Social Controls for Reducing Risk

Observations on U.S. & European approaches

By Bruce W. Main

Abstract: *In 2006, a group of safety specialists and designers gathered in Europe to discuss safety by design—primarily how to incorporate safety concerns early in the design process. This article examines some of the key ideas from the workshop.*

IN 2006, A GROUP OF SAFETY SPECIALISTS and designers gathered in Europe to discuss safety by design—primarily how to incorporate safety concerns early in the design process. The papers of the workshop appear in the journal *Safety Science,* available online at www.sciencedirect.com/science/journal/09257535. Although the papers address many similar themes by U.S. researchers on the same topic, the ideas presented provide a unique window to viewing the differences between the European Union (EU) and the U.S. on social controls to reduce risk.

Views on Acceptable Risk

A primary difference between the EU and U.S. pertains to achieving acceptable risk. In the EU, safety requirements in standards are considered upper-level requirements that define acceptable risk. The 2006 EU Machinery Directive specifies a presumption of conformance: "Machinery manufactured in conformity with a harmonized standard . . . shall be presumed to comply with the essential health and safety requirements covered by such a harmonized standard" (European Parliament & EU, 2006, Article 7.2).

Therefore, compliance with an EU regulation or European (EN) standard carries a presumption of acceptable risk. In the U.S., compliance with a government regulation or industry standard tends to be considered a minimum performance level and only one factor in attaining acceptable risk. Thus, compliance with a standard or regulation may or may not achieve acceptable risk depending on the market.

Standards and regulations trail the state of the art. Unless the state of the art is mature and relatively static, standards and regulations are rarely current for long. In dynamic situations where technology changes (such as with electronic control systems), standards and regulations may greatly trail the state of the art. Therefore, a compliance approach will not represent the state of the art and may not achieve a risk level as low as reasonably practicable. At the least, a compliance approach may not be applicable or provide good solutions in new product or process applications, and these are the most likely to need safety-through-design guidance to achieve acceptable risk.

In some ways the many differences between the EU and U.S. call into question the concept of an international standard with a single set of requirements. Should the U.S. and EU go their separate ways and maintain unique regulations and standards applicable to their respective regions? The question is moot. The pressure from industry to obtain harmonized international requirements is unrelenting (Manuele, 2005). Global companies cannot and will not support product lines, equipment or operations that are subject to separate standards.

Safety practitioners and design engineers cannot change these systems of social control—they must work within them. Thus, understanding the reasons for each approach may help manufacturers and safety practitioners to develop better machinery, products and systems; and standards writers to develop better harmonized standards. Equipment suppliers in one region that sell into the other region need to be aware of these differences and the implications on how to include safety in the designs. Understanding the differences in social controls to limit risk is important in developing and using international standards. Knowing the differences may help engineers and safety practitioners minimize frustration, protect manufacturers from product liability difficulties, and (literally) keep their managers out of European jails.

Social Controls for Reducing Risk

Perhaps the most enlightening idea in the workshop papers comes from Baram (2006), who examines the different social controls for reducing risk. Baram is affiliated with the Boston University School of Law but he clearly favors the EU approach to regulating safety. Baram examines four different social controls for reducing risk:

1) the marketplace;
2) self-regulation;
3) government regulation;
4) tort law.

He quickly dismisses the marketplace as inadequate for promoting safety because "market forces have proven to be an insufficient means of promoting safety for many reasons, and this has caused greater reliance on regulations." Similarly in the U.S., *caveat emptor*—let the buyer beware—is a marketplace method that

Bruce W. Main, P.E., CSP, *is president of design safety engineering inc., chair of the ANSI B11.TR7 Committee and the ASSE representative to the B11 Accredited Standards Committee. He is a professional member of ASSE's Greater Detroit Chapter and a member of the Society's Engineering Practice Specialty.*

Standards and regulations trail the state of the art. Unless the state of the art is mature and relatively static, standards and regulations are rarely current for long. In dynamic situations where technology changes, standards may greatly trail the state of the art. Therefore, a compliance approach will not represent the state of the art and may not achieve a risk level as low as reasonably practicable.

has largely been found insufficient in terms of ensuring safety concerns.

Baram (2006) also dismisses—rather harshly—self-regulation (voluntary standards) as an effective means. For example:

> Self-regulation: The self-regulatory approach to industrial safety is a particularly strong and reliable tradition in Germany where trusted industrial and engineering organizations . . . develop standards and procedures, some of which are later adopted by government regulatory programs. . . . However, the credibility of self-regulation is quickly diminished when harms occur, and is mistrusted by many because of its potential for bias, lack of transparency and inadequate self-enforcement, as in the U.S.

