RISK MANAGEMENT –
AN AREA OF KNOWLEDGE FOR ALL ENGINEERS

A Discussion Paper By:
Paul R. Amyotte, P.Eng.[1] & Douglas J. McCutcheon, P.Eng.[2]

[1]Chemical Engineering Program
Department of Process Engineering & Applied Science
Dalhousie University
Halifax, Nova Scotia, Canada B3J 2X4
<paul.amyotte@dal.ca>

[2]Industrial Safety & Loss Management Program
Faculty of Engineering
University of Alberta
Edmonton, Alberta, Canada T6G 2G6
<doug.mccutcheon@ualberta.ca>

Prepared For:
The Research Committee of the Canadian Council of Professional Engineers

October 2006

DALHOUSIE UNIVERSITY
Inspiring Minds

UNIVERSITY OF ALBERTA

SUMMARY

The purpose of this paper is to "seed" the discussion by the Research Committee of the Canadian Council of Professional Engineers (CCPE) on the topic of risk management. The paper is in part a research paper and in its entirety a position paper. As can be inferred from the title, the authors hold the firm opinion that risk management is an area of knowledge with which all engineers should have familiarity and a level of competence according to their scope of practice.

The paper first makes the distinction between *hazard* and *risk*. The two terms are often used interchangeably when in fact they are quite different. A hazard is a chemical or physical condition that has the potential to cause harm or damage to people, environment, assets or production. Risk, on the other hand, is the possibility or chance of harm arising from a hazard; risk is a function of *probability* and *severity* of consequences.

A description of the process of risk management is then given. A generic framework for risk management is presented to illustrate the essential activities of hazard identification and the analysis, assessment and management of risks. Key activities in this framework are the decisions that must be made on risk acceptability – whether to continue with an activity and monitor the risk, to implement risk reduction measures and then conduct a re-assessment, or to discontinue the activity because the risk is unacceptable and cannot be cost-effectively reduced.

The first of two main questions the paper seeks to answer is then analyzed: *Why risk management for engineers?* The argument in support of risk management knowledge being important for engineers is advanced on three fronts: moral/ethical, legal, and financial. A brief review is then given of educational needs on risk management in Canadian engineering schools, and the activities of some CCPE Constituent Members and selected Canadian engineering technical societies (discipline-specific) with respect to risk management activities and services.

A second question is then addressed: *Why risk management for <u>all</u> engineers?* The basic intent in this section is to counter the argument that risk management is only important for those engineers working in "high-risk" industries or for those engineers dealing with "dangerous" materials. The modern engineering team is examined from the perspective of its multi-disciplinary nature which necessitates particular attention to *risk communication*. Several international initiatives in risk management education and practice development are described to demonstrate that other countries do not make a distinction between artificial groupings of engineers who may or may not require risk management knowledge. To further illustrate this point, several case studies of differing origin are briefly reviewed. The Westray coal mine explosion that occurred in May 1992 in Nova Scotia is presented as a case study to show that this disaster holds important lessons for *all* engineers, not just those engaged in coal mining.

The final section gives several recommendations in the form of suggestions to advance the state of risk management education, training and practice by engineers in Canada. These recommendations are presented for consideration by the Canadian Engineering Accreditation Board, Canadian Engineering Qualifications Board, CCPE, CCPE Constituent Members, National Council of Deans of Engineering and Applied Science, Canadian engineering technical societies, and the CCPE Research Committee.

TABLE OF CONTENTS

INTRODUCTION

This paper has been written to facilitate discussion by the Research Committee of CCPE on the topic of risk management. The argument presented herein is that 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, it is the authors' view that 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 human beings. From choosing a mode of transportation to deciding on what to eat for lunch, potential concerns are identified, the consequences considered, and the probability of a mishap 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 pleasant trip or an enjoyable meal. 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 also 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.

The remainder of this paper attempts to explain the reasons for the authors' opinion that risk management is an area of knowledge with which all engineers should be familiar. We are not alone in this opinion; virtually all professional colleagues known to us personally are in agreement with this thesis. All could provide convincing anecdotes of the need for risk management awareness and competence on the part of professional engineers. We recognize, however, that evidence must come not only from specific examples, but also from the various stakeholders who motivate and define the practice of engineering in Canada – practitioners themselves, regulators, legislators, educators, international competitors, and the public. This is the focus of subsequent sections of the current document, together with a concluding set of recommendations for consideration by the Research Committee of CCPE. First, it is necessary to make a clear distinction between the terms *hazard* and *risk*, as done in the next section; this is followed by a brief explanation of the process of risk management.

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. 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. If one drives at normal highway speed during a winter storm at night, the risk from hazardous ice on the road would likely be considered to be high. (The probability is high and the consequences are potentially quite severe.) Waiting for the storm to end and the salt or sand trucks to complete their job, along with reducing speed and making the trip in daylight hours, lessen both probability and severity of consequences. Thus, the risk in this case would be considered to be lower than in the previous high-risk scenario.

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 (the subject of this paper), 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 (Alp, 2000). 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 professionals in all fields such as engineering, medicine and law. Often the issues of concern are liability with respect to professional practice (e.g. IRMI, 2006) and the performance of major undertakings from a business perspective (e.g. IRM, 2006). Thus, while the focus of the current paper is on technical or engineering risk, it is well-understood that financial risk is a critical feature in overall risk management efforts.

THE RISK MANAGEMENT PROCESS

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

> ***Risk Management:*** The complete process of understanding risk, risk assessment, and decision making to ensure 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 (Alp, 2000), 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.

<u>Planned Reviews</u>
This is a management function in which reviews are conducted to provide the data needed to monitor operations or develop new project designs. This is essentially the database 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.

<u>Identification of Hazards</u>
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.

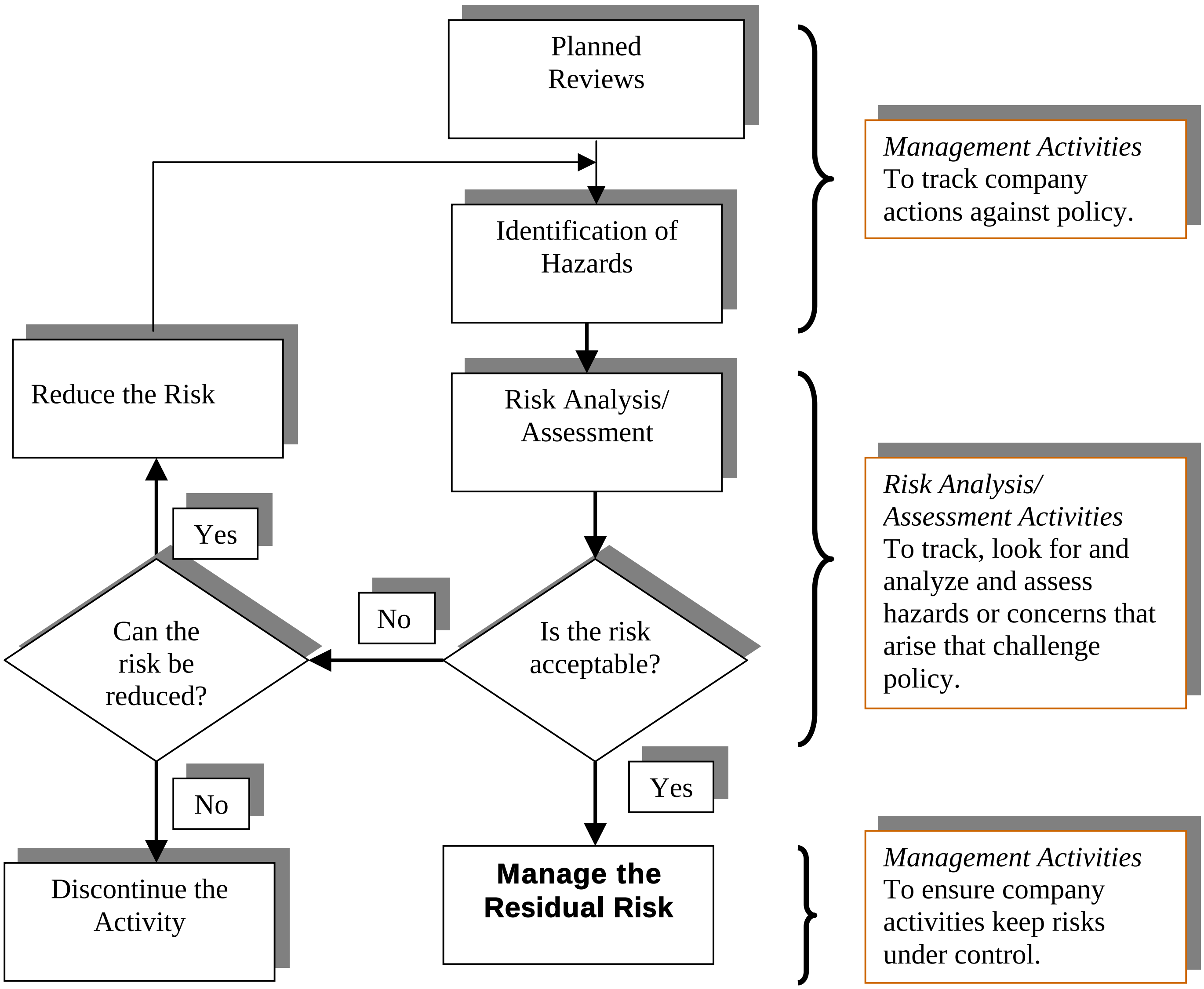

Figure 1 The risk management process.

