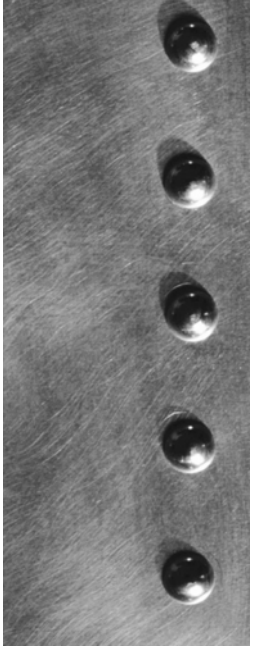

EXECUTIVE SUMMARY

Risk Assessment: Basics and Benchmarks

Written by: Bruce W. Main, PE, CSP

Everyone is busy. This overview summarizes the most significant points of the book for the reader in a hurry. In addition, many chapters include a summary of the key points at the beginning of those chapters.

This book was written to help introduce, explain and describe the basics of the risk assessment process, and to identify risk assessment benchmarks currently in use worldwide. More specifically, the book:

- discusses the basics of the risk assessment process;
- presents practical applications of implementing risk assessment in industry;
- provides numerous benchmarks on risk assessment activities across several industries and applications;
- compares the benchmark methods; and
- presents a roadmap for those seeking to develop an improved risk assessment process including eight principles for improvement.

Many other authors have written excellent works on the topic of risk assessment. Often the authors are specialists in one industry or method. This book draws on many of these works and extends the discussion by examining the risk assessment methods used across different industries.

SECTION I – BASIC CONCEPTS

The first section of this book reviews the basics of the risk assessment process including how it is a fundamental consideration in safety through design. Readers will find basic concepts about the different kinds and sources of risk, safety through design, and how risk assessment improves safety through design.

There are many forces pushing safety through design including: costs, competition, quality, international influences, legal requirements, the desire to capture knowledge and the costs of retraining engineers. In general, there is considerable support that safety needs to be addressed during the design process rather than as a retrofit activity, and risk assessment pushes safety into the design process. However, an engineer's ability to integrate safety into the design process is limited by the training and education he or she has received.

The goal of risk assessment is to reduce risks to an acceptable (or tolerable) level. A zero risk level is not attainable. A chapter is included on acceptable risk and how to make decisions about accepting residual risks. An argument is made that the terms "acceptable" and "tolerable" risk should be considered synonyms within the risk assessment process. Efforts to distinguish these terms can lead to inadvertent errors, even by organizations that wish to promote a difference in the terms. The terms are used synonymously in this book.

Risk reduction efforts to achieve acceptable risk must work within the real world constraints of feasibility, practicality and cost. Resources are always limited. Cost is an important factor in obtaining acceptable risk. A practical solution to achieving acceptable risk is a good faith application of the hierarchy of controls within the risk assessment process. This approach, coupled with the As Low As Reasonably Practical (ALARP) framework, are useful guides in reducing risks to an acceptable level.

Any organization discussing risk and risk assessment needs a common understanding of the applicable terms. Terms used in the risk assessment process are defined in Appendix A. Many terms have more than one meaning. Be certain that the risk assessment team is working with a common definition.

Risk assessments are conducted primarily to help in the decision-making process. Decisions on the adequacy of a design usually occur during a design review. Risk assessment supports the design review process by providing the underlying analysis on which safety decisions can be made. Risk assessments take time to conduct effectively, typically more time than can occur within a design review session. In most cases the assessment should occur separately from the design review. The design review process and the role of risk assessments are examined in this section.

Corrective actions that may be taken to introduce or improve safety through design efforts include formalizing existing but informal design processes that include elements of risk assessment, acquiring tools and training to conduct risk assessments, and advocating training on safety through design.

SECTION II – PRACTICAL GUIDANCE ON RISK ASSESSMENT

Section II is written for the practitioner who must actually conduct a risk assessment. When all is said and done, someone needs to get his or her hands dirty and actually do the risk assessment. This section focuses on the practical application of the risk assessment process and examines applications where risk assessments have actually been used. Individuals who are new to risk assessment will find Section II a resource for getting up to speed quickly on the different options available and the means to introduce and implement risk assessments.