Self-regulation suffers somewhat from a long-standing public relations hangover. Baram correctly notes that industry standards are often "driven by corporate and professional associations which strive to avoid government regulation." Coupled with this position is the impression that years ago some industry standards were allegedly created in back rooms by industry fiat primarily to protect industry interests. As a result, the self-regulatory approach of voluntary consensus industry standards became viewed as ineffective in protecting users from harm. This impression lingers even though most self-regulatory standards secretariats comply with the ANSI requirements establishing the principles of balance, transparency, consensus and due process.

Concerning tort law, a major thesis of Baram's paper focuses on critiquing:

> the common assumption that fear of tort liability causes companies to emphasize safety and minimize risk in designing and developing a new product or process . . . the fear is real but the influence is highly variable because tort liability is merely one of many factors considered in company decision processes.

Because of this high variability, Baram largely dismisses tort law as an effective social control to reduce risk. Instead, he favors government regulation, which he states is "the most visible system of social control." The following excerpts are representative of his position.

> Government regulation has become the dominant approach for reducing the risks posed by industrial *processes* which discharge pollutants. . . . Regulation to make *products* safe is also prevalent in developed nations, and is particularly comprehensive for medical, food, automotive and chemical products. Most other types of products are not regulated in the U.S. But in the EU, enactment of the Machinery Directive in 1998 provided a coherent mandate for regulating an expanding universe of products. . . . The standards address essential health and safety aspects of a product's design and fabrication, and prescribe methods of hazard analysis and risk assessment for the manufacturers to follow (emphasis in original).

> Since regulations are enforceable, and noncompliance is a *violation of law,* it is clear that companies must be attentive to existing and pending regulations that have direct and indirect implications for the design of their products and processes (emphasis added).

As a violation of law, a potential consequence of nonconformance is that the company representative who signs the Declaration of Conformance could go to jail if the product or machine is found not to comply with the essential safety and health requirements.

Baram's viewpoint was neither isolated at the workshop nor was it unanimous. In general, the workshop attendees showed a large faith in regulations rather than other means to address safety. Hale, Kirwan and Kjellen (2006) seem to conclude that regulations are a primary answer to improving safety through design. Thus, the stage would appear to be set for self-regulation versus government regulation as the most effective social control for reducing risk.

Alternate Views

Focus on Injury Prevention

A contrary view to government regulation has been expressed by Gary Kopps, manager of occupational safety and health at Deere & Co., a worldwide manufacturer of agricultural equipment and consumer products. Kopps indicates that Deere switched its focus to compliance efforts in the 1970s when OSHA regulations first came into effect in the U.S. (G. Kopps, personal communication, 2006). With this new focus, the company found that its occupational injury rates went up rather than down. The focus on regulatory compliance distracted the company from preventing occupational injuries. When the company realized that it had to focus on motivating engineers, employees and managers about accident prevention in addition to complying with regulations, the occupational injury rates started to trend downward again. Today, the company has exemplar statistics on lost worktime and is considered a leader in minimizing occupational injuries.

The Machinery Directive

The most recent version of the European Machinery Directive 2006/42/EC embraces the non-

binding status of standards, which would seem to support the self-regulatory approach.

> To help manufacturers prove conformity to these essential requirements and to allow inspection of conformity to the essential requirements, it is desireable to have standards that are harmonized at community level for the prevention of risks arising out of the design and construction of machinery. *These standards are drawn up by private-law bodies and should retain their non-binding status* (emphasis added) (European Parliament & EU, 2006, Preamble, 18).

Although the government regulatory aspect of the directive is mandatory, the actual conformance with the requirements is self-regulatory. In most cases, the application of the CE mark—a label indicating that the machine meets the applicable safety and health requirements—is a manufacturer self-certification. The presumption of compliance means that the only time most machines built in the EU are subject to a compliance evaluation is in the event of harm. Conversely, most machines built outside the EU are subject to compliance verification when entering the EU.

Indirect Effects

Baram (2006) also recognizes that regulation has important indirect effects on product and process design, including the ability to attract investment, affordability of insurance coverage and others. A similar effect occurs from self-regulation through industry standards in the U.S. Engineers and management often require compliance with industry standards as a condition for releasing a design to manufacture and ultimately the marketplace. U.S. companies have modified their product designs because they were unable to obtain product liability insurance. Complying with industry standards was one of the changes made to obtain such insurance.

These are four data points: Baram's views on self-regulation, Deere & Co.'s experience with focusing on compliance, the 2006 Machinery Directive's support of self-regulation and the indirect impacts of industry standards on design safety. Additional data would be useful in examining the different methods of social control to reducing risk and in preventing injuries.

Other Workshop Ideas

Standards Limiting Designer Responsibility

The workshop also examined how standards may limit perceived designer responsibilities. Several authors expressed concern about many designers relying solely on codified safety standards (Hale, et al., 2006). Because designers face severe time and cost pressures, they may be discouraged from seeking a deeper understanding of the safety implications of their designs, or looking for methods to reduce risks beyond that which is required by the safety standards. Hale, et al. (2006) note that:

> Fadier and De la Garza showed that designers place a great reliance on these standards as measuring sticks to judge their design, but also as a way of limiting their responsibility. If something is not in the standard, then they claim not to need to consider it. . . . [Standards] may lull the designer into a sense of false security. They may be substitutes for thinking about use situations and their challenge to design, instead of a stimulus to do so.