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.

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 here that management's responsibilities come to the forefront as they (managers) are assuming responsibility for accepting the risk.

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.). Safety management systems are recognized and accepted worldwide as best-practice methods for managing risk. They typically consist of 10 – 20 program elements (e.g. management of change) that must be carried out to manage the risks in an acceptable way. 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 company operations for concerns and taking proactive actions to correct potential problems.

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.

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.

Discontinue the Activity

A very important step is to recognize when the risk is too high. Management needs to be crystal clear on this and make the right decisions. 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 company in a negative fashion. Also, company employees will be watching their managers’ performance at this stage; employee support for management decisions on risk acceptance is essential.

An illustrative example drawn from everyday life (driving in a residential area) is given in Table 1. Here, the What-If methodology is used to identify hazardous scenarios and consequences of concern. Existing safeguards are then examined and the risk is analyzed in terms of probability of occurrence and severity of consequences, and assessed with respect to the acceptability of the risk. This assessment might be done by expert judgment in this simple case, or in a more complex scenario by using the previously mentioned concept of a risk matrix. If the risk is deemed unacceptable, then the recommendations column of Table 1 would provide guidance on possible risk reduction measures. These risk reduction measures would be implemented, and the risk management cycle (Figure 1) repeated to ensure that no new hazards have been introduced, and that the residual risk is being effectively managed. If the risk was deemed to be unacceptable even with the recommendations fully implemented, then the activity would be discontinued until such time (if ever) that it could be carried out with an acceptable level of risk.

Table 1 What-If example for the activity of driving in a residential area.

What If	Consequences	Existing Safeguards	Recommendations
A pedestrian suddenly crosses the street in front of your car?	• You may hit the pedestrian causing injury. • You may hit another vehicle causing damage. • You may stop suddenly, causing injury in your vehicle.	• Being attentive in residential areas. • Always keeping a safe distance from other vehicles. • Wearing seatbelt at all times.	• Do not drive through residential areas except when necessary. • Consider providing fences between roads and areas with likely pedestrian exposure – for example, schools or playgrounds. • Drive slowly in residential areas.

WHY RISK MANAGEMENT FOR ENGINEERS?

The answer to this question is multi-faceted. Part of the answer can be found in the actual process of risk management as described in the previous section. In this section, the words *manage*, *manager*, and *management* were extensively used; and for good reason – this is precisely what engineers do. Engineers *manage* projects (large or small), the risks these projects entail, and the people who perform these projects. Broadly speaking, an engineer will either be a *manager* or will work for/with a *manager*. Further, engineers in *management* positions have different risk-related responsibilities than the workers they employ.

Business and engineering decisions are increasingly being made on the basis of risk. It is therefore necessary for engineers to understand the process of risk management. An engineer might be actively involved in the process itself in various ways – identifying hazards, analyzing probability of occurrence and severity of consequences, assessing the level of risk in relation to company policy or an externally mandated standard, or implementing and monitoring risk reduction measures. Alternatively, an engineer might be faced with decision making on the basis of a qualitative or quantitative risk assessment performed by an outside consultant. Quantitative risk assessment (QRA) in particular can be highly specialized and involve complex mathematical and simulation techniques. Some degree of familiarity with the capabilities, limitations and assumptions of QRA methodologies is critical for informed decision making.

The reasoning in the above two paragraphs will usually convince some members of an audience that risk management is indeed an important component of an engineer's knowledge base. But it is seldom sufficient to convince the majority. Other considerations are needed to more fully answer the question: *Why risk management for engineers?* The remainder of this section attempts to provide these considerations from the following perspectives: moral/ethical issues, legal requirements, financial motivation, educational needs, CCPE constituent member activities, and technical society initiatives.

Moral/Ethical Issues

Why risk management for engineers? Because it is the right thing to do; not only is it the right thing to do – it is the professional thing to do. As professional engineers, we are called upon to regard our duty to public welfare as paramount (e.g. APENS, 1989). Our projects, products and designs must be developed with the primary objective of maintaining the well-being of the public. This does not mean that engineering activities must be conducted with no risk, but it does mean that the risks inherent in these activities must be well-managed. The backbone of quality assurance with respect to engineering education in Canada, the Canadian Engineering Accreditation Board, expresses the moral/ethical argument through its criterion 2.2.7 (CEAB, 2005):

Each program must ensure that students are made aware of the role and responsibilities of the professional engineer in society. Appropriate exposure to ethics, equity, public and worker safety and health considerations and concepts of sustainable development must be an integral component of the engineering curriculum.

The fundamental issue of whether a company believes it is possible to achieve a higher standard of safety – in essence whether a company believes safety is “the right thing to do” – has recently been addressed in the excellent book by Andrew Hopkins. Hopkins (2005) describes three concepts that address a company’s cultural approach to safety, and makes the argument that the three are essentially alternative ways of talking about the same phenomena:

- ***Safety Culture:*** The concept of a safety culture embodies the following subcultures:
  - A *reporting culture* in which people report errors, near-misses, substandard conditions, inappropriate procedures, etc.
  - A *just culture* in which blame and punishment are reserved for behaviour involving defiance, recklessness or malice, such that incident reporting is not discouraged.
  - A *learning culture* in which a company learns from its reported incidents, processes information in a conscientious manner, and makes changes accordingly.
  - A *flexible culture* in which decision-making processes are not so rigid that they cannot be varied according to the urgency of the decision and the expertise of the people involved. Hopkins (2005) uses the examples of the Challenger and Columbia shuttle disasters to explain this point. He comments that decisions in these cases were made by senior NASA officials operating under layers of bureaucracy, rather than by the engineers best equipped to make the decisions. Implicit in Hopkins’ argument is that the engineers involved understood the inherent risks.
- ***Collective Mindfulness:*** The concept of collective mindfulness embodies the principle of *mindful organizing* which incorporates the following processes:
  - A *preoccupation with failure* so that a company is not lulled into a false sense of security by periods of success. A company that is preoccupied with failure would have a well-developed reporting culture.
  - A *reluctance to simplify* data that may at face-value seem unimportant or irrelevant, but which may in fact contain the information needed to reduce the likelihood of a future surprise.
  - A *sensitivity to operations* in which frontline operators and managers strive to remain as aware as possible of the current state of operations, and to understand the implications of the present situation for future functioning of the company.
  - A *commitment to resilience* in which companies respond to errors or crises in a manner appropriate to deal with the difficulty, and a *deference to expertise* in which decisions are made by the people in the company hierarchy who have the most appropriate knowledge and ability to deal with the difficulty.
- ***Risk-Awareness:*** Hopkins (2005) claims that risk-awareness is synonymous with collective mindfulness (which is obviously closely related to the concept of a safety culture). We agree with this statement and would similarly argue that the risk management process shown in Figure 1 fits entirely with the above discussion on safety culture, collective mindfulness, and risk-awareness. There is a strong moral/ethical imperative for companies to practice risk management and for engineers to understand the fundamentals of risk management.

