Design Reviews: Checkpoints for Design

By BRUCE W. MAIN

Design reviews are proven methods of evaluating product and process designs against the set design criteria. If the criteria are met, then the design progresses to the next phase of development or production. If not, then the designers continue to work on the design until the criteria are satisfied. This article explains the design review process and discusses the safety practitioner’s role in that process. The different types of design reviews are presented, the mechanics of completing a design review are discussed, and implications for safety practitioners are explained.

Design reviews have been around for decades in the engineering community. The design review forms an essential part of modern industrial practice. Properly instituted it provides a mechanism whereby the total design activity can be carried out in a balanced and best compromise manner, leading to improved designs and products (Pugh).

Hunter euphemistically referred to “the good old days”:

[when] the only design reviews which were performed were those carried out on the first production version of a newly designed machine. The machine would be run for a while, or until something broke. This was the “build ‘em and bust ‘em” era. . . . An acceptable configuration was often reached by
some combination of repeated experiments, endless modifications, trial and error, animal cunning and good luck.

This “build ‘em and bust ‘em” era represents a rather inefficient process. An easier and more-efficient process facilitates a design that meets both design and safety performance criteria before it is released rather than trying to “retrofit” it to meet these criteria at the design review. Figure 1 illustrates these differences.

A safety practitioner should be involved in the design process early in order to help establish safety performance criteria that need to be included as the design evolves. This is the essence of safety through design. Through this process of early involvement, the anticipated outcome is a better, more-efficient design process.

Design reviews have been implemented as a means to ensure that designs for products and processes met necessary requirements before being released to production or the next phase of development. This form of checking a design before it progresses to its next phase continues today. This article presents a general overview of design reviews and their use.

PURPOSE OF A DESIGN REVIEW

Design reviews are a formal evaluation of a design to ensure that it meets criteria set forth for the project. Safety is typically only one element of these reviews. The nature of the design and company culture will determine the importance of safety criteria. In some product or process designs, safety is a critical element; in others, it is a relatively minor concern.

Several objectives drive most design reviews:

- identify and correct hazards to prevent injury and illness;
- ensure compliance with applicable regulations and standards;
- prevent property loss due to incidents, fires, spills and avoidable downtime;
- resolve any outstanding safety related issues;
- contain project cost by reducing redesign and rework;
- facilitate project planning, including installation and debugging (Adams).

DIFFERING PERSPECTIVES

The word “design” is used frequently in many circles—sometimes to describe very different situations. Engineers use the term to refer to the technical synthesis where a concept moves from an idea to a functioning product or system. Graphic artists also use the term to connote a creative process, but this usage tends to be artistic and aesthetic rather than technical. In the artistic instance, the term design may not involve any functional aspects, which can be confusing to engineers accustomed to thinking in terms of functional requirements. Furthermore, the term can be used to refer to both a process and a resulting product, as in “I am going to design a widget” or “The design is complete.” In this article, “design” is used in the engineering and technical context.

Design engineers have the primary responsibility for making a product, machine or system work in accord with established design criteria. This can be a challenge. Their focus tends to be on creating a functional result from new and existing components, concepts or parts. In discussing engineers’ focus, Hunter notes that “the emphasis was on getting the machine to work” (1992).

Safety practitioners have a different focus. They are concerned with how the design might “fail” should a component or user not perform as expected. In the latter case, engineers often feel justified that the design did not fail, but that the person using the design was the problem.

Both perspectives are important. Without the designer’s focus, a functional, working design will not result. Without the safety focus, foreseeable uses or misuses may be omitted, leading to problems after the design is in production.

TYPES OF DESIGN REVIEWS

Several different types of design reviews may be conducted. Designs may be reviewed according to a particular specialty, such as safety, marketing, cost or legal. Reviews are typically comprehensive, where all specialty concerns are addressed at one time, or as appropriate according to the design maturity. In most cases, several design reviews should be conducted during the course of a product design, including 1) marketing; 2) concept; 3) detail; 4) prototype manufacturing; 5) development; and 6) production (Pugh). In the context of a process review, Hammer presents a series of design reviews (Table 1).

Across different companies, the types of design reviews used vary. How many design reviews occur, what they are called and when they are conducted are less important than the decisions and analyses supporting the design decisions. Each company, and to a certain extent each
Perhaps the most critical of the various design reviews are the early ones, since the ability to change the design is greatest and associated costs lowest.

design, may have a slightly different design review process.

**TIMING OF A DESIGN REVIEW**

Design reviews should be held whenever the need arises to make key decisions on the design. At certain times, such meetings can be impromptu and informal, such as in the hallway or via e-mail. More formal reviews are typically conducted at the early stages of design and prior to its release to production.