More specifically, Jagtman and Hale (2006) state that "the designers may pass the responsibility for covering all plausible scenarios on to the authority that formulated the standards." While Hale, et al. (2006) recognize this issue, they try to minimize its significance via a complex, yet unconvincing discussion. Jagtman and Hale make a good point and this issue is significant. In today's competitive environment, nearly everyone involved in process and product design has more than enough to do. Although often phrased in many different ways, a common question is "What do I have to do?" Product designers, safety practitioners, engineers and managers seek a clear answer to this question so that they can meet the necessary objective and move on to the next requirement. A requirement that is vague, complicated or requires interpretation is often quickly passed over. Given this reality, regulations and industry standards need to be written in clear performance language that users can easily apply. Where explicit requirements cannot be written, clear processes need to be prescribed that will allow users to obtain reasonable solutions.

Examples of this approach can be found in North American industry standards such as robotics (ANSI/RIA R15.06 and CSA Z434), packaging machinery (ANSI/PMMI B155.1) and machine tools (ANSI B11 GSR). For example, the B155.1 committee wrote a standard that packaging machinery builders could use to "build to one standard, ship anywhere." The intent was to simplify the standards compliance process by making both the requirements and the process clear. Readers of the standard know what they needed to do and how to accomplish it. Subsequently, the U.S. machine tool industry has followed this approach within its B11 series of ANSI standards.

Learning vs. Bureaucracy

A natural tension exists between a standardized system structured to prevent errors for which solutions are known and a more dynamic learning approach that encourages new solutions to existing problems or application of existing systems in new ways. Jagtman and Hale (2006) present a telling observation of the design process. They describe a bureaucratic strategy in which designers use standards or guidelines that are imposed on the manufacturer/designer and that they must follow. The authors also identify an alternate proactive strategy that does not rely on regulatory standards but instead "seeks to learn throughout the design process . . . about all plausible safety problems and to decide upon preventing or controlling these problems while the system is still under design." They note that:

> The use of the bureaucratic strategy, with detailed standards, ensures that people design

according to current knowledge. This is not likely to lead to problems for established and well-known technologies, but does not provide a viable way to cope with safety issues that are currently unforeseen.

Thus, bureaucratic regulations may be less effective than a more proactive learning strategy. This is partly why private industry strongly prefers nongovernment solutions.

After-Market Safety

Baram (2006) also discusses the design process and suggests that an after-market safety approach occurs. He presents a three-phase cycle for designs: 1) premarket or development; 2) market; and 3) maturing market.

Baram presents a theoretical process in which safety is duly considered in each of the three development phases of a new product or process. In particular, efforts are made to identify and eliminate hazardous features in the first phase, safe use procedures are developed for the second phase, and an ongoing effort to monitor and address any further risks occurs in the third phase. In this theoretical process, most safety work occurs premarket and just before the design is released for sale or use. The maturing market phase is mostly a follow-up or monitoring task.

Baram also states that the theoretical process usually differs from what occurs in practice. Baram uses the term "progressive approach to risk reduction" to indicate that risk is reduced as the design progresses through the three phases.

> In practice, premarket efforts to eliminate risk are usually incomplete because of cost and considerable uncertainty about hazardous features, especially if the technology is new and complex. . . . Another reason is that most corporate attention at that time is usually given to [ensuring] that the product or process will work as intended. . . . Thus, the market phase, when such advances are put to actual use, provides the opportunity for identifying residual risks and for subsequently taking remedial action, such as design or operational change, that will eliminate the residual risks or at least reduce them to a level which is acceptable.
>
> This process of progressive risk reduction encourages rapid entry of technological advances into commerce, but is problematic in several respects. It allows companies to do less about identifying and eliminating foreseeable risks when designing the advances in the premarket stage, *unless required by regulation* . . . and induces them to wait for harmful consequences to accrue in the market phase . . . the progressive approach to risk reduction often leads to product recalls, process shutdowns, liabilities and other business losses until companies subsequently make costly design changes or take other remedial actions (emphasis added).

This view states that products are released to the market to see whether they work and subsequent safety efforts fix problems that may arise unless regulations prohibit doing so. This explicitly indicates that postrelease activities include ongoing risk reduction or that the user of the product or process design must be actively involved in ongoing risk reduction efforts.

The "progressive approach to risk reduction" seems a non-U.S. view. Although this approach might work for a process design where the supplier has frequent interaction and responsibility for system performance, it is not clear how this concept might apply to product manufacturing where the supplier and user have little communication or lack an ongoing relationship. For ongoing risk reduction to occur with product designs, the user would have to continue risk reduction after the product left the supplier.

