

Compromises in the Pursuit of Safety

Negotiation and communication improve outcomes

By George A. Peters and Barbara J. Peters

RECENT DEVELOPMENTS in the practice of safety have provided a broad array of robust techniques and methods to minimize risk. The general approach may be to prevent human error [Peters and Peters(c)]. Another approach is by design safety analysis, as illustrated by the 22 most commonly used methodologies in system safety (Ericson). Books on occupational ergonomics [Peters and Peters(a)]; legal aspects of safety practice (Peters); warnings and instructions [Peters and Peters(e)]; vehicle safety [Peters and Peters(a)] and many allied disciplines contain information that SH&E practitioner could use in problem solving. In fact, a recent search of Amazon for current books returned 4,354 occupational safety titles and 2,705 safety engineering titles. The Library of Congress has more than 10,000 occupational safety and safety engineering book titles. Such a wealth of available resources suggests the current growth, maturity and potential of the safety discipline.

Teamwork

A broader scope and more productive role for the safety discipline is suggested by the ready availability of relevant information sources (content knowledge), the development of many different techniques and methodologies (tools of the trade), and the ever-growing expectations of others [Peters and Peters(b); USAF; GAO; Alexander]. It may be unrealistic in some situations to expect just one safety specialist to know everything and to act alone. Instead, the SH&E professional should be aware of what is available and be able to organize team efforts to effectively and efficiently use the available knowledge and skills. The SH&E professional should lead and engage those in subdisciplines and allied disciplines. Such team efforts require negotiating skills, an understanding of the acts of compromise and a comprehension of how others' skills can be best used to achieve a common goal.

The Safety Matrix

Problem solving for the SH&E professional involves much more than a quick fix with common-sense remedies. Many safety problems require three major considerations.

1) **Holistic assumptions.** Start with an overview of the general enterprise or operation. This may be necessary to establish appropriate goals, the level of effort to be expended, the possible consequences of an uncorrected safety problem and the available resources for suitable preventive actions.

2) **Develop applicable algorithms.** These include the sequences, patterns, steps or rules that describe a process which should solve normal problems. It is a probabilistic set of instructions as to what should occur. It is the relevant workflow path network in which the safety problem is embedded and influenced.

3) **Use targeted remedies.** Based on the focus achieved by holistic assumptions and applicable algorithms, the root cause of a safety problem may be precisely identified, remedies installed, follow-up initiated and possible side effects determined. The permanent effectiveness and cost of the remedies are important variables—that is, one must realize it involves more than the fact that some action was taken. Compromises in the pursuit of safety are clearly identified so that future remedial action can be undertaken.

Ambiguity & Residual Problems

For many years, a fairly universal end-all approach in safety was to include compliance with government regulations, trade standards, contract and code

George A. Peters is a licensed safety engineer, a psychologist and a lawyer. A former ASSE vice president, Peters has also been president of the System Safety Society, and is a former member of the BCSP and BCPE boards of directors. He is a Fellow of the American Association for the Advancement of Science, the Institution of Occupational Safety and Health, and the Human Factors and Ergonomics Society. Peters's articles have been published in many legal, medical and engineering journals.

Barbara J. Peters, J.D., specializes in solving SH&E-related legal and technical problems. She has taught at the university level, lectured worldwide and delivered presentations to groups such as the American Psychological Association, Georgia Institute of Technology, Human Factors and Ergonomics Society, System Safety Society, Cal/OSHA and ASSE. She is a Fellow of the Roscoe Pound Foundation. With her father, George A. Peters, she has authored/edited 41 books.

Being best in safety is rewarding. Being merely passable in safety often means predictive uncertainty, probable future surprises and the possibility of the need for corrective action in the future.

requirements, industry practice and relevant legal requirements [Peters; Peters and Peters(d)]. The goals may have been compliance, acceptable safety, tolerable risk, or appropriate warnings and instructions [Peters and Peters(e)].

Such ambiguous goals may not be sufficient in the perspective of the current broad array of available sophisticated analysis techniques and advanced methodologies. For example, determining what is acceptable or tolerable is subject to broad interpretation and variation. Compliance may not result in immediate desired results. Warnings may address only residual risk and as a result may be only partially effective.

