engineerscanada
ingénieurscanada

Public guideline: Risk management

National model guide - August 2012

Notice

Disclaimer

Engineers Canada's national guidelines and white papers were developed by engineers in collaboration with the provincial and territorial engineering regulators. They are intended to promote consistent practices across the country. They are not regulations or rules; they seek to define or explain discrete topics related to the practice and regulation of engineering in Canada.

The national guidelines and white papers do not establish a legal standard of care or conduct, and they do not include or constitute legal or professional advice.

In Canada, engineering is regulated under provincial and territorial law by the engineering regulators. The recommendations contained in the national guidelines and white papers may be adopted by the engineering regulators in whole, in part, or not at all. The ultimate authority regarding the propriety of any specific practice or course of conduct lies with the engineering regulator in the province or territory where the engineer works, or intends to work.

About this Guideline

This national guideline was prepared by the Canadian Engineering Qualifications Board (CEQB) and provides guidance to regulators in consultation with them. Readers are encouraged to consult their regulators' related engineering acts, regulations and bylaws in conjunction with this guideline.

About Engineers Canada

Engineers Canada is the national organization of the provincial and territorial associations that regulate the practice of engineering in Canada and license the country's 295,000 members of the engineering profession.

About the Canadian Engineering Qualifications Board

CEQB is a committee of the Engineers Canada Board and is a volunteer-based organization that provides national leadership and recommendations to regulators on the practice of engineering in Canada. CEQB develops guidelines and white papers for regulators and the public that enable the assessment of engineering qualifications, facilitate the mobility of engineers, and foster excellence in engineering practice and regulation.

1 Purpose and introduction

Risk management is an area of knowledge with which all engineers should be familiar. The degree of familiarity, or depth of knowledge, will depend on the specific engineering discipline and the nature of the field of practice. Nevertheless, a constant awareness of the risk management process, and some degree of competence in its application, are essential for all engineers.

The assessment and management of risk are integral components of the daily activities of all engineers. From choosing a mode of analysis to deciding on what inputs are required to adequately frame a problem, potential concerns are identified, the consequences considered, and the probability of a failure debated. A decision is then made on the "best" course of action and steps are taken to prevent an undesirable outcome while attempting to ensure a product that fully meets the customer's requirements. All of this may occur in the blink of an eye, or may be the subject of a more deliberate exercise in risk management.

Engineering work requires the assessment and management of risk. Hazards need to be identified and consequences and probabilities analyzed. Management decisions must be made as to whether the risk is acceptable – in which case the activity would continue with appropriate risk reduction and monitoring measures – or whether the risk is unacceptable and the activity must not be undertaken. Simply put, the practice of engineering carries with it an inherent level of risk that engineers must seek to understand and manage.Further reference in the area of risk management may be found in the CSA Standard (1997), Risk Management Guidelines for Decision Makers.

This model guide is intended to help guide engineers:

- to pursue due diligence in the assessment and management of risk in all their engineering work; and
- to act ethically when incorporating the results of their risk assessment and management activities into their design or product.

Engineers are required to follow all provincial or territorial legislation regarding risk management. For example, the determination of acceptable levels of risks with respect to natural hazards may be specified in legislation or codes, which are established by government after considering a range of societal values, and therefore may not be in the engineer's jurisdiction. This model guide is not intended to bypass that legislation or to establish the level of risk review or management required of an engineer. The model guide merely serves to provide guidance to reach a level of analysis that would generally be accepted as adequate and reasonable.

2 Definition – hazard and risk

The terms *hazard* and *risk* are often used interchangeably. They should not be confused in this manner because hazard and risk are not the same thing. Functional definitions (Wilson & McCutcheon, 2003) of *hazard* and *risk* are as follows:

Hazard: The potential of a machine, equipment, process, material or physical factor in the working environment to cause harm to people, environment, assets or production.

Risk: The possibility of injury, loss or environmental injury created by a hazard. The significance of risk is a function of the *probability* of an unwanted incident and the *severity* of its consequence.