In the U.S., a company manufacturing a product or machine that explicitly followed this approach would likely be severely punished in a negligence lawsuit if an injury occurred. The situation Baram proposes would place a company at risk of significant punitive and exemplary damage awards. The concept of punitive damage awards was developed to explicitly punish manufacturers that demonstrate a careless disregard for their product users. Suppliers using the "progressive approach" would seem likely candidates for punitive damages. By waiting for hazards to appear through trial and error, the designer and safety practitioner would not be meeting their professional responsibilities. This approach more clearly resembles a marketplace, *caveat emptor* approach, and is not considered acceptable in the U.S., as demonstrated in the courts of law.

In terms of the workplace, putting a process into production, then fixing it to reduce risk to an acceptable level places workers at risk. This may occur in the context of a work cell design or manufacturing line where the user must sign off before acceptance, particularly where hazards require fixes from unanticipated situations for the system as installed or when debugging or system shakedown occurs.

However, reactive and retrofit solutions to reducing risk are not safety by design, the primary focus of the workshop. The progressive approach to achieving acceptable risk emphasizes a retrofit approach to safety—fixing problems in the field after they have occurred rather than identifying and preventing them during design. This strategy increases risk of injury and liability, and introduces considerable waste of retrofit and rework into the design process (see ANSI B11.TR7).

Perhaps more troubling is that Baram's observation on the practice of the progressive approach to risk reduction apparently occurs in the EU even where regulations exist under the Machinery Directive. This suggests that complying with the regulations is likely a design criterion to be addressed by engineers during the design effort. In the U.S. the self-regulatory standards serve a similar design criterion role. Apparently noncompliance occurs in both markets.

Company Decision Making

Company decision making is another factor to consider (Baram, 2006):

> A company may choose the less expensive path of adding additional warnings and instructions to a product or process rather than change its design, because liability law fails to provide clear guidance on this matter.

Baram recognizes that deliberations on safety involve technical, economic and legal considerations. However, he contends that the outcome of the deliberations does not ensure that greater attention to safety will occur in designing products or processes.

> In other words, design change is often no more than one of many options for addressing the company's main goal of minimizing economic loss. . . . As a result, dangerous products may continue to be sold without design change despite numerous lawsuits, and dangerous processes may continue operation without design change despite accidents and liability awards, until regulatory action is taken, or liability and other losses become overwhelming, or the marketplace or public outrage forces the company to respond with a safer design. *Thus the hypothesis that tort liability promotes safer design needs to be replaced with the more hesitant hypothesis that it promotes company deliberations about mitigating loss which may, under certain circumstances, lead to design of a safer product or process* (emphasis added).

Decisions about safety and residual risk are usually more complex than this. Often, products are sold with warnings because there are few other options to further reduce risk. The designers of many products, machines and systems must rely on users to follow safe procedures in use. In many cases, suppliers cannot reasonably eliminate the need for safe procedures through design changes. For example, there are many situations that appear on the warning label of an extension ladder that cannot be addressed by design changes.

Findings Similar to Others

EU-Centric Focus

Notably, none of the workshop authors reference efforts and advances made in other countries. Some of the questions addressed during this workshop are similar to those studied by several efforts in the U.S. such as the Institute for Safety Through Design (ISTD) (an initiative by the National Safety Council from 1996 to 2006), Prevention Through Design (a project sponsored by Centers for Disease Control and Prevention and NIOSH) and others. Considerable research and progress has been made in the U.S., Canada, Australia and elsewhere concerning safety by design, yet this work was not recognized at this workshop.

Several conclusions of the workshop appear to confirm those of ISTD and others (Hale, et al., 2006). For example:

> A common factor in accidents is the breakdown of a design when used outside its defined limits (Hammer, 1993; Manuele, 2003; Main, 2004).
>
> All this leads to the requirement that the design process should be explicit and transparent about its assumptions concerning situations of use. They need to be written down and, if necessary, updated based on user feedback and accident experience (Manuele 2003; Manuele & Christensen, 1999; ANSI B11.TR3).
>
> Underlying much of the discussion at the workshop, and reflected in the papers, is the question of the allocation of responsibility to ensure that safety becomes integrated in the design process (Manuele & Christensen, 1999; Manuele, 2001, 2003; ANSI/PMMI B155.1; ANSI RIA R15.06).
>
> It is clear from the papers in this special issue that the designer's inability to foresee the great variety of influences in the user environment is the cause of a significant number of safety problems which otherwise could be solved in the design stage (ANSI B11.TR3; Main, 2004; Manuele, 2003).

In the workplace, putting a process into production, then fixing it to reduce risk to an acceptable level places workers at risk. Reactive and retrofit solutions to reducing risk are not safety by design. Such strategies increase risk of injury and liability, and introduce considerable waste into the design process.

This last finding in particular has given rise in the U.S. to the task-based approach to risk assessment, which is discussed shortly.