A key objective for future safety efforts is to reduce the ambiguities (uncertainties) and residual risk (known statistical variance), particularly where compromises have been made in the pursuit of safety. To illustrate this problem, this article focuses on safety compromises made in the recent past. The emphasis is on design safety (system safety), but safety compromises are

common in all subdisciplines. The question is what to do about compromises in the pursuit of a high level of safety.

Safety Compromises

The system safety engineer may perform detailed design safety analyses, make appropriate risk assessments, and determine what constitutes effective alternative designs or remedies. This work may be very good, but it is incomplete unless action is taken to implement the recommendations. This generally requires negotiation—in the form of participating in formal design reviews, personally working with project engineers or managers to obtain desired changes, or convincing those specialists who control what appears on product engineering drawings, specifications and other relevant documents. The system safety recommendations may be initially accepted or rejected, modified or delayed, relegated to further research and study, or simply ignored.

Often, however, design compromises are made to accommodate everyone's opinion. A compromise may be a partial victory for each reviewer in a something-is-better-than-nothing philosophy. Initial compromises on high-risk hazards may motivate the system safety engineer to develop and refine the case to achieve a better compromise in subsequent negotiations. In any case, a core aspect of the product or system improvement process is the art of compromise.

Reliability & Authority

Some situations require compromise. For example, on an engineering drawing, a system safety specialist may observe the notation, "reliability 99.5%." Does this reflect a desirable goal, a minimum

requirement, something relating to a specific component test, an insertion copied from another drawing or specification sheet, or just an arbitrary number derived from a supplier's submission? What if it were just one component in a series (with a multiplicative reduction in system reliability), a part scheduled to be included in a product's lifetime warranty (perhaps 20 years or more with continuous self-test operation) and destined for large-scale production (at least 500,000 units per year)? Certainly, many questions could be asked, particularly if the component were to be part of a passive safety device, a critical safety assembly or a vital link in an active high-risk product.

If a knowledgeable engineer were the source of the reliability notation, would there be a friendly attempt to gain a further understanding while providing knowledge from the system safety perspective? Could such an inquiry result in some sort of a challenge and possible confrontation? Is it more likely to be a friendly accommodation and a compromise with a primary specialist on that topic? If the source was the project engineer, would a long explanation and strong recommendation ensue, or merely quick capitulation and deference (a compromise to an authority)? Negotiation for product improvement almost always involves personal ego and technical compromises, but the ultimate safety objective provides considerable leverage in obtaining desirable compromises.

New Systems & Integration

A recent publication discussed the design of automobile rear steering-by-wire (Alexander). It stated that in going through fault tree analysis "typically you have to look at the single failures from a DFMEA standpoint, but when you start dealing with these by-wire technologies, you have to look at interactions. You've got to protect yourself to multiple levels." This statement illustrates the fact that a more-detailed design safety analysis is required for new technologies such as electronic (by-wire) control of rear wheels, all four wheels, throttle, steering or stability systems.

System safety specialists have long known that their endeavors are particularly fruitful in the design of new systems, as well as where systems interact and integrate. More teamwork is evident when dealing with unknowns for the first time; more cooperativeness emerges between established disciplines when attempting to identify and resolve problems on equipment compatibility and effectiveness; more appreciation is given for information useful in achieving a common objective; and more understanding is provided of the need to proactively reduce predictable error variance (Peters). These are substantial factors in minimizing important adverse compromises on design safety.

Cost Controls

In one passenger automobile airbag system, an attempt was made to eliminate remote sensors (to reduce costs), along with their wiring harnesses and connectors (to further reduce costs and complexity). A

centralized integrated design seemed to meet cost/benefit requirements and its simplicity met customer cost reduction objectives (manufacturing, installation and servicing). However, the system controller (computer) had programmable discrimination algorithms that required either expensive testing or subjective extrapolation (gross estimation with a loss of sensitivity and accuracy). The resultant algorithms were based on minimal testing, past experience with other systems and "educated" extrapolations. It was a design compromise that favorably considered cost/benefit factors, but actually compromised (degraded) design safety in a final analysis of product performance. This was because continued cost controls minimized the testing actually needed, a predictable event by others in the chain of use of the system.

Information Sources

A company became aware of significant safety problems from comparative warranty summaries and other in-field sources. A special committee was created to discover the root cause of the problem. Two years passed, with vigorous committee activity and increasing management pressure, yet no specific cause was identified and validated.