There are several features of these definitions worth noting:

- Risk arises from hazards. Thorough hazard identification is key to the effective management of risk; one cannot manage the risk arising from a hazard that has not been identified.
- Harm or damage can occur in four broad areas – people, the environment, assets (equipment, property, etc.), and production (or process, i.e. business interruption). Recognition of these distinct categories leads to an integrated approach to risk management that encompasses all potential losses. Integrated risk management also encompasses a variety of engineering activities and potential hazards.
- There are two aspects to risk – probability and severity. The terms *likelihood* or *frequency* are sometimes used instead of *probability*. While there are subtle differences in the meanings of these words, particularly between frequency and probability, the differences are not critical to the discussion in this paper.

A hazard, then, is a potential source of loss; risk is the chance of actually experiencing a loss of some degree of severity by virtue of coming into contact with a hazard. Consider an example from everyday life. Ice on a highway is a hazard because it is a physical condition that has the potential to cause harm or damage when driving. While the existence and extent of the ice is a given as a hazard in the operation of a vehicle, the engineering design response tries to lessen the severity of the consequences of driving on ice by the addition of traction control and antilock braking systems. Risk is the actual acceptance of those conditions and use of the highway with appropriate driver precautions aided by onboard vehicle systems. The risk from this hazard is a function of both the probability of encountering ice while driving on the highway, and the severity of the consequences of driving over an icy patch. The combination of driver caution and design safety systems, therefore, lessens both probability and severity of any consequences. Thus, the risk in this case would be considered to be lower than without the design input.

It is also important to distinguish between pure financial risk and what might best be termed as technical or engineering risk. In the former case, for people with a business or commerce background, risk management will usually mean the prudent management of resources so as to avoid unacceptable financial losses. In the case of technical or engineering risk, risk management is taken to mean the process of analyzing exposure to loss and taking appropriate steps to eliminate the risk or reduce it to acceptable levels. Key in this definition is the previously mentioned concept of an integrated approach to reducing loss exposure; i.e. the recognition that loss can occur in a number of areas (people, environment, assets and production). With this approach to risk management, engineers focus on hazards relevant to their work (e.g. chemicals, thermal radiation, mechanical forces, electricity, etc.), and analyze the risk from these hazards with regard to injuries, environmental damage, destruction of property, and business interruption (all of which would typically involve financial loss).

Notwithstanding the discussion in the previous paragraph, a degree of knowledge with respect to financial risk management would be expected of engineers. Often the issues of concern are liability with respect to professional practice and the performance of major undertakings from a business perspective.

3 The risk management process

A functional definition (Wilson & McCutcheon, 2003) of *risk management* is as follows:

Risk Management: The complete process of identifying risks, understanding them, assessing them, and then making decisions to ensure that effective risk controls are in place and implemented. Risk management begins with actively identifying possible hazards leading to the ongoing management of those risks deemed to be acceptable.

Embodied in this definition of risk management, and that given in the previous section, is the cycle of risk analysis, which enables risk assessment, which in turn enables risk management (Bird & Germain, 1996). In essence, engineers *analyze risk* (for probability and consequences), so they can *assess risk* (with respect to acceptability), so they can ultimately *manage risk*. As previously described, it is simply not possible to commence this cycle without first effectively identifying the hazards of concern.

This process of risk management is shown in Figure 1, which represents best practice throughout the world, particularly for hazardous industries but spreading to others. Each step requires different activities to be conducted in differing formats. The result is a process that has been employed globally for the past two decades and is considered to be the best currently available. The various steps given in the generic framework shown in Figure 1 are briefly explained below.