Legal Requirements

Broadly speaking, in Canada we do not have the full legislative and regulatory requirements of the United Sates or European countries in relation to the management of risks arising from major industrial hazards. The Canadian approach has typically been to rely more heavily upon voluntary initiatives for health, safety and environmental programs. In no way should these statements be taken to mean that there are no laws in Canada to regulate public health, worker safety, environmental protection, transportation of dangerous goods, and the like. Such legislation and regulations do, of course, exist. The fact remains, however, that the general regulatory regime in Canada with respect to risk management is different than in many other parts of the world (compared with, for example, the Risk Management Program promulgated by the US Environmental Protection Agency, the Process Safety Management Rule enforced by the US Occupational Safety and Health Administration, and the Seveso II Directive mandated throughout the European Union for the control of major hazards involving dangerous substances). *[Aside: In 1976, a release of approximately 2 kg of dioxin, along with much larger amounts of other hazardous materials, occurred from a chemical manufacturing facility in the small town of Seveso, Italy. This incident, its causes, and the resulting consequences have been a prime motivator for the control of major hazards throughout much of Europe.]*

The discussion in the above paragraph can be best understood by reference to the work of Lacoursiere (2005a). This paper is the archival version of the presentation made by Jean-Paul Lacoursiere, ing. at the International Conference on the 20th Anniversary of the Bhopal Disaster: *Bhopal Gas Tragedy and its Effects on Process Safety*, IIT Kanpur, India (December 1-3, 2004), also attended by one of the current authors (PRA). Lacoursiere is a widely recognized and respected risk management consultant (J.-P. Lacoursière inc.) and educator (Université de Sherbrooke). In Lacoursiere (2005a) he describes the Canadian response to the Bhopal disaster which occurred in 1984 and is undoubtedly the worst industrial accident to date. Thousands of people in the city of Bhopal, India were killed in the early morning hours of December 3, 1984 following the release of approximately 25 tons of toxic methyl isocyanate (MIC) from a Union Carbide facility manufacturing agricultural pesticides. Thousands more died in the ensuing weeks, and many thousands of people in Bhopal suffer to this day. The Bhopal disaster is a shameful example of woefully inadequate engineering risk management.

Lacoursiere (2005a) outlines the Canadian response with a timeline showing significant developments such as the Responsible Care® initiative undertaken by the Canadian Chemical Producers' Association (CCPA), and the establishment by Environment Canada of the Major Industrial Accidents Council of Canada (MIACC, now dissolved). He explains the voluntary, best-practice approach to control of major hazards in Canada and, most importantly, summarizes several recent happenings that herald a possible change in the Canadian regulatory climate with respect to hazard control and risk management. The following points are well worth noting because of their impact on the risk management practices of engineers:

- ***CEPA 200:*** Recent changes to the Canadian Environmental Protection Act, Section 200, require installations having any substance on a prescribed list to develop and test an environmental emergency plan covering prevention, preparedness, response and recovery (PPRR) with respect to potential emergencies involving these substances (Shrives, 2004).

- ***Bill C-45:*** Amendments to the Criminal Code of Canada, in effect March 31, 2004, were made to significantly extend the criminal liability of corporations with respect to health and safety; this is generally known as the Westray bill (in reference to the Westray mine explosion described in a subsequent section of the current paper). For any person who directs how another person performs their work (e.g. managers and directors of corporations), actions that demonstrate reckless disregard for worker and public safety open the door to a charge of criminal negligence (Stelmakowich, 2004).
- ***Quebec Civil Protection Act:*** The new Quebec Civil Protection Act was adopted in 2001 largely in response to the 1998 Saguenay region floods and the 1999 ice storm. Its purpose is to protect people and property in the event of a disaster by means of some of the basic components of effective risk management – e.g. emergency response planning and disaster mitigation measures (Lacoursiere, 2005a).
- ***Ontario Emergency Management Act and Program:*** Emergency management changes in the province of Ontario, not unlike those mentioned above in Quebec, have occurred in response to recent events such as the 1999 ice storm, Y2K, September 11, and the SARS epidemic. These changes have potentially significant impacts for emergency planning at the municipal level (Lacoursiere, 2005a).

There is thus a strong legal mandate for good risk management practices in engineering endeavours in Canada. The regulatory regime in Canada is changing to some degree and is different from the United States and Europe. This latter point is especially important for those engineering firms that practice globally. The bottom line concerning Canada's risk management practices is that these will definitely ***not*** be viewed as "voluntary" by the courts should a loss-producing event occur. Due diligence will be expected by the courts, and this means engaging in best-practice, state-of-the-art risk management activities as the only accepted way to do business. Such activities would include basic concepts with which engineers are quite familiar – codes, standards, and management systems; specific risk management examples of these include the following:

- ***Process Safety Management Systems:*** PSM (Process Safety Management; Guide available from the Canadian Society for Chemical Engineering).
- ***Occupational Health and Safety Management Systems:*** AIHA OH&SMS (American Industrial Hygiene Association, Occupational Health and Safety Management System); BSI/OHSAS 18001 (British Standards Institute/Occupational Health and Safety Assessment Series 18001).
- ***Environmental Management Systems:*** ISO 14001 (International Organization for Standardization 14001).
- ***Risk Management Standards:*** CSA-Q850-97 (Canadian Standards Association; Risk Management: Guideline for Decision-Makers).
- ***Emergency Response Standards:*** CSA-Z731-03 (Canadian Standards Association; Emergency Preparedness and Response).

Financial Motivation

The first duty of business is to survive, and the guiding principle of business economics is not the maximization of profit – it is the avoidance of loss. – Peter Drucker, as quoted on the front cover of Wilson (1998). This quotation concisely and effectively conveys the financial motivation for risk management. As mentioned previously, the integrated approach to risk management recognizes and attempts to prevent and mitigate loss in each of four main areas: people, environment, assets and production, all of which have the potential for financial loss (as illustrated in the next paragraph).

In CCPS (2001), the Center for Chemical Process Safety in the United States presents the business case for managing process safety. This is essentially a business case for risk management, and involves the following elements (CCPS, 2001):

- ***Self-Determination:*** Effective risk management provides a company with the freedom to manage its business, grow responsibly and profitably, and satisfy its stakeholders. Company operation and expansion can then occur with the support of both the public and regulators.
- ***Avoiding Major Losses:*** Effective risk management leads to the avoidance of loss-producing incidents and enables a company to minimize:
  - Loss of life and injuries to employees, contractors and members of the public.
  - Damage to property (assets). CCPS (2001) gives a process industry-average cost of US $80 million per major incident.
  - Business interruption (loss to process or production), including loss of market share until the company's reputation is restored (if, in fact, it is ever restored).
  - Regulatory fines and litigation costs.
  - Costs of incident investigation and implementation of remedial measures.
- ***Corporate Responsibility:*** Effective risk management relies on creating a culture of risk-awareness within a company as described earlier (Hopkins, 2005). Corporate responsibility ensues, such that the company is seen to be "doing the right things" as a responsible member of the industry and the community. This is the essence of CCPA's Responsible Care® program for its member companies (Lacoursiere, 2005). As a result, employees will have higher morale and loyalty and the company may experience higher sales and market share.
- ***Value:*** Effective risk management means "doing the right things right". This leads to increases in revenue and productivity and reductions in product cost. A particularly important point made in CCPS (2001) is that for smaller companies, because of product stewardship requirements, demonstration of good risk management practices may be a prerequisite to doing business with larger companies more versed in risk management.

Educational Needs

The previous three sections have demonstrated the moral/ethical, legal, and financial framework of needs for risk management to be conducted by practicing engineers. It therefore stands to reason that the Canadian system for engineering education should address the topic of risk management. There are some signs that this is the case, but also that a more concerted effort is needed. We first offer the following evidence of activity, albeit anecdotal and limited to the knowledge of the authors:

- The Faculty of Engineering at the University of Alberta has, for over a decade, operated the *Industrial Safety & Loss Management Program (ISLMP)*. This unique program in Canada was initiated under the leadership of then Dean of Engineering, Dr. Fred Otto, P.Eng. and was chaired initially by Professor Laird Wilson, P.Eng. The program continues today with the support of Dean David Lynch, P.Eng. and is chaired by one of the current authors (DJM). ISLMP enjoys strong industry support and offers elective courses to both engineering and business students in *Industrial Safety & Loss Management* and *Industrial Safety & Risk Management*.
- The Department of Process Engineering and Applied Science at Dalhousie University offers a mandatory course in *Industrial Safety & Loss Management* to its chemical engineering and environmental engineering undergraduate students. A graduate course on *Loss Prevention & Risk Assessment* is also offered. Additionally, twelve lectures on *Industrial Safety & Loss Management* are given in a mandatory course titled *Engineering in Society II* for students in biological, civil, electrical, materials, mechanical, and mining engineering. The other author of the current paper (PRA) teaches these courses.
- The Faculty of Engineering & Applied Science at Memorial University of Newfoundland has established an exceptionally strong program in undergraduate and graduate education and research in risk management (offshore oil and gas engineering, environmental engineering, asset integrity management, reliability engineering, etc.). Dr. Faisal Khan, P.Eng. is a key member of the risk team at Memorial.
- Université de Sherbrooke has developed risk management offerings in engineering with the extensive involvement of Jean-Paul Lacoursiere, ing.
- The University of Waterloo has, since 1982, housed the Institute for Risk Research (IRR). IRR’s primary objective is to assist governments, public organizations and industry in risk management decisions and policies.
- Dalhousie University recently announced the formation of the RBC Centre for Risk Management. Interestingly, although the official home for the Centre is the Faculty of Management, the director of the Centre is Dr. Ron Pelot, P.Eng. of the Department of Industrial Engineering. Dr. Pelot is a subject expert in marine transportation risk and understands well the importance of risk management in engineering.

