1

RISK ASSESSMENTS: THEIR SIGNIFICANCE AND THE ROLE OF THE SAFETY PROFESSIONAL

FRED A. MANUELE

Hazards Limited, Arlington Heights, IL, USA

1.1 OBJECTIVES

- Introduce developing trends in the use of operational risk assessments
- Provide a broad overview of standards and guidelines requiring risk assessment
- Emphasize the importance of risk assessment in the safety profession

1.2 INTRODUCTION

Throughout the world, there has been a proliferation of activity resulting in provisions being included in safety standards, guidelines, and operational risk management systems requiring or promoting that risk assessments be made. This trend has had an impact on the knowledge and skills that safety professionals are required to have in their employment. It will also provide career enhancement opportunities and job satisfaction for them.

Working with design and operations personnel to assess risks and to give counsel in the decision making to achieve acceptable risk levels adds an easily recognized value. Imaginative safety professionals will recognize this opportunity to be additionally perceived as members of the management team and increase their value to their organizations.

An addendum for this chapter consists of a list of standards, guidelines, and initiatives that require or promote making risk assessments. To avoid having the list become overly lengthy, 2005 was selected as the year to commence recordings. Although data is included for 35 subjects, it is more than likely the list is not complete.

To provide guidance for safety professionals on the trending throughout the world on requirements for risk assessments and recognition of the need for safety professionals to have risk assessment capability, this chapter will comment on the following:
• Activities initiated by the American Society of Safety Engineers (ASSE)
• A guideline that gives risk assessment high priority within an operational risk management system
• Selected standards and guidelines to demonstrate
  • the pace and import of recent activity;
  • the variations in content for risk assessments in the standards and guidelines;
  • specificity or, lack thereof, in their content.

There are similarities and differences in the approaches taken by the drafters of these standards and guidelines. Some are industry specific. Others apply across all industries. The message they give is clear: Safety professionals will be expected to have knowledge of a variety of hazard analysis and risk assessment methods and how to apply them.

1.3 WHAT IS A RISK ASSESSMENT?

Two definitions, taken from standards, are presented here. Their interrelationship is obvious. In the introduction for ANSI/ASSE Z690.3-2011 – Risk Assessment Techniques (nationally adopted from IEC/ISO 31010:2009), this is the guidance given.

Risk assessment is that part of risk management which provides a structured process that identifies how objectives may be affected, and analyzes the risk in term of consequences and their probabilities before deciding on whether further treatment is required. Risk assessment attempts to answer the following fundamental questions:

• What can happen and why (by risk identification)?
• What are the consequences?
• What is the probability of their future occurrence?
• Are there any factors that mitigate the consequence of the risk or that reduce the probability of the risk?
• Is the level of risk tolerable or acceptable and does it require further treatment?

ANSI Z690.3-2011 is an adoption of IEC/ISO 31010:2009. Additional comments will be made about this standard, and of Z590.3, later.

ANSI/ASSE Z590.3-2011 is the standard for Prevention through Design: Guidelines for Addressing Occupational Hazards and Risks in Design and Redesign Processes. This is its definition of risk assessment:

**Risk Assessment.** A process that commences with hazard identification and analysis, through which the probable severity of harm or damage is established, followed by an estimate of the probability of the incident or exposure occurring, and concluding with a statement of risk.

As described in more detail later, risk assessment is a fundamental component of the risk management process and an essential core competency for safety professionals. Examples follow that provide clear indications of the rising importance given to risk assessment.

1.4 ACTIVITIES AT THE AMERICAN SOCIETY OF SAFETY ENGINEERS (ASSE)

Several officers of ASSE had recognized that requirements for risk assessment were more frequently included in safety-related standards and guidelines and that ASSE should provide its members with educational opportunities through which the necessary skills could be acquired. A presentation on the
subject was made at the February 2013 board of directors meeting, the outcome for which was the creation of the Risk Assessment Institute.

A committee was formed and its members are working on literature, videos, webinars, and other materials that could be presented at chapter meetings and at conferences. The significance of this activity is that awareness had developed among the leaders of a technical organization with an international scope that its members would be well served if they were provided means to acquire risk assessment skills. This is an important step forward for the practice of safety. The Risk Assessment Institute website can be accessed at http://www.oshrisk.org/.

1.5 AN EXAMPLE OF A GUIDELINE THAT GIVES RISK ASSESSMENT DUE RECOGNITION

Entering “ExxonMobil’s OIMS” into a search engine will lead to a brochure on ExxonMobil’s Operations Integrity Management System. Within that brochure, there is a depiction of its OIMS arrangement. An adaptation of it follows in Figure 1.1.

Element 1 in this 11-point outline is what would be expected – management leadership, commitment, and accountability. But note that risk assessment and management follows item 1 immediately. That is an indication of the importance given to risk assessment within ExxonMobil operations.

And facilities design and construction follows risk assessment. In the design and redesign processes, risk assessments would be made continuously as needed.

Safety professionals should not be surprised if other companies produce similar outlines as greater recognition develops that the most effective and economical method to deal with hazards and risks is to address them in the design and redesign processes.

