



An Engineer's Guide: Reduce Design Time, Cost and Risk
Essential Information on optimizing product development and liability

Summary

Before your product is sold, you make significant considerations regarding product quality and safety. But have you considered the significant impact post-sale problems can have? Functionality problems, product returns, and possible product recalls can all have a direct effect on your reputation. However, your risk can be minimized if you have the correct risk management measures in place.

It's natural to assume that compliance with product safety standards equals risk mitigation. However, individual standards rarely cover all likely sources of potential harm. Since the standard development process is often lengthy, even the newest standards often lag behind current technology. In addition, there are many occasions in which a product has met a standard, but presents risks when operated.

Minimizing the risks associated with a new product is, perhaps, the manufacturer's primary responsibility. Indeed, regulatory authorities worldwide are moving away from a reliance on compliance with standards alone and toward product acceptance criteria based on the level of risk that the product poses to the end user. Manufacturers intent on developing safe, innovative, and effective products that will be marketable globally must therefore adopt a risk analysis strategy that spans every stage of product development.

After discussing the differences between standards-based and risk-based focuses, this whitepaper outlines the principles underlying the risk-based approach to product safety, as well as the steps involved in performing a risk analysis.

Standards Versus Risk Analysis

Among the factors driving the move from a standards-based approach to ensuring product safety to one that focuses on risk-based analysis is the speed of technological innovation. While many relevant international standards have been developed over the past two decades, particularly for electromechanical products, these documents are based on the then-current state of the art and can never keep pace with technological advances. In addition, regulation based on standards alone tends to stifle innovation because designers must spend their time looking for ways to comply with the standards, rather than developing new technologies that may lead to inherently safer products.

Furthermore, even when standards exist to cover all of a product's design elements, compliance with multiple standards carries no guarantee that the product will be free of risk. Simply demonstrating compliance with standards is not sufficient to ensure product safety. There are many occasions in which a product has met a standard, but presents risks even when operated for its intended use. For example, an electric wheelchair's intended environment, as defined by the standard, is indoors. Once an electric wheelchair enters an open-air environment, it has the potential to be subjected to stray radio frequency, which may impact its normal operation.

How do the standards-based and risk-based approaches differ? When using a risk-based approach to safety, a manufacturer assumes that risks exist, identifies them, attempts to eliminate them, and tests the product to technical standards to verify that particular risks (e.g., fire, electric shock, or mechanical hazards) are minimal. This is opposite to the way many companies use technical standards today, in which the product is tested to determine that the standards are met in full and risk analysis is used as a supplementary procedure.

The following example illustrates the difference between the two approaches. The manufacturer of a manually propelled wheelchair who is pursuing a standards-based strategy would research the applicable standards and then conduct testing to demonstrate compliance with those requirements. If the manufacturer were committed to a risk-based analysis approach, however,

the research effort would address a two-part question: what are the applicable product standards for this wheelchair, and what hazards could be associated with its use? The manufacturer would then list all materials, parts, and assemblies used to produce the wheelchair and identify the possible failure modes related to each item.

The results of this exercise would be the identification of many different scenarios in which the user could be harmed, some of which could even cause fatalities. Steps would then be taken to eliminate or mitigate these possibilities. When the standards-only approach is used, the scenarios leading to potential fatalities might be overlooked. If so, the plaintiff in a later product liability suit would be able to maintain that the manufacturer had not exercised due diligence because the product failure was foreseeable.

