ENGG404

A Handbook for Becoming a Leader in Safety and Risk Management

ENGG 404 Table of Contents

ENGG404

Chapter 1:
Fundamentals of Risk Management

Chapter 1: Introduction and Fundamentals of Risk Management

An Introduction to this Handbook:

The core message for this handbook is that all workplace incidents can be prevented. Unfortunately, despite our efforts, loss incidents occur. This unfortunate reality has been demonstrated many times in incidents such as:

- Piper Alpha, UK (1988), where 167 people died after an explosion and fire at an offshore platform;
- Bhopal, India (1984), where a gas leak killed over 20,000 people in the surrounding area; and
- Vajont Dam, Italy (1963), where 2,000 people downstream lost their lives after a landslide generated a tsunamic wave within the dam reservoir.

The reader should not be deceived in thinking these incidents only threaten operations or industries with immature safety cultures. NASA's Challenger (1986) and Columbia (2003) occurred in what was at the time, and still is, a leader in safety protocols and culture. Moreover, these are not losses of the past. More recent incidents include:

- Lac-Mégantic train derailment (2013) in Quebec, which killed 47 people;
- Mount Polley tailings storage facility breach (2014) in British Columbia, causing a spill of 10 million m^3 of water and 4.5 million m^3 of mining waste into the environment, including the nearby surface waters; and
- BP Macondo Deepwater Horizon (2010) blowout in the Gulf of Mexico, killing 11 and seriously injuring 16, releasing over 200 million gallons of crude oil, with an inestimable impact on the marine environment, wildlife, and fisheries.

The good news is that industries with strong leadership in engineering safety and risk management have demonstrated a substantial year-over-year decrease in lost time incidents, as well as improvements in productivity. This, in turn, can minimize the potential for large consequence events similar to those mentioned above. This handbook emphasizes that not only is risk management necessary to avoid loss incidents, but it also goes a long way towards improving productivity, efficiency, quality, and ultimately, business sustainability.

The following sections present the fundamentals of a risk management system and its elements; an overview of the risk assessment process, management of change and incident investigations; and a tool kit for practicing risk management at different levels within an organization. This handbook underscores the importance of creating a robust safety culture within an organization, including upper management, supervisors, front-line workers, regulators, and contractors. The intricacies of human behaviour and their effect on safety are also examined and tools are provided for positively influencing the safety culture around you. The lessons in this handbook are further illustrated with a suite of case studies provided as a separate chapter.

Section 1.1: The Engineer's Survival Guide

Unfortunately, disasters have happened. Engineers, business leaders and managers, most being good people with the best of intentions, have made decisions that ended in disaster—a disaster beyond anything these good people had envisioned. None of them set out to cause harm to others, damage property, impact the livelihood of others, nor adversely impact the environment. Being at the centre of such disasters, these people came to tragically understand the impact of their decisions.

Poor decisions are made when an engineer is pressured to make quick decisions without fully understanding the consequences of those decisions. The application of the Engineer's Survival Guide will help an engineer avoid a poor decision.

It is our intent that you apply sound risk management principles, that none of you becomes central to a tragic incident, and that none of you becomes the author of a future case study in engineering safety and risk management. As case studies are reviewed, keep the **Engineer's Survival Guide** in mind (i.e., which point(s) could have averted the conditions or situations that arose, and prevented the catastrophic event?).

The Four Key Points of the Engineer's Survival Guide

1) **Understand organization values**
   - Review organization policy (core values and corporate ethics) and determine whether safety is a value.
   - When safety is elevated from being a priority to becoming a value, it supports sustainable safety and risk management. Remember that priorities change, values do not. Values are the compass that set the culture in an organization.

- Check if the organization has a safety culture: a culture where safety considerations come ahead of any action to complete a task; a culture where safety considerations are the basis for decision making when considering a course of action.

2) **Understand your program**
   - Determine if the organization has a safety and risk management program, understand your personal responsibilities to meet program requirements, and undertake those responsibilities diligently. People's lives and your organization's business may depend on it.

3) **When you make decisions, put safety ahead of any other objective**
   - Even under compelling or stressful circumstances, safety takes precedence over production, cost, schedule, and any other competing objective.
   - When safety takes a backseat to other objectives, we are exposing people, the environment, and the organization to increased risk. Continued operation at increased risk means it is not a matter of "if" but rather "when" a tragic incident will occur.

4) **Pay attention to failures in safety systems and act**
   - As an engineer you must intervene when the intended engineering controls and/or the administrative controls are bypassed, de-activated, fall into disrepair or disuse or misuse, fail, are being circumvented, ignored or not followed, or otherwise become compromised in some detrimental manner.
     - For engineering controls, this includes: safety equipment, sensors/controls/alarms that have failed, or are being bypassed, or are being ignored.
     - For administrative controls, this includes: noncompliance with, short-cutting of, or falsifying records required by safety policies, standards, and procedures such as ignoring alarms or skipping steps in a critical procedure.
   - When such substandard conditions and/or practices occur, you must work to correct them. Accepting these variances means you will be part of the inevitable spiral to disaster, and you do not want to be the author of your own case study.

How to Apply the Key Points of the Engineer's Survival Guide

It is highly beneficial for students to examine real-life experiences (i.e., case studies) involving risk management practices. Case studies can highlight both sound and deficient decisions and practices, and can focus on any aspect of risk management central to an organization's purpose and operations.

The method described herein is a special process in that any one of the Key Points of the **Engineer's Survival Guide** can be applied in any situation (e.g., in the decision-making process for the assessment of a case study or for a dilemma in the workplace).

The purpose in applying a Key Point is to make a decision using the **Engineer's Survival Guide** (i.e., a recommendation with available resources) to maximize or optimize the realization of a desired outcome or acceptable condition.

To do so, consider these points of discussion and answer in terms relative to the applicable Key Point:

a) What is the Loss Incident?
The loss incident is the case which is being examined, and includes a simple statement of facts, such as the facility, the location, and the nature of the loss incident.

b) What Key Point was met or violated?

c) What is the situation or circumstance?
This is the description of the activity, not a long description of the sequence of events of the loss incident. This can include:
- The facility or operation;
- The hazards and risks posed by the facility/operation prior to the loss incident; and/or
- A brief summary of any deficiencies in the control measures of the activity.

d) What is the issue or concern with that situation?
This delves into the details of the deficiencies in the control measures of the activity leading to the particular loss incident and relates the situation/circumstance to the issue/concern in terms relevant to the selected Key Point. This is best described by the hazard (process or occupational), the risk of that hazard becoming uncontrolled under the current deficiencies, and a notion about management's awareness of the issue or concern.

e) What would you do/have done or what should have been done?
Describe one action (or more) that would address the concern, how that action addresses that concern, and how that action is aligned with satisfying the selected Key Point.

f) What would have been the probable outcome had it been done?
Describe the status of the risk associated with the activity and the outcome of the activity.

The following examples illustrate the application of the Key Points of the **Engineer's Survival Guide**.

Case Study Example #1
A response at this level of detail would be expected of an undergraduate student with limited industry experience.

a) Loss Incident: *The Imperial Sugar Refinery dust explosion.*

b) What Key Point was met or violated?
Key Point #4: Pay attention to failures in safety systems and act.

c) What is the situation or circumstance?
The existing ventilation systems were not functioning; thus, air-borne dust was not filtered nor vented. This led to a buildup of dust, and it settled onto the surfaces inside the plant buildings, posing a fire hazard. Very fine particles of sugar dust are explosive when suspended in air.

d) What is the issue or concern with that situation?
The issue is that the ventilation system, a process safety system, had failed, and the failure was ignored. Ignoring this failure (i.e., taking no action to repair it or other remedial action) created the conditions for an explosive dust cloud and the chain reaction of subsequent dust cloud explosions. Management did not pay attention to the failed ventilation system.

e) What would you do/have done or what should have been done?
I would have recognized that the ventilation system had failed, and would have learned about the potential consequences of its failure. I would have shut the plant down until it was fixed and the dust was cleaned up.

f) What would have been the probable outcome had it been done?
Had such action been taken, the dust hazard would have been eliminated or controlled. This would have prevented the explosion or significantly reduced the consequences as there would have been much less dust in the air to fuel the explosion.

Case Study Example #2
A response at this level of detail would be expected of a post-graduate student with several years of industry experience.

a) Loss Incident: *The Imperial Sugar Refinery dust explosion*

b) What Key Point was met or violated?
The actions as described below clearly violated Key Point #3: "When you make decisions, put safety ahead of any other objective". The engineer was under stressful conditions and chose – under pressure – production, cost, and schedule over process safety considerations in this case.

c) The situation or circumstance:

- *The situation is an early-career experience of a production engineer in a chemical plant.*
- *The process unit operation was a distillation tower that splits the feed from a chlorohydrocarbons reactor into its two pure components: carbon tetrachloride and perchoroethylene.*
- *The tower was overhauled during a maintenance turn-around and had been re-assembled. The post-maintenance job was to dry the tower using vapourized nitrogen (liquid nitrogen delivered by tanker truck, vapourized in the heater integrated into the tanker truck, and fed to the tower).*
- *Drying is critical to successful start-up and long-term operation because any residual water can react with the chlorohydrocarbons to produce hydrogen chloride, a corrosive, that can attack the reactor, process piping, and down-stream equipment*

d) What is the issue or concern with that situation?

- *The drying specification is to reach a dew point of -40°C on the nitrogen vent outlet from the reactor.*
- *A period of 48 hours was allowed for the drying job to be completed.*
- *About 44 hours into the job, the outlet dew point was -38.5°C.*
- *Management is pressing to know when the job will be done and is anxious to complete this job for several reasons: delays in this job can postpone other maintenance jobs as well as the scheduled startup date and resumption of production; the delay will ultimately cost more money through additional labour costs and loss of production.*
- *At 48 hours into the job, the dew point is -39.5°C, and Management has been pressing hard to complete the job over the past few hours to get back into production.*
- *Shortly after the 48 hours had past, the Job Leader, an engineer early in their career, made the decision to stop the job despite not having reached the required specification.*
- *The substandard condition (i.e., dew point not reached) could lead to premature failure of some process piping or equipment component due to corrosion.*

e) What would you do/have done or what should have been done?

- *The engineer should have continued with the job to reach the required drying specification of -40°C.*
- *This would have required direct dialogue between the engineer and managers such that management clearly understood the implications of stopping the drying job prematurely.*
- *Depending on the corporate culture, management may align with or override the engineer's decision.*
- *The dialogue may have triggered an investigation as to why the dew point was not being reached. In fact, an investigation was held after the distillation tower was put back on-line. See* **Point g** *below).*

f) What would have been the probable outcome had it been done?