ExxonMobil’s OIMS initiative pertains to all operational risks, including occupational, environmental, product, and public safety. An example is given later in this chapter of an activity that also combines occupational and environmental safety.
1.6 ANSI/AIHA/ASSE Z10-2012: THE STANDARD FOR OCCUPATIONAL HEALTH AND SAFETY MANAGEMENT SYSTEMS

This standard continues to gain recognition as a sound outline for an occupational safety and health management system. In the first version of Z10, approved in 2005, management was required to have processes in place: “To identify and take appropriate steps to prevent or otherwise control hazards and reduce risks.” While that verbiage may have implied that risk assessments were to be made, that is as close as the original version of the Z10 standard got to promoting risk assessments. A specific requirement that risk assessments be made was not included in the original standard.

Thinking changed. The 2012 version of Z10 has a “shall” provision on risk assessment at 5.1.1. It says:

The organization shall establish and implement a risk assessment process(es) appropriate to the nature of hazards and level of risk.

Safety professionals should recognize the significance of this revision. It reflects the awareness developed by the writers of the standard that making risk assessments should be an element within a safety and health management system.

1.7 ANSI/ASSE Z590.3-2011: PREVENTION THROUGH DESIGN: GUIDELINES FOR ADDRESSING OCCUPATIONAL HAZARDS AND RISKS IN DESIGN AND REDESIGN PROCESSES

This standard was approved by the American National Standards Institute on September 1, 2011. The core of Prevention through Design is risk assessment. Making risk assessments early in the design and redesign processes and continuously as needed throughout the life cycle of the system or product reduces the potential for incidents occurring. Logic in support of that premise follows:

1. Hazards and risks are most effectively and economically avoided, eliminated, or controlled in the design and redesign processes.

2. Hazard analysis is the most important safety process in that, if that fails, all other processes are likely to be ineffective (Johnson – p. 245).

3. Risk assessment should be the cornerstone of an operational risk management system.

4. If, through the hazard identification and analysis and risk assessment processes, specifications are developed that are applied in the procurement process so as to avoid bringing hazards and their accompanying risks into a workplace, the potential for injuries occurring is reduced greatly.

5. The entirety of purpose of those responsible for safety, regardless of their titles, is to manage their endeavors with respect to hazards so that the risks deriving from those hazards are acceptable.

The practice of safety is hazard based. Thus, Johnson wrote appropriately that hazard analysis is the most important safety process. Since all risks in an operational setting derive from hazards and since the intent of an operational risk management system is to achieve acceptable risk levels, it follows that risk assessment should be the cornerstone of an operational risk management system.

Figure 1.2 depicts the theoretical ideal. Prevention through Design is moved upstream in the design process. The intent is to have hazards and risks analyzed and dealt with in the Conceptual and Design steps. But, that requires unattainable perfection from the people involved. Hazards and risks will also
be identified in the Build and Operation and Maintenance steps for which redesign is necessary in a retrofitting process.

The hazard analysis and risk assessment process is the longest section in the Prevention through Design standard. First, an outline of the hazard analysis and risk assessment process is given. That is followed by the “how” for each of its elements. The outline follows:

- Select a risk assessment matrix.
- Establish the analysis parameters.
- Identify the hazards.
- Consider failure modes.
- Assess the severity of consequences.
- Determine occurrence probability.
- Define initial risk.
- Select and implement hazard avoidance, elimination, reduction, and control methods.
- Assess the residual risk.
- Risk acceptance decision making.
- Document the results.
- Follow up on actions taken.

For many hazards, the proper level of acceptable risk can be attained without bringing together complex teams of people. Safety and health professionals and design engineers having the experience and education can reach the proper conclusions on what constitutes acceptable risk. For the more complex risk situations, management should have processes in place to seek the counsel of experienced personnel who are particularly skilled in risk assessment for the category of the situation being considered.
Reaching group consensus is a highly desirable goal. Sometimes, for what an individual considers obvious, achieving consensus on acceptable risk levels is still desirable so that buy-in is obtained for the actions taken.

1.8 THE ANSI/ASSE Z690-2011 SERIES

Three American national standards that constitute a set should be of interest to safety generalists who want to become familiar with risk assessment techniques. The ASSE is the secretariat.

1. ANSI/ASSE Z690.1-2011: Vocabulary for Risk Management (National Adoption of ISO Guide 73:2009). This standard provides definitions of terms that, the originators hope, will be used in other standards.

2. ANSI/ASSE Z690.2-2011: Risk Management Principles and Guidelines (National Adoption of ISO 31000:2009). The intent of this standard is to provide a broad-range primer on risk management systems that could be applied in any type of organization. The requirement for risk assessments is introduced in Section 5.4: Risk Assessment.


ANSI/ASSE Z 690.3-2011, particularly, is a valuable resource. A list of the 31 risk assessment techniques follows. Some could be applied only by experienced safety professionals who had knowledge of system safety concepts and techniques. Other techniques would be used by probabilistic specialists. But knowledge of a few of them will serve for a huge percentage of the needs of a safety generalist.

B01 Brainstorming
B02 Structured or semi-structured interviews
B03 Delphi
B04 Checklists
B05 Preliminary hazard analysis
B06 Hazard and operability studies
B07 Hazard analysis and critical control points
B08 Environmental risk assessment
B09 Structure – What-If analysis
B10 Scenario analysis
B11 Business impact analysis
B12 Root cause analysis
B13 Failure mode effect analysis
B14 Fault tree analysis
B15 Event tree analysis
B16 Cause–consequence analysis
B17 Cause-and-effect analysis
B18 Layer of protection analysis
B19 Decision tree
1.9 ANSI B11.0-2015: SAFETY OF MACHINERY. GENERAL SAFETY REQUIREMENTS AND RISK ASSESSMENT – A STANDARD OF MAJOR CONSEQUENCE

Because of the breadth of its coverage, ANSI B11.0 has major importance. This is its stated purpose: “This standard describes procedures for identifying hazards, assessing risks, and reducing risks to an acceptable level over the life cycle of machinery.”