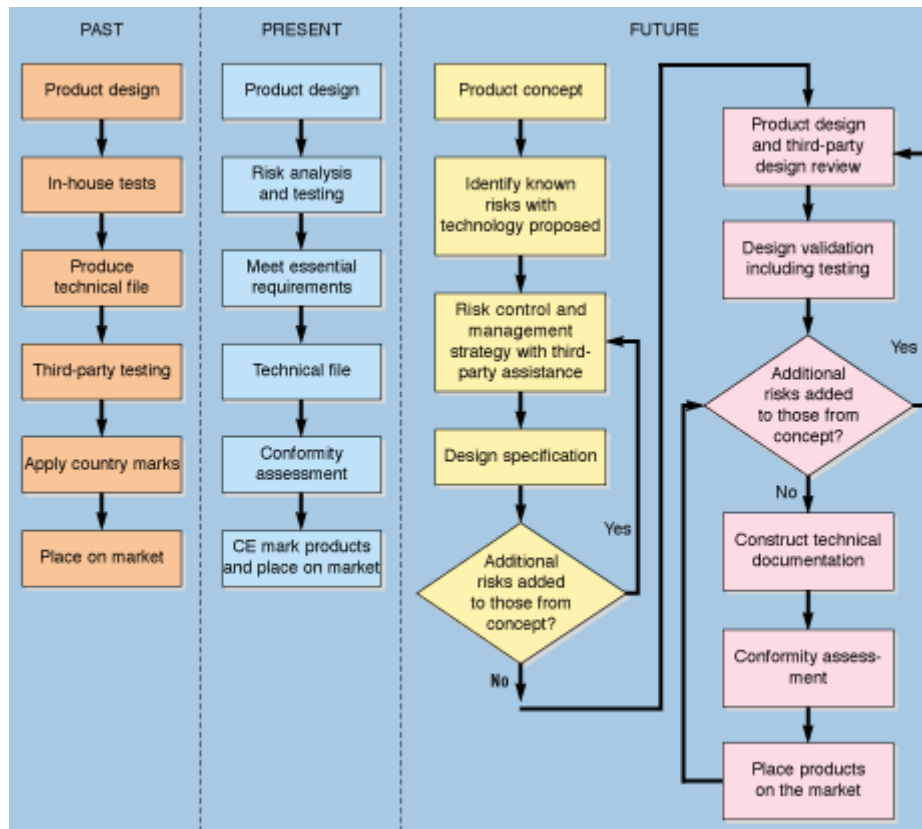


Figure 1. Routes to achieving market entry in the European Union.

Manufacturers adopting a risk-based strategy can expect the number of procedures that will be necessary to meet the requirements for entry into the global marketplace to increase, but the procedures themselves should become simpler (Figure 1). One of the major changes—and advantages—of risk-based compliance is that the manufacturer's design processes will become more visible to the regulatory agencies while proprietary information will be guarded from would-be competitors. Risk-based approaches tend to be procedures. These procedures become part of a quality system, which is audited by regulatory agencies or notified bodies.

Getting Started

Companies that are reorienting their approach to ensuring product safety with a risk-based strategy need to understand its underlying principles, which are listed below.

- Eliminate or reduce risks as far as possible. Any remaining undesirable side effect must constitute an acceptable risk when weighed against the performance intended.
- Protect products, end users, and operators against risks resulting from the influence of environmental conditions that are reasonably foreseeable (e.g., electromagnetic fields).
- Where appropriate, integrate protective measures such as alarms and interlocks into the design to mitigate risks that cannot be eliminated.
- Inform users of the residual risks associated with failures of the protective measures.
- Clearly define the product's intended use and reflect that use in the labeling and other instructions.
- Clearly and unambiguously document the process of determining what risks were considered to be "reasonably foreseeable." Seek outside assistance, if needed, from clinical experts.
- Wherever possible, use technical consensus standards to verify that the identified risks have been minimized during the design phase.

Logistics: Manpower and Timing. The fundamental task of risk analysis is to identify foreseeable hazards and tabulate them against their probability and severity, which will give a value for criticality. Critical and high-level risks can then be addressed and eliminated.

Adopting this approach affects two key operational logistics—who is involved in the process and when it takes place. In terms of manpower, the company needs to dedicate sufficient personnel with the necessary skills to perform the risk analysis. Compliance engineers must understand risk identification, control, and management, while designers may need to focus their attention on ergonomics, safety, and functionality in a new way.

As for timing, the risk analysis process should begin as early as possible in the product development cycle. The earlier hazards are identified and addressed, the greater the chances for successfully minimizing risk.