At the end of 2 years, one member left the committee. Several months later, he found a book that described the problem and outlined remedies. Review of engineering drawings revealed ongoing dimensional, geometric and material changes made over the course of the 2 years. They were made without reference to, consideration of or knowledge about the root cause of the problem. The design had been compromised many times during the 2-year committee activity. No system safety analysis had been conducted, merely attempts to apply past experience as remembered by senior staff, key technicians and project engineers. Design compromises were speculative at best.

Technical books and reports are also often ignored. There seem to be cycles in which problems emerge, are studied and resolved, only to reappear in a cycle a decade or 2 later. Fortunately, the system safety engineer can be armed, either with information from company archives or with the vast amount of information available on the Internet.

Many external technical and research reports can be instructive and useful as well. Worldwide patents serve to identify problems and solutions. Trade standards may help but are not crutches. Chat rooms provide informal contact with peers. International conferences provide opportunities for informal technical discussions that may provide insight, concepts, methodology and information on new instrumentation and technical equipment, all without a loss of proprietary information or decline in company loyalty. These external sources of information have become increasingly valuable to design safety efforts.

Prototypes

Fabrication of parts with unconventional materials may present novel problems with design safety implications. Examples are carbon fiber (like that

used in structural members which can suffer damage in routine parts handling) and cable harnesses (with connectors to sensitive electronic assemblies that are inadvertently damaged during conventional installation procedures). Should system safety become more involved in manufacturing operations or, at least, preliminary (prototype) assembly and field operations testing? It would give full meaning and value to the word "system" in system safety [Peters and Peters(b)]. It could reduce problems in handling, installation and service. It could bring the lessons learned back home to engineering design and provide fodder for subsequent remedial changes and next-generation design improvements. More realistic design compromises can be made if system use is better understood [Peters and Peters(b); (d)].