- *If the job were continued to completion to reach -40°C, there would have been essentially no risk of premature failure of some process piping or equipment component due to corrosion.*
- *There would certainly have been some additional delays to the plant outage, but these delays would be insignificant compared to the impact on people, environment, assets and production (PEAP) associated with premature failure and an unplanned release of chlorohydrocarbons to the environment.*
- *There would certainly have been some additional costs to the plant, but these costs would be only a fraction of the costs associated with the environmental clean-up costs, damage to process equipment, costs for non-scheduled maintenance resources, the unplanned interruption of production, and the reputation of the organization.*

g) The Findings of the Investigation

- *After the distillation tower was put back online, an investigation was held to learn why the engineer made the decision to stop the job despite not having reached the required specification.*
- *The post-incident investigation revealed the dew point analyzer was out of calibration. For the given condition, the dew point analyzer was reading -38.5°C before calibration, and -41°C after calibration.*
- *Based on the re-calibrated result, it was found that the distillation tower was sufficiently dry.*
- *The decision to stop the job and proceed to re-assemble the distillation tower had no consequence—in this instance. The decision was made for the wrong reason—pressure to get back into production overrode safety. From a career standpoint, it needs to be recognized that these kinds of decisions in leading organizations where the culture is not tolerant of taking on unacceptable risks, whether knowingly or unknowingly, can damage the individual's reputation.*
- *Learning point: conduct investigations to learn from planned activities that do not go according to plan.*

Section 1.2: What is PEAP? Why is PEAP Important?

In the early 1900s, the public began to question and object to the fact that there were too many fatalities in the workplace—over 500 deaths in the steel industry in Pennsylvania in one year alone. Since then, significant steps were made to make the workplace safer and healthier. In the eyes of the public and government, workers must not to be exposed to unsafe conditions. As managers, we have a responsibility to pay attention to this.

In the 1960s, 70s and 80s, the environmental movement gathered momentum. At the same time, organizations began to realize the prevention of incidents resulted in lower production costs, more profit, better public image, and improved competitiveness. Prevention of incidents also protects the environment from unintended exposures. Governments also have adopted this view and are moving towards more regulation to enforce safety, health and environmental standards.

Leading managing practices now include paying proper attention to safe and healthy working conditions by implementing environmentally accepted practices and by protecting the organization's assets and ability to do business. Safety and risk management keeps people from harm, saves lives and is simply the right thing to do.

Safety and risk management includes all levels of management continually paying attention to manage risk to ensure the success of their organization as well as their own personal success. It is a subject that requires and demands a great deal of informed judgment on risk exposure, where you, as a manager, are required to make decisions that could create an adverse impact (consequence) if not properly managed.

What is PEAP?

Incidents are not limited to impacts on people (e.g., temporary injury, permanently disabling injury, long-term health impacts, or death). The risk of harm to people usually incurs other losses that can be categorized as: **People – Environment – Assets – Production** or PEAP. Each is further explained below:

People	• Occupational health and industrial hygiene: injury / fatality / acute and long-term illness • Worker or the public
Environment	• Air, water, land • Working environment
Assets & Business Interests	• Process and manufacturing equipment • Facility and infrastructure equipment • Finished products and raw materials • Buildings, vehicles, trains, ships, planes • Computer hardware / software, including computer systems access • Proprietary knowledge and intellectual property, information and data; proprietary technology; patented technology; includes experienced personnel and experts • Organization name / credibility / reputation, and the legal or social license to operate • Organization funds: current account, invested capital, and lines-of-credit • Stock price, outstanding shares, capitalization (for publicly listed and traded organizations)
Production / Productivity / Productive Output / Business Activity	• Refers to production of goods (barrels per day of oil refined) or services (number of rail-cars loaded and shipped) • Can be sporadic Interruptions (intermittent or unexpected) • Can be chronic Interruptions (ongoing problems) • Can occur within the entire Main Organization, or Plant / Facility, or Section / Department

In addition to the above, two emerging concerns are Sustainable Development, and Security and Vulnerability. While both certainly can be considerations for Risk Management, this course will not address these dimensions of Risk Management, given their specialized nature.

Sustainable Development	• "Triple Bottom Line" of economic profit and financial responsibility, environmental performance and responsibility, and social responsibility and community support.
Security and Vulnerability	• Terrorism and violent attacks: any deliberate act of sabotage on physical assets or attacks on personnel • Theft, including embezzlement, and fraud • Unauthorized access to computer systems, including software sabotage, and espionage via cyber-attacks and cyber-threats (attacks on an organization's information systems)

Why is PEAP Important?

The toll on human life for early industry prompted societal and government action to establish worker safety programs. Leading organizations have an overall risk management program to protect PEAP and, more recently, to include sustainable development and security and vulnerability. Risk management programs should be integrated with an organization's business plan because the reduction in losses in these areas (i.e., PEAP) can improve the organization's performance overall.

Peter Drucker: "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*."

Louis Allen: "*Minimizing loss* is as much an improvement as *maximization of profit*."

Why do we try to minimize/avoid loss?

Think about this in the simplest of terms through the Loaf of Bread Model: the profit margin on a one-dollar loaf of bread is about 10 cents (i.e., it costs 90 cents to make a loaf of bread). If one loaf of bread falls on the floor, the "incident", the merchant needs to sell an additional nine loaves to recover the cost of the incident or significantly reduce costs to manufacture those additional nine loaves. How much more effort does it take to sell more loaves or reduce manufacturing costs of those loaves, versus the effort to prevent the loss incident?

Making efforts to improve worker or public safety by itself can produce good results, especially if top management is involved and committed. However, to obtain first-class results, any organization or organization must work on all four areas together—people, environment, assets and production. They are all interconnected, as will be seen in the following examples.

Alberta Workplace Injury Statistics

The statistics below demonstrate that safety performance has a great deal of room for improvement in Alberta's workplaces. The number of claims by classification from 2010 to 2017 are shown below. On average in Alberta:

- About once every three days, **a person is killed** on the job in Alberta.
- 134 workers died on the job in 2017, resulting from disease (68), workplace incidents (35), and motor vehicle incidents (31).
- There were 48,834 injury claims by workers in 2017. In other words, three in every 100 workers were injured in 2017.
- Sectors with the highest injury claim rates in 2017 were manufacturing, processing & packaging and provincial & municipal government, education & health services.
- Occupations with the highest injury claims in 2017 were transport truck drivers and retail sales.
- Top three causes of injuries among workers are overexertion 22%, falls 18%, and bodily reaction 13%.

Table 1.1 Summary of Alberta Injury and Fatality Claim Statistics

	2010	2011	2012	2013	2014	2015	2016	2017
Worker-years	1,729,355	1,792,557	1,951,724	2,044,739	2,044,739	1,988,633	1,836,559	1,862,169
Lost-time Claims	24,343	26,629	27,545	27,619	27,577	26,291	24,158	25,542
Lost-time Claim Rate	1.41	1.49	1.41	1.35	1.31	1.32	1.32	1.37
Modified Work Claims	35,365	38,517	41,725	43,428	44,359	38,357	36,098	39,028
Disabling Injury Claims	46,151	50,622	53,126	54,500	55,245	48,582	44,964	48,834
Disabling Injury Claim Rate	2.67	2.82	2.72	2.67	2.63	2.44	2.45	2.62
Fatal Claims	136	123	145	188	169	125	144	166

Source: Occupational Injuries and Diseases in Alberta, 2011 Summary, published 2012 by Work Safe Alberta, Alberta Human Services, The Government of Alberta; and Government of Alberta, 2017 Workplace Injury, Disease and Fatality Statistics Provincial Summary

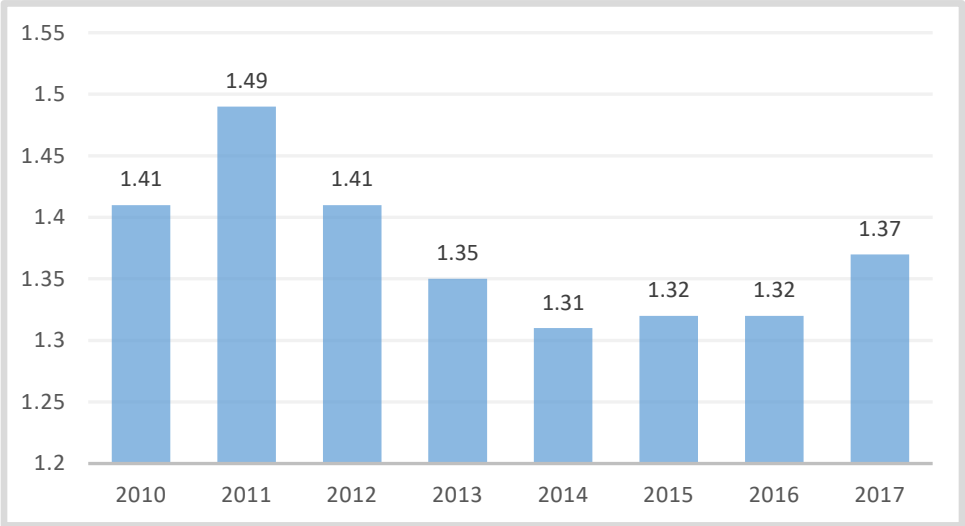


Figure 1.1 The lost-time claim rate in Alberta (2010-2017). *Source: Occupational Injuries and Diseases in Alberta, 2012 Summary, published 2013 by Work Safe Alberta, Alberta Human Services, The Government of Alberta. http://humanservices.alberta.ca/documents/2012-OHS-Data.pdf; and 2017 Workplace Injury, Disease and Fatality Statistics Provincial Summary*

Example of a Small Event: Poor maintenance impacting PEAP

The following event was small in terms of the activity levels, but was certainly significant in that a worker was injured and the environment was harmed.

A day shift maintenance crew at a refinery was working on a valve and piping system around an oily water pump-out. They completed the task, but left the area untidy with tripping hazards (i.e., pieces of pipe, gaskets, scaffolding, etc.). The afternoon shift process worker had to pump-out a drum in this area. While setting valve positions and preparing to startup the pump, the worker tripped and fell, hurting their back. They called in on the radio for help to finish the task.

A less experienced worker helped complete the task. In the hasty exchange of information between the process worker and the less experienced one, incomplete and confusing verbal instructions were given. The less experienced worker unknowingly turned the wrong valves, which allowed oily phenolic water to flow undetected through the wrong system, and ultimately to the river. Some time passed before the contaminated flow was detected.