Establishing a Risk Analysis Team. A risk analysis team consisting of the following members could direct the risk management process.

- A risk analysis manager with responsibility for ensuring that the analysis is performed in a structured and purposeful manner. Ideally, the manager should be very familiar with the tools used to perform a risk analysis and have a general understanding of the product being analyzed, as well as a working knowledge of the relevant technical standards.
- A project manager with responsibility for ensuring that any necessary complementary studies are performed and that preventive measures and other design changes are implemented.
- A designer whose task is to describe the functionality of the product to the group prior to the risk analysis of each function block.
- One or more independent engineers who are familiar with the product type in technical respects, but have not been involved in developing the design specifications. The

independent engineers are included on the team to provide advice on design improvements and changes.

- Marketing personnel may also be included on the team to convey user needs, and quality and customer service staff may be consulted regarding the complaint history of similar products.

Defining the Project. Once the team is in place, the analysis process begins by defining the object to be analyzed, its intended purpose, and the types of risks to be analyzed. All of the possible risks associated with, or related to, the product or any of its parts are then analyzed. Among the factors that should be considered at this early stage of the process are areas where the product interfaces with the human body and with other equipment or modules. The operating environment must be fully defined, including temperature, humidity, barometric pressure, dust or contaminant ingress, electromagnetic compatibility, and voltage supply.

Risk Analysis Tools

Each of the three major risk analysis tools focuses on a different aspect of risk, but they are all used to achieve the same end result—a product with risks that are as low as reasonably possible (ALARP). It is the responsibility of the risk analysis team to identify which method or methods are most appropriate. Obviously, if a product is simple the level of risk analysis can be lower than that for a complex product. There is no right or wrong analytical method. However, it is often safer to analyze the same product using various tools to minimize the chance of something being overlooked. Whichever methods are used, the results become the basis for efforts to mitigate the probability and severity of product-related risks.

FMECA versus FMEA. Failure mode effects and criticality analysis (FMECA) is a more involved process than failure mode and effects analysis (FMEA), which is widely used today in industry as a "what if" process. The difference is that FMECA attaches a level of criticality to the failure modes so that redesign efforts can be prioritized and assigned to appropriate personnel in a consistent manner.

FME(C)A						
System/Devices:				Date:		
Participants: _____				Page () _____		
Subsystem	Function	Failure Mode	Effect/Consequence	Probability	Consequence	Comments

Figure 2. Example of a failure mode effects and criticality analysis form.

FMECA begins by breaking down the product into individual function blocks using a tree structure. One way to do this is to create a block diagram of the product, or of the processes associated with the production of the product, or both. The breakdown is documented, and an FMECA form (Figure 2) is then filled in for each of the function blocks. In addition to columns for identifying the subsystem (i.e., function block) and its function, the FMECA form contains the following columns:

- Failure mode: How might the subsystem fail? Possible failure modes include component failure (e.g., open circuit, short circuit, etc.), handling failure, design failure, component aging or wear, environmental impacts, and incorrect use.
- Effect/Consequence: What will happen when the failure mode occurs? The scenario should be described, including the presence and effects of indicators or alarms.

- Probability: How likely is this failure mode to occur?
- Consequence: What effect will the failure have on the user, operator, or product (e.g., electric shock, fire, none, etc.)?
- Comments: What specific additional information regarding the above items is important to note? Preventive measures should be documented, and relevant standards cited. Possible additional measures to lessen the severity or probability of the failure can also be documented.

As part of the failure mode analysis, the criticality of the failure modes is calculated in terms of severity and probability. The severity level (*se*) is a measure of the possible consequences of a failure and can be expressed using a numerical scale. For example, death can be rated 10 and a malfunction that has no direct effect on the operator or user could be given a 1, with various levels of discomfort and injuries ranked between them. The scale should not be so large that it is difficult to distinguish one level from another or so narrow that it becomes insensitive to differences between effects. The probability level (*pr*) is the estimated likelihood of a failure occurring within a time period or under certain circumstances. It also can be expressed on a scale of 1 to 10 and is usually based on data from previous models or similar products for which failures and their causes have been documented. Criticality (*cr*) is calculated by multiplying the severity by the probability: $cr = se \times pr$. Risks with a high criticality value require an in-depth consideration of design solutions, as do those with high severity and probability levels alone.

