional member of ASSE's Middle Tennessee Chapter.*

Figure 1

Hazard Identification Paradox

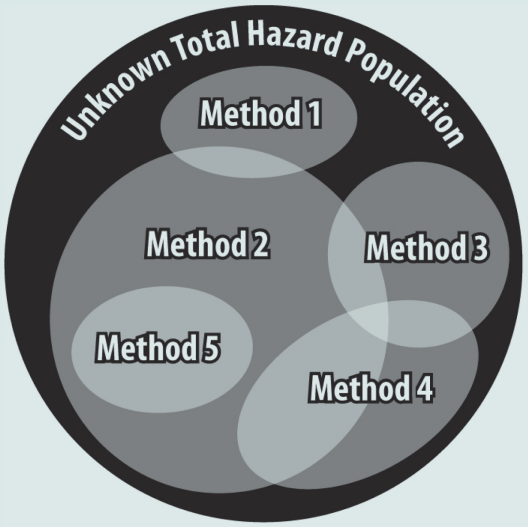


Figure 1: Each hazard identification method identifies some, but not all, system hazards.

thoroughness with which system hazards are identified? Surely the most appealing way would bring the practitioner face to face with the noted problem. Using whatever method is to be tested, the number of hazards actually found would be compared to the total number actually present. This would be uncomplicated, direct and simple, and, based on the earlier discussion, completely impossible.

Pioneering work on resolving this problem has been conducted at the Technical Research Center of Finland (Suokas, 1988; Suokas & Veikko, 1989). The work has been reported in the literature (Suokas & Veikko, 1989; Suokas, 1988; Suokas & Kakko, 1989). However, few U.S. system safety practitioners are familiar with it.

The Finnish method produces results by an approach characterized in Figure 2. The first step is to note the number of hazards discovered by assiduously applying the hazard identification method undergoing evaluation as a primary technique. In this example, hazard and operability analysis (HAZOP) is under evaluation. It has identified H_e hazards.

Added to that number are the other hazards uncovered by successive use of supplemental follow-on hazard search methods. Still later, the additional hazards found during system commissioning and shakedown or early operation may also be added if they are available. The ratio of the initial hazard population (H_e) to the last one (H_s) reflects the effectiveness of hazard identification for the initial primary method undergoing evaluation. Expressed as a percentage, hazard identification effectiveness (HIE) % = (H_e/H_s) x 100.

Notice that the unknown true total of all hazards present within the system (H_T in Figure 2) may be approached but is unlikely to ever be reached. Those efforts added beyond H_e afford no assurance of identifying all the hazards. The approach nonetheless provides a relative measure of HIE for the primary method that had produced the H_e result.

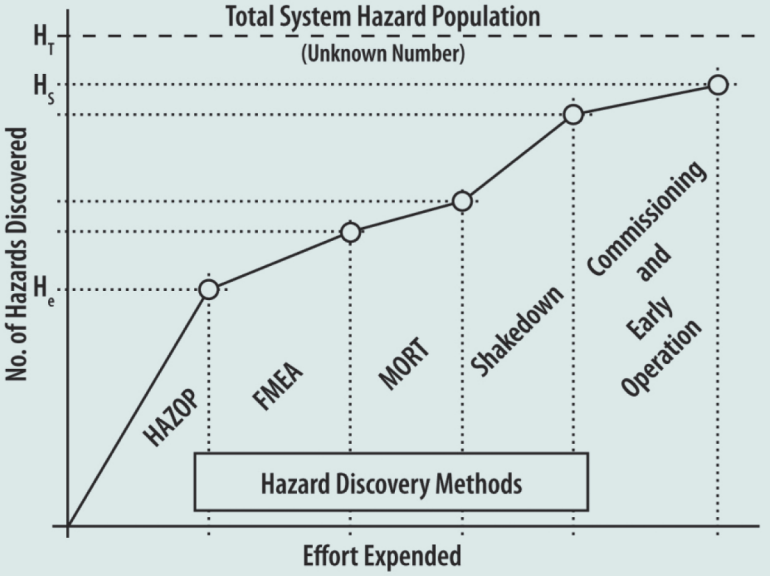
Notice that because not all hazards will have been found even by the combined methods, the HIE ratio is somewhat higher than would have resulted had the actual total hazard population, H_T, been known and used in place of H_s. Thus, for the technique being investigated and for the system type at issue, it can be said with confidence that this method produces a measure of HIE which cannot be exceeded. Notice also that a falsely high HIE will be the result of following the initial method with a battery of feeble ones.