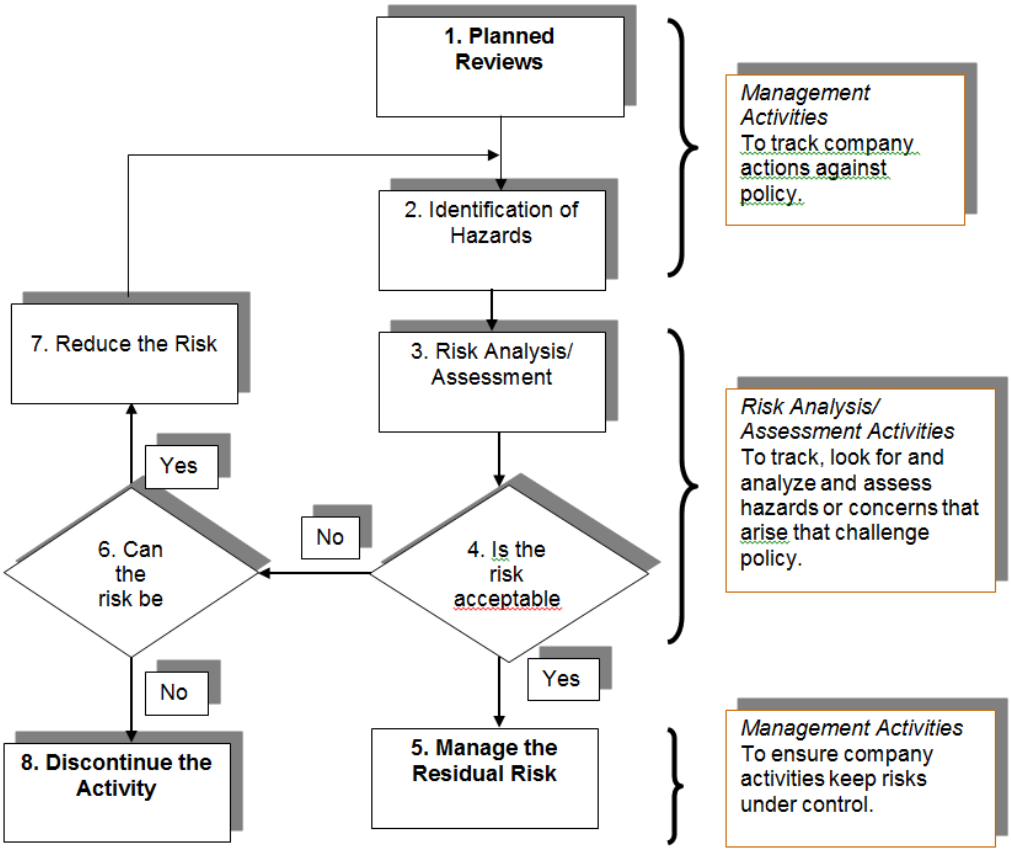

Figure 1 The risk management process.

Figure 1 The risk management process.

1 Planned reviews

Planned reviews are a management function conducted to provide the data needed to monitor operations or develop new project designs. These data are essential for an effective safety and loss management system. It would include incident investigations, insurance company reviews, regulatory activities (pressure vessel inspections, environmental reporting, asset renewal needs, changes to laws, code updates, etc.) – in addition to the regular data collected on business operations and maintenance activities. The objective in this step is to be proactive, so that gathering the data and doing trend analyses in conjunction with statistical analyses will keep a company out of difficulty.

2 Identification of hazards

One of the outcomes of doing the above mandated reviews (as a management team and by paying attention to industry activities in general through trade associations and the news), will be the identification of hazards (or “concerns”). A company’s management team will receive the data and, in the judgment of the team, will determine what needs to be considered further by means of a risk analysis. There are a variety of tools available for hazard identification – for example, Hazard and Operability Study (HAZOP), What-If Analysis, Checklist, Fault Tree, etc.

3 Risk analysis/assessment

Similarly, there are many tools available to help with risk analysis and assessment. Risk analysis involves gaining an understanding of the risk components – probability and consequences. Probability pertains to the failure of systems, humans, equipment, etc., and in many instances is readily quantifiable. Some data are available generically, but the most pertinent data are often found in a company’s maintenance records, operational logs and incident investigation reports.

There also exist a number of methodologies to quantify the consequences of many of the hazards encountered in engineering practice, such as fires (thermal radiation and smoke), explosions (blast wave overpressures), toxic cloud dispersion, toxic exposures, lethality, noise, water pollution, etc. Once the probability and severity of consequences are known and the risk estimated, risk assessment is conducted to determine whether the risk is acceptable or not.

It may be that the extent of the risk itself is unknown. The worst case scenario is that the hazard is unknown and there is no knowledge of the possibility of this hazard. In this case there would be no opportunity to address the risk and deal with it. If the possibility of a hazard and consequent risk is known but the details are not know, the situation can, at least, be addressed even if much effort is required. The best situation is that of a known hazard and risk which can be managed with some degree of confidence for a positive outcome.