Table 1.2: Effect on PEAP

People	First process worker was off work for four days due to a back injury (long-term effect unknown)
Environment	Wrong valves operated in the confusion, allowing oily phenolic water to flow into clean water system and then into the river
Assets	Valve and piping system needed to be replaced due to the inadvertent flow of oily phenolic water through them.
Production	Because oily slop was not pumped out quickly and effectively, the main production unit had its rate cut back for approximately one hour

An Example of a Large, Fatal Event: Union Carbide's pesticide plant in Bhopal, India – December 3, 1984

This event was large in terms of the number of people harmed.

There was a major release of a methyl isocynate (MIC) vapour cloud from the plant (40 tonnes), which "floated" over shantytowns surrounding the plant. Permission was granted for the shantytown to be constructed despite zoning bylaws. Due to a poor piping design, inadequate maintenance procedures, inexperienced crews, and uncommitted management, among other causes, the major disaster struck at 12:40 a.m.

Table 1.3: Effect on PEAP

People	• 500,000 affected • 20,000 fatalities (respiratory failure) • 100,000 still suffer incident-related health problems today
Environment	• 40 tonnes of toxic MIC spread over city
Assets	• $1 billion to date by Union Carbide in compensation + additional law suits + loss of sales • Union Carbide sold off other plants and assets to help pay for losses • Union Carbide's name around the world suffered so much that they no longer exist as an organization
Production	• Plant shutdown permanently

Example of a Large, Fatal, and Environmentally Damaging Event: BP Deepwater Horizon Oil Spill

In addition to fatalities and worker injury, this event was large in terms of the damage to the environment, business interruption, asset losses, and the total liability (>US$40 Billion).

On April 22, 2010, contractor Transocean's drilling rig Deepwater Horizon exploded in BP's Macondo Prospect Oil Field ~60 km off the coast of Louisiana. The explosion and subsequent fire resulted in the largest massive offshore oil spill in US history. The unrestricted seafloor gusher flowed for 87 days.

BP leadership focused on systems for occupational safety, but had overlooked concerns in process safety. The leadership of the service contractors (Transocean, Haliburton, and Cameron) did not address management gaps concerning process safety (process safety management is a program used to eliminate, control, or mitigate process hazards).

Table 1.4: Effect on PEAP

People	• 11 workers killed, 16 workers injured • The livelihood of thousands on the Gulf Coast were immediately affected, and many remain so today
Environment	• An estimated 4.9 million barrels (780,000 cubic meters) of crude oil were released to the marine environment • Innumerable marine life of broad varieties were impacted
Assets	• BP fined $4.525 billion • BP-Amoco has filed $40 billion worth of lawsuits against Transocean and other service contractors • BP-Amoco has sold off assets to help pay for losses, clean-up costs, and liabilities • BP-Amoco reputation has suffered
Production	• Lost—no salvageable production capability

A Detailed Look at PEAP

1) People: Occupational Safety & Health

Occupational Safety and Health (the latter sometimes referred to as industrial hygiene) is devoted to the anticipation, recognition, evaluation, and control of factors/stressors that arise in and from the workplace. When unchecked, stressors will cause (or are reasonably believed to cause) sickness, impaired health and well-being, or significant discomfort and inefficiency, including both short-term and long-term health effects. An occupational health program must:

a) recognize the exposure sources;
b) evaluate their origin;
c) evaluate potential exposures; and
d) design and implement controls (engineering / mechanical / substitution / elimination; administrative policies and procedures; protective equipment, etc.).

Occupational Health programs work to mitigate risks for at least four categories of hazards that can result in potential exposures. These include: Chemical Exposures, Physical Agents, Biological Agents, and Psychological Stressors. Each is further discussed here:

I. **Chemical Exposures:** Mists, vapours, gases, fumes, dusts, liquids, etc., are often referred to as toxic substances. Exposure to toxic substances in the workplace is a primary concern to organizations. The Globally Harmonized System (GHS) is a required (legislated) Canada-wide system that is utilized to ensure employees are adequately aware (their knowledge on safeguards against unintentional exposure) and informed (the right to know regarding potential exposure). The specific requirements are:
   - Identify hazardous chemicals used in the workplace in a systematic and standardized way.
   - Provide knowledge, protection, and consistency for the worker and management.

   GHS requires that employers:
   - Train all employees on the system
   - Review Safety Data Sheets (SDS) with employees
   - Have SDS available for employee access
   - Supply correct labeling and SDS (update every 3 years).

   GHS requires that employees:
   - Learn from training
   - Apply the information received

   Example: Inhaled chemicals can be rapidly absorbed into the blood stream and carried to all parts of the body. Lungs are thin-walled membranes with a surface area of ~30 square feet, allowing rapid absorption into the blood stream. About 90% of all industrial poisonings are due to inhalation. Variables are: concentration, route of exposure, drug interactions, controls in use, environment, chemical mixtures, etc. Consider **Hydrogen Sulphide (H_2S)**, a very toxic substance, as per the table below.

   Table 1.5: Hydrogen Sulphide Effects

H_2S Concentration	**Health Effect**
0.01 – 0.3 ppm	Odour threshold (can be smelled)
1 – 20 ppm	Offensive odour, possible nausea, tearing of the eyes or headaches with prolonged exposure
20 – 50 ppm	Nose, throat and lung irritation; digestive upset and loss of appetite; sense of smell starts to become fatigued; acute conjunctivitis may occur (pain, tearing and light sensitivity)
100 – 200 ppm	Severe nose, throat and lung irritation; ability to smell odour completely disappears.
250 – 500 ppm	Pulmonary edema (build-up of fluid in the lungs)
500 ppm	Severe lung irritation, excitement, headache, dizziness, staggering, sudden collapse (knockdown), unconsciousness and death within a few hours, loss of memory for the period of exposure
500 – 1000 ppm	Respiratory paralysis, irregular heartbeat, collapse and death without rescue.
>1000 ppm (0.1%)	Rapid collapse and death

   Source: Government of Alberta, 2010, Alberta Workplace Health and Safety Bulletin: CH029 — Hydrogen Sulphide 1.

   Nitrogen is an even bigger hazard, as more people are killed this way than by H_2S. An atmosphere of less than 19% O_2 in air can be a danger: nitrogen can cause the brain to shut down all activities (immediately if you breathe 100% nitrogen), yet air contains 79% N_2. These conditions, unfortunately, have resulted in multiple fatalities, sometimes referred to as the Two-Death Syndrome:
   - The first worker collapses in a poisonous / toxic atmosphere (greater than 500 ppm H_2S or excessive nitrogen that depletes oxygen concentration to less than 15% O_2).
   - A second worker goes into the contaminated space (the tank, the hole in the ground, the building) without taking proper precautions (self-contained breathing air supply or air purifying respirators) with the intent to rescue a fallen worker, but succumbs to the same toxic atmosphere.
   - Now, no one knows they have both collapsed, and there is then no means to initiate a proper emergency rescue until they are discovered.

II. **Physical Agents** include noise, temperature, humidity, illumination, vibration, radiation, etc. Physical agents also include ergonomics (worker / machine / environment interface, workstation, work posture, repetitive motion, work rest cycles, monotony, work pressure, etc.).

III. **Biological Agents** include insects, molds, fungi, bacteria, viruses, gastrointestinal parasites, etc. Working conditions can be impacted through lack of hygienic care for the workplace, particularly the welfare facilities and waste handling / disposal. Working the in the natural environment can potentially expose workers to insect / animal bites and stings (e.g., West Nile Virus, Lyme Disease, rabies, etc.). Working in the health care field can expose workers to innumerable diseases such as pathogens transmitted via bodily fluids. Some workplaces represent a particular concern, such as hotels / cruise ships, restaurants, pharmaceutical organizations, hospitals and health clinics, medical labs, etc.

IV. **Psychological Stressors** include personal factors, such as off-the-job concerns; on-the-job concerns (e.g., unrealistic supervisory expectations or relationship stressors regarding respect, dignity, diversity, etc.); and personal security and violence in the workplace.
- Excessive stress can be part of, or result from, all of the above and can result in work-related mental / psychological illnesses.
- Employee stress is also a concern in Alberta's workplace. It can be due to unreasonable conditions; poor relationships in the organization; boredom; or a sense of little control over one's own life.
- Stress is more than just psychological imbalance: it can surface as physical ailments such as hypertension, cardiac failure, ulcers, headaches, etc.
- Stress often leads to abuse of alcohol, drugs, tobacco, etc. This ultimately affects job performance.

2) The Environment and Environmental Protection

Environmental damage issues range from air quality to acid rain, depletion of the ozone layer, drinking water supplies, water bodies, subsurface water sources, damage to land, consumption (development) of land, and land reclamation. A poor environment can seriously affect our quality of life, our health, and our longevity. We have a limited eco-system of limited capacity in which to dispose our toxic and non-degradable waste; thus industries, governments, and the public must all play their part in providing solutions.

Pollution and contamination are global problems that do not respect borders. Examples include: acid rain; radioactive contamination via water-drift or atmospheric fallout; waste disposal, landfill leaching, and contaminants from waste incineration; greenhouse gas emissions; oil and gas leaks and spills, as well as leaks and spills of other toxic substances; widespread distribution of persistent, bio-accumulate toxics (heavy metals and chlorinated organic compounds found in the high Arctic); and the list goes on.

Manufacturing Industries: Manufacturing plants with emissions of "polluting byproducts" must have a license / permit to operate from the government agency responsible for the environment. Typically, the permit sets limits on the release of pollutants such as SO_2, NOx, waste water, phenols, H_2S, CO_2, etc. In addition, monitoring stations (for the atmosphere or outfalls to natural water bodies or groundwater) surround the plants or groups of plants to monitor the relevant conditions and parameters, and report the data directly to the government agency responsible for the environment. Typically, deviations from standards must be reported within certain timeframes, sometimes within 24 hours. As well, any releases to the environment (spills or leaks or ruptures) must be reported to the government agency “forthwith”; in other words, as soon as the release has been discovered. Some organizations benchmark this as within one hour. Government agencies can and have shutdown operations or imposed cuts in production. These production restrictions directly and severely impact the organization’s financial bottom line.