Over the past few years, the authors of this paper have been engaged with other team members from industry and academia in planning and delivering a “Summer Institute” for Canadian chemical engineering faculty (Amyotte, 2004 & 2005; Amyotte & McCahill, 2004). The Summer Institute program is aimed at expanding the knowledge base in academia concerning the fundamentals of process safety and risk management. The basic premise is that these topics can, and should, be taught in the undergraduate chemical engineering curriculum. Just as topics such as process control, heat transfer, and separation processes form an integral part of a chemical engineer’s education, so too should the principles of process safety and risk management.

The Summer Institute program is a partnership between the Process Safety Management (PSM) Subject Division of the Canadian Society for Chemical Engineering (CSChE), and Minerva Canada Inc., a not-for-profit organization having the objective of introducing the concepts and principles of occupational health and safety management into the curriculum of engineering and business schools. The first Institute was held in Sarnia, ON from May 30 – June 2, 2004 with strong financial support and hosting from several industrial sponsors. The inaugural Summer

Institute class consisted of 24 attendees, with at least one faculty member (and in a few cases, two) from 18 of the 20 accredited chemical engineering programs in Canada, as well as a colleague from an affiliated mechanical/process engineering program. The second Institute was held from May 29 – June 1, 2005, again in Sarnia, ON; this event brought together 34 professors and industrial practitioners from Vancouver to St. John's, as well as the United States.

The Institute curriculum is designed to introduce faculty members to the essential building blocks of process safety and risk management. Topics include (among several others): management systems, safety program elements, consequence analysis, risk management tools such as the Dow Fire & Explosion Index and the Dow Chemical Exposure Index, and company and public expectations with respect to safety and risk management. Of necessity, the primary technical hazards addressed are fires, explosions and toxic gas releases; these are the main hazards which process safety seeks to prevent and mitigate, and with which chemical engineers in a process environment will be concerned.

The Summer Institute model is, however, fully adaptable to other disciplines and professions. The 2006 Institute, planned for late May in Windsor, ON, is being lead by Minerva Canada and will focus primarily on business professors from across Canada. The 2007 Institute will be led by the CSChE PSM Subject Division and will again focus on engineering (chemical, but also with an attempt to involve mechanical engineering educators). This model has the potential over time to expand to virtually any engineering discipline for which a core group of risk management "champions" can be identified.

This requirement – risk management education for engineers – has also been identified by the NSERC (Natural Sciences and Engineering Research Council) Chairs in Design Engineering and Environmental Design Engineering. In their report, *Towards a Blueprint for Educating Design Engineers: Design Competency* (NSERC, 2005), they highlight the need for education in risk management and related topics on numerous occasions. Several examples from this report follow; page numbers refer to those in the report (NSERC, 2005):

- ***Page 16:*** The report quotes the CEAB definition of engineering design: *Engineering design integrates mathematics, basic sciences, engineering sciences and complementary studies in developing elements, systems and processes to meet specific needs. It is <u>a creative, iterative and often open-ended process subject to constraints that may</u> be governed by standards or legislation to varying degrees depending on the discipline. These degrees may <u>relate to economic, health, safety, environmental, social or other pertinent factors</u>.* (Underlining added to emphasize that this definition of engineering design embodies the essence of risk management.)
- ***Page 24:*** In the section on established skills for design engineers, the report refers to specific design-process activities such as Failure Modes & Effects Analysis (FMEA), safety methodologies, and human factors.
- ***Page 25:*** In the same section on established skills for design engineers, the report refers to required business skills including risk analysis.
- ***Page 26:*** In the same section on established skills for design engineers, the report refers to required technical skills such as familiarity with codes and standards as having been identified in industry surveys.

- ***Page 30:*** In a table giving the proposed definition of the design engineering competency, the report again identifies FMEA under the heading "knowledge of procedures". Under the heading "specific knowledge in a professional environment", the topics of standards, regulations, safety, liability, and ethics are all mentioned. Under the heading "cognitive skills", this listing appears: *To know one's limitations, to create, to look at the big picture, to manage projects (including the systems engineering perspective), to learn how to learn, to manage information and knowledge, to define a problem, to define potential solutions, to learn from past experience, to manage resources, to take risks (risk management).*
- ***Page 31:*** The report explains the design competency for safety with this opening line: *The practice of engineering is fundamentally about the protection of public safety*. The next sentence in this section is also very supportive of the thesis of the current paper: *As designers, graduating engineers should have been exposed to and had some experience with one or more of the classical techniques to identify and reduce safety risks.* (What is meant here is to identify hazards and then reduce the risks posed by these hazards.) The report identifies Hazard and Operability Studies (HAZOP), Failure Modes & Effects Analysis (FMEA), and Failure Trend Analysis (FTA) as three common techniques for hazard identification.
- ***Page 31:*** The report explains the design competency for liability with an explanation that the need to consider liability arises because engineers choose the degree of safety (i.e. the risk) appropriate for each product or service. If the choice is inappropriate, litigation is the likely result.
- ***Page 32:*** In explaining the design competency for codes, laws and regulations, the comment is made that all graduating engineers should be knowledgeable about WHIMIS (Workplace Hazardous Materials Information System) and its impact on their designs.
- ***Page 32:*** The explanation of the design competency for standards makes the point that standards play an essential role in raising levels of quality, safety and reliability. Environmental management systems such as ISO 14001 are also given as a necessary element for student exposure in the engineering curriculum.
- ***Page 34:*** In discussing the need for performance assessment against criteria and constraints, the comment is again made that safety is an important factor in all designs. HAZOP, FMEA, FTA, risk analysis, and comparison with existing codes and standards are all again mentioned as being useful in assessing the safety of a given design.
- ***Page 39:*** Finally, the required cognitive skill of risk management is identified as having the following purposes: *specifically identify factors that are likely to impact the objectives of a project with regard to scope, quality, time and cost; quantify the likely impact of each factor; give a baseline of project noncontrollables; mitigate impacts by exercising influence over project controllables*. These are precisely the objectives of the risk management process presented earlier in Figure 1.

A specific case in support of the general arguments advanced in NSERC (2005) can be found in the paper by Friesen et al. (2005). Here the authors describe their qualitative study of a three-course sequence in Biosystems Engineering design at the University of Manitoba. These educators list one of their goals for the second design course as being the introduction of project planning theory, safety, and human factors engineering. It is interesting to note the close match of this instructor goal with the students' perception of the course goals, which was to develop skills in communication, teamwork, time management, and consideration of safety in design.

Engineering educators and their industrial counterparts in the United States have also commented on the need for elements of risk management education in the undergraduate engineering curricula. In their report, *Educating the Engineer of 2020: Adapting Engineering Education to the New Century* (NAE, 2005), the US National Academy of Engineering makes the following recommendation:

In the interest of promoting success and avoiding failure, we recommend that engineering educators should explore the development of case studies of engineering successes and failures and the appropriate use of a case studies approach in undergraduate and graduate curricula.

The use of case studies is a widely accepted pedagogical tool in risk management education. This approach provides valuable information to facilitate the improvement of procedures, designs, operating conditions, etc. In the words of Crowl and Louvar (2002), one learns from history or one is doomed to repeat it. This is especially true in the field of risk management where one can learn from case studies and avoid hazardous situations, or ignore previous events and become involved in potentially life-threatening incidents.

CCPE Constituent Member Activities

The Canadian Council of Professional Engineers is a member-driven organization. The constituent members (CMs) of CCPE represent the twelve provincial and territorial regulatory associations. In attempting to answer the question: *Why risk management for engineers?*, it is therefore important to consider the question: *What are the activities of the CM's with respect to risk management?* The following list gives a partial answer based on the authors' personal knowledge; a more complete picture is needed and this is the subject of a recommendation made later in this paper:

- ***British Columbia:*** The issue of the required qualifications for structural engineers has been a prominent one for APEGBC for several years, in part because of the "leaky condo" issue. This, and other factors, lead to the formation some years ago of a CCPE task force on specialization and certification of professional engineers. As a participant on this task force, one of the authors of this paper (PRA) recalls the issue before the task force as being essentially a matter of risk assessment and management.
- ***Alberta:*** APEGGA has recently revised its *Guideline for Management of Risk in Professional Practice*, which focuses on what professional members can do to assess and manage the risks associated with their professional practices. APEGGA has previously produced the document, *Basic Learnings in Industrial Safety and Loss Management* (Wilson, 1998) for use by its professional members.
- ***Ontario:*** Similar to the matter of additional qualifications for structural engineers in British Columbia, PEO and its members have been faced with the issue of the qualifications required to conduct environmental site assessments and risk assessments in the revitalization of brownfields (contaminated industrial and commercial sites; Mastromatteo, 2005).