The Institute for Safety Through Design has been a strong champion for the cause of having safety issues considered early in the design process (ISTD). Figure 2 presents a model developed by ISTD to illustrate this point as it relates to safety. This model emphasizes that once tooling is made or production begins, safety efforts are more costly, more difficult to implement and less effective than addressing hazards during design stages. After a product or process starts to be built, any safety activities are considered retrofitting. Safety through design seeks to take advantage of the better ease of implementing safety early in design and avoid the increasing costs of retrofitting. Ideally, safety should be considered during the early business concept evaluation.

Perhaps the most critical of the various design reviews are the early ones, since the ability to change the design is greatest and associated costs lowest. As the design matures, the cost of making changes—and the hurdles to implementing them—increase considerably. This cost-feasibility paradox has been highlighted previously in quality discussions. Manuele emphasizes the timing issue as follows:

In the design process, the goal is to avoid bringing uncontrolled hazards into the workplace. That presents much opportunity for upstream involvement by safety professionals who would influence those making design and purchasing decisions. Their activities would include providing design specifications, giving consultation to those who design on safety goals to be achieved, assisting in design reviews, and developing specifications . . .

It is a hard truth that most of the significant, work-related safety decisions are made in the design process. That is why the emphasis . . . is so strong in support of safety professionals taking an anticipatory and proactive approach to hazards to avoid their being brought into the workplace (Manuele).

This view is shared by many others.

**DESIGN REVIEW MECHANICS**

Design reviews are typically conducted by a team. Team members will vary depending on the product or facility being designed, and the stage of the development process. Design engineers and others intimately involved in creating the design should be part of this team. Specialists in safety, marketing, production, finance, quality, legal, etc., should be included as appropriate. The team leader

<table>
<thead>
<tr>
<th>Type</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Concept</td>
<td>Establish baseline for product.</td>
</tr>
<tr>
<td>Preliminary Design</td>
<td>Review initial design based on proposal selected at Concept Review.</td>
</tr>
<tr>
<td>Development “Go Ahead”</td>
<td>Evaluated technical, financial, marketing, and other factors.</td>
</tr>
<tr>
<td>Evaluation Critical Design</td>
<td>Evaluate detailed designs and analysis.</td>
</tr>
<tr>
<td>Prototype Review</td>
<td>Evaluate prototype design before it is actually built.</td>
</tr>
<tr>
<td>Production “Go Ahead”</td>
<td>Evaluate advisability of proceeding with full-scale production.</td>
</tr>
</tbody>
</table>

**TABLE 1**

**FIGURE 2**

Moving Safety Upstream

In the Design Process

From an afterthought to a forethought in process, product, and facility design

©Institute for Safety Through Design
Design reviews are typically conducted by a team. Team members will vary depending on the product or facility being designed, and the stage of the development process.

should be someone who will take a balanced view of the process.

As noted, during the review, a design is evaluated against established criteria or requirements. The goal is to ensure that the design meets all criteria or that trade-offs made between criteria are appropriate and necessary. Beginning this process without design specifications or benchmarks will likely lead to frustration and wasted time since issues will arise out of the review that require further analysis and examination.

Design criteria/desired attributes are typically set by management, marketing, manufacturing, finance or others. Criteria can come from outside sources such as standards, legal requirements or customers as well. These requirements are often combined into one or more checklists so that no requirements are overlooked.

The primary checklist may include references to subchecklists that include more-detailed criteria. For example, the primary checklist could refer to the “safety checklist” or “environmental checklist.” Not until all items on the subchecklist are satisfactorily completed can that element on the primary checklist be released.

Checklists typically come from within a company based on its past experience. For example, with an evolutionary design (improvements to an existing design), the prior design and its checklist(s) would form the basis for the subsequent design. The checklist would be updated to include more-recent information from field experiences, revised standards and similar details.

Checklists from outside the organization are often introduced and integrated in whole or part into a company checklist. For revolutionary designs (new development for which little prior design experience is available), the tools noted earlier can have limited potential due to the design’s new and unknown nature. For example, checklists may not be applicable, industry standards usually do not exist and experience may be limited.

In these cases, a risk assessment or other safety analysis must be developed to guide review decisions.

Increasingly, design reviews are being based on risk assessments. The review employs a risk assessment to ensure that all hazards have been identified and that risks associated with those hazards have been reduced to an acceptable level. (See Manuele (2001), Main (2000), ANSI B11 TR3 (2000), ANSI/RIA (1999) for details on how to conduct a risk assessment.)