Specific Requirement or a Process

When writing standards, technical experts gather to address safety concerns that have arisen through various means. The writers need sufficient technical expertise to address the issues and render requirements that in their technical judgment achieve a risk level that is acceptable in society. The standards writers develop specifications or performance requirements thereby making decisions on acceptable risk. Engineers are then expected to develop designs that meet the specifications. This process is intended to limit designer flexibility because not complying with the requirements can lead to safety problems.

Recent U.S. efforts have focused on writing standards that provide a *process* by which companies/designers can achieve an acceptable outcome for any application that falls within the scope of the standard (e.g., ANSI/RIA R15.06, ANSI/PMMI B155.1, and ANSI B11.GSR). Thus, the diversity of applications requires flexibility in the regulations or standards; in some cases, U.S. companies prefer process standards that provide such flexibility over inflexible requirements that cannot be adapted to situations not considered by the standard or its writers.

Recent U.S. efforts have focused on writing standards that provide a process by which companies/designers can achieve an acceptable outcome for any application that falls within the scope of the standard. The flexibility allows companies to develop specific solutions that may not meet a specification, yet achieve acceptable risk.

The flexibility allows companies to develop specific solutions that may not meet a specification, yet achieve acceptable risk through new solutions. The design must be defendable in a court of law because the noncompliance would certainly be discussed in the event of an injury. With the requirements that risk assessments be documented, reaching defendable decisions concerning risk become increasingly important.

ANSI/PMMI B155.1 and ANSI B11.GSR are performance standards that contain process requirements. Designers and users of packaging machinery and machine tools are expected to achieve acceptable risk by following the risk assessment process described in these consensus (self-regulatory) standards. Several findings from the workshop are already written into these standards including:

- more specific responsibilities of suppliers and users;
- documenting risk assessment and information for use;
- use of existing standards.

These standards also allow new technological solutions within the concept of acceptable risk. That is, new technology can be used or new applications of existing technology can be applied as long as an acceptable level of risk is obtained. If a company can demonstrate that acceptable risk is achieved, the new solutions will comply with these standards.

In the EU, designers seem to want a specific design requirement against which a decision can be made without requiring a risk assessment for the specific application. EU designers seem to want the regulation or standards writers to work through the risk assessment process and provide the answer for acceptable risk in the regulation. Thus, a *process* standard may not be well received in the EU.

Operational Input to Design

Hale, et al. (2006) state that "the single most important issue in improving the design process from a safety point of view is how to ensure operational input." They also conclude that as a means to achieve operational input "*communication between [the designer and user] needs to be mandated*" (emphasis added). Although they allow that such communication will necessarily vary per activity, industry or technology, the suggestion that communications need to be mandated is befuddling. As a general principle, increased communication between the designer and user is a very good concept. But the logistic details of how, when and what communication must occur is a fatal flaw to such a proposed mandate.

Some workshop participants supported training as a solution to increasing safety by design. Hale, et al. (2006) state that one task in supporting the process is to help minimize error making by providing training and information to designers, and by providing them with design tools to avoid errors. A second task is to enhance error detection and correction by "formalizing the milestones at which safety checks are carried out and providing the tools to conduct those checks."

Fadier and De la Garza (2006) indicate that designers need to know more about how people use the designs. They suggest that:

> A safety training for the design actors seems essential, so that they understand how operators are likely to use their products and what risks that produces.

But simply training designers in safety methods is not the answer, nor is training safety practitioners in the design process (Main & Ward, 1992). If the solution were that simple it would have occurred long ago. More complicated questions being studied by U.S. researchers are "What specific skills do design engineers and safety practitioners need to incorporate safety through design?" and "What should designers do to ensure that safety is appropriately considered?"

Some U.S. standards writers have addressed the operational problem through the task-based approach to risk assessment. Originally pioneered by the General Motors Corp., this approach to identifying hazards was first written into ANSI/RIA R15.06:1999 and ANSI B11.TR3:2000. Since 2000, it has migrated to several other standards including ANSI/PMMI B155.1, ANSI B11.GSR and the entire B11 family of standards.

The advantage of the task-based approach is that it requires communication between the user and the designer. Often the safety practitioner helps facilitate this communication. The discussion focuses on how users interact with the product, machine or system, and what hazards can result from these interactions. This approach helps identify more hazards than other methods, which is why it has been increasingly adopted in U.S. standards.

By understanding the tasks individuals perform with products and processes, designers are better able to identify hazards and reduce risks to an acceptable level, often with productivity gains as well. Thus, the earlier conclusion of the workshop is valid in terms of its intent. In this regard, the workshop could have greatly benefited from examining the progress made in the U.S.

The Problem of Keeping Up With Standards

Fadier and De la Garza (2006) identify a key problem faced by those concerned with standards.

> The increasing number of standards and the difficulties that users, and even the standards

writers, experience in mastering the resulting complexity make it difficult to apply this approach.