Note that its scope, as follows, has only one exclusion – portable hand tools: “This Type-A standard applies to new, existing, modified or rebuilt power driven machines, not portable by hand while working, that are used to process materials by cutting; forming; pressure; electrical, thermal or optical techniques; lamination; or a combination of these processes” (ANSI B11.0-2015).

The standard includes an explicit requirement that machinery suppliers, reconstructors, modifiers, and users achieve acceptable risk levels. ANSI B11.0 is the most comprehensive standard outlining the risk assessment process currently applicable to machinery for all of the operational categories just previously mentioned.

The foreword says “Prevention through Design or PtD is a recent term in the industry; the objectives of risk assessment, risk reduction and elimination of hazards as early as possible are integral to and not new to this standard.” This objective is also taken from the foreword:

*The objective of the B11 standards is to eliminate injuries to personnel from machinery or machinery systems by establishing requirements for the design, construction, reconstruction, modification, installation, set-up, operation and maintenance of machinery or machine systems. This standard should be used by suppliers and users, as well as by the appropriate authority having jurisdiction. Responsibilities have been assigned to the supplier (i.e., manufacturer, the reconstructor, and the modifier), the user; and the user personnel to implement this standard. This standard is not intended to replace good judgment and personal responsibility. Personnel skill, attitude, training and experience are safety factors that must be considered by the user.*

The following sentence appears in the foreword of ANSI B11.0-2015.

*This standard has been harmonized with international (ISO) and European (EN) standards by the introduction of hazard identification and risk assessment as the principal method for analyzing hazards to personnel to achieve a level of acceptable risk.*

That statement presents an interesting and weighty concept. If all safety professionals accept that hazard identification and risk assessment are the first steps in preventing injuries to personnel, a major concept change in the practice of safety will have been achieved.
Adopting that premise takes the focus away from what have been called the unsafe acts of workers and redirects the emphasis to making risk assessments in the design and redesign of work systems and work methods to achieve and maintain acceptable risk levels. In this author’s view, that is sound thinking.

1.10 EUROPEAN UNION: RISK ASSESSMENT

In August 2008, the European Union launched a two-year health and safety campaign focusing on risk assessment. Their bulletin (at http://osha.europa.eu/en/topics/riskassessment) says:

Risk assessment is the cornerstone of the European approach to prevent occupational accidents and ill health. If the risk assessment process – the start of the health and safety management approach – is not done well or at all, the appropriate preventive measures are unlikely to be identified or put in place.

The statement made by the European Union is seminal. Consider the significance of its campaign and its huge implications. The premise quoted recognizes the significance of risk assessment within an occupational safety and health management system, promotes the idea that the risk assessment process is where the management approach to safety should start, and specifically states that if risk assessment is not done well or not at all, the needed preventive measures are unlikely to be identified or taken.

The Europeans have been leaders in recognizing the importance of risk assessments and promoting their application. For example, employers in the United Kingdom are required to make risk assessments by law since 1999. Indications of other European involvement follow.

1.11 EN ISO 12100-2010: SAFETY OF MACHINERY. GENERAL PRINCIPLES FOR DESIGN, RISK ASSESSMENT, AND RISK REDUCTION

This standard, issued in 2010 by the International Organization for Standardization (ISO), has had an interesting history. It combines three previously issued ISO standards and replaces them. Note that “risk assessment and risk reduction” are included in the title. That is significant as it displays the status that risk assessment has attained in designing for the safety of machinery. The impact of this standard, worldwide, has been substantial.

ISO 12100-1 was titled Safety of Machinery. Basic Concepts, General Principles for Design – Part 1. It presented general design guidelines and required that risk assessments be made of machinery going into a workplace. ISO 12100-2 was titled Safety of Machinery. Basic Concepts, General Principles for Design – Part 2: Technical principles. Part 2 gave extensive detail on design specifications for the “safety of machinery.” ISO 14121 was titled Safety of Machinery. Principles of Risk Assessment. It set forth the risk assessment concepts to be applied. EN ISO 12100-2010 combines these three standards and retains their content.

EN ISO 12100-2010 is truly an international standard and has had considerable influence worldwide. Its existence implies that a huge majority of countries agree on the principle that hazards should be identified and analyzed and their accompanying risks should be assessed in the design processes for machinery.

The EN that precedes ISO in the title indicates that the origins of the standard were in the European Community. Several standards that were applicable in the European Community that had titles commencing with the EN designation became ISO standards. Some of the relative EN standards were written in the 1990s.
The European Community standards have had considerable influence on manufacturers throughout
the world. An example follows. Suppliers of products that are to go into a country that is a member
of the European Community are required to place a “CE” mark on the products to indicate that all
operable European Community directives have been met. Risk assessment provisions in EN ISO
12100-2010 are among those requirements.

1.12 ADDITIONAL EUROPEAN INFLUENCE

Other developments originating in Europe have also had a noteworthy impact throughout the world.
Comments on one that has achieved worldwide significance follow.