THE DECISION-MAKING PROCESS

Design reviews integrate into a basic decision-making process. The general steps in such a process are:

1. Identify the problem.
2. State the basic objective or goal.
3. State the constraints, assumptions and facts.
4. Generate possible solutions.
5. Evaluate and make a decision.
6. Analyze.
7. Create a detailed solution.
8. Evaluate the solution.
10. Implement the decision.
11. Check the results.

The design review addresses step 8. In many cases, if the solution is found lacking, then the team begins to reevaluate constraints and generate new or differing possible solutions (returning to steps 3 and 4). If sufficient information is available at the time of review, the team can work through the rest of the steps to arrive at a recommendation. If additional information or analyses are needed, the team usually defers a decision and reevaluates the design once analyses have been completed.

In the context of safety standards, the analysis step can be straightforward when government regulations or industry standards apply. Such an evaluation is considered a compliance evaluation. The question to be answered is simple: Does the design comply with the requirements of the standard? A single design may have several standards that must be checked. Once the team is satisfied that the design complies with regulatory requirements, the design progresses along the development or production process.

However, designs are rarely an exact copy of existing systems. Design is a creative process that generates new and unique solutions to ever-changing customer demands. In many cases, industry standards do not exist to address the specific design being developed. Industry standards may apply, but the new design ventures into areas not directly covered by those standards.

When standards are less defined, a compliance evaluation is inadequate. In these cases, a separate safety analysis must be conducted to make sure the design meets the required level of performance. In the context of costs, a financial analysis would be used to ensure that cost objectives are satisfied and to identify opportunities to further reduce costs beyond the basic requirement. In the context of safety, a risk assessment or other safety analysis will serve to identify opportunities for improvement and ensure the design reduces risks to an acceptable level.

SEPARATING THE ANALYSIS & REVIEW

Step 6 (analyze) is a critical one. In the context of other engineering disciplines, analyses are fairly well accepted (e.g., a structural question requires a finite element analysis; a ventilation question requires an air flow or heat transfer analysis; a finance question requires calculating the net present value or break-even production measures). These analyses provide support for making decisions.

However, in the past, many safety-related decisions were made by the design review team or management without a supporting risk assessment or safety analysis. Safety decisions are almost always subjective; they are made to determine whether the design’s risks are acceptable. Since people make decisions on risk acceptability every day, they tend to believe that they have a basis for evaluating a design’s risk acceptability.

Hunter blurs the difference between the analysis and decision steps:

Design reviews are now an essential part of the process of recognizing that a hazard exists, defining the nature and severity of that hazard, and discovering ways to design the hazard out of the product before the product is created.

Although the difference is subtle, it is significant. The hazard analysis, risk assessment and risk reduction should occur before the design review rather than at the same time, except for less-complex designs. Although hazard recognition might occur at a review based on team observations, the assessment should primarily occur away from the design review session.

Separating decisions made by the design review team from the safety analysis used can help support the team’s decisions. Just as a heat transfer, structural or financial analysis would likely be conducted outside the design review, a risk assessment or safety analysis should be performed separately.
However, in many design reviews, no separate or formal safety analysis is conducted to support safety decisions. In these cases, the review team makes a subjective assessment at the same time it is evaluating the design. Although this approach may be reasonable for relatively simple designs, a separate risk assessment or safety analysis should be performed for more-complex designs.

**Types of Safety Analyses for Design Reviews**

A large number of safety analyses can be used in support of a design review. These include: checklists; preliminary hazard analysis; risk assessment; failure modes and effects analysis (FMEA); and fault tree analysis (FTA). [Further discussion of these techniques is beyond the scope of this article. See Main (2000), Clemens and Simmons (1998), Roland and Moriarty (1990), Hammer (1993) and others for further discussion.]

The key point is that these analyses take time to conduct effectively, typically more time than can be allotted within a design review. Thus, the analysis should occur separate from the design review.

**Decision Criteria**

Where do design criteria come from? They derive from several sources—including customers (e.g. features), management (e.g. basic functionality, manufacturability or cost) and design standards.

**Government Standards**

Government standards/regulations in effect at the international, federal and state levels (e.g., EU, OSHA, DOT and CPSC) are among the most-obvious information sources available to a design review team. Noncompliance with a regulation is a violation of law and is a very serious concern if it occurs.

**Industry/Nongovernment Standards**

Industry standards (e.g., those promulgated by groups such as ANSI, ASME and NFPA) are a common source of safety criteria as well. These standards provide technical information, promote consistency, ensure a minimum level of safety, and provide an excellent information source for hazard elimination and control.