Fault Tree Analysis. Using the FMECA process, the risk analysis team can determine the effects of single subsystem failures; however, the effects of combined failures are difficult to identify. Fault tree analysis (FTA) is used to examine such linkages. Based on the possible harm a product can cause, FTA begins by stating how a user or operator is affected. The effect may be death or serious injury (something that the user or operator is unlikely to recover from), moderately serious injury (something, although painful or extremely uncomfortable or debilitating, that the user or operator will recover from eventually), or negligible injury (something that the user or operator will recover from in a very short time). More levels can be added to make the analysis more sensitive.

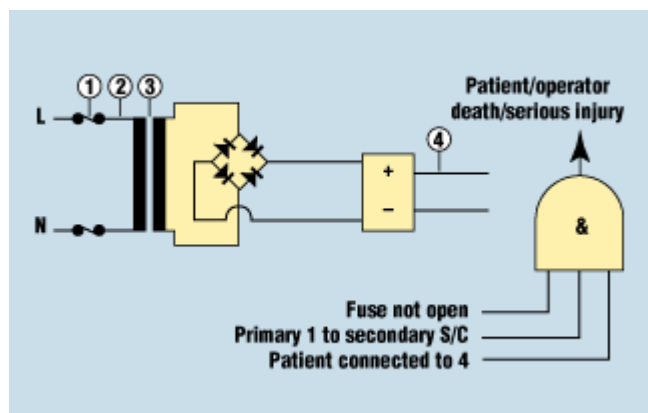


Figure 3. Example of a fault tree analysis for a simple circuit.
The three events linked by the AND gate must all occur to trigger the potentially fatal effect.

The next step is to establish what combination of events would lead to the various effects. The risk analysis team graphically depicts situations and failures that jointly or individually cause injury using logical operators such as AND and OR gates (Figure 3). An AND gate indicates that several events must happen simultaneously in order for the failure to occur further up in the tree, whereas an OR gate indicates that one or several events can occur independently of one another. Naturally, AND gates are preferable.

The number of simultaneous events that need to occur in an AND junction can assist in calculating probability. The finished tree will show where the risks are and which base events must interact in order for each risk to arise. The FTA for a simple circuit shown in the figure indicates which three events must happen simultaneously for the user or operator to receive a fatal shock.

Action Error Analysis. Another risk measurement tool, known as action error analysis (AEA), analyzes interactions between humans and machine. Its purpose is to provide answers about what happens if an operator does something right but at the wrong time, or does the wrong thing at the right time, or does nothing at all. An AEA can be used to analyze product start-up procedures and to discover deficiencies in instructions for performing multiple product actions.

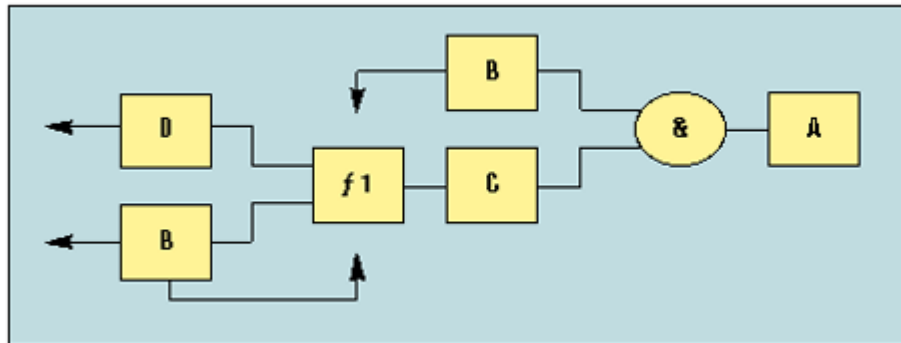


Figure 4. Example of an action error analysis event tree.