4 Is the risk acceptable?

Many company managements have developed a risk matrix describing what is a low-level risk (acceptable), medium-level risk (acceptable with certain conditions), and high-level risk (unacceptable). Such matrices clarify to employees what they must do and what is acceptable. The low-level risks are usually acceptable without any further management involvement or design additions. With respect to medium risk, management needs to be actively involved to ensure the risk is kept under control; it is worthwhile noting that management's responsibilities come to the forefront as they (managers) are assuming responsibility for accepting the risk. This applies to the management of business risks but engineers are cautioned that technical risks may transcend these where ethical or moral issues are involved.

Corporate attitude may be a factor in the assessment and reaction to risk. The tolerance that a corporation has to risk may be driven by the product that is being developed, the maturity of the technology involved, or the desirability for corporate success. Where public safety is involved, risk is to be avoided at all costs. However, where the risks are to the business performance and/or reputation, high risk may not only be acceptable but highly desirable if the consequences of success bring with them high rewards. The ability for a company to absorb financial or "good will" losses will depend upon the perceived positive benefits that accrue and that will balance off any consequences of failure.

5 Manage the residual risk

Once a risk is determined to be acceptable, it must be managed. This is arguably the most important step in the process as responsibility has now been taken for assuming the risk and preventing any undesirable incident from occurring. A key engineering tool employed in this stage is a management system appropriate for the risks being managed (e.g. health, occupational safety, process safety, equipment reliability, etc.). Once a risk is accepted, it does not go away; it is there waiting for an opportunity to happen unless the management system is actively monitoring engineering and company operations for concerns and taking proactive actions to correct or mitigate potential problems.

6 Can the risk be reduced?

Often there are ways to reduce the risk once its level is determined to be unacceptable. The term *inherent safety* is used to imply methods which will eliminate or reduce the risk by tackling the underlying hazards themselves (e.g. by substitution of a less hazardous material; Khan & Amyotte, 2003). Additionally, further controls, management systems, protective features, and the like can be added to reduce the risk to an acceptable level.

7 Reduce the risk

If the proposed risk reduction measures are viable, then the necessary changes must be made to equipment, procedures, hazardous inventories, etc. It is important to note that once a change is made, the risk management cycle is once again used to evaluate possible new hazards and risks. Changes in engineering processes often create additional potential problems that can unintentionally (and perhaps unknowingly) lead to increased operational risk.

8 Discontinue the activity

A very important step is to recognize when the risk is too high. Individual engineer's and company values and objectives come into play at this stage – including the factors of lost profits, personal promotions, professional defeat, etc. Discontinuing an activity because the risk is unacceptable is a key decision because it says that a company will not do something that is unsafe, pollutes the environment, damages assets, risks business opportunities needlessly, or impacts the public's view of the engineer or company in a negative fashion.

4 Typical risk management checklist

Absorb new knowledge

- » Plan for the long term.
- » Update the plan regularly based on review of recent research and case histories.
- » Instill a culture of continuous improvement which should include:

- regular updates to meet new standards;
- the ability to alter existing construction for changing conditions; and
- incorporation of new knowledge into operation and maintenance.

Provide redundancy

- Design criteria should routinely provide redundancy so that if one part fails, all is not lost.
- Think about what could go wrong, and use a second line of defense wherever it is needed.

Understand, manage, and communicate risk

- Provide a rigorous, risk-based approach to selecting an appropriate level of protection for public safety, health, and welfare.
- Use risk management to enable a comparison of alternatives for managing consequences.
- Inform the public in clear and concise terms of potential consequences of decisions being made.
- Designs and operation and maintenance must account for issues that go beyond the bounds of a specific project – for example:
  - regional subsidence;
  - sea-level rise;
  - regional geologic hazards; and
  - sustainability.

Build quality in

- Use a rigorous internal review processes as part of the organizational Quality Assurance / Control programs to ensure that designs meet company goals.
- Use external peer review to effectively:
  - embed an appropriate margin of safety into the culture of the design process; and
  - ensure that designs meet the appropriate standards of practice.
- Ensure that there is an understanding of the expectations of all stakeholders.
- Ensure that the performance of design, construction, and operation and maintenance meets those expectations.