International standards are playing a more-dominant role in designs. As manufacturers design, build and sell products “anywhere and everywhere,” the pressure to use international standards in product and process designs has increased. According to one international company, over the past two decades, the standards used have moved from primarily company or national standards to international standards. This trend is expected to continue.

Industry standards are beneficial since they capture an industry’s experiences with a particular design. They often represent the result of safety analysis and an industry’s considerable collective experience. Compliance with objective measures included in standards and recommended practices is an important part of a design review. A manufacturer that fails to conduct these tests and meet these minimum requirements should seriously reexamine this practice. However, it should be recognized that much design activity ventures into the area of new features, new capabilities and new applications where few standards exist or directly apply.

**Risk Assessment**

An increasingly overt design criterion has become whether the residual risks of a design have been reduced to an acceptable or tolerable level (ANSI B11.TR3). This criterion has long been used in business, but rarely was the decision explicit, formalized or documented. With newer risk assessment advances, these decisions have been brought forward and made with supporting analyses. For situations without specific design standards, risk assessments will help identify criteria for evaluating a design.

**Benchmarking**

Benchmarking against competing designs or products/processes is another means of evaluating a design. This process may help the team determine whether risks are acceptable or if alternate designs should be developed. Benchmarking can include researching technical literature. It usually occurs before design criteria are set.

**Checklists**

Checklists are used in both the design and safety communities. A checklist typically includes safety-related items that must be addressed for a design. Checklists are most helpful in repetitive design tasks or operations where product variation is small. A safety checklist is useful because its creation requires a safety analysis, with the resulting checklist tailored to a particular design. This same checklist can be used for subsequent designs if strong similarities exist between the designs.

However, using an old checklist for a new design is akin to using finite element analysis results from one design to another; when designs differ, the checklist could obscure serious hazards. For example, a new, lightweight design developed to replace a steel bracket fixture could include plastic components. A checklist developed for the steel design is not likely to detect or account for creep.

Checklists are often used simply as reminders of issues that must be considered. The designer may refer back to
A safety practitioner can make the greatest contribution to safety if s/he is involved as early as possible in the design process.

Company Information

Part of a design criterion may be to determine whether a product design is consistent with a company’s other designs. This internal consistency can be important for both safety and liability reasons. Several different types of information within a company may be used in the design review; these include internal standards, written company procedures, product tests and simulations, statistical data, product histories, and engineering analyses and evaluations.

Personal Experience

Personal experience is an important and necessary part of design as well. Engineers rely on their experiences along with those of fellow engineers to avoid past mistakes. However, relying too heavily on personal experience creates opportunity for errors. For example, a company’s experience may be limited or no longer be resident within the company. Furthermore, a designer’s experience may lead to unintended biases that create hazards. For example, users may not be as technically trained, or may use the product differently than the designer.

Other information sources that can be useful in design reviews and in conducting safety analyses for the reviews include product history, legal or liability history.

SAFETY PRACTITIONERS’ ROLE IN A DESIGN REVIEW

A safety practitioner can make the greatest contribution to safety if s/he is involved as early as possible in the design process. Involvement in the business concept of a design is not too early to get involved. In this way, the safety professional can interact with designers concerning the design and the appropriate safety criteria.

How does one become involved early in the process? By demonstrating value added to the design development. Engineers are familiar with the design and its components from a design perspective. They understand what will happen to the design if a force (e.g., mechanical, thermal, electrical) is applied at a particular location. As a result, they are well-suited to conduct an FMEA.

However, engineers are often less well equipped to view a design from the operator or user perspective. They may be less likely to understand or anticipate when or why the force may be applied. By contrast, the safety professional has spent considerable time on the plant floor; has experience identifying hazards in occupational settings; and understands how equipment is really used/misused on a daily basis. Bringing this knowledge to bear early in the design process helps identify hazards and establish safety-related design criteria.

If these factors are identified early, the engineer can include them in the trade-offs and decisions made during development—which is the essence of safety through design. If safety-related issues are raised after the design nears completion, the ability to make changes greatly diminishes, can be extremely costly and will likely be viewed as detrimental to the design development schedule.

As a result, the safety professional should assume a lead role in conducting and revising a risk assessment or other safety analysis. In many cases, s/he will be more familiar with the tasks users perform and can identify any associated hazards. By conducting the risk assessment, s/he will develop a better appreciation of the design and the users’ interactions with it. By being actively involved in this process, the safety practitioner can also help set design criteria related to safety performance.