BS OHSAS 18001: 2007 is the designation for a guideline titled Occupational Health and Safety
Management Systems – Requirements. It is a British Standards Institution publication. In some con-
tract situations, particularly in Asian countries, a bidder for a contract is required to establish that its
safety management system has been “certified.”

Among other things, the British Standards Institution has attained prominence as a certifying entity
and 18001 is the base upon which certification is granted or withheld. In a 2007 revision of 18001,
requirements for risk assessments became more explicit. The guidelines now say in 4.3.1:

The organization shall establish, implement and maintain a procedure(s) for the ongoing hazard
identification, risk assessment, and determination of necessary controls.

As an indication of how broadly this guideline is known and used, Singapore adopted it fully as
law in 2009.

PRACTICE FOR SYSTEM SAFETY

It was a seminal document at that time and has continued to be an important reference.

MIL-STD 882 has had considerable influence on the development of hazard identification and anal-
ysis, risk assessment, risk elimination, and risk control concepts and methods. Much of the wording
on risk assessments and hierarchies of control in safety standards and guidelines issued throughout
the world relate to that in the several versions of 882.

Four revisions of 882 have been issued over a span of 43 years. As is said in the foreword for
882E, “This Standard is approved for use by all Military Departments and Defense Agencies within
the Department of Defense.” Certain contractors engaged by those departments and agencies are
required to meet the requirements of the standard.

The 882 version was approved May 11, 2012. It is available at http://www.system-safety.org/.
Scroll down and click on MIL-STD-882E in the right-hand column for a free copy. This author
strongly recommends that safety professionals obtain a copy of this standard for informative purposes.

MIL-STD-882E extends the previous issue – 882D – considerably. For example, the 882D version,
including addenda, had 26 numbered pages: the 882E version has 98 numbered pages. It replaces some
of what was in 882C that was not included in 882D. In 882E:

- Achieving and maintaining acceptable risk levels dominates.
- Revisions were made in the system safety process that give additional emphasis to hazard anal-
  ysis and risk assessment.
- The use of a risk assessment matrix is required.
- Noteworthy revisions are made in the design order of preference.
Appropriate emphasis is given to managing high and serious risk levels.

A major section is devoted to software and software assessments.

Excerpts follow, some of which are modified to avoid governmental terminology. Section 4 in 882E is titled “General Requirements.” It sets forth the “requirements for an acceptable system safety effort.” Section 4.3 and the following subsections of 4.3 outline and comment on the eight elements in the system safety process, as follows:

Element 1: Document the system safety approach. Describe the risk management effort and how the program is integrated into the overall business process.

Element 2: Identify and document the hazards. Hazards are identified through a systematic analysis process that includes the system hardware and software, system interfaces (to include human interfaces), and the intended use or application and operational environment.

Element 3: Assess and document risk. For each identified hazard, across all system modes, the mishap severity and probability are established in accord with the definitions given. A mishap risk assessment matrix is used to assess and display the risks.

Element 4: Identify and document risk mitigation measures. Potential risk mitigation(s) shall be identified, and the expected risk reduction(s) of the alternative(s) shall be estimated and documented. The goal should always be to eliminate the hazard as practicable.

When a hazard cannot be eliminated, the associated risk should always be reduced to the lowest practicable acceptable risk level within the constraints of cost, schedule, and performance by applying the following system safety design order of precedence in their order of effectiveness:

1. Eliminate hazards through design selection. Ideally, the hazard should be eliminated by selecting a design or material alternative that removes the hazard altogether.
2. Reduce risk through design alteration. If adopting an alternative design change or material to eliminate the hazard is not feasible, consider design changes that reduce the severity and/or the probability of the mishap potential caused by the hazard(s).
3. Incorporate engineered features or devices. If mitigation of the risk through design alteration is not feasible, reduce the severity or the probability of the mishap potential caused by the hazard(s) using engineered features or devices. In general, engineered features actively interrupt the mishap sequence and devices reduce the risk of a mishap.
4. Provide warning devices. If engineered features and devices are not feasible or do not adequately lower the severity or probability of the mishap potential caused by the hazard, include detection and warning systems to alert personnel to the presence of a hazardous condition or occurrence of a hazardous event.
5. Incorporate signage, procedures, training, and personal protective equipment (PPE). Where design alternatives, design changes, and engineered features and devices are not feasible and warning devices cannot adequately mitigate the severity or probability of the mishap potential caused by the hazard, incorporate signage, procedures, training, and PPE. Signage includes placards, labels, signs, and other visual graphics. Procedures and training should include appropriate warnings and cautions. Procedures may prescribe the use of PPE. For hazards assigned catastrophic or critical mishap severity categories, the use of signage, procedures, training, and PPE as the only risk reduction method should be avoided.

Element 5: Reduce risk. Mitigation measures are selected and implemented to achieve an acceptable risk level. Consider and evaluate the cost, feasibility, and effectiveness of candidate mitigation methods as a part of the overall operation process.