The step by step basics of the risk assessment process appear in Section II. Although many companies and industries use different risk assessment methods, the fundamentals of the risk assessment process are common:

- identify hazards,
- assess risk,
- reduce risk, and
- document the results.

A general risk assessment process describes the seven basic steps in completing a risk assessment. One step in particular, identifying hazards, is critical because if hazards are omitted the associated risks will remain unknown. A task-based approach to identifying hazards has been shown to be very effective and is recommended where applicable.

Several practical, real world applications of risk assessment demonstrate the risk assessment process and the results drawing on the author's experiences in conducting risk assessments in industry. The examples include work process designs, product designs, and interactions with government authorities in different industries. A detailed risk assessment of a student design for a medical device is included to illustrate the risk assessment process, and how the process can be successfully introduced to engineering design classes. An example from the food industry is presented that illustrates a risk assessment failure. Common themes are discussed including that risk assessment offers a flexible tool that can be applied to many different situations.

Integrating risk assessment in an organization is a process that generally follows a sequence of phases. A typical sequence is discussed. To be effective, the company culture must be willing to embrace the risk assessment process, and cultural acceptance stems from management leadership. Engineering design needs to change to include the risk assessment process to more effectively move safety into design. Only by changing the design process will risk assessment efforts succeed. Issues such as changing the design process to include risk assessment are critical to address for the risk assessment effort to be successful in a company. As with any new process or substantive change, people may resist. Guidance is shared on how to change the design process to include risk assessment, and what resistance may be encountered in doing so.

A team of interested persons should conduct the risk assessment. The team members can be drawn from several areas such as engineering, operations, safety, users and others. They may include different participants as the assessment evolves. To integrate risk assessment into the design process engineers will likely need education and training on risk assessment in some form.

Unfortunately, most engineering design efforts do not currently include formal risk assessments. Engineering design must include the risk assessment process to more effectively move safety into design. Introducing the risk assessment process will explicitly change the design process, allowing hazards to be identified and risk reduction methods to be incorporated early in the design process. If the design process does not change, long term efforts to improve worker and product user safety will fail even if risk assessments are deployed.

Risk assessment does have limitations. Several limitations are discussed in order to minimize unrealistic expectations. Successfully integrating the risk assessment process into an organization requires time and effort.

In consumer product and component product applications, the manufacturer is responsible for conducting the risk assessment, if applicable. Product users typically have no risk assessment responsibilities beyond using the product in conformance with the product information. In industrial product or process applications, both equipment suppliers and users should perform risk assessments and be involved in the risk assessment process.

This section provides tips and guidance on how to most effectively introduce the risk assessment process to an organization, and how to conduct them thereafter. Practical guidance is shared to help companies get started and make progress in the risk assessment process. Topics addressed include: the time to complete an assessment, forming a team, what to expect, when to stop a risk assessment, what to do in cross industry situations, when to revise an existing risk assessment, making changes to the protocol, results of risk assessment, and others.

"Risk scoring system" is the term that describes how risks are assessed. There are many variables, factors and combinations that must be considered in selecting a risk scoring system, and these are examined in detail in the book. Since there are many different systems used to arrive at risk levels, a chapter on risk scoring systems presents the different variables that are used to rate risk. The three most common types of risk scoring systems are qualitative, semi-quantitative and quantitative. A discussion explains the variables that make up a risk scoring system and how to make decisions between different systems.

Given the subjective nature of rating risk, risk scoring systems will likely continue to emerge and proliferate as users refine and improve their risk assessment process. This divergence of methods should be considered healthy. In time, convergence to one or a few risk scoring systems may occur as efforts to harmonize and standardize risk assessment methods occur. This process will require some time.

SECTION III – BENCHMARKS

Section III of the book examines the many benchmarks methods that exist today from a variety of industries and applications. A very broad cross section of methods documents the current state of the art and wealth of activity in the risk assessment process. Often more than one approach appears within an industry. This section permits readers to identify the similarities and differences in the different benchmark methods. Both novices and specialists should find useful information in this section. Those who are familiar with the risk assessment process will find Section III useful to identify the depth and breadth of current risk assessment activity.

The benchmark methods are presented based on publicly available documents. Although the benchmarks presented include great breadth, the compilation by its nature is not exhaustive.