- ***Quebec:*** OIQ is currently working at defining a profile of competency for engineers engaged in the performance of risk studies. A subsequent phase of this work will be to develop a matrix of training courses (Lacoursiere 2005b).

In addition to the above partial listing of CM activities, all CMs have for the past few years been working on recommendations for their members on adapting engineering designs to the effects of climate change. CCPE has also worked in concert with the CMs to develop an action plan for climate change adaptation; risk management is an essential component of this plan to assist with the issue of uncertainty in climate change projections for design. A life-cycle design approach – again made possible only through deliberate assessment of risks – is required to deal with climate change impacts on the products of engineering work (Lapp, 2005). This is one of a number of practice areas where the need for knowledge of professional liability insurance arises on the part of engineers.

Technical Society Initiatives

In addition to being a member of a regulatory body (e.g. APENS and APEGGA, respectively, in the case of the current authors), many engineers in Canada also belong to their relevant discipline-specific technical society. For the authors of this paper, this means that we are also members of the Canadian Society for Chemical Engineering (CSChE). In addition to examining CCPE CM activities in the area of risk management, it was felt to be a useful exercise to briefly examine the activities of selected technical societies in this area. The examination here is indeed brief, and is incomplete; nevertheless it is somewhat revealing.

Both authors of this paper are members of the executive of the Process Safety Management (PSM) Subject Division of the CSChE. This is one of the more active subject divisions in the society and is predominantly made up of industrial members (in a technical society that overall draws its membership primarily from academia). Even a cursory look at the PSM division web site (PSM, 2006) will identify many helpful (and free) products, including:

- ***Site Self-Assessment Tool:*** This is a question-based document that is useful in establishing a baseline of a facility's current level of risk-awareness and use of the important techniques for preventing process-related incidents. The tool can also assist in identifying priority areas for improvement.
- ***Guidelines for Site Acute Risk Communication:*** This document provides guidance on communication of risks from sudden events resulting from site operations and their implications for the surrounding community.
- ***Process Safety Management Guide (Third Edition):*** This document gives an overview of process safety management (PSM, the management system) for facilities handling hazardous materials.

Risk management for the Canadian Society for Chemical Engineering is taken seriously as the above listing demonstrates (and as would be expected given the hazards and risks faced by chemical/process engineers in industry). An "experiment" was conducted for the purposes of this paper to see if other Canadian engineering technical societies posted risk-based information on their web sites. This exercise was conducted in a half-hour search (total) of the web sites of the technical societies for three major engineering disciplines (as of mid-January 2006). The admittedly unscientific results are as follows:

- ***Canadian Society for Mechanical Engineering:*** The CSME web site (CSME, 2006) contained a notice of the Climate Change Technology Conference being organized by the Engineering Institute of Canada (EIC) for May 2006 in Ottawa. There was also a notice for the CSME Forum 06 to be held in Calgary in May 2006. The Call for Papers for this conference lists *Reliability Engineering* and *Safety Engineering* as suitable mechanical engineering topics for presentation.
- ***Institute of Electrical and Electronics Engineers, Inc.:*** The IEEE web site (IEEE, 2006) offered an online newsletter (Spectrum); the December 2005 issue contains a short article on potential risks from nanotechnology. Another link yielded a recent review of a book titled *Information Security Risk Analysis*. A third link housed a PowerPoint presentation from a 2004 IEEE Power Systems Conference, titled *Asset Management, Risk, and Distribution System Planning*.
- ***Canadian Society for Civil Engineering:*** The CSCE web site (CSCE, 2006) yielded perhaps the most interesting result – the 2004-05 annual report of the society. In this report, the executive director commented on the results of a recent workshop held to determine the CSCE focus for the coming year. Eight focus areas were listed as strategic priorities, three of which have direct and strong links to risk management: *safety/health concerns; applications of sustainable development (i.e. water management/communities, climate change); infrastructure renewal (asset management, intelligent transportation systems, etc.).*

Are these indications of significant risk management activities within technical societies other than the CSChE? As in the previous section on CM activities, only a partial answer can be given at present – *perhaps*. Again, a more complete picture is needed and this is the subject of a recommendation made later in this paper.

WHY RISK MANAGEMENT FOR *ALL* ENGINEERS?

It is our belief that the answer to this question has already been given by the nature of the discussion in the previous section: *Why risk management for engineers?* The points raised previously have been general and for the most part have not been targeted at any one, specific engineering discipline. Granted, some of the examples have come from the world of process engineering; this is simply a reflection of two basic factors. First, and most obviously, the education and training of the authors is as chemical/process engineers. Second, process plants and facilities often involve severe operating conditions and the potential for disaster is ever-present. This does not excuse events such as Bhopal and Seveso, but it does help to explain why when things go wrong in a chemical plant, the consequences can be catastrophic and the public and regulatory reactions strong.

Engineers in different disciplines may well face different hazards and subsequent consequences, but the generic process of managing risk (Figure 1) is universal. It is reasonable to expect that a chemical engineer would be familiar with HAZOP as a means of identifying hazards, whereas an electrical engineer might not. Similarly, a mechanical engineer would likely be familiar with FMEA because of this technique's use in identifying failure modes of equipment and machinery (e.g. a valve or a pump). An electrical engineer might be well-suited to an understanding of Fault Tree development, particularly for quantitative risk assessment, because of the Boolean logic involved.

The above comments are somewhat stereotypical, but the point is made that different hazard identification and risk analysis tools exist for a variety of engineering applications. Of course, engineering work does not always settle out along disciplinary lines as the previous paragraph might seem to suggest. The nature of modern engineering work further highlights the need for risk management knowledge by ***all*** engineers.

The Engineering Team

Engineering projects are often undertaken by a multi-disciplinary team. In a narrow sense this would mean a team of engineers from different primary disciplines. Taking a broader view, this would mean a "true" multi-disciplinary team with some or all of the following qualifications: engineers (with different skills and knowledge), technologists, scientists from the natural or social sciences, lawyers, business graduates, policy makers, public relations experts, etc. For the engineers in such a team, it would be critical that they understand the process of managing risks. Additionally, they must be aware of the fact that their own view of risk management will not necessarily be the same as that held by someone with a different background. It is not an oversimplification to state that an engineer may focus on mitigating the risk from fire or explosion, a business manager may concentrate on reducing financial exposure, and a lawyer may attempt to reduce liability in the case of future litigation. Each, in their own mind, is engaged in the process of risk management.

The previous paragraph touches on an important aspect of risk management that to this point has not been explicitly discussed, but which nevertheless is implicit in all of the points raised. This aspect is *risk communication*. It is sometimes said that there are actually three components to risk – probability, severity, and *perception*. The risk management process can easily break down if the recognition is not made that different people perceive risk in different ways and have different levels of risk tolerance. This may be the case within the risk management team itself (as described above), but it is arguably even more critical when considering the ways in which risk is perceived by the various stakeholders affected by risk management decisions – company employees, shareholders, regulators, community neighbours, the general public, etc. Effective risk communication at all stages shown in Figure 1 is essential for the process to succeed.

For example, community awareness around risk is growing in Canada and several communities are developing policy in the form of bylaws and development guidelines. This in itself is evidence of the need for the engineering world to become more knowledgeable and better trained in the field, as engineers become more involved in conducting such community-based risk assessments. The need for good risk communication skills will become evident as engineers explain their risk studies not to other engineers, but to regulators and the public. An additional point to note is that engineering companies within these communities will themselves become subject to the results of these risk studies; knowledge of the risk management process then becomes important from a business operation perspective.

These features of multi-disciplinary risk teams and broad-based community needs for risk management have been recognized in many quarters – for example, the federal government. In March 2004, the Natural Sciences and Engineering Research Council (NSERC) and Public Safety and Emergency Preparedness Canada (PSEPC) announced a joint program to fund research in the area of critical infrastructure interdependencies. The following excerpts from the announcement (with underlining for emphasis) are particularly relevant to the argument that risk management is required knowledge for all engineers:

- *Under the program, <u>scientists and engineers in the academic, industrial and government sectors</u> will work together to understand the connections between the country's major <u>energy, communications, finance, health care, food, water, and transportation systems</u>, and <u>what happens when a system fails</u>. Each is complex, but their interdependencies, which can leave them vulnerable to cascading collapses, are even less well understood.*
- *Our key underlying infrastructures in this country are becoming increasingly complex and interconnected, said Janet Walden, NSERC's Vice-President, Research Partnerships Program. It is important that we understand the links between our critical infrastructures and their vulnerabilities so that we can <u>minimize the risks to Canadian society in the event of failure</u>.*
- *Recent events, including the August 2003 blackout in Ontario and northeastern USA, have clearly demonstrated the domino effect possible when a failure in one system due to an accident, natural disaster or act of terrorism can lead to multiple failures in other systems, said NSERC President Tom Brzustowski. NSERC is proud to be partnering with PSEPC to support this important research whose goal is <u>to protect us all from the potential harm of such eventualities</u>.*

The last bullet above identifies a new set of risks for industry that have come to the forefront in the past four or five years – acts of terrorism. While sabotage has long been recognized as an issue of concern, the post-September 11 world lives with a heightened awareness of the need for risk management of its nuclear reactors, chemical plants, oil refineries, transportation systems, food and water supplies, etc. Issues of site security and vulnerability to acts of terrorism are receiving increasing attention. For example, one of the authors of this paper (PRA) regularly attends the annual Loss Prevention Symposium of the American Institute of Chemical Engineers. Whereas years ago the papers presented would deal almost exclusively with risk from major process hazards, the past couple of years have seen presentations on facility protection and site security (e.g. by means of physical barriers), as well as "balanced" communication of on-site hazards and risks to off-site stakeholders.