Element 6: Verify, validate, and document risk reduction. Verify the implementation and validate the effectiveness of all selected risk mitigation measures through appropriate analysis, testing, demonstration, or inspection. Document the verification and validation.
TABLE 1.1 Risk Assessment Matrix

<table>
<thead>
<tr>
<th>Severity of Consequences</th>
<th>Catastrophic (1)</th>
<th>Critical (2)</th>
<th>Marginal (3)</th>
<th>Negligible (4)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Occurrence Probability</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Frequent (A)</td>
<td>High</td>
<td>High</td>
<td>Serious</td>
<td>Medium</td>
</tr>
<tr>
<td>Probable (B)</td>
<td>High</td>
<td>High</td>
<td>Serious</td>
<td>Medium</td>
</tr>
<tr>
<td>Occasional (C)</td>
<td>High</td>
<td>Serious</td>
<td>Medium</td>
<td>Low</td>
</tr>
<tr>
<td>Remote (D)</td>
<td>Serious</td>
<td>Medium</td>
<td>Medium</td>
<td>Low</td>
</tr>
<tr>
<td>Improbable (E)</td>
<td>Medium</td>
<td>Medium</td>
<td>Medium</td>
<td>Low</td>
</tr>
<tr>
<td>Eliminated (F)</td>
<td>This category is used only for identified hazards that are totally removed</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>


Element 7: Accept risk and document. Before exposing people, equipment, or the environment to known system-related hazards, the risks shall be accepted by the appropriate authority in accord with established acceptance authority levels. Definitions (in Tables and Matrices in this standard) shall be used to define the risks at the time of the acceptance decision, unless tailored alternative definitions and a tailored matrix are formally approved. The user representative shall be a part of this process and shall provide formal concurrence before all serious and high-risk acceptance decisions are made.

Element 8: Manage life-cycle risk. After the system is fielded, the system program office uses the system safety process to identify hazards, assess the risks, and maintain acceptable risk levels throughout the system’s life cycle.

An instruction given in Element 7 says that “Definitions (in Tables and Matrices in this standard) shall be used to define the risks at the time of the acceptance decision, unless tailored alternative definitions and/or a tailored matrix are formally approved.”

Table I presents severity categories. Table II contains probability levels. Table III in 882 is shown here as Table 1.1. It is a risk assessment matrix that combines the severity and probability categories and includes numerical and alpha indicators.

Numerical and alpha indicators are the base for expressing assessed risks in a risk assessment code (RAC), which is a combination of one severity category and one probability level. For example, a RAC of 1A is the combination of a catastrophic severity category and a frequent probability level.

For emphasis, it is said again that MIL-STD 882E is an excellent educational and resource document. Its base is hazard identification and analysis and risk assessment.

1.14 CERTAIN GOVERNMENTAL VIEWS

In a July 19, 2010, letter to the OSHA staff, Assistant Secretary David Michaels wrote on several subjects, one of which follows: “Ensuring that American workplaces are safe will require a paradigm shift, with employers going beyond simply attempting to meet OSHA standards, to implementing risk-based workplace injury and illness prevention programs” (Michaels, 2010).

If elements in injury and illness prevention programs are to be risk based, activity will be necessary to identify and assess the risks. That starts with hazard identification and analysis and, then, takes the next step to establish the risk level.

OSHA has not shown that it is adopting the concept of risk-based decision making. This statement by Dr Michaels is noteworthy because it demonstrates that the head of a major governmental entity involved in occupational safety and health has recognized that injury and illness prevention programs should be risk based. As will be seen, personnel in other governmental agencies have reached similar conclusions.
RISK ASSESSMENTS: THEIR SIGNIFICANCE AND THE ROLE OF THE SAFETY PROFESSIONAL

In the December 8, 2010, Federal Register, the Federal Railroad Administration issued an advance notice of proposed rulemaking for certain railroads to have a Risk Reduction Program. The Federal Register entry said “It is proposed that the Risk Reduction Program be supported by a risk analysis and a Risk Reduction Plan” (Federal Railroad Administration Risk Reduction Program, 2010). Enter “Federal Railroad Administration Risk Reduction Program” into a search engine and the following appears.

1.14.1 Risk Reduction Program

The primary mission of the Risk Reduction Program Division is ensuring the safety of the nation’s railroads by evaluating safety risks and managing those risks in order to reduce the numbers and rates of accidents, incidents, injuries, and fatalities.

Our mission is accomplished by:

- Identifying, collecting, and analyzing precursor accident data to identify risks
- Developing voluntary pilot programs in cooperation with stakeholders that are designed to mitigate identified and potential risks
- Propagating and institutionalizing best practices and lessons learned to the entire rail industry
- Providing analytical support, data, and recommendations needed by stakeholders to develop strategies, plans, and processes to improve safety and promote positive organizational change
- Developing and enforcing regulations promulgated in response to the Rail Safety Improvement Act of 2008.


This Final Rule incorporates by reference, and makes mandatory, the American Petroleum Institute’s Recommended Practice for Development of a Safety and Environmental Management Program for Offshore Operations and Facilities (API RP 75), Third Edition, May 2004, reaffirmed May 2008. BOEMRE mandated that by November 15, 2011, all operators and lessees working in the Gulf of Mexico had to submit a comprehensive SEMS plan to the regulator. This plan must address the 13 elements of API RP 75, the third of which is hazard analysis.

This development is of particular interest for two reasons. Operators and lessees affected are required by regulation to make hazard analyses (the first step in making a risk assessment). Also, the plan required is a combination that includes occupational safety, public safety, and environmental safety in one instrument. That combination deserves continual observation. Several safety directors were polled by this author to determine what proportion of the safety professionals at their locations has responsibilities for both occupational safety and environmental concerns. The range was from 50% to 90%.