Transportation: The prevention of environmental damage, loss of products, waste, etc. in transportation can be a significant area of concern. Some notable events:
- MMA Rail train derailment, explosion, and fire in Lac Mégantic, Quebec
- CN Rail derailment and spill of pollutants to Lake Wabamun, Alberta
- Enbridge pipeline failure and oil spill, Michigan, USA
- Exxon Valdez Supertanker oil spill, Prince William Sound, Alaska

3) Assets – the Aspects of Insurance

Insuring organization assets can be a major expense, particularly if the organization has a poor performance record in safety and losses. When setting rates, insurance underwriters, through their risk management consultants and auditors, review:

- Facility design versus global standards;
- The safety and risk management program, particularly how well it is implemented;
- Facility conditions;
- The history of incidents, fires, explosions, etc. with a focus to presence (or absence) of investigations, the thoroughness of those investigations, and the effectiveness of the follow-up (corrective) actions;
- The strengths (and weaknesses) of management and employees;
- The risk analysis/assessment and risk management processes; and
- The emergency preparedness plan – planning, preparation, resources (equipment and people), and emergency drills.

4) Production / Business Activity / Productive Output: Business interruption

Every organization generates a productive output, whether it is barrels per day, tonnes per hour, kilograms per second, or students per year. Any loss incident in the organization can negatively impact the productive output of the organization and result in a business interruption, which is usually quantified in monetary terms. The organization is not only impacted by the costs to recover, but also by the lost revenue stream.

For both Assets and Production, the best performing organizations conduct in-depth integrated audits with the same vigour, thoroughness, and seriousness as third-party audits. Through concentrated efforts, some oil sands operators have been able to lower their annual insurance premium costs, resulting in net savings of millions per year off the bottom line. This is due to its strong safety and loss management program and committed management team. Safety and loss management certainly pays off in reduced insurance rates.

The best performing organizations conduct detailed audits on all aspects of their risk management program, using expertise from within the organization. These audits serve well to proactively identify system weaknesses and ensure timely correction and to prepare the organization for insurance audits and inspections, as well as for any other third-party stakeholders such as industry association certifications (e.g., CIAC Responsible Care ® Certification).

“Loss is Wasted Profit” – Frank Bird

Frank E. Bird identified that management is concerned with quality of products and services, reduction in costs, and the “triple bottom line” (sustainability). Further, he identified 18 topics of interest where losses occur:

1. Occupational injury and illness
2. Off-the-job injury and illness
3. Fire and explosion loss
4. Loss from natural events
5. General property damage
6. Shrinkage and wasteful materials use
7. Theft of ideas and materials
8. Disorder
9. Absenteeism
10. Alcohol and other drug abuse
11. General and administrative liability
12. Substantial quality and liability
13. Environmental health loss
14. Legislative violations
15. People time waste
16. Machine and equipment time waste
17. All other waste
18. Management system inadequacies

Summary

Recall from the introduction, you will be managing a myriad of risks such as financial, schedule, productivity, and quality. Thus, the avoidance of loss or minimizing loss is the same as maximizing profit. As an engineer and as a future leader it is imperative to understand why we must implement a risk management program to avoid losses in our interests (i.e., PEAP).

ENGG404

Chapter 2:
What Is Risk?

Section 2.1: Why is Risk Management Important?

In the early stages of industrial development, accidents were accepted as inevitable, so the approach taken was to minimize the loss, hence the name loss management. As leaders of corporations and governments, and people and workers became less tolerant of actual loss events, the scope of practice evolved to include loss prevention. Ultimately, the scope of practice has evolved to match our current belief that all unwanted events can be prevented or mitigated through appropriate risk management.

The name **Engineering Safety and Risk Management** thus captures the broader scope of preventing and mitigating incidents by managing the risk of activities in any operation (not solely industrial operations), as implemented through a risk management system, founded on engineering principles championed by engineering leadership. Within the industrial setting, it may be referred to as Industrial Safety and Risk Management, Industrial Safety and Loss Prevention, Industrial Safety and Loss Management, or Process Safety Management.

Engineering Safety and Risk Management is defined as the integrated approach to the management of the continuous reduction of risks to people, environment, assets and production in the industrial setting. Those who benefit from this risk reduction are organization personnel, associated contractors, the public at large and, consequently, the stockholders (owners).

As will be seen in the following sections, risk management is done to meet the needs of:

- The Investors (profits, liability, etc.)
- The Organization (competitiveness, success, etc.)
- The Employees (happy to come to work; not fearing for their safety, health and livelihood)
- The Contractor (protection, can create risks, etc.)
- The Public at Large including governments (demands, expectations)

Why so much effort in Engineering Safety and Risk Management?

The cases studies in this course exhibit the tragic consequences when risks are not managed in industrial operations, which often are the results of deficient risk management systems. Consider the **positive** impacts of an effective safety and risk management system on PEAP:

People:

- Elimination of injuries and deaths, and short- and long-term suffering to victim and families.
- Attract and retain the best employees.
- Reduce absenteeism and/or turnover rate.
- Positive effect on morale.

Environment:

- Protect the environment: air, surface water, land / soil, subsurface water, terrestrial and aquatic life.
- Protect and enhance our working environment and conditions.
- Environmental incidents are minimal or eliminated, thus avoiding the high costs to clean up and remediate.

Assets:

Losses and associated costs to rebuild in the following areas is avoided or reduced:

- Equipment, manufacturing plant, & infrastructure.
- Public property.
- Product damage (in plant / transportation).
- Stock value.
- Corporate image and “social license”.

Production, Productivity / Business Activity:

- Excellent safety performance most often goes hand-in-hand with efficient operations.
- The organization meets and often exceeds government rules and regulations.
- Litigation and law suits are not the norm, and do not drive the organization to financial ruin.
- Lost production minimized (delays and interruptions are more costly than asset damages).
- Improved productivity: not only are workers more satisfied with their workplace, their abilities and energies can be utilized on improvements in all areas instead of fighting fires.
- Retention of customers because the ability to supply products/services is not disrupted.

It is worth mentioning two more impact areas:

Sustainability:
- Economic Responsibility: improved return on investment; able to invest for the future and take advantage of growth opportunities; local plant image, organization image and industry image upheld.
- Social Responsibility: able to meet the needs of societies and build community capacity.
- Environmental Responsibility: on-going ability to protect and enhance the environment; address issues concerning the life-cycle of products and resource consumption.

Security and Vulnerability:
- Threats to business operations and personal information are minimized or eliminated.

The Business Case for Risk Management

When an organization has a good risk management program, their projects have a better than average performance. This table is an actual example:

Organization X (in 2017)	***Expansion***
• Total Capital	$700 M
• Estimated efficiency savings	$ 80 M
• Estimated **minimum** savings due to excellence in safety and risk management	$ 10 M

- At 95% completion, about 4 million worker-hours accumulated
- 8 injuries over the course of the project, counting **both medical treatment** AND **lost time injuries**
- Injury frequency rate: 0.40 as calculated by the organization including both MTC's and LTI's

Compare this organization's total injury rate of **0.40** (MTC's + LTI's) with the Alberta Industry Average of **1.37 for 2017** (the most recent year for which full statistics are readily available), not only an astounding difference (*lost-time claim rate for the organization was even lower than 0.40*). This demonstrates the performance of a leading organization.

Now consider if effective risk management programs were expanded to include all industry across Alberta today: instead of the **25,542** lost time claims in 2017, the better-performing frequency rate of 0.4 would have reduced this to approximately 7,450 lost time claims per year across Alberta industry. Although 7,450 is still too many, it could mean that **18,093 others would not have been seriously hurt** on the job!

Year	Worker-Years	Lost Time Claims	Lost Time Claim Rate	Lost Time Claims if IFR = 0.4	Difference
2017	**1,862,169**	**25,542**	**1.37**	**7449**	**18,093**

Source: Workplace Injury, Disease, and Fatality Statistics Provincial Summary in Alberta, 2017 Summary, published 2018 by Alberta Labour, Alberta Human Services, Government of Alberta.

Incident Cost Iceberg

The cost of any incident can become quite large because of hidden costs. Consider Bird and Loftus' (1976) Incident Cost Iceberg (Figure 2.1). Each incident is unique and will have specific, contextual impacts to its particular operations, organization and personnel. The following are examples of the hidden costs of incidents:

a) Injured Worker Time
- Productive time is lost by the injured employee.
- The injured employee is replaced by a temporary worker (often at premium rates).
- Upon return to work, where organizations investigate in detail, productive time is lost by injured employee in the investigation.

b) Co-Worker time
- Time is lost by the co-workers at the scene when assisting and aiding the injured, and when participating in the post-injury investigation.

- Work interruption occurs at the time of injury and post injury due to sympathy or curiosity, discussing the case, exchanging similar stories and opinions of cause, expressing negative sentiments, etc.
- Incidental lost time results from the cleanup, collection of donations to aid the employee and his or her family, review hearings, etc. The cost of other employee overtime required to accomplish the injured employee's work and the time spent by safety organization personnel on the accident should be included.

c) Supervisor Time

- Assisting injured employee, investigating the incident cause (i.e., initial investigation, follow-up, research on prevention, etc.) and preparing internal incident reports (injury, property damage, variance, etc.)
- Arranging for work continuance, getting new materials and rescheduling operations.
- Selecting and training replacement worker, which may include recruiting applicants, evaluating candidates, and training the new employee or transferred employee.

d) General Losses

- Production time is lost due to upset, shock or diverted interest of workers, the slowdown of other workers, and discussion by others (applies to employees of other units or locations not directly affected by the incident).
- Losses result from work stoppage of machines, vehicles, plants, facilities, etc., which can be temporary or long term and can affect related equipment and schedules.
- The injured employee's effectiveness is often reduced after return to work (e.g. work restrictions, reduced efficiency, physical impediments such as crutches or splints, etc.)
- Loss of business and goodwill, adverse publicity on image / reputation / credibility, problems in obtaining new hires, etc. are common general losses.
- Penalties, fines and/or citations levied.
- Cost can increase for insurance reserves and tax multipliers which are, respectively, small annual percentages of the gross incurred losses, and taxes based upon the dollar value of losses, that are tied up in reserves.
- Increases in insurance premiums for Workers' Compensation Board (all provinces in Canada).

e) Property Losses

- Expenditure of emergency supplies and equipment.
- Cost of equipment and materials above use derived and salvage.
- Material cost of repair and replacement parts.
- Time and cost of equipment repair and replacement in terms of productivity lost and delay of scheduled maintenance on other equipment.
- Cost of corrective actions other than repair.
- Obsolescence losses of spare parts in stock for the equipment destroyed.
- Pro-rata cost of rescue and emergency equipment.
- Production lost during period of employee reaction, investigation, clean up, repair and verification / recertification of equipment.

f) Legal Issues

- Time away from work for employees in order to:
  - Be interviewed by agencies for incident reports (injury, property damage, motor vehicle, police, government environmental or occupational investigation, etc.);
  - Participate in hearings, interviews, interrogations, investigations or litigation on the incident case; and/or
  - Preparation with the organization's legal representatives prior to participating in hearings, etc.
- Costs of preparing for civil litigation (i.e. defending and costs of settlement) and for defense of due diligence (without due diligence as a norm within the organization, the organization is open to being convicted of criminal offence charges).
- Legal expenses arising from compensation, hearings, liability claims handling, etc., that involve contracting legal services, rather than the insurance carrier legal expense that appears in direct costs.