This last point is particularly important given that one of the basic principles of the previously mentioned Responsible Care® program is to communicate with the public on the hazards and risks posed by chemical facilities in their communities. The information provided clearly must be well thought-out and balanced between the needs of the public to know, and the needs of a company to protect its people and physical assets from malicious acts. This is an evolving area of risk management for the modern engineering team.

Another feature of the engineering team today that highlights the need for risk management knowledge by all engineers is the common practice of outsourcing or contracting of engineering services. Engineering contractors routinely provide specialized services to other engineering firms. This is often the case on large projects where partnerships and joint ventures are formed, but may also apply to smaller projects through the awarding of subcontracts. Success on these projects is in large measure determined by the degree of commonality in risk management practices among the different parties. Not the least of the concerns is whether there is a common set of expectations for safety performance and risk-awareness (Horwood, 2005).

The need for risk management competence in the field of project management is further highlighted by the activities of the Project Management Institute. The web site (PMI, 2006) of this organization representing over 200,000 professionals worldwide gives several examples of risk management applications – for example, courses and seminars on risk management, a "special interest group" (SIG) dedicated to risk management, and a body of knowledge for project management that includes a separate section on risk management principles.

As a final note to this section, reference is made to three international efforts on risk management. These examples serve two purposes. First, they provide a snapshot of some of the risk management activities occurring or originating outside Canada. Second, these examples fully support the argument advanced in this paper that risk management is an area of knowledge required for all engineers. Each of these initiatives is multi-disciplinary and involves all members of "the engineering team":

- ***OECD Workshop:*** In September 2003, the OECD (Organization for Economic Co-operation and Development) held a workshop in Montreal, QC in conjunction with OIQ, titled *Sharing Experience in the Training of Engineers in Risk Management*. The key Canadian organizer was Jean-Paul Lacoursiere, ing. and there were approximately 80 attendees from 13 countries. Participants were unanimous in their endorsement of the position that professional engineers need to be made aware of their responsibilities to their colleagues, their employers and society, and that they need to integrate risk management into their work. There was also strong consensus that risk management should be part of the undergraduate education for all engineers (Lacoursiere, 2003).
- ***Hydrogen Safety:*** The University of Ulster in the UK is leading an international consortium to develop an "e-Academy of Hydrogen Safety" under the auspices of the European Network of Excellence – Safety of Hydrogen as an Energy Carrier (NoE HySafe). The motivation for this effort comes from the fact that the onset and further development of the hydrogen economy are being constrained by safety barriers as well as by the level of public acceptance of new applications (Dahoe & Molkov, 2005). A focal point of the work is the development of educational and training programs in hydrogen safety.

  The description given by Dahoe & Molkov (2005) indicates that the approach is one of an undergraduate education based on an engineering science core (fluid dynamics, thermodynamics, kinetics, solid mechanics, and heat and mass transfer), supplemented by topics and additional courses with an emphasis on hydrogen safety, as well as postgraduate degree programs dedicated to hydrogen safety. With this model, hydrogen safety education is seen to be relevant to the following branches of engineering:

aerospace, chemical, civil, electrical, environmental, fire and explosion safety, materials, mechanical, and nuclear.

This important work has progressed to the point where an *international curriculum in hydrogen safety engineering* has been developed and is available for viewing on the HySafe web site (HySafe, 2006). This curriculum contains a module on risk assessment having the following components:

- General risk assessment and protective measures for hazardous materials processing and handling.
- Effect analysis of hydrogen accidents.
- Risk assessment methodologies.
- Hazard identification and scenario development.
- Vulnerability analysis.
- Application of hazard identification in the basic processes of the hydrogen economy.
- Application of vulnerability analysis to mitigation technologies in the hydrogen economy.

- ***ETPIS:*** The European Technology Platform on Industrial Safety (ETPIS) was launched in late 2005, with Jean-Paul Lacoursiere, ing. present from Canada. This is a massive, multi-year, multi-disciplinary, international research program aimed at improving the competitiveness and sustainability of European industry through improved risk management. The draft strategic research agenda for this program (ETPIS, 2005) is itself a massive document (127 pages) which the authors of the current paper have not yet had time to thoroughly review. Based on a quick scan, it seems that the program is extremely comprehensive in scope with respect to risk assessment and management methodologies, human and organizational factors, emerging and cross-cutting risk areas, areas of practice, and educational/training needs. It is our belief that this is an important international initiative of which Canadian engineers should be well aware; further information can be found on the ETPIS web site (ETPIS, 2006).

  The introductory portion of the executive summary (ETPIS, 2005) is reproduced below to give an indication of the wide-ranging program scope described above; the following passage also serves to reinforce the thesis of the current paper:

  It is expected that improvement of industrial safety will promote the competitiveness of the European industry. Improved risk control will support the sustainable growth of the European industry. There is benefit to be expected from a co-ordinated effort in research across industry sectors. Today this is fragmented.

  The ETPIS recognizes that only an integrated approach to risk assessment and management, including man-machine interactions, organizational and cultural factors and the influence of safety culture, is able to cope adequately with the aim of introducing better and integrated safety standards and practice across the European industry. It also recognizes that only through education and training is it possible to achieve the necessary condition in which managers, technology developers and designers create safe systems and operators use and maintain the systems in a safe way.

> *The methods include modelling the risk, reliability and availability of the systems throughout their lifetime so as to be able to study the impact of new maintenance and repair schemes on system safety, life cycle costs, reliability, serviceability and quality. Another major problem facing many industrial products, structures and facilities in general is the need to extend lifetime and to ensure that this extension does not degrade the safety level of operation. This problem is being dealt with in different industries, using the same main theoretical background but developing different strategies and approaches. Thus, methods for the assessment of existing structures and equipment will be addressed as well as approaches and criteria for extending the lifetime of products and industrial systems safely and with adequate levels of risk, reliability and availability.*
>
> *For safety to be maintained throughout the operational life, safety management systems are required, which deal with physical systems, processes and people using measures that include prevention, control and mitigation, emergency response and recovery, which will be used in different mix depending on the nature of hazards, precursors, escalation scenarios and potential loss.*
>
> *The ETPIS will closely co-operate with the industry-specific platforms to turn the methods and technologies developed within the Platform into practical, accessible and easy to apply principles and tools, which requires an industry-specific approach. This will help the industry practitioners to identify and prevent potential risks, understand and improve safety culture, and understand what other factors have an influence on safety.*

It is our opinion that an accurate paraphrasing of the above passage would be: *Risk management is an area of knowledge required by all engineers*.

Case Studies

We have previously remarked that case studies are one of the most effective tools for risk management education. There is a tendency when using this approach to place grater emphasis on engineering failures rather than successes. The fact that such case studies are readily available in the literature, and cover a spectrum of industrial applications and engineering disciplines, is a sobering reality.

To further support the argument of risk management being essential knowledge for all engineers, we have provided a brief review of the case studies in three selected references (one of which was co-authored by one of the authors of the current paper – DJM):

- ***Hopkins (2000):*** In his book, *Lessons from Longford: The Esso Gas Plant Explosion*, Andrew Hopkins describes the 1998 gas plant explosion at Longford, Victoria (Australia) initiated by cold metal embrittlement of a heat exchanger. Relevant engineering disciplines would include chemical, materials, mechanical, and petroleum. Hopkins (2000) also describes the 1994 explosion at the Moura coal mine in central Queensland, Australia. The relevant engineering discipline in this case is mining.
- ***Hopkins (2005):*** In this previously referenced book, *Safety, Culture and Risk*, Andrew Hopkins first describes the 1999 train crash that occurred outside the Glenbrook station in

Sydney, Australia. Here, it is more instructive to identify the areas of engineering practice that would be relevant; these include scheduling, and systems design and control. Hopkins (2005) also provides an interesting case study of the Royal Australian Air Force over an approximately 20-year period (late 1970's to 2000). The case involved work on the fuel tanks of the Air Force's F111 fighter bombers in which serious health issues were incurred by numerous personnel. The relevant engineering activity here is maintenance; the area of concern is not an acute safety issue (as with Longford, Moura and Glenbrook), but rather one of occupational health and industrial hygiene.