Risk assessments have been made for many years in the branches of the military, the National Aeronautics and Space Administration, some chemical operations, the atomic energy field, pharmaceutical companies operating under the rules of the Food and Drug Administration, research activities pertaining to public health, traffic control studies, and other fields.

That additional Federal governmental entities have become risk conscious and are requiring that risk assessments be made is an indication of the trend.

1.15 CANADA

CSA Standard Z1000-2006 is titled Occupational Health and Safety Management. It was issued in the year following the first edition of Z10 and has a close relationship with respect to the content and order in the American standard.
Section 4.3.4 reads as follows: The organization shall establish and maintain a process to identify and assess hazards and risks on an ongoing basis. The results of this process shall be used to set objectives and targets and to develop preventive and protective methods. (CSA is the designation for the Canadian Standards Association.)

The excerpt above is all that is said in the standard about hazard analysis and risk assessment. The subject is dealt with further in Annex A, which is informative. But the intent of the hazard analysis and risk assessment provision is amplified in the “shall” provision of the standard at Section 4.4.7, “Management of Change.”

The organization shall establish and maintain procedures to identify, assess, and eliminate or control occupational health and safety hazards and risks associated with

1. new processes or operations at the design stage
2. significant changes to its work procedures, equipment, or organizational structure and so on.

In September 2012, CSA Z1002-12: Occupational Health and Safety – Hazard Identification and Elimination and Risk Assessment and Control was issued. This is a major undertaking. It supports the purpose of Section 4.3.4 in Z1000-2006.

The standard relates entirely to hazards and risks in the workplace. Its issuance is another indication of the trend throughout the world whereby organizations are encouraged to have processes in place to identify and analyze hazards, to assess their accompanying risks, and to achieve acceptable risk levels.

1.16 FIRE PROTECTION

There are four entries in Addendum A for this chapter pertaining to activities of the National Fire Protection Association (NFPA) and the Society of Fire Protection Engineers (SFPE).

In 2007, NFPA issued “Guidance Document for Incorporating Risk Concepts into NFPA Codes and Standards.” This is an impressive, thought-provoking, risk assessment-related document that will have a long-term effect in the fire protection field. It is available at http://www.nfpa.org/assets/files/PDF/Research/Risk-Based_Codes_and_Std.pdf.

As an example of how risk concepts are being incorporated into NFPA standards – the 2012 edition of NFPA 70E, Standard for Electrical Safety in the Workplace has a new section on risk assessment (NFPA 70E, 2012).

SFPE developed an interesting course titled “Introduction to Fire Risk Assessment,” which is available on the Internet (no publication date is shown, but it probably was 2006). A paraphrased and brief version of what is said about the course on the Internet follows.

This 5 h equivalent course is presented free of charge by the Society of Fire Protection Engineers. Although the course was developed primarily for fire service and fire prevention officers, it may be of value to engineers and students who would like to understand fire risk assessment. The full course consists of 19 lecture sessions each of which can be viewed in about 15 min.

This course is largely generic and deserves a look. Additional information, including the titles of the lecture sessions and how to access them, can be found at http://www.sfpe.org/SharpenYourExpertise/Education/SFPEOnlineLearning/FireRiskAssessment.aspx.

In 2006, SFPE also issued the Engineering Guide to Fire Risk Assessment. This is a technical book that would be of particular interest to engineers. Nevertheless, its issuance demonstrates leadership by SFPE with respect to risk assessment.

1.17 DEVELOPMENTS IN AVIATION GROUND SAFETY

One of the most interesting innovations regarding hazard analysis and risk assessment can be found in the Safety Handbook: Aviation Ground Operation developed by the International Air Transport Association.
TABLE 1.2 The Risk Management Process

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Identify the hazard</td>
</tr>
<tr>
<td>2.</td>
<td>Assess the risk</td>
</tr>
<tr>
<td>3.</td>
<td>Analyze risk control measures</td>
</tr>
<tr>
<td>4.</td>
<td>Make control decisions</td>
</tr>
<tr>
<td>5.</td>
<td>Implement risk controls</td>
</tr>
<tr>
<td>6.</td>
<td>Supervise and review</td>
</tr>
</tbody>
</table>


TABLE 1.3 Hazard Analysis and Risk Assessment Methodologies

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Operations analysis: Purpose – To understand the flow of events</td>
</tr>
<tr>
<td>2.</td>
<td>Hazard analysis: Purpose – To get a quick survey of all phases of an operation. In low hazard situations, the preliminary hazard analysis may be the final hazard identification tool</td>
</tr>
<tr>
<td>3.</td>
<td>“What-If” analysis: Purpose – To capture the input of personnel in a brainstorming-like environment</td>
</tr>
<tr>
<td>4.</td>
<td>Scenario process tool: Purpose – To use imagination and visualizations to capture unusual hazards</td>
</tr>
<tr>
<td>5.</td>
<td>Change analysis: Purpose – To detect the hazard implications of both planned and unplanned changes</td>
</tr>
</tbody>
</table>


Section of the National Safety Council. The Air Transport Section is truly international, having representation from all of the populated continents. A sixth edition was published in July 2007. Chapter 2 is titled “Risk Management” (National Safety Council, 2007). The following text is taken from that chapter.

Risk management takes aviation safety to the next level. It is a six-step logic-based approach to making calculated decisions on human, material, and environmental factors before, during, and after operations.