Risk assessment methods are being deployed in many industries, and that the momentum will likely continue. Performance-based standards have been a key driver in the growth of risk assessments because they are the primary means to demonstrate that risks have been reduced to an acceptable level. Although the level of sophistication varies from industry to industry and within industries, the general risk assessment process applies across all industries and applications.

SECTION IV – IMPROVING THE RISK ASSESSMENT PROCESS

Section IV contains an analysis and comparison of the different risk assessment benchmarks presented in Section III. Section IV is written for the advanced reader who is dissatisfied with his or her current risk assessment method, is interested in improving the risk assessment process, or seeks to harmonize the risk assessment process.

A chapter compares the different benchmark methods and draws conclusions concerning the differences and similarities among them. A chapter also compares a risk assessment approach to other safety analyses used to assess risk. Note that the risk assessment process comprises only one method to identify hazards, assess risks and reduce residual risks. Other methods have value and should be used as appropriate.

A heated debate often occurs when discussing the issue of documenting risk assessments. There remains considerable resistance to creating risk assessment documents from the legal community primarily due to product liability concerns. However, good engineering practice, continuous improvement and risk assessment requirements all push for documenting risk assessments. Documenting the risk assessment process is required or recommended by every guideline, standard or technical description of risk assessment. Therefore, a chapter explores the arguments for and against documenting a risk assessment.

There are many variations in risk scoring systems because different risk scoring systems work well in different applications. There are many risk scoring systems in use, each offering its strengths and weaknesses. This variation reflects the great diversity of opinion on risk assessment. Some of the most significant differences between risk assessment methods used today involve how risk is assessed. There is a continuum of risk scoring systems from qualitative to quantitative that effectively address a variety of risk assessment applications. Very few benchmarks use quantitative risk scoring systems. However, there is no indication that any particular risk scoring system is better than another for all applications.

One of the most critical considerations in selecting an approach to risk assessment is logistics. In many instances logistics can be the overriding criteria due to implementation challenges that arise. The costs and logistics of performing quantitative risk assessments are prohibitive in many industries. In these applications new methods, approaches, or software tools may be needed rather than those developed for the sophisticated situations. With the level of activity occurring today in risk assessment, there remains plenty to learn.

In many instances an individual or organization starts with an existing risk assessment method and finds it to be lacking in one or more respects. Thus begins a search for a better method. The search can take one of two paths – look for other methods and adopt all or part of them, or modify the existing approach to create a method better suited for the application. Chapters in this section provide a framework readers can use as they explore options for a better method. The benchmarks of Section III provide a wealth of information to start researching other methods and from which the search can be quickly narrowed. Although no specific solution is proposed, the different variables that can be adjusted and the implications of doing so are discussed.

Section IV also looks at international initiatives to harmonize the risk assessment process and offers some suggestions on aspects that are well-suited and less well-suited for harmonization. There are several reasons for and against harmonizing the various risk assessment methods. Although both viewpoints have merit, some basic steps toward harmonization appear achievable. However, complete harmonization is not likely to occur soon.

If a harmonized risk assessment process is to be developed, flexibility will be a critical factor to its success. Although most standards specifically seek to avoid flexibility, a harmonization effort will likely fail unless a standard framework can be provided that permits flexible application of the details.

There appears to be very little value in attempting to compare the results of risk assessments from vastly different applications to one another. Such comparisons provide no useful information to achieving acceptable risk. Since the goal of the risk assessment process is achieving acceptable risk, the risk assessment method one uses to attain this goal is less important than achieving the goal.

Based on the Benchmarks of Section III and the analyses in Section IV, a chapter presents the following eight principles for improving the risk assessment process.

PRINCIPLE #1 MINIMIZE THE USE OF LABELS

The use of labels to describe portions of the risk assessment process need to be minimized. The terms used in assessing risk can be very confusing. There exists confusion or at least no common understanding as to the meanings of the following terms:

- Risk assessment
- Risk analysis
- Risk estimation
- Risk evaluation

The term “risk assessment” can mean the specific steps related to calculating a risk level, an overall term for the entire process, or to refer to any method that assesses risks. Efforts at harmonizing, standardizing or even communicating are severely hampered by the current confusion and different uses of the term “risk assessment” and others.