- ***Wilson & McCutcheon (2003):*** In *Industrial Safety and Risk Management*, Laird Wilson, P.Eng. and Doug McCutcheon, P.Eng. give several case studies covering a variety of engineering disciplines, activities, hazards, and risks:
  - *Flixborough (UK, 1974)* – cyclohexane vapour cloud explosion at a chemical facility; 28 fatalities.
  - *Piper Alpha (North Sea, 1988)* – gas and oil explosions on an offshore platform; 167 fatalities.
  - *Challenger Space Shuttle (USA, 1986)* – explosion; 7 fatalities.
  - *Hyatt Regency (Kansas City, 1981)* – collapse of two suspended walkways in a hotel; 114 fatalities.
  - *Titanic (Atlantic Ocean, 1912)* – sinking of passenger vessel; over 1500 fatalities.
  - *Lodgepole (130 km southwest of Edmonton, 1982)* – gas well blowout/major fire; 2 fatalities.
  - *Syncrude (Fort McMurray, 1984)* – hydrocarbon fire in Coker 8-2; no fatalities.

What distinguishes each of these case studies from the others is that they give quite specific examples for each engineering discipline and area of practice. There are, however, two key unifying factors. First, each incident resulted in varying degrees of loss in all four categories of people, environment, assets and production. Second, all of these incidents have the same fundamental cause. Only on a very superficial level did cold metal embrittlement cause the Longford explosion, a violation of procedures cause the Glenbrook crash, and an iceberg cause the Titanic to sink. The root cause of all these cases (Hopkins, 2000 & 2005; Wilson & McCutcheon, 2003) is ***inadequate risk management***. This means that there are useful lessons to be learned from each case study for all engineers regardless of their background. The following case study demonstrates the validity of this statement.

Westray

Worker Safety Not My Responsibility Says Ex-Westray Engineer
(newspaper headline during Westray trial)

The Westray coal mine explosion occurred in Plymouth, Nova Scotia on May 9, 1992, killing 26 miners. The methane levels in the mine were consistently higher than regulations, a situation caused by inadequate ventilation in the mine. Flammable dust concentrations were also higher than permissible levels due to inadequate cleanup of coal dust and the fact that there was no crew in charge of rock dusting (inerting the coal dust with limestone or dolomite). These and many other factors contributed to the poor work conditions that continually existed in the Westray mine and made it an incident waiting to happen. All of these substandard conditions and practices could be attributed to the lack of concern that management held towards safety issues in the mine, which was one of the primary root causes of the problem at Westray.

The analysis that follows (Goraya et al., 2004) relies exclusively upon public domain references, primarily the Report of the Westray Mine Public Inquiry – Justice K. Peter Richard, Commissioner (Richard, 1997). Use is made of a technique known as the domino loss causation model (Bird & Germain, 1996), which is a helpful tool for understanding the root causes of an incident. This technique facilitates the identification of immediate causes and then more fundamental causes existing at the management level (Amyotte & Oehmen, 2002).

The first step is to define the incident itself – an explosion in the Westray mine on the morning of May 9, 1992. This incontrovertible fact means that the fire triangle criteria (fuel, oxidant and ignition source) were satisfied. Richard (1997) gives the fuel source as initially an accumulation of methane (due to methane layering at the mine roof) which, once ignited, triggered a full-scale coal dust explosion. The oxidant was the oxygen in the mine atmosphere. The methane ignition source is postulated to have been sparks from the continuous miner striking pyrites or sandstone at the coal face being worked in the Southwest section of the mine (Richard, 1997).

In a matter of seconds, the Westray site changed from that illustrated in Figure 2 (pre-explosion) to the destruction depicted in Figure 3. The No. 1 main portal shown in Figure 3 is located behind the two concrete silos pictured in Figure 2.

The next step in the domino model is to identify the losses through consideration of the categories of people, environment, assets and production. Losses resulting from the Westray explosion include the following:

- Deaths of 26 human beings and the enormous personal losses faced by the 26 miners' families. These losses are the most devastating legacy of the Westray explosion.
- Extensive damage to the mining equipment and the mine itself (which was eventually purposely flooded).
- Bankruptcy of the parent company, Curragh Resources. The mine was closed because it had been rendered inoperable; this removed an additional company revenue source.
- Default of millions of dollars in provincial and federal government loans; millions of dollars in severance, worker's compensation, pension plan, and unemployment insurance payments.
- Cost of holding a public inquiry and running an extensive criminal investigation and trial involving the mine and underground managers.
- Loss to Nova Scotia Power (electrical utility company) of approximately 700,000 tonnes of Westray coal.

The domino model next identifies immediate causes. These, as the name implies, are factors that immediately precede and thus lead to an incident. They can be broken out into the categories of substandard practices and substandard conditions, which for Westray include the following:

- ***Substandard Practices:***
    - Poor housekeeping with respect to clean-up and removal of coal dust.

Figure 2 Aerial view (pre-explosion) of Westray mine site (from Richard, 1997).

Figure 3 Damage to portal at No. 1 main, Westray coal mine (from Richard, 1997).

    - Storing fuel and re-fuelling vehicles in non-flame-proof areas.
    - Improper use of ventilation system (e.g. re-routing without provision for miners).
    - Inadequate application of rock dust (a thermal explosion inhibitor).
    - Continuation of mining in spite of inoperable methane detection devices.
- ***Substandard Conditions:***
    - High methane concentrations.
    - Thick layers of coal dust on the mine floor, having a high level of combustible matter.
    - Inadequate ventilation system design and capacity.
    - High concentrations of airborne coal dust.
    - Inadequate system to warn of high methane concentrations in the mine.

The next layer of model causation is known as basic causes, which are the underlying or root causes for the existence of immediate causes. These are broken out into two broad categories – personal factors and job factors. These factors for Westray include the following:

- ***Personal Factors:***
    - Physiological stress caused by methane overexposure and fatigue due to 12-hour shifts.
    - Lack of mining experience of personnel working in the mine.
    - Lack of knowledge of safe underground work practices.
    - Improper motivation by which production proceeded at the expense of safety.
    - Psychological stress due to fear of reprisal for reporting safety concerns.
- ***Job Factors:***
    - Inadequate follow-through on recommendations from mine inspectorate personnel.
    - Inadequate engineering during mine design and planning with respect to potential loss exposures (e.g. mine ventilation; intersecting geological fault lines leading to frequent roof-falls).
    - Lack of safe work practices and procedures.
    - Inadequate purchasing and maintenance of rock dust inventory.
    - Inadequate leadership in terms of assignment of responsibility (e.g. mine examiner and production supervisor responsibilities undertaken by the same person).
    - Lack of proper orientation and training for new employees.
    - Poor communication of standards (e.g. concerning the roles and responsibilities of occupational health and safety committees).

The final model step is to look for evidence of causation at the management level of the company; in essence, to look for management system deficiencies that permit the existence of the immediate and basic causes. The domino model helps to identify lack of management control factors in three areas: the loss management program or system itself, the standards identified and set for the loss management program, and the degree of compliance with such standards. As described in previous sections of this paper, safety management systems, standards, and compliance with standards are all key concepts in the risk management process – i.e. the identification of hazards, analysis and assessment of risk, and implementation of risk reduction and risk monitoring measures.

This final level of incident analysis is, then, a structured search for risk management deficiencies, which for Westray include the following:

- ***Inadequate Program Elements:***
  - Management commitment and accountability to safety matters.
  - Management of change procedures.
  - Incident investigation (including near miss reporting and investigation).
  - Training (orientation, safety, task-related, etc.).
  - Task definition and safe work practices and procedures.
  - Workplace inspections and more detailed hazard identification methodologies.
  - Program evaluation and audits.
- ***Inadequate Program Standards:***
  - Concern expressed by management toward safety matters.
  - Follow-through on inspections for substandard practices and conditions.
  - Action on hazard reports submitted by employees.
  - Job instructions for employees.
  - Equipment maintenance.
  - Scheduling of management/employee meetings to discuss safety concerns.
- ***Inadequate Compliance Factors:***
  - Correlation between management actions and official company policy concerning the relationship between safety and production.
  - Compliance to industry practice and legislated standards concerning numerous aspects of coal mining: methane concentrations, rock dusting, control of ignition sources underground, etc.