Follow the money

- Try to ensure that the people responsible for design and construction decisions have some influence on the control of the purse strings.
- Realize that the pressure for tradeoffs and low-cost solutions compromise quality, reliability, and safety.
- Ensure adequate safeguards so that money is spent as intended.
- Tie responsibilities for funding and for technical decision-making together.

$\sum$ parts ≠ a system

- Ensure that a system that is constructed piecemeal over an extended period of time (i.e. years or decades) has a system-wide approach to design, operation and maintenance.
- Ensure that the system is designed for changing climates.
- Focus on the system, not just its parts.
  - A system-wide approach to planning, design, and operations and maintenanceenables optimizing performance of project components and guards against unanticipated impacts and consequences.
- A chain is only as strong as its weakest link

Beware of interfaces

- Numerous failures occur at interfaces between system components.
- Organizational discontinuities between jurisdictions put public safety at risk.
- No amount of engineering can offset organizational dysfunction.
- Recognize that problems concentrate at interfaces – for example:

- between materials;
- between jurisdictional entities;
- between members of the design team; and
- between project participants (owner, sponsor, designer, and constructor).

Build resilience in

- Beware and deal with single point failures.
- System resilience is key to avoiding catastrophic failure.
- Design criteria should routinely provide resilience to reduce vulnerability.
- Plan for failure and take steps to avoid it.

5 Reaction to risk

What is “risk” as it relates to engineering practice and designed projects? One must deal with the perception of risk; how it is perceived by the engineer and how it is perceived by the user/public.

“A thing is safe if its risks are judged to be acceptable” (Lowrance, 1976). This quote touches on the issue of perception of risk and its need for reaction. Each individual will have a different reaction to risk and will act accordingly; not always as expected.

Another way of saying this is that a thing is safe if, were its risks fully known, those risks would be judged acceptable by a reasonable person in light of their settled value principles. This, then, comes down to how a person will judge whether the risk is “fairly” safe or “relatively” safe. A risk is acceptable when those affected are generally no longer (or not) *apprehensive* about it (Rowe).

Apprehensiveness depends on whether:

- The risk is accepted voluntarily.
- The effects of knowledge on how probabilities of harm (or benefit) are known or perceived.
- The risks are job-related or other pressures exist that cause people to be aware of or to overlook risks.
- The effects of the risk are close at hand or immediately noticeable.
- The potential victims are immediately identifiable beforehand.

6 Bibliography

Amyotte, Paul R. & McCutcheon, Douglas J. (2006). Proceedings from Engineers Canada Board meeting October 2006:*Risk Management - An Area of Knowledge for All Engineers.* Ottawa, Ontario.

Association of Professional Engineers and Geoscientists of British Colombia. (2010).*Guidelines for Legislated Landslide Assessments for Proposed Residential Developments in British Columbia*. Vancouver, British Columbia. Retrieved from http://www.apeg.bc.ca/ppractice/documents/ppguidelines/guidelineslegislatedlandslide1.pdf

Bird, F. E. & Germain, G. L. (1996). *Practical Loss Control Leadership*. Loganville, GA: Det Norske Veritas.

Canadian Standards Association. (1997). *Risk Management: Guideline for Decision Makers* (CSA Publication No. CAN/CSA-Q850-97 (R2009)).

Engineers Canada. (2011). *Public Infrastructure Engineering Vulnerability Committee Protocol.* (Engineers Canada Publication No.). Ottawa, Ontario.

Khan, F. I. & Amyotte, P. R. (2003). How to make inherent safety practice a reality.*Canadian Journal of Chemical Engineering*, 81, 2-16.

Lowrance, W. W. 1976. *Of Acceptable Risk: Science and the Determination of Safety*.

Los Altos, CA: W. Kaufmann

Rowe, W. D. 1977. *An Anatomy of Risk*. John Wiley & Sons Inc.

Wilson, L. & McCutcheon, Douglas J. (2003). *Industrial Safety and Risk Management*. Edmonton, AB: University of Alberta Press.