The practitioner trying to conduct a risk assessment does not care about terms or labels. He or she just wants to know what they need to do to complete the risk assessment. Extra terms detract from this objective. Unnecessary terms that add no value should be removed from the risk assessment process. Labels that provide no value only add confusion.

PRINCIPLE #2 SIMPLIFY THE RISK ASSESSMENT PROCESS

Use Active Verbs

The steps of the risk assessment process should be written using active verbs rather than labels or titles.

Simplify the Steps

The steps of the risk assessment process need to be simple and straightforward, and provide the reader very clear direction on what he or she needs to do. There are many instances where clear direction is lacking or the steps are unnecessarily confusing or ambiguous. Simplifying the risk assessment process by using active verbs and clear and simple steps will assist those engaged in conducting risk assessments.

PRINCIPLE #3 ADOPT "RISK ASSESSMENT PROCESS" AS THE OVERALL TERM

The term "Risk Assessment Process" should be adopted to describe the overall process of identifying hazards, assessing risk, and reducing risk.

The terms "risk analysis," "risk assessment," "risk management" and others have different definitions depending on the industry using them. The two most frequently used terms to describe the overall risk assessment effort are "risk assessment" and "risk management." Although arguments can be made for either term, the use of "the risk assessment process" seems the best for referring to the overall process of identifying hazards, assessing risks, and reducing risks.

PRINCIPLE #4 THE RISK ASSESSMENT PROCESS INCLUDES RISK REDUCTION

There is no point in assessing the risks of a system, design, process or product unless one plans to perform risk reduction. The risk reduction effort is always completed even though not every residual risk requires further risk reduction (the risk may already be acceptable). This implies that risk reduction is a necessary part of, and should be included in, the overall risk assessment process regardless of the term used to describe that overall process.

Although other documents, guidelines and standards argue that risk reduction is not included in risk assessment, from the perspective of a person tasked with conducting a risk assessment in industry, separating risk assessment and risk reduction makes little sense. Separating risk assessment and risk reduction may make sense for government agencies or other organizations that are not involved with, or responsible for, the risk reduction effort. However, for persons in industry risk reduction is an integral part of the risk assessment process.

PRINCIPLE #5 ADOPT THE RISK ASSESSMENT PROCESS FLOW CHART

Figure 1 presents the risk assessment process incorporating Principles #1-4. This figure should be adopted because it simplifies the process and reflects how risk assessment is conducted in industrial practice.