There are clearly lessons to be heeded from Westray for the coal mining industry and mining engineers – reminders of the importance of, for example, rock dusting and underground ventilation. These reminders are technical in nature, and would seem to find little application in other practice areas and engineering disciplines, other than perhaps by extension into the realm of explosion suppression and mitigation techniques such as relief venting. The most critical lessons from Westray, however, are the ones that transcend industrial boundaries and are related to the basic principles of risk management.

These lessons are found in the risk management deficiencies previously identified. These deficiencies clearly indicate the need for attention to both *system* and *attitude* (or *cultural*) perspectives. A risk management *system* – implemented, supported and enforced by management personnel – is absolutely essential. The only acceptable *attitude* toward industrial safety – both morally and, in the case of present-day Nova Scotia, legally – is expressed by the Internal Responsibility System, or IRS. This concept, which is the foundation of occupational health and safety legislation in Canada, states that every individual in an organization is responsible for health and safety. Primary responsibility lies with each person (manager, supervisor, employee, contractor, etc.) to the extent of their authority and ability to ensure a safe and healthy workplace. The IRS, in the terminology of Hopkins (2005), is intended to facilitate *risk-awareness* in a company. This is clearly a lesson applicable to ***all*** engineers.

RECOMMENDATIONS FOR THE ENGINEERING PROFESSION IN CANADA

Based on the analysis in this paper we offer the following suggestions to advance the state of risk management education, training and practice by engineers in Canada:

- ***Canadian Engineering Accreditation Board (CEAB):***
  - Consider the retention of risk management as a required graduate attribute in the draft revised accreditation criteria.
  - Consider the development of specific questions and measuring tools concerning risk management for use by accreditation visiting teams.
- ***Canadian Engineering Qualifications Board (CEQB):***
  - Consider the development of a national *Guideline on Risk Management for all Professional Engineers*, the concept being similar to the existing national *Guideline on the Environment and Sustainability for all Professional Engineers* (in that risk management is an area of knowledge for ***all*** engineers).
  - Consider the development of documentation that is more detailed than a national guideline; such documentation would be practice-oriented and would provide best-practice methodologies for specific applications.
- ***Canadian Council of Professional Engineers (CCPE):***
  - Consider holding a national workshop on risk management, the concept being similar to the previous CCPE-organized national workshop on climate change adaptation.
  - Consider mechanisms to enable Canadian engineers to benefit from international initiatives in risk management education and development of practice methodologies.
- ***CCPE Constituent Members (CMs):***
  - Consider participation in a survey of CCPE CMs concerning risk management activities and needs of the CM and its members. Such a survey could be part of a wider CCPE-led consultation with the CMs.
- ***National Council of Deans of Engineering and Applied Science (NCDEAS):***
  - Consider surveying Canadian Faculties of Engineering concerning risk management courses, programs, and integration of concepts in coursework. Both undergraduate and graduate offerings would be useful information to know.
- ***Engineering Technical Societies:***
  - Consider participation in a survey of Canadian engineering technical societies concerning risk management tools, courses, case studies, and other products and services available through the society.
- ***CCPE Research Committee (RC):***
  - Consider co-ordination of the above activities (e.g. surveys) as appropriate.

These recommendations are made, in most cases, with little knowledge of the current work plan of these organizations. It may be that a specific suggestion is too labour intensive for the group identified, or perhaps the recommendation falls outside the group's mandate. Although this may be the case, we believe that the substance of the recommendation would remain valid.

CONCLUDING REMARKS

We have attempted to present the case that risk management is an area of knowledge with which all engineers should be familiar. There are significant activities already underway within Canadian industry, government and universities. There is more, we believe, that could and should be done. There are also major risk management initiatives underway in other countries from which Canadian engineers could benefit.

We have made several recommendations for other organizations to consider with the intention of advancing risk management education, training, and practice competency in Canada. We are personally prepared to assist in this process, and are confident that our colleagues engaged in risk management education and practice would also be willing to contribute.

REFERENCES

Alp, E. (2000). *Personal Communication*.

Amyotte, P.R. (2004). A meeting of the minds. *Canadian Chemical News*, **56** (2), 14-15.

Amyotte, P.R. (2005). CSChE-PSM summer institute – round two. *Canadian Chemical News,* **57** (8), 34-35.

Amyotte, P.R. & McCahill, P. (2004). A meeting of the minds – part 2: report on the 2004 CSChE-PSM summer institute. *Canadian Chemical News*, **56** (9), 27-31.

Amyotte, P.R. & Oehmen, A.M. (2002). Application of a loss causation model to the Westray mine explosion. *Process Safety and Environmental Protection*, **80**, 55-59.

APENS (1989). *Canons of Ethics for Engineers*. Appendix to By-Laws, The Nova Scotia Engineering Profession Act, Halifax, NS: Association of Professional Engineers of Nova Scotia.

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

CCPS (2001). *Making EHS an Integral Part of Process Design*. New York, NY: American Institute of Chemical Engineers.

CEAB (2005). *Accreditation Criteria and Procedures*. Canadian Engineering Accreditation Board, Ottawa, ON: Canadian Council of Professional Engineers.

CSCE (2006). *Canadian Society for Civil Engineering*. www.csce.ca (February13, 2006).

CSME (2006). *Canadian Society for Mechanical Engineering*. www.csme-scgm.ca (February 13, 2006).

Crowl, D.A. & Louvar, J.F. (2002). *Chemical Process Safety – Fundamentals with Applications*. Second Edition, Upper Saddle River, NJ: Prentice Hall PTR.

Dahoe, A.E. & Molkov, V.V. (2005). *Towards Hydrogen Safety Education and Training*. University of Ulster, UK (Personal copy communicated by A.E. Dahoe).

ETPIS (2005). *Safety for Sustainable European Industry Growth: Strategic Research Agenda*. Draft Version 4, European Technology Platform on Industrial Safety.

ETPIS (2006). *European Technology Platform on Industrial Safety*. www.industrialsafety-tp.org (February 13, 2006).

Friesen, M., Taylor, K.L. & Britton, M.G. (2005). A qualitative study of a course trilogy in biosystems engineering design. *Journal of Engineering Education*, **94**, 287-296.

Goraya, A., Khan, F.I. & Amyotte, P.R. (2004). An inherent-safety based incident investigation methodology. *Process Safety Progress*, **23**, 197-205.

Hopkins, A. (2000). *Lessons from Longford: The Esso Gas Plant Explosion*. Sydney: CCH Australia Limited.

Hopkins, A. (2005). *Safety, Culture and Risk*. Sydney: CCH Australia Limited.

Horwood, J. (2005). *Personal Communication*.

HySafe (2006). S*afety of Hydrogen as an Energy Carrier*. www.hysafe.org (February 13, 2006).

IEEE (2006). *Institute of Electrical and Electronics Engineers*. www.ieee.com (February 13, 2006).

IRM (2006). *Institute of Risk Management*. www.theirm.org (February 13, 2006).

IRMI (2006). *International Risk Management Institute*. www.irmi.com (February 13, 2006).

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

Lacoursiere, J.-P. (2003). *Personal Communication*.

Lacoursiere, J.-P. (2005a). Bhopal and its effects on the Canadian regulatory framework. *Journal of Loss Prevention in the Process Industries*, **18**, 353-359.

Lacoursiere, J.-P. (2005b). *Personal Communication*.

Lapp, D. (2005). Engineers and climate change: what you need to know. *Engineering Dimensions*, **26** (2), 51-53 (Professional Engineers Ontario).

Mastromatteo, M. (2005). Brownfields: waiting for the other shoe to fall? *Engineering Dimensions*, **26** (2), 54-57 (Professional Engineers Ontario).

NAE (2005). *Educating the Engineer of 2020: Adapting Engineering Education to the New Century*. National Academy of Engineering of the National Academies, Washington, DC: National Academies Press.

NSERC (2005). *Towards a Blueprint for Educating Design Engineers: Design Competency*. Version 7.0 (February 21, 2005), NSERC (Natural Sciences and Engineering Research Council) Chairs in Design Engineering and Environmental Design Engineering.

PMI (2006). *Project Management Institute*. www.pmi. org (February 13, 2006).

PSM (2006). *Process Safety Management Subject Division, Canadian Society for Chemical Engineering*. www.cheminst.ca/divisions/psm/index.htm (February 13, 2006).

Richard, Justice K.P. (1997). *The Westray Story – A Predictable Path to Disaster*. Report of the Westray Mine Public Inquiry, Halifax, NS: Province of Nova Scotia.

Shrives, J. (2004). Environment Canada’s new environmental emergency regulations. *Canadian Chemical News*, **56** (2), 17-21.

Stelmakowich, A. (2004). Dutifully yours. *OHS Canada*, **20** (1), 34-39.

Wilson, L. (1998). *Basic Learnings in Industrial Safety and Loss Management*. Edmonton, AB: Association of Professional Engineers, Geologists and Geophysicists of Alberta.

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