Risk management enables senior leaders, functional managers, supervisors, and others to maximize opportunities for success while minimizing risks. Failure to successfully implement a risk management process will have a financial, legal, and social impact (p. 9).

The air transport group has outlined a way of thinking about and dealing with hazards and risks, applying a logical and sequential methodology. They have developed a “process to detect, assess, and control risk.” The captions in their “six-step logic-based commonsense approach” are shown in the handbook’s Table 1 (p. 11). The process is shown here as Table 1.2. Discussions of each step in the text are extensive. Comments will be made here on the first two, only. For the first step – identify the hazards – the following hazard analysis and risk assessment methodologies, as in the handbook’s Table 2, are discussed (p. 10) as Table 1.3.

For Step 2 – assess the risks – the text says: The assessment is the application of quantitative or qualitative measures to determine the level of risk associated with a specific hazard. This process defines the probability and severity of an undesirable event that could result from the hazard. The risk assessment matrix is a very useful tool in categorizing the effects of probability and severity as they relate to risk levels (p. 12).

This Safety Handbook: Aviation Ground Operation is a good, thought-provoking, not overly complex resource document. It is an example of what a trade group could do as a service to its members.

### 1.18 OSHA REQUIREMENTS

OSHA’s Rule For Process Safety Management Of Highly Hazardous Chemicals, 1910.119, issued in 1992, applies to employers at about 50,000 locations, many of which are not considered chemical
companies. With respect to requirements for hazard analyses being included in standards, this OSHA standard merits a review by safety practitioners. The standard requires that:

The employer shall perform an initial hazard analysis (hazard evaluation) on processes covered by this standard. The process hazard analysis shall be appropriate to the complexity of the process and shall identify, evaluate, and control the hazards involved in the process. The employer shall use one or more of the following methodologies that are appropriate to determine and evaluate the hazards of the process being analyzed:

- What-If;
- Checklist;
- What-If/Checklist;
- Hazard and Operability Study (HAZOP);
- Failure Mode and Effects Analysis (FMEA);
- Fault Tree Analysis; or
- An appropriate equivalent methodology.

Although affected employers are to make hazard analyses, the methodologies previously listed are risk assessment techniques. This author’s recollection is that commenters on the standard prior to its promulgation expressed concern over having to use probability data – of which there is little that is statistically sound. OSHA responded favorably. This appears in the preamble to the standard.

OSHA has modified the paragraph (editorial note – paragraph on consequence analysis) to indicate that it did not intend employers to conduct probabilistic risk assessments to satisfy the requirement to perform a consequence analysis.

However, all risks are not equal. Some require attention prior to others. And managements do assess and prioritize risks in their decision making when determining which resources are to be allocated for individual projects.

1.19 EPA REQUIREMENTS

The Environmental Protection Agency (EPA) and OSHA have different legal authorities with respect to accidental releases of harmful substances. The concerns at EPA center on off-site consequences: that is, harm to the public and the environment. At OSHA, the legal authority pertains to on-site consequences.

On August 19, 1996, EPA issued Rule 40 CFR Part 68, Risk Management Programs for Chemical Accidental Release Prevention (EPA, 1996). Risk Management Plans required of location managers by the rule were due by June 21, 1999. Although the provisions of the rule are extensive, only the specifications for hazard analyses will be addressed here.

Processes subject to this rule are divided into three groups, labeled by EPA as Programs 1, 2, and 3. Program levels relate to the quantities and extent of exposure to toxic and flammable chemicals. For locations qualifying for program levels 1 and 2, those with lesser exposure, EPA will accept hazard reviews done by qualified personnel using suitable checklists.

Hazard reviews must be documented and show that problems have been addressed. In its literature, EPA comments on the desirability of using the “What-If” hazard identification and analysis process. EPA also proposes the use of more involved analytical techniques if findings suggest that to be desirable.

Hazard review requirement for program level 3 locations are more specific and extensive. But those locations that are compliant with the OSHA rule for Process Safety Management of Highly Hazardous Chemicals will need to do little new, although they do need to extend their hazard analyses to consider
the probability of harm to the public or to the environment. As with OSHA, a team must complete the process hazard analyses required by EPA. One member of the team, at least, is to have experience with the process.

For American industry, EPA has obviously extended knowledge and skill requirements regarding hazard analysis techniques.

1.20 THE CHEMICAL INDUSTRY: THE EXTENSIVE BODY OF INFORMATION

Completing hazard analyses was a common practice in the chemical industry many years before requirements for them were established by OSHA and EPA. The body of information in the chemical industry on hazard analysis is extensive. But reference will be made here to only one publication because of its particular significant.

The Center for Chemical Process Safety is a part of the American Institute of Chemical Engineers. One of its books is titled *Guidelines for Hazard Evaluation Procedures, Second Edition with Worked Examples* (Center for Chemical Process Safety of the American Institute of Chemical Engineers, 1992). Publication of the text by a chemically oriented group should not dissuade those who want an education in the following evaluation techniques. Their descriptions are generic.

- Safety review
- Checklist Analysis
- Relative ranking
- Preliminary hazard analysis
- What-If Analysis
- What-If/Checklist Analysis
- Hazard and operability analysis
- Fault tree analysis
- Event tree analysis
- Cause–consequence analysis
- Human reliability analysis.

These techniques are dealt with broadly in the *Guidelines* within chapters titled “Overview of Hazard Evaluation Techniques” and “Using Hazard Evaluation Techniques.”