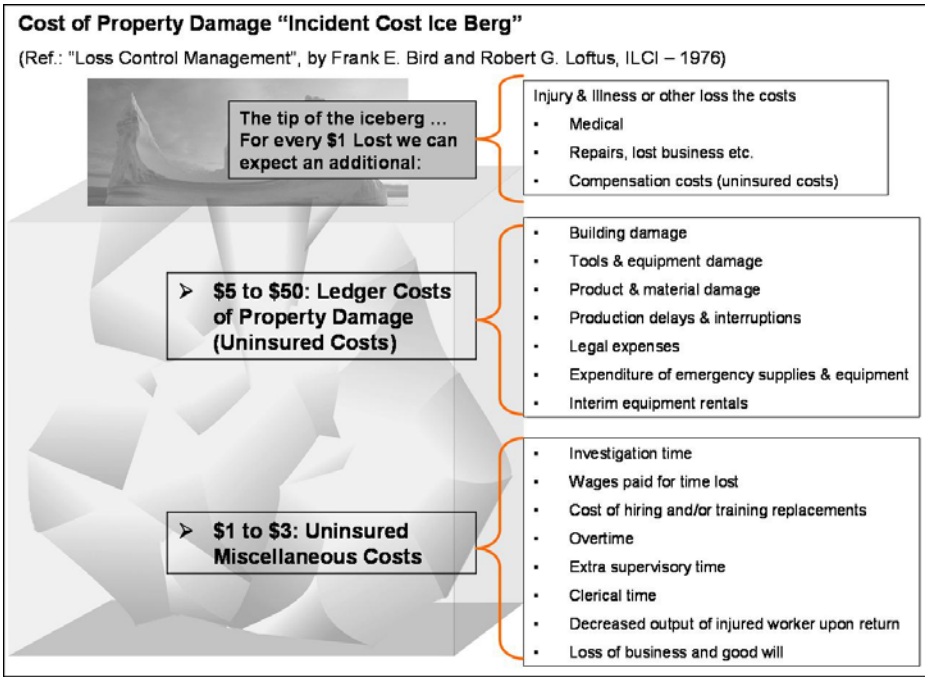


Figure 2.1 Bird and Loftus' (1976) Incident Cost Iceberg.

What's in it for YOU as you begin your career?

Organizations want new graduates to understand the fundamentals before they embark on their careers because they (you!) will be making decisions very quickly. Additionally, those who are aware of risk management:

- Understand the effect of risk management on the sustainable development of organizations (profitability / economic, social responsibility, environmental protection)
- Experience increased job satisfaction when working in a safe environment that is not in continual crisis mode and supported by a solid safety and risk management foundation
- Understand key performance criteria concerning risk management and performance
- Contribute to avoiding or reducing human suffering to both victims and dependents

The key priority for superior organizations is risk management and acquiring engineering talent with safety and risk management expertise. The increase in the number of engineers in leadership who value safety and risk management is leading to a broad base of safer and higher performing industrial operations, one where safety and risk management will not be compromised by other objectives. As already discussed, superior risk management does, and will continue to, benefit society through reductions in incidents that would have negatively affected society at large.

Safety is a core value, risk management is the means to attain it, and neither safety nor risk management should be compromised by other objectives.

The Engineer's Role and Career Challenges

Overview of the Engineer's Role:
You will find yourself in several different roles as you progress through your career.

- Engineering, Design, Procurement
- Project Management and Construction
- Operations and Maintenance
- Management and Executive Leadership
- Consultant and Professional Responsibilities
- Other non-engineering e.g. as Finance, Human Resources, Sales & Marketing, Regulatory, etc.

In each role you will need to understand the concept of risk management and its application to decision making. In many cases, you will be the manager / leader within that role. This includes being leaders of people and technology leaders (experts in your field), whether internal to your organization or external for other organizations.

Challenges:
Your role in business and management will be challenged by many objectives throughout your career, and you must not lose sight that risk management applies to all of them! The many objectives include:

- Project idea and initiation through to completion and operation
- Project costs and approvals
- Rate of Return on Investment and Net Present Value
- Operating costs and cost variances, and Profit and Loss
- Understanding the technical issues to ensure effective decisions
- Managing people: managing with limited resources, needing to do more with less
- Managing organization image and its impact on business
- Business and strategic planning
- Litigation and law suits
- Public interface and public perceptions

So, as you progress through this course which is intended to emulate those challenges, think of yourselves as being managers – leaders – within your future employer organization!

Q: How will you manage risk? A: Keep your Engineer's Survival Guide at hand!

Benefits of a Risk Management Program

The effective implementation of a risk management program protects people and helps organizations avoid losses. Good safety and risk management programs require a team approach; this is a synergistic effect in that good teams support risk management and risk management supports good teams. Further, these lead to an improvement in overall organizational effectiveness and the efficiencies derived from such. When the manager in the organization effectively manages safety, every other aspect of operations or work dimensions (costs, productivity, quality, schedule, people, etc.) can be managed just as effectively. In fact, there are many examples of projects and operations where the results exceeded expectations in all aspects. Why? Because safety and risk management demands good planning and good execution; thus, all activities benefit as do the benchmarks by which the performance of these activities are measured.

Who are Stakeholders?

Stakeholders are people and entities that are affected by industrial incidents. These include the public, organization employees and shareholders / investors, the industry, and regulators, as well as other associated industries (e.g. insurance industry).

Section 2.2: The Anatomy of an Incident

Recall the definition of a Loss Incident: it is an unplanned, undesired specific event or sequence of events that has resulted in harm to people, the environment, assets or loss of production (or any combination of these). **Loss** is the description (quantitative and/or qualitative) of the consequences or impact of an event or incident on PEAP. An **Incident**, in its simplest definition, is an unintended event with negative consequences. To ensure a successful and rigorous root cause analysis / investigation (see Chapter 4), the **Incident Description** must be clearly and correctly defined and stated.

Incidents result in varying degrees of severity of harm to PEAP. In Chapter 7, we will be discussing the **Incident Pyramid**, with near miss events in lower layers and fatalities at the pinnacle. The nature of incidents can be sporadic or chronic.

- Sporadic: a sudden unexpected change in the status quo resulting in loss. These tend to be sudden and often dramatic, and usually these demand immediate attention.
- Chronic: a long-standing condition that has not been corrected yet and repeatedly results in loss and interruption to service or production. Sometimes the situation becomes the status quo and managers begin to accept it as normal. In this case, managers have come to accept the unacceptable. This has been termed organizational complacency or normalization of deviance, and is a symptom of an unhealthy organization with a failing management system.

Models of the Anatomy of an Incident

To minimize and preferably avoid loss due to an incident, the causes / hazards / risks that result in losses must be understood. To understand the causes, the components of what makes an incident must be understood. Two models are presented to explain how loss incidents happen and as aids to identifying hazards. For both models, the severity of the loss incident or injury depends on whether the energy source exceeds the threshold energy or not.

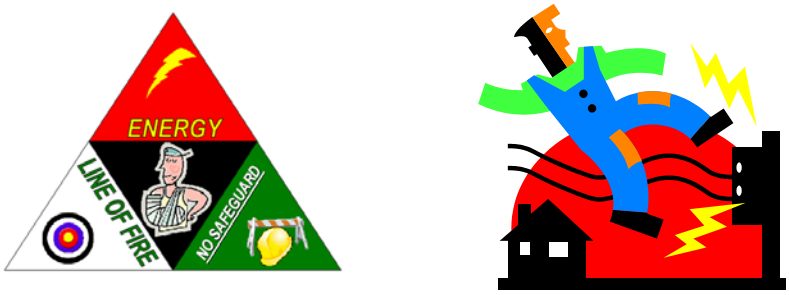


Figure 2.2 Two models for the Anatomy of an Incident. Left: Model #1. Right: Model #2.

Model #1 of the Anatomy of an Incident

An incident occurs when a set of circumstances arise as a result of one or more immediate, basic and/or latent causes. One model, the **Injury Triangle**, as depicted in Figure 2.2, describes the set of circumstances as three components as follows:

1) **The Release of Energy or Source of Energy.** Examples of different forms of energy include:
   - Chemical: toxic, corrosive, flammable, explosive, reactive, oxygen deficient atmospheres
   - Pressure: pressurized gases or liquids
   - Electrical: in live circuits or in stored systems (batteries, capacitators)
   - Potential / gravitational: able to fall to same or lower level

2) **In the Line-of-Fire.** The presence of a body, object, material, etc. that can be impacted and harmed by the uncontrolled release of energy. A person (worker or the public) or asset (process equipment, transportation equipment, facilities and infrastructure assets, the natural environment, etc.) is subject to or exposed to the release / source of energy.

3) **No Safeguards.** Safeguards and control measures are a) personal protective equipment; b) engineered controls (engineered systems, designs); c) administrative controls (policies, procedures, check-list); or d) a

combination thereof. “No Safeguards” means that safeguards and control measures are absent, inadequate, defective, ineffective or not followed.

Now consider the third component (i.e. **the safeguard**) under either circumstance where the person intends or does not intend to be in the line of fire. The lack of or inadequacy of a safeguard can result in any one of these three conditions: a) an uncontrolled release of energy; b) an unintended exposure to a source of energy; or c) a person or equipment / asset is in the line of fire of a controlled release of energy. A loss incident will result when all three conditions are fulfilled.

Any combination of Energy (controlled or uncontrolled release or protected / unprotected source), and Line-of-Fire (intentional or not intentional), and Lack of Safeguard will result in a loss incident (injury, fire, explosion, chemical release or spill, etc.).

Model #2 of the Anatomy of an Incident

Model #2 is similar to Model #1 and can be used in the same manner for understanding the three components of incidents as follows:

1) **Energy.** The first component, as described in Model #1.

2) **In the Line-of-Fire.** The second component, as described in Model #1.