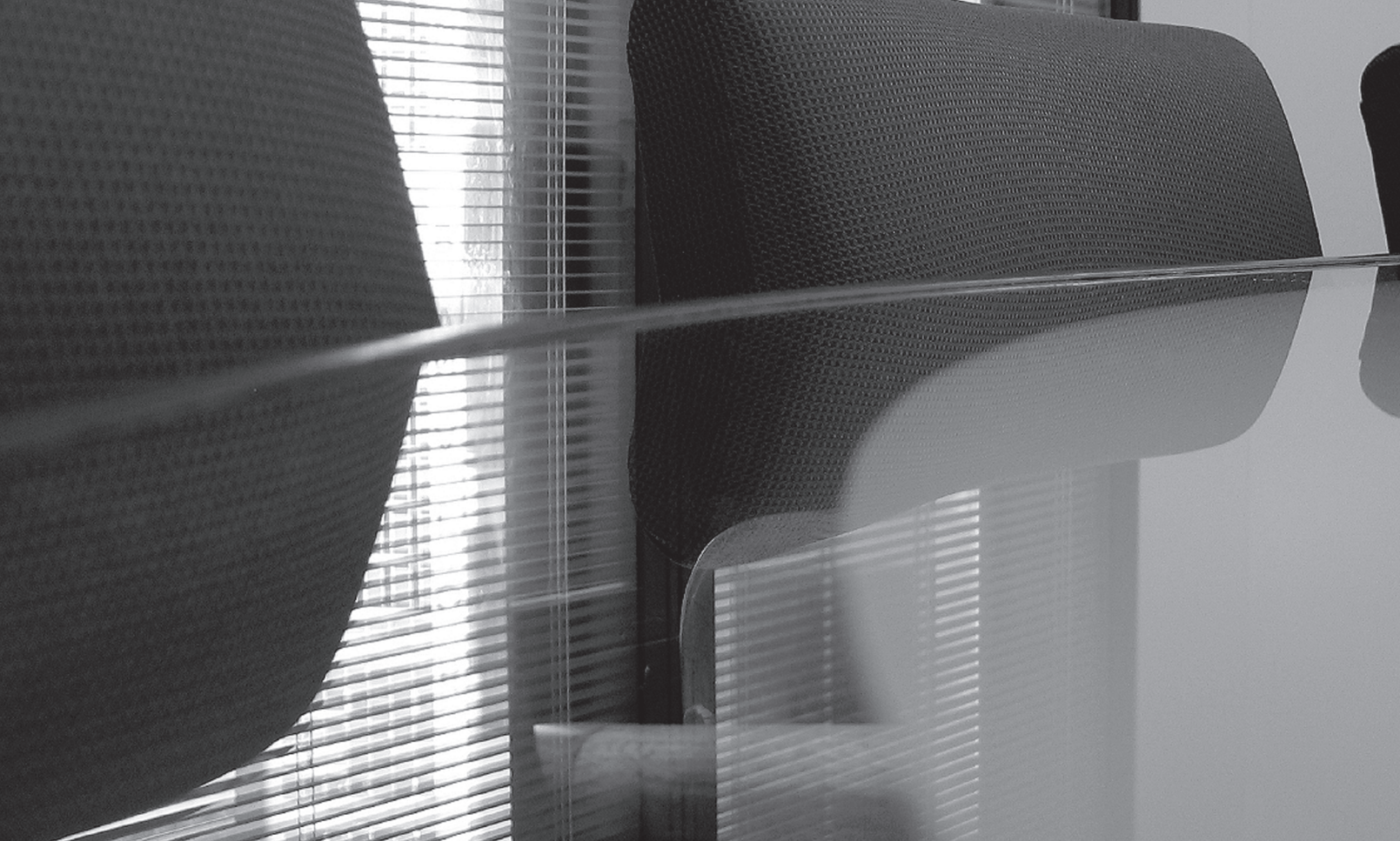
The Gateway

The negotiation of design safety improvements is the gateway to preventive action. When design decisions and approvals are made, the devil is often in the details. Thus, there should be informed design compromises with some consideration of the rule-set (legal context) of a largely globalized world. It may include overcoming resistant managerial obstacles, yet remaining a good team player. It may involve persistence when rejections are snap decisions, particularly in preemptive corrective actions including recall planning and execution. While the term "design safety" often operates, to some degree, as a broad license, it also carries with it an inherent defined responsibility and accountability. This requires adherence to ethical codes and self-protection [Peters and Peters(d); GAO]. Self-protection includes transparency so that when scapegoats, whistleblowers and covert actions are uncovered, the system safety activities will be found to have provided appropriate information to those ultimately responsible.

Most system safety specialists are well aware of the media coverage of events involving moral and ethical transgressions, regulatory violations, class action and product liability awards, and unsettling reports of serious personal injury, property damage, forced mergers and corporate bankruptcies. The system safety engineer may feel as if the crosshairs of responsibility and accountability are targeting safety endeavors.

If system safety recommendations are compromised during negotiations with other specialists and managers within the organization, what could be the result if a major safety problem became manifest a few years later? Typically, the system safety specialist's name and function do not appear on the design drawings and specifications (i.e., there is anonymity). Others within the organization make the design decisions, initiate and approve the compromises, and assume ultimate responsibility and accountability for the final (released) design.

As employees of a corporation, system safety specialists are usually given personal immunity. They generally must rely on data and information made available, in part, by others. Thus, these specialists are



subject to the personal perspectives, motivations, biases, objectives and other limitations of the ultimate decision makers. Therefore, compromise is both a fact of life in system safety and a means of shifting ultimate responsibility to others in the organization.

However, one must still conform to customary core practice (USAF), act prudently and responsibly [Peters and Peters(d)] and not ignore the obvious [Peters and Peters(b)]. The safety engineer is morally and ethically responsible for the proper performance of assigned duties regardless of opinions regarding possible anonymity, shifting of responsibility or the decisions of others.

Testing

In-field tests should include tests of warnings and instructions. Warnings are used for residual risks [Peters and Peters(e)], but are they effective enough? What residual risk remains after a warning is used? A design compromise to use a warning—rather than altering a component—may be good or bad depending on the effectiveness of the warning. Without testing, what residual risk remains in any design change?

Testing should yield results that can be used to prepare a design checklist which could be used in fault tree analysis, design review sessions and design audits. It could be bolstered by a review of historical company documents. Such information could be the basis of better-informed design compromises. It may be the data that tilt the balance or produce a small gain (rather than settling for less) when negotiating a design improvement related to personal and property damage. Testing helps to remove uncertainty [Peters; Peters and Peters(a)].