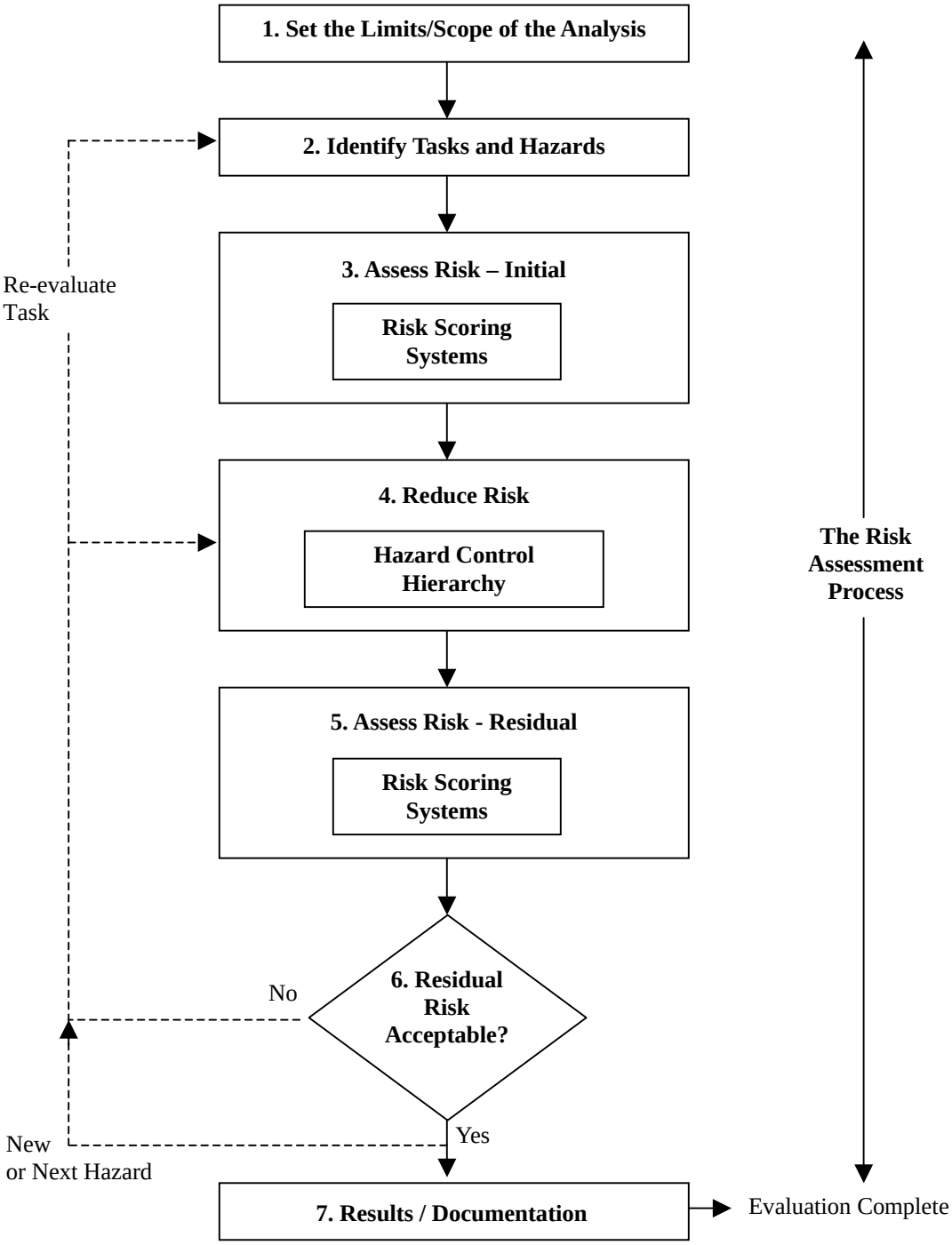

Figure 1 – The Risk Assessment Process

PRINCIPLE #6 SUBJECTIVE JUDGMENT NEEDS TO BE ACCEPTED

Subjectivity is a necessary part of risk assessment. Even in quantitative risk assessments subjective judgment occurs. However, the subjectivity does not diminish the value or credibility of the risk assessment process. Safety is not an absolute state, but a relative one. Engineers, safety practitioners and decision makers need to become comfortable with subjectivity, and recognize that the subjective risk assessments do offer value.

PRINCIPLE #7 ACCEPT UNCERTAINTY

Uncertainty is an integral part of all the risk assessment benchmarks in Section III, whether explicitly addressed or not. Uncertainty enters risk assessment as assumptions, estimates and subjective judgments. Even in quantitative assessments there often remains substantial uncertainty. Risk is uncertain. Performing a risk assessment does not create the uncertainty. Uncertainty is, and should be accepted as, an integral part of the risk assessment process.

PRINCIPLE #8 DEFINE “RISK ASSESSMENT”

Very different definitions of the term “risk assessment” exist. The two primary differences tend to be whether the term is used as a verb to mean any method used to assess risk (such as FMEA, What if, HAZOP, Fault Tree Analysis, and others), or used as a noun to refer to a specific type of analysis. No current consensus exists in this regard. It could be very difficult for those seeking to harmonize the various risk assessment methods to make significant progress until some agreement is reached on the definition of the term. Engineers, safety practitioners, risk assessment teams, and standards writing committees need to develop a common definition within their working group(s).

CLOSURE

The current state of the art is such that most companies are not performing formal risk assessments, but this is changing. The leaders in risk assessment tend to be the companies actually performing them rather than any particular industry, country or standard.

The preceding principles focus on simplifying the risk assessment process, improving it to reflect current practices in industry, and advancing deployment of the risk assessment process. The team conducting the risk assessment needs to quickly come to a common understanding of the terms it uses, its goals and objectives, and the process to attain them. These eight principles should assist.