3) **Triggers or Triggering Event.** The third component is any circumstance or mechanism that can cause the energy to be released in an unplanned or uncontrolled manner. Examples are explosions, workplace conditions, equipment failure, tripping and falling, weather, and contact with moving parts or equipment or machinery. In effect, there was a <u>failure</u> or <u>deficiency</u> in some manner (use, installation, operation, maintenance, etc.) of the **engineered control**, and/or **the administrative control**, and/or the **personal protective equipment**. In many ways, a triggering event is the same as or results in “No Safeguard”.

Any combination of Energy (controlled or uncontrolled release), and Line-of-Fire (intentional or not intentional), and Triggers can result in a loss incident (injury, fire, explosion, chemical release or spill, etc.).

Applications of the Models

As will be discussed in the next section, the application of these models can be used from two different approaches: the <u>reactive</u> (or responsive) approach and the <u>proactive</u> approach. Both approaches focus on the examination or analysis of the components in the models to determine how these components **did** (reactive / responsive) or **may** (proactive) come together, and how it resulted in or may result in a loss incident.

- The **reactive/responsive application** analyzes a loss incident to learn from it, to identify immediate causes, and to implement corrective actions to prevent similar incidents. The **Incident Investigation and Root Cause Analysis Process** is applied for reactive / responsive application (i.e. post-incident) to determine the causes of incidents and to implement appropriate corrective actions to prevent loss incidents.
- The **proactive application** analyzes a set of conditions or circumstances of a situation (i.e. a conceivable loss incident scenario) to identify hazards and risks (i.e. find possible pathways to a loss incident) and to implement preventative actions before a loss incident occurs. This proactive application is **The Risk Assessment Process**, which may use many risk assessment methodologies (i.e. before an event happens) to understand the hazards, risks, and possible causes, and to implement appropriate control measures to prevent loss incidents.

The application of these models can be used to analyze work activities (within the scope of <u>occupational safety</u>) or process unit operations or equipment / infrastructure installations (the scope of <u>process safety</u>), either reactively or proactively. Regardless of which model is used or applied, if all three elements in a model happen at the same time, there will be a loss incident as depicted in the incident models.

<u>Section 2.3: Hazard Identification</u>

The **Risk Management Work Process** (presented in Chapter 3) begins with the specific activity designed to evaluate the business for potential hazards. This ongoing activity is set up through the management system to identify hazards, monitor the operations for hazards and to address those hazards. What are some of the hazards

or concerns? How are they found? These two questions are discussed in this section, and two different methods for identifying hazards will be presented.

What are Hazards?

A hazard is any source of potential damage, harm or adverse health effects on something or someone (CSA Z1002 Standard 2019, from https://www.ccohs.ca/oshanswers/hsprograms/hazard_risk.html). A number of examples of potential hazards are presented below in Table 2.1. For example, consider the uncontrolled release of a flammable gas (i.e. the hazard) into a chemistry laboratory which ignites (i.e. the loss incident). The consequences of this unchecked hazard and resulting loss incident can include burn injuries, release of products of incomplete combustion to the environment, damaged lab equipment, and inability to resume activities in the lab until clean-up and repairs have been completed.

Table 2.1 A list of potential hazards

Flammability	Fire	Explosion / Detonation	Security Breach
Corrosion	Corrosive Liquids	Lack of Oxygen	Oxygen Deficiency
Pressure / Excess Pressure	Toxic & Noxious Materials	Biological Hazards	Chemical Reactivity / Run-away Reaction
Gravity: Falling Objects, Working at Heights	Electricity: Arc / Weld Flash, Electrocution	Unrestrained Body / Body Part Movement	Tripping Hazards and Slippery Surfaces
Mechanical Equipment Failure in any form i.e. rupture, collapse, test to destruction / failure	Mechanical Energy Vibration, Rotational / Centrifugal, Crush)	Radiation (radioactive materials, x-rays, laser light, excess sunlight)	Physical elements: Noise, ambient temperature, contact with hot / cold surfaces

Most hazards are seen as occupational safety issues to all persons within the operation (workers working and managing the hazard, and those who are observing this work or working nearby), as all persons are potentially exposed to the hazards in their daily work activities. Workers successfully manage their exposure to many of the hazards listed in Table 2.1 on a daily basis and do so without incident. However, in most cases, loss incidents occur because the hazard was not recognized or because the safety measures were inadequate or non-existent.

Hazards can stem from a variety of sources. Consider the hazard wheel below with its categories of potential hazards.

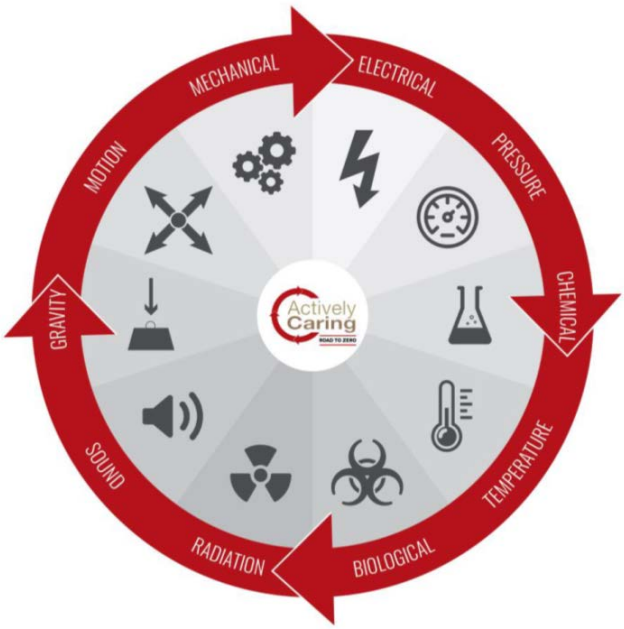


Figure 2.3. The Hazard Wheel. *Adapted from Tixier, A. J. P., Albert, A., & Hallowell, M. R. (2017). Proposing and Validating a New Way of Construction Hazard Recognition Training in Academia: Mixed-Method Approach. Practice Periodical on Structural Design and Construction, 23(1).*

Other examples of potential hazards in these categories (as well as others) include:
1) **Chemical hazards**: Mists, vapors, gases, fumes, dusts, liquids, uncontrolled chemical reaction, flammability, toxicity and exposure;
2) **Electrical hazards**: Electrocution from contact with live electrical conductors or charged systems and exposure to weld flash or arc flash;
3) **Physical hazards**: Noise, temperature extremes (thermal stress / cold exposure), humidity, lighting / illumination, vibration, slips, trips, falls, confined spaces / excavations, pressurized systems, machinery / equipment with moving parts, contact with hot / cold surfaces, gas / jet streams, water-blast streams, and mobile equipment / exposure to traffic (road and rail).
4) **Ergonomic hazards**: excessive force and / or forceful exertions, awkwardness or poor posture / body positioning, repetition, and duration (continuous work without breaks);
5) **Biological hazards**: Bodily fluids, virus strains, bacteria, molds, mildew, fungus, insects (bees, wasps, hornets), animal and bird feces, wild animals, and infectious diseases.
6) **Psychological hazards**: Stress, fatigue, working alone, workplace violence and harassment, depression, drug and alcohol abuse, family issues, and financial concerns.

Corrosion as a Special Case

Now consider corrosion from Table 2.1. Is corrosion a hazard or is the corrosive liquid the hazard? Corrosive liquids do cause corrosion; thus corrosion is a consequence (Impact on Asset). Corrosion can cause a leak, and uncontrolled release of energy, so corrosion is a hazard from this perspective. Now consider the structural steelwork for decking in an industrial complex. Heavy corrosion on the supports is a hazard because the supports can potentially fail under load. One must keep these subtleties in mind when looking for hazards and trying to eliminate or mitigate them, or their effects. Therefore, corrosion on piping, corrosion on structural steel, and by extension other sub-standard conditions can be considered hazards.

Differentiating Between a Hazard, Severity of Hazard, and Impact on PEAP

Sometimes it is difficult to differentiate between these three terms. A hazard and the consequence or severity of a hazard are quite closely aligned. For example, noise can be a hazard, but as the loudness (sound pressure) increases, the severity of the hazard increases. This is similar to the Consequence Scale of the Risk Matrix. It is helpful to note that lost organization reputation, fatalities and disabling injuries, environmental impact, and insurance cost impacts are not hazards, but are consequences of a loss incident (i.e. the impact on PEAP).

Confusion abates when taking another look at the definition of hazard ("a potential source of serious harm to people, environment, assets, or production"). Thus, an energy source (noise, combustion, electricity) can be viewed as a hazard; however, it most certainly is a hazard when it is an uncontrolled source of energy, or an unexpected release of energy, or persons are sufficiently exposed to that source of energy that harm results.

A condition can also be recognized as a hazard; that is, some means or mechanism that is intended to contain energy or control energy is defective, deficient, inadequate, or absent. The condition of that means or mechanism has the potential to cause the source of energy to become uncontained (an unexpected release) or cause the source of energy to be released uncontrollably.

Table 2.2 Types of bodily injuries as a result of exposure to hazards

Type of Energy	Primary Injury Produced	Examples and Comments
Mechanical	Displacement, tearing, breaking and crushing of body tissues and organs	Injuries resulting from the impact of moving objects such as bullets, hypodermic needles, knives and falling objects and from the impact of the moving body with relatively stationary structures, as in falls and plane and auto crashes. TThe majority of injuries are in this group.
Thermal	Inflammation, coagulation, charring and incineration of the body	First-, second- and third-degree burns. The specific result depends on the location and manner in which the energy is dissipated.
Electrical	Interference with neuromuscular function and coagulation, charring and incineration of the body	Electrocution, burns, interference with neural function as in electroshock therapy. The specific result depends on the location and manner in which the energy is dissipated.
Ionizing radiation	Disruption of cellular and subcellular components and function.	Reactor accidents, therapeutic and diagnostic irradiation, misuse of isotopes, effects of fallout. The specific result depends on the location and manner in which the energy is dissipated.

Chemical	Generally specific for each substance or group.	Includes injuries due to animal and plant toxins, chemical burns, as from KOH, Br_2, F_2 and H_2SO_4 and the less gross and highly varied injuries produced by most elements and compounds when given in sufficient dose.
Acoustical (sound)	Long term exposure to high levels can reduce hearing ability. Sudden, high noise levels can damage eardrums.	Generally, exposure to levels over 85 dB(A) over a 8-hour periods will slowly reduce hearing ability. A sudden overpressure (shock wave) of more than 25 kPa will break ear drums.

Severity of Hazard Example: Exposure to Cold Environments

Exposure to extremely cold temperatures is sometimes obscure, but it is very much a real hazard. It conceivably can be the cause of someone doing something wrong because they are becoming sluggish. It is a common physical hazard when working in outside during the winter. At the opposite end is exposure to elevated temperatures. This can result in hyperthermia and heat stress, or heat stroke.