Results of Using the Method: An Irrefutable but Dismal Outcome

The approach described here was used to evaluate several hazard discovery techniques as they have been applied to various systems (Suokas & Kakko, 1989; Suokas & Pyy, 1988). The work was performed by competent, trained, experienced analysts. Example findings are reported in Table 1 (p. 34). This table shows results from evaluations of two hazard

Figure 2

Evaluating Hazard Identification Thoroughness



Note. *Adapted from "Quality Control in Safety and Risk Analysis," by J. Suokas and R. Veikko, April 1989,* Journal of Loss Prevention in Process Industry, 2, *pp. 67-77.*

Abstract: *While methods exist for identifying hazards, no single method or combination of methods can assuredly identify all hazards within a system. Despite this, the claim is often made that all hazards in a particular system have been found. To gauge the degree of thoroughness of a given method to identify hazards, one must know how many hazards actually exist. This implies that all hazards within the system must first be found, which creates an obvious logic conundrum: If there were a method for finding all hazards, then that absolute method would be used universally. Researchers in Finland have employed a practical approach to gauge thoroughness. It is reviewed here.*

Figure 2: The first step in assessing thoroughness is to note the number of hazards discovered by applying the hazard identification method undergoing evaluation as a primary technique. In this example, hazard and operability analysis is under evaluation.

Table 1

Results of Multiple Evaluations

Analytical technique	HIE[a]	Follow-on techniques[b]	System type
HAZOP	22%	Commissioning and early operation	Chemical process plant (system 1)
HAZOP	80%	Commissioning and early operation	Chemical process plant (system 2)
AEA	60%	Commissioning and early operation	Chemical process plant (system 1)
AEA	20%	Commissioning and early operation	Chemical process plant (system 2)
HAZOP	77%	AEA; WorkSafety analysis (cf, JSA/JHA); mishap investigation or mishap database	Gas release, two load-unload systems
HAZOP	36%	AEA; FMEA; MORT	Chemical process (7 plants)

Note. *Data compiled from "On the Problems and Future of Safety and Risk Analysis," by J. Suokas and R. Kakko, 1989,* Journal of Hazardous Materials, 21, *pp. 105-124, and "On the Reliability and Validity of Safety Analysis," by J. Suokas, 1985,* Technical Report Publications 25, *Espoo, Finland: Technical Research Center of Finland.*

[a]*Hazard identification effectiveness % =* $(H_e/H_s) \times 100$. [b]*Discussions of the techniques are found in* Lees' Loss Prevention in the Process Industries, *by S. Mannan, 2005, Burlington, MA: Elsevier Butterworth-Heinemann.*

Table 1: These results provide an opportunity to compare side-by-side the performance of the two techniques applied to the same systems.

discovery techniques, HAZOP and action error analysis (AEA), that were applied in 11 plant settings of assorted kinds. As shown, when applied singly, these two primary techniques found only 20% to 80% of the total number of hazards identified later when the methods being evaluated were augmented by other, dissimilar techniques.

The first four entries in Table 1 provide an interesting opportunity to compare side-by-side performance of the two techniques when applied to the same systems, identified here as System 1 and System 2. The performance comparison is more readily appreciated in Figure 3.

In the System 1 case, when used as the primary hazard identification method, HAZOP discovered 22% of the total number of hazards eventually identified. On that same basis, AEA discovered 60%, suggesting that it is a superior technique. This impression is reversed in the results from applying the techniques to System 2, where HAZOP finds 80% and AEA only 20%.