When a safety practitioner has been involved in the design development and in the analysis supporting safety performance, the design review should proceed smoothly. By including safety in the design, few—if any—outstanding hazards will be identified during the design review that have not been reduced to an acceptable level. With a supporting risk assessment, the safety practitioner and the engineer can intelligently discuss and make decisions about risks and their control.

In some instances, the safety practitioner may not be involved in a design review until the final walkthrough. If this occurs, the reviewers will need to closely examine the design against the safety performance criteria to be certain it meets the criteria. Design decisions without a supporting risk assessment or safety analysis should be subjected to a great deal of scrutiny, if not tabled until such an assessment is completed.

CASE STUDY

A manufacturing facility was developing a design for a new production line. A situation on an existing production line at a sister facility revealed several safety challenges related to means of egress, ergonomics and machine guarding. Analysis of the existing situation and potential solutions showed that substantially changing the existing layout was prohibitively expensive. Practicable risk reduction methods for the line were restricted to developing standardized operating procedures and specialized training. This was the best practical solution available given the circumstances, but all involved knew it was less than ideal.

In the sister facility, management wanted to minimize or eliminate hazards identified in the existing facility. A risk assessment was conducted to identify hazards and the associated risks of the conceptual design. Several identified hazards produced risks that were higher than desired. Risk reduction methods were developed; these included moving structures and equipment, modifying worksite locations and planning for stairs and catwalks. In addition, standard practices were identified that would require training and signage.

Since the hazards were identified during the design process, modifications were made easily, with minimal costs. Automated work cells helped to eliminate repetitive ergonomic hazards. Not all proposed risk-reduction methods were implemented. Financial constraints precluded the safety optimum design. For example, in some places, personnel must use catwalks rather than egress at floor level, and training to avoid certain hazards is still required. However, the process changes permitted increased productivity with considerably less risk to personnel.

PRACTICAL CONSIDERATIONS

The safety practitioner will face some challenges when joining design review
teams. One is the ability to work comfortably with the technical content of a design (such as engineering drawings and being able to visualize the design in three dimensions). S/he must be able to converse with engineers and understand the many constraints that must be balanced in developing a design. At the very least, the safety practitioner must be able to understand these other constraints in order to participate in the discussions about safety performance.

By being involved early in the process, the safety practitioner can also avoid the perceived role of being a “naysayer.” S/he must realize that safety performance is only one of many criteria that the design engineer must balance. Although safety can play a key role in that balance, the practitioner should realize that safety may not be the most important criterion. Trade-offs in this regard are necessary and appropriate provided the residual risks are acceptable. This may mean that the risks are not reduced to the achievable minimum. Management or the design team may determine that the balance is appropriate for that design.

Finding the appropriate level of involvement for the various ongoing design projects within a company is another potential challenge. Although the safety practitioner should be involved early, the level of involvement may not be very high. As noted, however, involvement too late in a project can lead to problems.

The pace of design in a company may also be a challenge. Many safety practitioners juggles many differing responsibilities. If many designs are in the pipeline, the practitioner may be faced with trying to assess too many designs in a very short time. In such cases, having design engineers complete the risk assessment before the design review can be of great assistance. For example, a safety analysis could become a written requirement to reach the final design review. This will help ensure that the analysis is completed before the review is held.

Companies that do not use design reviews for safety may believe that they increase development time and delay completion. This can be a significant obstacle:

A big challenge for the safety professional and engineering manager is changing the design culture; for example, from one where safety is viewed as a costly add-on, to a culture where safety is fully integrated and is seen as a strategic advantage. This is made even more challenging by today’s environment of outsourcing, globalization and rapidly changing organizational structures (Adams).

LIMITATIONS

Design reviews are not the nirvana of safety. Alone, they are somewhat inefficient from a cost perspective and may not deliver adequate incident prevention (Adams). This is particularly true if they tend to be compliance exercises, occur late in the design process and do not involve the safety practitioner until very late. The review will likely result in new design criteria or hazards being identified that will require additional engineering efforts to resolve. In turn, this will slow the development cycle and can leave the safety practitioner with a negative perception.

CONCLUSION

Design reviews are commonly used to evaluate a design before it advances to production, the market or other design milestone. These reviews are useful because they allow a team to evaluate a design against criteria and ensure that risks are—or are being—reduced to an acceptable level.

The safety practitioner needs to be involved early in the design process to have the most impact. S/he must pay close attention to the basis for safety-related decisions during the review process. If decisions are being made without a supporting risk assessment or safety analysis, then the safety practitioner should question the process, just as a financier would question financial decisions made without supporting data. Participating in design reviews can be rewarding for the safety practitioner who is willing and able to become engaged in the design process.

REFERENCES