How to Identify Hazards

1) **The Knowledge-Based Approach:** Hazards can be identified using two knowledge-based approaches: the simple knowledge-based approach and the expert knowledge-based approach. Recall the definition of a hazard is "a potential source of serious harm to people, environment, assets or production". There are risks associated with any activity, but the first step towards understanding what those risks mean (i.e. risk analysis/assessment) is the identification of the hazards. The simplest approach for identifying hazards (for both process hazards and occupational hazards) is to inspect it for any of the groups and types of hazards as noted in the above sections. This approach is based on the inspector's knowledge and/or documented checklists for use during an inspection.

   In an expert knowledge-based approach, one determines the possible adverse consequences of an activity-gone-wrong and identifies hazards that result from the activity-gone-wrong or the cause that will make the activity to go wrong. This approach is based on the knowledge of one or more experts. It is broad based in that it starts with the systematic identification of potential consequences on PEAP, and then determining the hazards that can lead to those consequences. It is, in effect, a reverse approach of the discovery approach, described later, and requires an extensive knowledge base to proceed. Hazard identification involves two key tasks:

   a) **Identify specific undesirable or adverse consequences (impact on PEAP):** These can be broadly classified as human impacts, environmental impacts, asset damage impact and business damage impacts. They constitute adverse consequences that could transpire from any incident within the facility. While these are relatively straightforward to identify, being thorough in the review is necessary to ensure all hazards are uncovered.

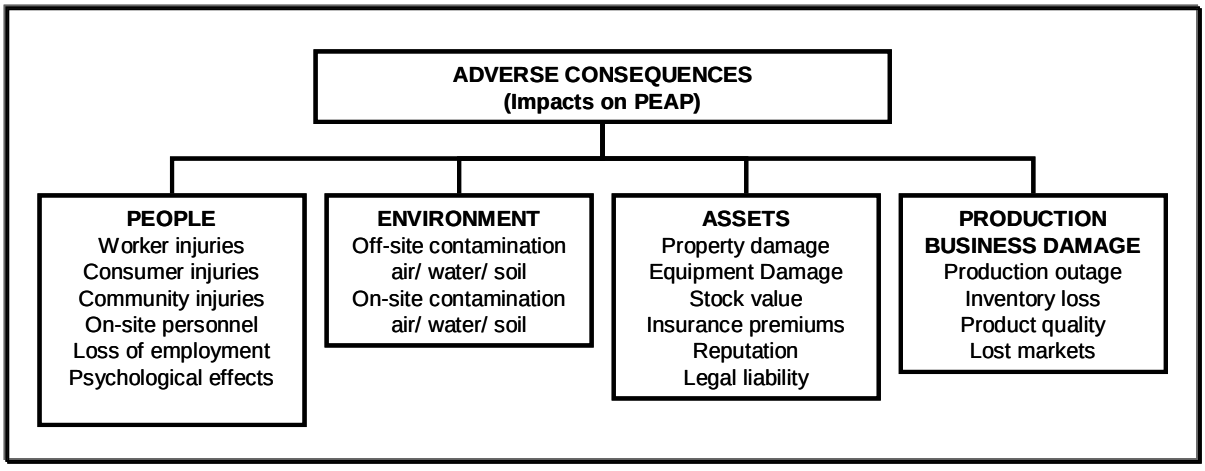


Figure 2.4 Potential impacts of a hazard on PEAP

   b) Identify process hazards, substances, and agents that cause those consequences: In your operation, project, business activity, product, etc., identify materials, substances, agents, unit

operations / process manufacturing parameters, and operational parameters that could produce those adverse consequences. Being thorough is important. The use of several techniques should generate an overlap of conclusions and findings – not only should this verify the hazards, but it also demonstrates thoroughness of the team and process. Organizations often develop specific approaches for hazard identification to assure themselves that hazards in their applications / processes / business are understood. Finally, it is important to have a method to rank hazards; otherwise the evaluation process will be overwhelmed. When ranking, one must take care that important concerns are not overlooked, with the negative result that measures taken to reduce the risk to a manageable level may be inadequate or may not be appropriate.

Most importantly, access and use the knowledge and expertise of employees. A hazard identification process cannot be thorough without the input of people who undertake the activities associated with the hazards. Their input will support a thorough evaluation where the organization:

- has identified all the hazards,
- knows where the identified hazards can exist or can occur,
- knows what priority to put on addressing the identified hazards, and
- gains important knowledge on effective ways to address the identified hazards.

Management can greatly benefit from the substantial contributions of knowledgeable employees and can build substantial buy-in and commitment with effective follow-up on identified concerns.

2) **The Discovery Approach:** In some cases, the hazards, whether process or occupational, are not obvious or cannot be picked from a list of common hazards. This can be the case in pure research settings where new materials are being synthesized, or where known materials are being combined in new or novel ways, or where new equipment or machinery has been fabricated or developed and being tested. In these cases, the hazards are not so obvious and a menu of hazards is inadequate in ensuring all potential hazards are analyzed and addressed.

   This approach can be learned and applied by those who are new and unfamiliar with the setting and the associated hazards, including mature settings such as industry, construction, and even teaching-learning settings. In such a case, a discovery approach using the fundamentals of an injury must be applied.

   To apply the discovery approach, one must understand the fundamental components that must come together for a loss incident to occur (i.e. the anatomy of an incident). Recall that an incident is an unplanned, undesired specific event or sequence of events that has resulted in harm to people, the environment, assets or loss of production (or any combination of these). Thus, by mitigating one or more of these components that cause an incident, incidents can be more effectively prevented.

   To become a skilled observer in searching for hazards and preventing loss incidents, it is useful to re-examine the two models of the anatomy of an incident. Incidents happen when the three components in either model combine. To identify hazards, it is essential to understand these components. Each component is associated with hazardous conditions which in turn identify opportunities for incident prevention. This can be done by rephrasing the components of the models as follows:

   - Find the **Energy Source**: mechanical, electrical, chemical, thermal etc.
   - Look for the **Line-of-Fire**: bodies, assets, and environment that could be harmed by a release of the energy source.
   - Find the **Trigger**: the circumstances or mechanisms that will cause the release of the energy source.
   - Look for **No Safeguards**: the absence of the barrier or control measure or safeguard that is preventing or limiting or controlling exposure to the energy source.

   The hazards become evident when assessing an activity or workplace with these components in mind. It is in this manner that a sharp observer can see hazards that may not be obvious to others and then can take steps to address the hazard and avoid an incident. In effect, this is working on the immediate causes of incidents; thus eliminating the possibility of an incident.

Hazard Analysis Team

The composition of the hazard analysis team is crucial to its success. Careful thought is needed to ensure the right people are involved in order to cover all the concerns. The optimum size of a team is 5-6 people. Having too many people may result in the ineffective use of resources. Having an insufficient number of people can mean a gap in knowledge for the hazard analysis. The same team may continue into risk assessment, etc. The team should consist of subject matter experts, a risk management expert, workers and senior management.

Guidelines for the Process to Identify Hazards

The purpose of the hazard identification process is to identify hazards only (i.e. to find all conceivable problems). This is a brainstorming process to discover the problems and is called “opening the problem space”. This is a different mindset than for the members of a problem-solving team. Often it is difficult to persuade people to refrain from solving the identified hazard. Although this is natural, it distracts the team from its primary objective: to identify hazards, and NOT to address those hazards. A good facilitator can help with the process.

Although this team is skilled to identify hazards, it is not necessarily the right team to resolve the hazards. Most of the identified hazards can be solved in different ways, and this requires a careful review of the options by persons with the right skills. Once a hazard is identified, there is an ethical and legal responsibility to inform anyone potentially affected (employee or public) of that hazard. Further, the hazard must be monitored and controlled within acceptable risk criteria. Careful documentation, identified communications, the necessary training and certification of workers, project reviews and follow-up are all part of the due diligence needed to properly manage the hazards as they are identified.

Section 2.4: Risk as a Function of Consequence and Probability

In our lives, there is always risk. Everything we do involves the acceptance of some level of risk. If we as a society could not accept any risk, we would not have progressed to where we are today. However, we make decisions in our everyday lives whether we want to proceed with an activity or not (i.e. we accept the risk associated with an activity and go ahead, or we discontinue an activity because the risk is not acceptable to us). We intuitively know what risk is, especially when we relate it to an activity, but within Risk Management it is important to understand risk more fully in order to communicate it, assess it, and manage it.

Any activity – task, procedure, job, operation, etc. – has risk: it has the potential for something to “go wrong”. “How bad it can be” is expressed as the **consequence**. “How likely it can happen” is expressed as the **probability**.

Consequences are understood to be the severity of a hazard when it becomes uncontrolled.

Probability is understood as the likelihood of that hazard becoming uncontrolled.

These two factors express **Risk**. Risk represents both the possibility and extent of injury, loss, or environmental incident created by a hazard. The significance of a risk is then determined by assessing the probability of an unwanted incident and the magnitude of the consequence of the incident. Often these two factors are relatively straightforward and simple to determine in many cases. However, in some cases, quantifying these factors may require significant effort and the application of complex engineering concepts, as will be discussed in subsequent chapters.

The Fundamental Risk Matrix Explained

The fundamental risk matrix (see Figure 2.5) correlates probability and consequence to determine a risk category of an activity or condition. A corporate risk management standard (the “risk criteria table” discussed later in this chapter) will define the increasing levels of probability and consequences, and assign risk categories (in this example: Low, Medium, and High) for the different combinations of these parameters. The risk category so defined then determines what constitutes an acceptable action or response. Acceptable actions are, in turn, defined by corporate risk management policies and may differ as will be seen in a subsequent chapter.