This is not an insignificant observation. Different system types lend themselves to different analytical methods and forcing a fit could arguably lead to the extreme range of findings noted. For an extreme example, use of the HAZOP technique on a biological system is unlikely to find as many hazards as, say, fault tree analysis. The skills, experience and preparedness of the analyst are unlikely to overcome the mismatch in technique and subject.

Conversely, the most appropriate technique is only as effective as the analyst using it. Prior experience conducting such analyses, and performing the necessary legwork to understand the system to be assessed, are crucial to achieving the desired outcome—identifying as many hazards as possible.

Figure 3

Effectiveness Comparisons

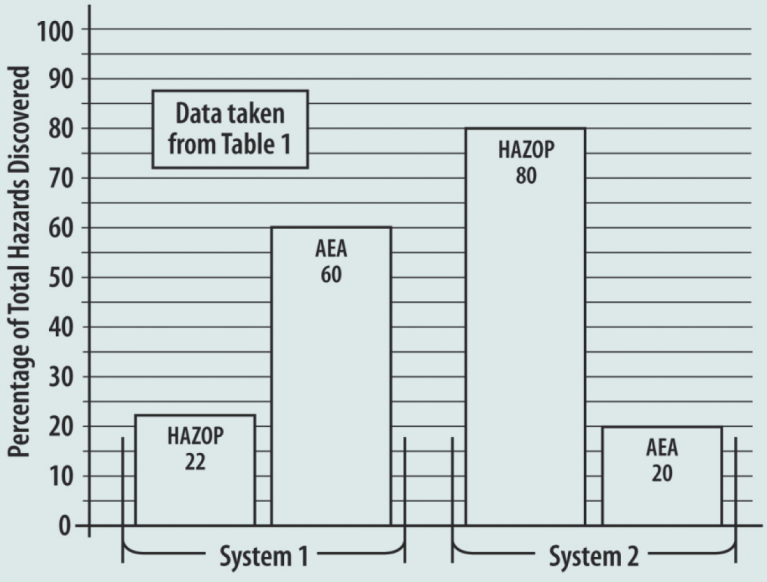


Figure 3: Different systems lend themselves to different analytical methods and forcing a fit could lead to an extreme range of findings.

Limitations: Insufficient Data?

This study of HIE can be faulted for having dealt with only a limited body of data. It must be recognized, however, that data of these kinds are rare in the open literature of system safety practice. Moreover, the database presented in Table 1 represents studies of analyses conducted in 11 plant facilities, not an insignificant population. Of greater concern is the fact that only two primary hazard search techniques are represented, HAZOP and AEA. That concern deserves consideration.

Those two techniques are quite different. Both are well described by Mannan (2005). HAZOP is carried out by a team of analysts who have special knowledge of the system. The team explores possible deviations from normal performance at each of several system operational nodes. Credible performance deviations that may lead to harm are recognized as hazards. Both equipment and human operators are considered as system elements.

AEA, less familiar to U.S. analysts, concentrates principally on hazards arising from human operator errors. The AEA analyst views intended system functions, moving the analysis from operational phase to operational phase, and considers the consequences of operator-system faults at each operating step within each phase. In doing so, the analyst also

Promoting Thoroughness

Several methods improve the thoroughness of hazard identification:

- Use of several complementary identification approaches.
- Use of more than one analyst.
- Special wariness of systems employing new technology or old technology in new ways, or change of operating environment.
- Developing a high degree of system savvy through:
  a) design studies;
  b) inspections and real or virtual operational walk-throughs;
  c) user/operator interviews;
  d) studies of mishap performance records of like systems.
- Being mindful that one never analyzes a system. Instead, one analyzes a conceptual model of a system. These must be made to match in all important aspects.

recognizes the additional threats from equipment faults that may coexist with operator errors.

Each technique may be taken as a valid representative of the various others that share its logic framework as to the manner of hazard discovery. On these arguments and with these explanations, it is posited that the methods and results reported have sufficient worth to support the conclusions drawn.

Improving the Practice: How Might We Do It Better?