Keeping current with standards as they evolve is a challenge for everyone. Unfortunately, this problem presents a significant challenge to designers intent on complying with current regulations, standards and state-of-the-art knowledge. This challenge is not addressed by the overall regulatory approach seemingly advocated at the workshop.

Hale, et al. (2006) recognize the problem of keeping standards current:

> We need processes that ensure timely update of design standards. This is not feasible for industry standards that undergo extensive and bureaucratic revision processes. Rather, the individual design house or customer must develop internal design standards as a complement to the industry standards that are possible to keep updated with the most recent user experiences.

A company-specific approach to developing design standards seems a poor process solution for all but the largest organizations. Companies are expected to comply with government regulations which were recognized in the workshop as being subject to a slow, bureaucratic revision process—by definition, this implies that they trail the state of the art. In addition, it implies that government regulations only apply to static technology and that designers will find little benefit in looking to regulations for new technologies or new applications of existing technologies. To be useful, standards and regulations need to be current. As a result, companies are expected to generate and track their own design standards.

Relying on ISO Standards

Hale, et al. (2006) offer several ideas for integrating safety into design, although some of the ideas seem to be incomplete solutions. For example:

> We believe that a standard of "good design practice" such as described in . . . the EN standard 292 (CEN, 1991), would be a powerful incentive to systematize and make design explicit, and could be used in court cases as a touchstone for assessing state-of-the-art design and whether each party had lived up to its responsibility. Such a standard of good practice would need to reflect differences per technology in the distribution of power and competence between the designer and user. [*Note that this is an example of the difficulty of keeping current with standards. EN 292 was revised as the international standard ISO 12100 with the current version released in 2007.]* (emphasis added)

This is a fine idea, except that the guidance ISO 12100, Safety of Machinery, provides is general, open-to-interpretation and hard-to-determine compliance. For example, ISO 12100-2:2007 states in Section 4.7, Provisions for maintainability:

> When designing a machine, the following maintainability factors shall be taken into account:
>
> • accessibility, taking into account the environment and the human body measurements, including the dimensions of the working clothes and tools used;
>
> • ease of handling, taking into account human capabilities;
>
> • limitation of the number of special tools and equipment.

How does a designer demonstrate that s/he has met these provisions? How does a safety practitioner provide input to a design in a way to demonstrate conformance to this requirement? Other than circumstantial evidence of an event occurring, how would a compliance officer or lawyer prove that a designer did not "take into account" these issues in the design and, thus, failed to meet the standard requirements?

The machine tool industry in ANSI B11.GSR and the packaging machinery industry in ANSI/PMMI B155.1 address this issue in the following way. In Section 4.11, Operational working space:

> The user shall provide and maintain sufficient access and working space about the machine tool to permit safe operation and maintenance of the machine [B11.GSR].

A designer can apply this requirement to a design and demonstrate that adequate working space is provided for all required tasks. To do so the designer or safety practitioner must identify how much space is required and provide or specify that space. Conversely, a compliance officer or lawyer could demonstrate that the space provided for a task was insufficient and did not comply with this requirement.

Thus, although ISO 12100 has many good ideas, the proposal from Hale, et al. (2006) fails because the standard does not serve well in terms of performance language for either the designer or the regulator. This is one example where a government regulation provides less suitable requirements than voluntary industry consensus standards (self-regulation).

Baram (2006) views government regulation as the only viable method to ensure safety by design. He and other workshop participants place great faith in the ability of the standards writers to both be aware of all the safety issues necessary to prevent harm and to be able to write text that clearly conveys what designers need to do. This assumption fails.

Standards writers from all countries are typically skilled, knowledgeable and experienced in technical subject matters. Yet, they often do not, and cannot, know all relevant safety and design concerns, particularly with dynamic technology or new applications of existing technology. In many cases, this knowledge can only come from users in the field who know firsthand the problems and constraints of designs. In this regard, the standards writers face the same dilemma as product or system designers—they do not know the potential failings of their designs/text and often do not know what they do not know. Thus, they cannot write standards for applications they do not fully understand or appreciate.

Documenting Design

According to Hale, et al. (2006):

> Above all, the attention for safety in design needs great transparency in making and documenting design decisions and the assumptions on which they are based. . . . This is not a strong point of designers, but without a record of why decisions in design were taken as they were, it is difficult to learn how they could have been made better. . . . Without such documentation it is hard to assess the implications of changing aspects of the design at a later stage. Designers therefore need efficient tools to document history on decisions and assumptions for communication further down the design process.

Although not all design decisions need to be documented to improve safety, more documentation is needed than often currently occurs. Requiring that all decisions be documented could impede the design development process to the point of becoming unworkable. In terms of safety, the bases for many design decisions are implicitly captured in a risk assessment. Design features or systems that are included in order to reduce risks are documented in the risk assessment. Later considerations to modify or remove these design features or systems can then be viewed in terms of how they impact risks. This is a key reason why every risk assessment standard, technical report and guideline requires that the risk assessment be documented (Main, 2004).