Testing is crucial in human error reduction and control. It provides an objective basis for design

decisions. However, some system safety engineers ignore the human factors aspects of a system by assuming that this is largely an uncontrollable user problem. Others may not share that belief.

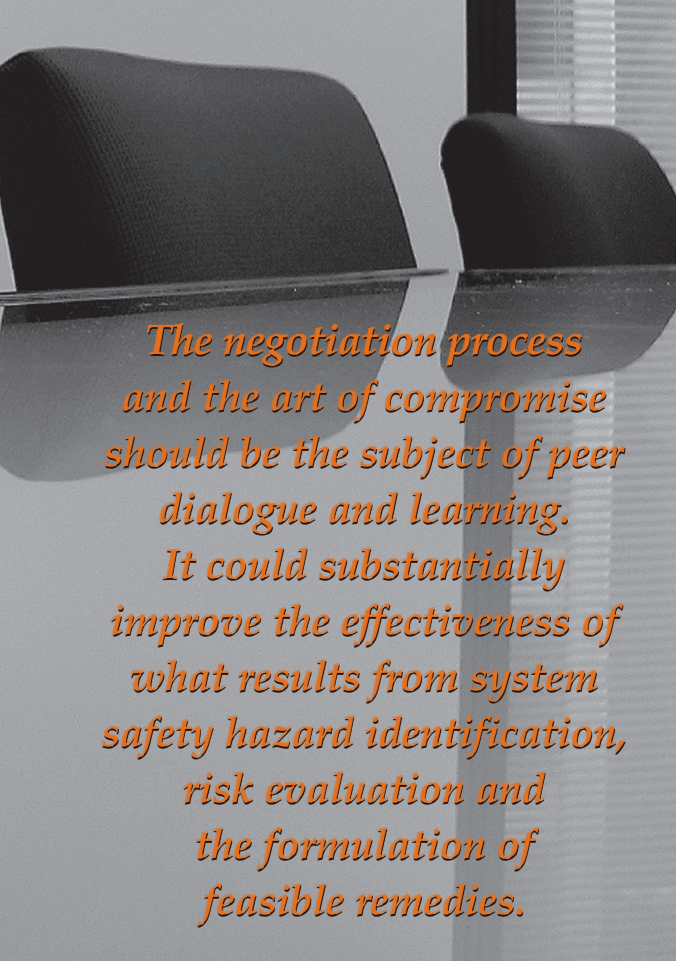
For example, a driver may become inattentive, drowsy and distracted and be drifting out of a lane on a crowded highway. What can be done in design about such a vehicle user problem? One vehicle manufacturer now has a lane departure warning system to alert the driver via an instrument panel warning light and an audible warning buzzer if the vehicle is about to move out of its lane. It senses lane markings, distance and lateral velocity at speeds above 45 mph. Human error should not always be considered intractable or ungovernable.

Tolerance for risk is in the eye of the beholder and may be quite different as perceived or understood by the producer as opposed to the target (user). Testing may help to establish the risk tolerance boundaries for those involved with the system. Appropriate testing should help to define what constitutes a reasonable compromise under the circumstances.

Conclusion

1) Safety compromises are customary even when dealing with important safety issues. The clarity of expressed logic, the abundance of relevant information and a demonstrable personal value system all tend to prevail at critical decision points in the design process. Compromises are to be expected and can be potentially good, ineffectual or adverse to safety objectives.

2) The degree and character of past and current compromises generates a personal reputation. The peer acceptance of recommended design changes or actions depends on the imputed credibility of the person making the recommendations, as well as the



The negotiation process and the art of compromise should be the subject of peer dialogue and learning. It could substantially improve the effectiveness of what results from system safety hazard identification, risk evaluation and the formulation of feasible remedies.

apparent significance of the foundational facts and the perceived consequences. Personalities can prevail over poorly presented analytical logic.

3) Inappropriate safety compromises may lead to hidden or latent problems that are time-delayed in their manifestations. Safety problems are created; they are not an undiscoverable, inevitable, unpreventable or a necessary trial-and-error impediment to progress. System safety should be an objective search for all potential problems past, present and future.