In a discussion of this kind, and although it is not the principal purpose, it would be remiss not to mention methods known to be helpful at improving thoroughness in identifying system hazards. The sidebar below lists a selection of these. More information on achieving success in the search for hazards can be found in Ericson (2005).

What Have We Learned? What Does It Mean?

From the work described, several important conclusions can be drawn:

- Despite the best efforts of system safety practitioners, it remains true that no single technique exists for identifying system hazards capable of finding them all, and no method for verifying that it might have done so.
- An orderly, disciplined technique (e.g., HAZOP) may identify as much as 80% of all system hazards when applied by trained, knowledgeable, seasoned practitioners.
- That same technique may find fewer than 40% of all system hazards when used as the exclusive discovery method.
- It follows that to succeed, the analyst must select a primary technique that is appropriate for the system to be analyzed.
- As a corollary to that conclusion, it is apparent that supplementing the use of a primary hazard identification technique with the use of others based on differing search principles can significantly improve the effectiveness of hazard discovery.
- System safety practitioners would do well to avoid making declarations that they have discovered all system hazards and should disregard such statements made by others.
- The Finnish method, as described in the literature and encapsulated here, provides a well-defined, disciplined approach to evaluating and expressing the effectiveness of a hazard identification technique at discovering the hazards in a particular system type.
- The effectiveness expression is quantifiable and, when treated as such, will always be at least slightly optimistic.
- The degree of expressed optimism diminishes and a true value of effectiveness is approached as hazards are discovered by additional methods supplementing the one used as the principal technique undergoing evaluation. ■

References

Ericson, C. (2005). *Hazard analysis techniques for system safety.* New York: John Wiley and Sons.

Leveson, N. (1995). *Safeware: System safety and computers.* Reading, MA: Addison-Wesley.

Mannan, S. (Ed.). (2005). *Lees' loss prevention in the process industries.* Burlington, MA: Elsevier Butterworth-Heinemann.

Manuele, F. (2008). *Advanced safety management focusing on Z10 and serious injury prevention.* New York: John Wiley and Sons.

Suokas, J. (1985, Sept.). *On the reliability and validity of safety analysis* [Technical Report Publications 25]. Espoo, Finland: Technical Research Center of Finland.

Suokas, J. (1988). Evaluation of the quality of safety and risk analysis in the chemical industry. *Risk Analysis, 8*(4), 581-591.

Suokas, J. & Kakko, R. (1989). On the problems and future of safety and risk analysis. *Journal of Hazardous Materials, 21,* 105-124.

Suokas, J. & Pyy, P. (1988). *Evaluation of the validity of four hazard identification methods with event descriptions* [Research Reports 516]. Espoo, Finland: Technical Research Center of Finland.

Suokas, J. & Veikko, R. (1989, April). Quality control in safety and risk analysis. *Journal of Loss Prevention in Process Industry, 2, 67-77.*

Acknowledgments

The authors express their sincere gratitude to Dr. Jouko Suokas of the Technical Research Center of Finland for his generosity in sharing descriptions of his unique, pioneering work and its results.

Hazard Discovery Techniques: A Partial List

FMEA: Failure modes and effects analysis. A bottom-up technique that methodically explores the separate outcomes (effects) of failures of system elements in each of the failure modes available to it, seeking those having harmful outcomes.

FTA: Fault tree analysis. A top-down method using Boolean algebra and logic diagramming to model and analyze failure processes within systems. Hazards are discovered in exploring paths to predesignated loss events.

AEA: Action error analysis. Methodically analyzes interactions between machines and humans. Similar to FMEA, but with increased focus on steps in human procedures rather than viewing hardware exclusively.

HAZOP: Hazard and operability analysis. A methodology for identifying and dealing with potential loss events, especially in industrial processes, based on design of the system and its operation, potential failures and consequences of those failures.

MORT: Management oversight and risk tree analysis. Uses a predesigned logic/decision tree to explore systems and assess safety processes. Relies on inquiry and comparison methods. Developed by the U.S. Atomic Energy Commission.