Complex Models

Several workshop papers present fairly complex models and systems that appear to have limited use except for their specific application. For example, Kirwan (2006) describes a safety plan for air traffic management, where "the safety plan explains what needs to be done, and is signed by the safety manager and by the research area manager. Typically it is a 50-page document. . . ."

The time and effort required to prepare and approve a 50-page document is likely well beyond the practical limit for general industry, so this is not a suitable model for general industry or perhaps many industries at all. If the answer to the question "What do I have to do" is "create a 50-page safety document," it is highly likely that this would only occur if a government regulation required it. There seems to be little need or support for such an analysis from engineers, safety practitioners or anyone else for other than the most high-risk/high-consequence systems where significant safety resources can be made available (e.g., air traffic management, nuclear systems, space operations, dam construction).

The Desired Result

Hale, et al. (2006) describe a desired result for safety by design as follows:

> The best situation is not when designers are merely answering safety questions, but when they are themselves asking such questions. . . . What we are looking for is that the designer has a coherent and systematic way of considering possible safety problems and how to avoid them.

One indication that safety is being considered by design occurs when engineers begin to discuss hazards, risk reduction methods and acceptable risk in those terms. Unfortunately, design engineers often do not receive this type of training in their undergraduate study (Main & Ward, 1992). A few universities are beginning to address this shortcoming (King & Christensen, 2002; Schleyer, Duan, Stacey, et al., 2006). As industry standards have incorporated the risk assessment process and engineers have learned the concepts, these conversations are taking place. The desired transition has occurred in several companies and it is indeed an exciting and encouraging sign that safety is being considered in design.

Implications

Government Regulations

The view that government regulations are the most effective way to include safety in design seems common in the EU. Although the U.S. legal tort system is often criticized and held up as a model to avoid at all costs, the more aggressive U.S. tort law system may explain why self-regulation works in the U.S. while the lack of a similarly aggressive tort system in the EU may be an underlying cause of the government regulation bias.

Although self-regulation has its weaknesses, the system seems to work well in the U.S. in terms of compensating persons harmed by defective products and in influencing suppliers to reduce risk and prevent injuries. Self-regulation will work well only if there is a strong incentive for companies to comply with the industry standards. In the U.S., one of the primary influencing factors to comply with industry standards is the fear of tort law judgments. Although Baram (2006) states that the fear is real, he does not place much significance on the actual threat. Thus, without a more aggressive tort law system, self-regulation in the EU may well be ineffective and government regulation is the (next) best solution in that legal environment.

Writing Regulations

In the U.S. and other countries, promulgating new government regulations is a difficult battle, as evidenced by many OSHA regulations being 20 years old or more. The history of the ergonomics regulatory standard is a case in point. Although many organizations supported the regulation, many others fought it. In the end, the standard was repealed.

Even some U.S. government agencies recognize the bureaucratic challenge of developing regulatory standards and are looking to private industry to assist. Several U.S. government agencies are looking to trade organizations to develop consensus standards that the government can then adopt by reference. The agencies recognize that writing regulations within the current rulemaking process

would require far more time and be subject to more political influences than working through the self-regulatory industry trade organizations. In this manner, partnering between industry organizations and governments may prove to be an effective means to increase safety in designs. This approach may provide the benefits of self-regulation with the enforcement of government regulations.

International Standards Efforts

The U.S. needs to remain involved in the international standards development process. It must work within the international standards development process to create harmonized standards that work in both systems, then apply them within the different social systems of the U.S. and EU. If the U.S. does not participate, the standards will be written without U.S. input or concerns, and may result in standards that create significant challenges to U.S. manufacturers and global companies wanting to ship machinery to the EU.

U.S. suppliers and safety practitioners will be held accountable to the EU requirements for their products shipped to the EU, which may or may not be more restrictive than U.S. standards. Similarly, EU suppliers and safety practitioners will be held accountable to U.S. standards shipped to the U.S. In the U.S. market, mere compliance with regulations may not be sufficient to demonstrate that risks have been reduced to an acceptable level, a situation contrary to EU presumptions. The EU view that compliance is all that is necessary to achieve acceptable risk could lead to some painful lessons in the U.S. court system. The safety practitioner should evaluate machinery, products or systems from any source (EU, U.S. or other) using the risk assessment process to ensure that acceptable risk is achieved.

Conclusion

The EU and U.S. approaches to safety by design and social control of risk differ, but one is not better than the other. Each system operates in a different legal and social environment and the methods used to control risks are reflected in their respective approaches. Safety practitioners and design engineers cannot change these systems but must work within them.