Figure 4 provides an example of an event tree used in AEA. The top event is A on the far right. The AND gate indicates that in order for it to occur, events C and B must occur simultaneously. However, for event C to occur, either or both B and D on the lower level must occur. The symbol at the entry to event D indicates that this event corresponds to the lowest level of the tree; the symbol at the entry to event B indicates that the events that cause B to occur are found on another tree. The out arrow at the bottom of the box indicates that event B is found in other places on the same tree, in which case Boolean algebra is used to derive the minimum set.

Conclusion

Manufacturers interested in changing their approach to product safety must keep in mind that in today's current environment testing to standards still prevails as the recognized, in most cases required, means of demonstrating product safety. There's no question that adopting a risk-based approach to product safety will bring changes to the industry. As harmonization continues, this concept will undoubtedly spread and products will increasingly be judged against product risk.

From a logistical standpoint, manufacturers will need to assemble risk analysis teams who understand the principles and procedures of a risk-based approach. Product development schedules will need to be altered so risk analysis can be performed as early as possible in the design process, enabling designers to make modifications that will eliminate or mitigate risks.

In the end adopting a risk-based approach can result in the design of superior products that lessen the risk of failure and injury, reduce liability, and protect brand. Regulatory authorities throughout the world continue to develop harmonized standards that incorporate risk analysis procedures. Organizations who have implemented these principles well in advance will certainly gain a global competitive edge.

For more information on how to implement a risk management strategy or for more specific testing and certification information, please contact Intertek at 1-800-WORLDCON, email icenter@intertek.com, or visit our website at www.intertek-etlsemko.com.

Bibliography

Analysis Techniques for System Reliability—Procedures for Failure Mode and Effects Analysis (FMEA), IEC 60812. Geneva: International Electrotechnical Commission (IEC), 1985.

Dependability Management—Part 3: Application Guide—Section 9: Risk Analysis of Technology Systems, IEC 60300-3-9. Geneva: IEC, 1995.

Fault Tree Analysis (FTA), IEC 61025. Geneva: IEC, 1990.

Medical Devices—Risk Analysis, EN 1441. Brussels: European Committee for Standardization, 1998.

Medical Devices—Risk Management, Part 1: Application of Risk Analysis, ISO/DIS 14971-1. Geneva: International Organization for Standardization (draft).

Medical Electrical Equipment, Part 1: General Requirements for Safety, Section 4: Collateral Standards: Safety Requirements for Programmable Electronic Medical Systems, IEC 60601-1-4. Geneva: IEC, 1993.

About Intertek

Intertek does more than simply help our clients comply, we give them the competitive advantage they desire. Our solutions offer comprehensive services including, product testing and analysis, certification and corporate education appropriate for all types and levels of business. Intertek is a leader in global environmental compliance, technology services and product stewardship.

We provide quality and safety solutions to a wide range of industries, through a network of 24,000 people in 1000 laboratories and offices in 100 countries around the world. Through our global network of labs, Intertek can test and certify your products to meet British, European and North American codes and standards, including ANSI, ASTM, CSA, EPA, ICBO, UL, and ULC. We offer manufacturers access to some of the most recognized safety certifications in the world. Our WH (Warnock Hersey) Mark for building products is recognized among industry leading manufacturers and code officials across North America and around the world. Our ETL Mark for electrical/electronic products is the fastest growing safety certification mark in North America, widely accepted by AHJs and building code officials.

The next step

Call or e-mail Intertek to get expert advice on validating your “Green Claims” and learn more on participation in the Environmental Certification Program for Building Products:

- Phone: 1 800 WORLDLAB
- Email: icenter@intertek.com
- Web: www.intertek.com

This publication is copyright Intertek and may not be reproduced or transmitted in any form in whole or in part without the prior written permission of Intertek. While due care has been taken during the preparation of this document, Intertek cannot be held responsible for the accuracy of the information herein or for any consequence arising from it. Clients are encouraged to seek Intertek's current advice on their specific needs before acting upon any of the content.