1.21 CONCLUSION

The message is clear. Including provisions requiring hazard analyses and risk assessments in safety standards and guidelines is becoming ordinary. It is logical to assume that this trending will continue and that safety professionals will be expected to have the knowledge and skill necessary to give counsel on applying those provisions. Emphasis on practical applications of risk assessments is key and is the primary focus of this text.

REVIEW QUESTIONS

1. Name three new initiatives in the United States that promote and support the practice of operational risk assessment.
2. How does the United States compare to other parts of the world regarding the use of risk assessments?


4. In 2010, ANSI adopted a series of standards on risk management from ISO, which are considered fundamental to the risk profession. List these standards and describe their application.

5. Provide five other standards that have requirements for risk assessment that have been established since 2005.

6. What standard addresses risk in the life cycle of a system? Provide the stages of the life cycle of a system or product.

7. List two compliance standards that have requirements for performing hazard analyses.

REFERENCES


**APPENDIX 1.A**

**A LIST OF STANDARDS, GUIDELINES, AND INITIATIVES THAT REQUIRE OR PROMOTE MAKING RISK ASSESSMENTS: COMMENCING WITH YEAR 2005**

1. ANSI/AIHA Z10-2005: *Occupational Health and Safety Management Systems standard.* Z10 sets a benchmark provision requiring that processes be in place: to identify and take appropriate steps to prevent or otherwise control hazards and reduce risks associated with new processes or operations at the design stage.


3. In 2006, NIOSH announced a major national initiative on Prevention through Design, the core of which is risk assessment.

4. SFPE – *Engineering Guide to Fire Assessment,* 2006. This is a technical book that would be of particular interest to engineers.

5. SFPE – *Introduction to Fire Risk Assessment [Believe release date was 2006].* Enter the title in a search engine for course modules on fire risk assessment.


7. The Industrial Safety and Health Act of Japan was revised, effective in April 2006. It stipulates – without penalty – that employers should make efforts to implement risk assessment.
9. In 2007, the OSHA Alliance Construction Roundtable developed a video training program titled “Design for Construction Safety.”
   In the 2007 revision, requirements for risk assessments are more explicit. The guidelines now say: “The organization shall establish, implement and maintain a procedure(s) for the ongoing hazard identification, risk assessment, and determination of necessary controls.”
   They are as follows: (1) Describe the material and its application; (2) profile life cycle(s); (3) evaluate risks; (4) assess risk management; (5) decide, document, and act; and (6) review and adapt.
15. The Health and Safety Executive in the United Kingdom issued five steps to risk assessment in 2008.
16. All employers in the United Kingdom must conduct a risk assessment. An HSE bulletin says: “The law does not expect you to eliminate all risk, but you are required to protect people as far as is ‘reasonably practicable’.”
17. In August 2008, the European Union launched a two-year health and safety campaign focusing on risk assessment. Their bulletin says:
   Risk assessment is the cornerstone of the European approach to prevent occupational accidents and ill health. If the risk assessment process – the start of the health and safety management approach – is not done well or not at all, the appropriate preventive measures are unlikely to be identified or put in place.
   Foreword: Coupled with use of the system safety risk mitigation order of precedence, functional hazard analysis lets a program identify early in the life cycle those risks which can be eliminated by design, and those which must undergo mitigation by other controls in order to reduce risk to an acceptable level.
22. ExxonMobil issued its *Operations Integrity Management System* in July 2009. It pertains to safety, health, the environment, and product safety. The first 4 of 11 elements in this management system are:
1. Management leadership, commitment, and accountability
2. Risk assessment and management
3. Facilities design and construction
4. Information and documentation


   This standard combines three previously issued ISO standards (including item 8 in this listing) and replaces them. Risk assessments are explicitly required.

25. In a July 19, 2010, letter to the OSHA staff, Assistant Secretary David Michaels wrote on several subjects, one of which follows:
   Ensuring that American workplaces are safe will require a paradigm shift, with employers going beyond simply attempting to meet OSHA standards, to implementing risk-based workplace injury and illness prevention programs.

   Purpose: This standard describes procedures for identifying hazards, assessing risks, and reducing risks to an acceptable level over the life cycle of machinery.

27. In the December 8, 2010, Federal Register, the Federal Railroad Administration issued an advance notice of proposed rulemaking for certain railroads to have a risk reduction program.
   It is proposed that the Risk Reduction Program be supported by a risk analysis and a Risk Reduction Plan.

28. ANSI/PMMI B155.1 – March 2, 2011: *Safety Requirements for Packaging Machinery and Packaging-Related Converting Machinery*.
   Foreword: This standard has been harmonized with international (ISO) and European (EN) standards by the introduction of hazard identification and risk assessment as the principal method for analyzing hazards to personnel to achieve a level of acceptable risk.

   Hazardous Materials Regulations are to be modified to require that risk assessments be made of loading and unloading operations.

    Hazard and risk assessments have to be carried out to identify what could cause harm to workers as well as property so that appropriate preventive and protective measures can be developed and implemented.

   The core of Z590.3 is risk assessment to be performed as a continuum in the design and redesign processes.


The second version of Z10, approved in June 2012, now contains a specific requirement for a risk assessment process to be in place.

5.1.1 Risk Assessment.

The organization shall establish and implement a risk assessment process(es) appropriate to the nature of hazards and level of risk.