Thus, equipment suppliers in one region that sell into the other region need to be aware of these differences and the implications on how to include safety in the design of their systems, equipment, machinery and operations. Understanding these different systems and the requirements will likely lead to safer designs and prevent injuries. ■

References

ANSI/Association for Manufacturing Technology (AMT). (2000). ANSI B11.TR3-2000: Risk assessment and risk reduction—A guide to estimate, evaluate and reduce risks associated with machine tools. McLean, VA: AMT.

ANSI/AMT. (2007a). ANSI B11.GSR-2007: General requirements for the safety of machine tools. McLean, VA: AMT.

ANSI/AMT. (2007b). ANSI B11.TR7-2007: Designing for safety and lean manufacturing—A guide on integrating safety and lean manufacturing principles in the use of machinery. McLean, VA: AMT.

ANSI/Packaging Machinery Manufacturers Institute (PMMI). (2006). ANSI/PMMI B155.1-2006: Safety requirements for packaging machinery and packaging-related converting machinery. Arlington, VA: PMMI.

ANSI/Robotic Industries Association (RIA). (1999). ANSI/RIA R15.06-1999: Safety requirements for industrial robots and robot systems. Ann Arbor, MI: RIA.

Baram, M. (2006). Liability and its influence on designing for product and process safety. In A. Hale, B. Kirwan & U. Kjellen (Eds.), *Safety by design: Based on a workshop of the New Technology and Work Network.* Published in *Safety Science, 45*(1-2), 11-30.

European Parliament & European Union (EU). (2006). Machinery directive 2006/42/EC of the European Parliament and of the Council, *Official Journal of the EU.*

Fadier, E. & De la Garza, C. (2006). Towards a proactive safety approach in the design process: The case of printing machinery. In A. Hale, B. Kirwan & U. Kjellen (Eds.), *Safety by design: Based on a workshop of the New Technology and Work Network.* Published in *Safety Science, 45*(1-2), 199-229.

Hale, A., Kirwan, B. & Kjellen, U. (2006). Safe by design: Where are we now? In A. Hale, B. Kirwan & U. Kjellen (Eds.), *Safety by design: Based on a workshop of the New Technology and Work Network.* Published in *Safety Science, 45* (1-2), 305-327.

Hammer, W. (1993). *Product safety management and engineering* (2nd ed.). Des Plaines, IL: ASSE.

International Organization for Standardization (ISO). (1999). EN 292-1/ISO 12100-1:1999. Safety of machinery—Basic concepts, general principles for design—Part 1: Basic terminology, methodology. Geneva, Switzerland: Author.

ISO. (2007). ISO 12100-1:2007. Safety of machinery—Basic concepts and general principles for design—Part 1: Basic terminology and methodology. Geneva, Switzerland: Author.

ISO. (2007). ISO 12100-2:2007. Safety of machinery—Basic concepts and general principles for design—Part 2: Technical principles. Geneva, Switzerland: Author.

ISO. (2007). ISO 14121-1:2007. Final Draft International Standard. Safety of machinery: Risk assessment, principles. Geneva, Switzerland: Author.

ISO. (1992). ISO/TR 12100. Safety of machinery—Basic concepts, general principles for design, basic terminology, methodology. Geneva, Switzerland: Author.

Jagtman, E. & Hale, A. (2006). Safety learning and imagination versus safety bureaucracy in design of the traffic sector. In A. Hale, B. Kirwan & U. Kjellen (Eds.), *Safety by design: Based on a workshop of the New Technology and Work Network.* Published in *Safety Science, 45*(1-2), 231-251.

King, P.H. & Christensen, W.C. (2002). Teaching safety through design in biomedical engineering design. In *Proceedings of the 2002 American Society for Engineering Education (ASEE) Annual Conference & Exposition, Montreal, Canada.*

Kirwan, B. (2006). Safety informing design. In A. Hale, B. Kirwan & U. Kjellen (Eds.), *Safety by design: Based on a workshop of the New Technology and Work Network.* Published in *Safety Science, 45*(1-2), 155-197.

Main, B.W. (2004). *Risk Assessment: basics and benchmarks.* Ann Arbor, MI: design safety engineering inc.

Main, B.W. & Ward, A.C. (1992, August). What do engineers really know and do about safety? Implications for education, training and practice. *Mechanical Engineering, 114*(8).

Manuele, F.A. (2001). *Innovations in safety management.* New York: John Wiley and Sons.

Manuele, F.A. (2003). *On the practice of safety* (3rd ed.). New York: John Wiley and Sons.

Manuele, F.A. (2005, Nov.). Global harmonization of safety standards: Examining the European influence on the practice of safety. *Professional Safety, 50*(11), 41-46.

Manuele, F.A. & Christensen, W.C. (1999). *Safety through design.* Itasca, IL: NSC Press.

Schleyer, G., Duan, R.F., Stacey, N., et al. (2006). Educating engineers in risk concepts. *Proceedings of the International Conference on Innovation, Good Practice and Research in Engineering Education, Liverpool, England,* 496-501.