4) Safety compromises made to serve one narrow (domestic) market may not be acceptable in other major markets and could lead to unexpected problems. Compromises should be made keeping in mind the utility of international standards, the general aspirations for world-class products, the predictable human cultural user differences, and successive or remote customer satisfaction. Being best in safety is rewarding. Being merely passable in safety often means predictive uncertainty, probable future surprises and the possibility of the need for corrective action in the future. Design to exceed, rather than rely on good luck, regulatory exceptions or future evasive maneuvers.

5) Safety compromises should be modified by moral, ethical and liability considerations. These societal principles have been long standing, enforcement often faltering and future penalties uncertain. Corporate and personal risk may be manageable, even in a world trade context, by informed specialists able to use appropriate guidelines and safeguards.

6) The quality of compromises can be improved by accessing available information sources. External data can enrich the process, particularly when in-house data are scarce or unreliable. Books, patents and supplier representations are often underused as well.

7) As with all aspects of system safety, opinions differ considerably as to the application of specific basic system safety techniques (tools) to varied situations, demands, objectives, needs and available resources. Legitimate arguments may arise with respect to risk assessments or the scope of system safety. Not all industries are alike organizationally, in acceptable practice or in what may be considered reasonable in design compromises. Contractual, technical, political or societal constraints or requirements may exist as well. In essence, what might be a good (appropriate) compromise in one context may be a bad (inadequate) compromise in another. In other words, one should expect some diversity in applying system safety theory, practice, tools, evaluation criteria and procedures in various organizational interrelationships. Negotiated design compromise may be a relative, conditional, creative, interpersonal, tolerant and persistent affair. It may be direct or result from alternative creative means.

8) Design compromises are at the heart of the communication process essential to implementation of most system safety recommendations. Therefore, the negotiation process and the art of compromise should be the subject of considerable peer dialogue and learning among system safety specialists. It could substantially improve the effectiveness of what results from system safety hazard identification, risk evaluation and the formulation of feasible remedies. It could be a key aspect of future professional growth and the enhancement of the discipline. ■

References

- Alexander, D. "Chassis Integration." *Automotive Engineering International*. May 2004: 54-58.
- Center for Chemical Process Safety. *Inherently Safer Chemical Process: A Life Cycle Approach*. New York: American Institute of Chemical Engineers, Center for Chemical Process Safety, 1996.
- Ericson, C.A. *Hazard Analysis Techniques for System Safety*. Hoboken, NJ: John Wiley & Sons, 2005.
- Peters, G.A. "Product Liability and Safety." In *The CRC Handbook of Mechanical Engineering*, 2nd ed., F. Kreith and D.Y. Goswami, eds. Boca Raton, FL: CRC Press, 2005. 20-11 to 20-15.
- Peters, G.A. and B.J. Peters(a). *Automotive Vehicle Safety*. New York: Taylor & Francis, 2002.
- Peters, G.A. and B.J. Peters(b). "The Expanding Scope of System Safety." *Journal of System Safety*. 38(2002): 12-16.
- Peters, G.A. and B.J. Peters(c). *Human Error: Causes and Control*. Boca Raton, FL: CRC Press, 2005.
- Peters, G.A. and B.J. Peters(d). "Legal Issues in Occupational Ergonomics." In *Fundamentals & Assessment Tools for Occupational Ergonomics*, W. Karwowski and W.S. Marras, eds. Boca Raton, FL: CRC Press, 2005. 3-1 to 3-17.
- Peters, G.A. and B.J. Peters(e). *Warnings, Instructions and Technical Communications*. Tucson, AZ: L&J Publishing Co., 1999.
- U.S. Air Force (USAF). "Safety Engineering of Systems and Associated Systems, and Equipment, General Requirements for Military Specification MIL-S-38130" (Preceded MIL-STD-882D, Standard Practice for System Safety, 2000). Washington, DC: U.S. Department of Defense, Sept. 30, 1963.
- U.S. Government Printing Office (GAO). *Trials of War Criminals Before the Military Tribunals Under Control Council Law. No. 10, Vol. 2, Oct. 1946-April 1949*. Washington, DC: U.S. Government Printing Office, 1947. 181-183 (The Nuremberg Code).

Acknowledgement

This article was adapted in part from the article, "Design Safety Compromises," which appeared in the Nov./Dec. 2004 issue of the *Journal of System Safety*.