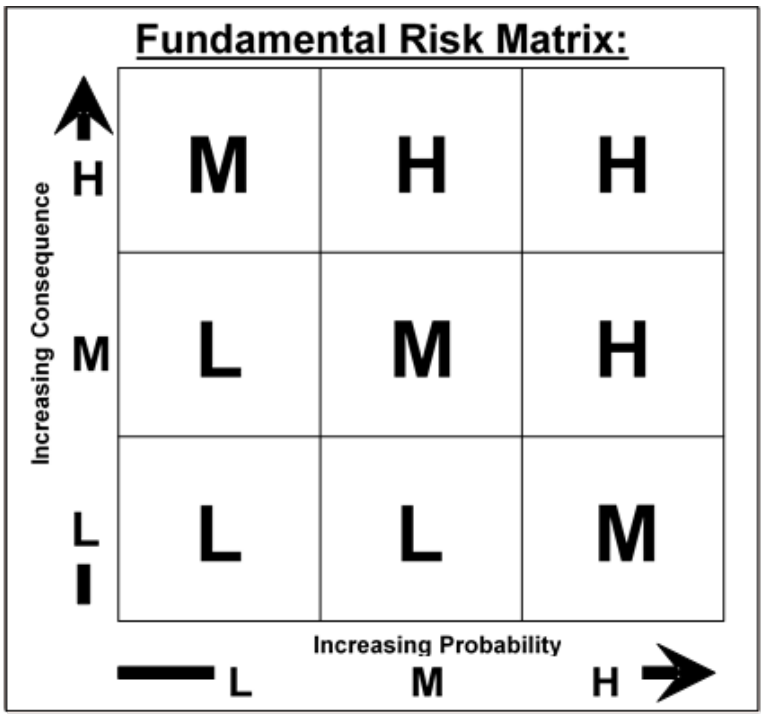


Figure 2.5 The fundamental risk matrix.

An Example of Risk in an Industrial Operation

There are many different kinds of hazards and their associated risks in industrial operations. In all cases, it is intended that there is some means of control to reduce the risks that the hazards pose to an acceptable level. The remaining risk after control measures are in place is termed the **residual risk**. The residual risk must be continually managed to prevent the risks from becoming uncontrolled; otherwise an incident occurs.

Consider the case of a high-pressure natural gas transmission pipeline in operation through a city. In terms of energy, there is a flammable gas and there is pressure. One possible risk posed by the pipeline is a leak. A leak originates with a breach in the integrity of the pipe wall by any number of causes. With the flammable gas escaping under pressure, the leak (which is called the initiating event) can result in many other possible outcomes beginning with no ignition and dispersal, immediate ignition and a fire, or delayed ignition and a vapour cloud explosion.

What can be done? Nothing can be done to eliminate the properties of transmitting natural gas because it is and always will be a flammable gas under high pressure. However, work can (and must) be done to prevent the leak or mitigate the consequences of a leak; thus, other factors come into consideration. When looking at risk as a function of consequence and probability, consider:

a) Factors that negatively affect probability (factors leading to a leak) and the control measures to prevent or mitigate these factors (see Table 2.3), and
b) Factors that negatively affect the consequence (the size of the leak and that may cause it to escalate) and the control measures to prevent or mitigate these factors (see Table 2.4).

Table 2.3 Factors that negatively affect probability and associated control measures

Factors Negatively Affecting Probability	**Control Measures**
Pipeline Integrity – Initial: ➢ Substandard condition of pipeline: poor choice or quality of materials of construction; defects during manufacturing or fabrication; damaged during installation	➢ Robust design, appropriate materials of construction, good fabrication & installation with inspections and defects corrected
Pipeline Integrity – On-going in Operation: ➢ Substandard maintenance practices: lack of planned preventative maintenance, lack of inspection, lack of follow-up on inspection results;	➢ Good maintenance;

➢ Substandard operating practices: excessive pressure, excessive flowrate, internal erosion, poor controls on impurities; poor cathodic protection, pitting corrosion, gas acidity and humidity; ➢ Proximity of activities to the pipeline and non-intended contact and breach of pipeline wall integrity	➢ Good operations within specifications ➢ Clear and visible pipeline route markers, and protocols for excavating along pipeline routes e.g. “Call Before You Dig”

Table 2.4 Factors that negatively affect consequence and control measures

Factors Negatively Affecting Consequence	**Control Measures**
Proximity to high-user areas (residences, schools, etc.) and other facilities	Good development planning i.e. increase spacing; emergency response plan by local authorities
The potential quantity released in event of a loss of containment.	Automatic process controls and emergency block valves that detect a leak (loss in pressure or flow or mass balance) and initiate closure of valves on the monitored section to isolate it
The presence of a potential ignition source.	Warning signs posted in area; control access to the area; control development in the area; control hot work in the area

Risk Analysis and Risk Assessment: The topics of risk analysis and risk assessment are more fully discussed in The **Risk Management Work Process** (Chapter 3).

Chapter 2.5: What is an Acceptable Level of Risk?

The concept of risk involves determining the probability of an incident happening along with the possible consequences. Together, these two factors determine the “risk”. As discussed in previous sections, everything we do involves risk and the acceptance of some level of risk. As a professional, you will be making decisions (choices) as a regular course of your daily duties within your operation. Regardless of your position / role in engineering, design, research, or manufacturing / operations, the risk decision-making process will be a regular tool you need to use. In the **Risk Management Work Process (presented in Chapter 3)**, we conduct analyses and assessments to determine the risk of an activity or an operation. And we compare those risk levels to an “acceptable level” of risk before deciding whether to continue with the activity or not.

Who is “at Risk”

From an organization’s perspective, the risks that people face can be categorized as: 1) Voluntary risk versus Involuntary risk, and 2) Individual Risk versus Societal Risk. For example, workers who perform a job take on the risks voluntarily, and the risks of the job are imposed on the individual doing it. Contrast this with a large, chemical process plant: the community around the plant faces a societal risk, and despite the fact they can choose to move away, but given most community members are not really aware of their risk exposures, their exposure to the risk is considered involuntary. Most of the calculations used today examine risk in terms of involuntary individual risk. Sophisticated calculations along with detailed databases now provide accurate measurements of risk. Since the Bhopal Incident, the quality of consequence analyses and probability data has greatly improved.

Unfortunately, risks can result in injury and death. The probability of dying depends on the risks and hazards of the nature of the activity the person faces. Is the person retired, old, and living out their daily life? Are they working in a manufacturing plant? The risk of dying while working in manufacturing is based on the hazards and consequences of an event, and the probability of that event happening. As can be seen, the quantification of risks can become very complex. Thus, the quantification of the risk of a fatality is based on a lot of data from a variety of sources, collected over a number of years, and rolled up into one calculation.

An Acceptable Level of Risk

Acceptable risk is defined by societal norms that limit risks to certain levels. These norms in turn may influence legislation and regulations, and corporations should set internal policies that ensure their risk exposures align with, or even improve on society's expectations for risk management. Societal norms can also change over time (e.g. an increasing intolerance for impacts on the environment), and proactive corporations adjust their policy positions accordingly. It is increasingly evident that a corporation's right to operate (or social license) is judged in the court of public opinion. When risk is not managed to meet or exceed the expectations of the public, it may constrain or stop a corporation from operating (e.g. consider the pipeline industry in the wake of spill incidents). The acceptable level of risk for a corporation is set by corporate policy.

The acceptable level of risk depends on the activity and what risks individuals are willing to voluntarily accept. Safeguards and control measures can be implemented to reduce the risk of an activity to an acceptable level. Thus, "high hazard potential" does not necessarily mean "high risk" in the presence of good safeguards and control measures.

Establish Risk Criteria

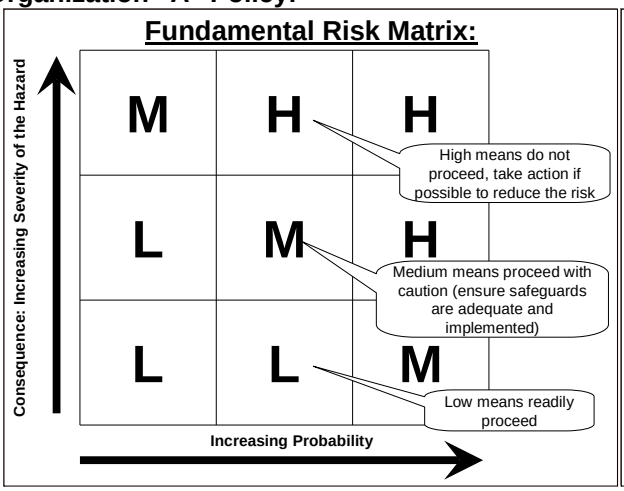
Establishing risk criteria means establishing thresholds for probability and consequence that in turn are used to determine risk. Properly done, the resulting risk levels can be used to determine the acceptability of an activity. Without this guidance, it would be difficult to set the correct priority on a problem. By establishing the level of "acceptable risk" and by using the organization's "risk criteria", managers are enabled to determine priorities and allocate resources to get the problems solved. In other words, management can provide a policy or a set of directions for others in the organization to empower others to make decisions about activities and the risks associated with those activities (i.e. to accept the risk and undertake the activity, to determine and implement additional control measures to reduce the risk of the activity to an acceptable level, or to reject the risk and stop the activity because risk is too high). <u>These thresholds are subjective and differ from organization to organization.</u>

Recall the fundamental risk matrix. The intent was to show that with increasing probability or increasing consequence, the risk also increased. Different risk criteria between different organizations define varying levels of risk, even though the classification is the same. Thus a "medium" risk in one organization may be higher that a "medium" risk in the other and drive a different response as a result.

Interpretation of the Risk Matrix

The levels or categories of risk can drive actions that may differ between organizations. This reflects that corporations may have different policy positions on risk management which lead to alternate portrayals and standards for how to proceed once a risk level is determined. Compare the risk matrices below for two different organizations:

Organization "A" Policy:



Organization "B" Policy:

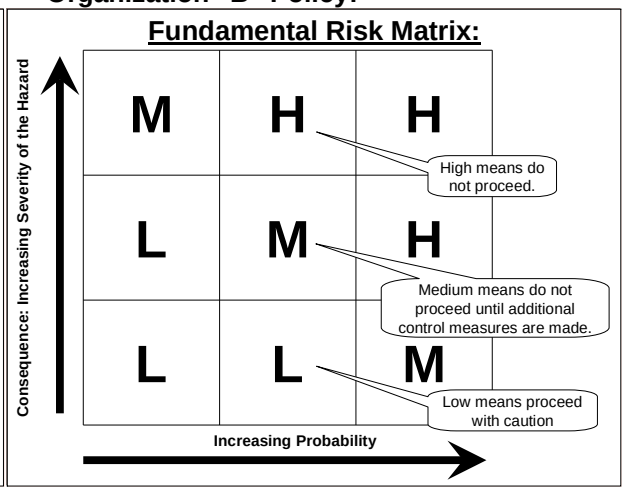


Figure 2.6. Two examples of corporate risk matrices.

Organization "A" policy may state:

- Management would readily proceed with an activity with a low risk level ("L" for "Low").

- Management would proceed with caution (ensure safeguards are adequate and implemented) for an activity with a medium risk level ("M" for "Medium").
- Management would not proceed with an activity with a high risk level ("H" for "High") and would take action to reduce the risk to an acceptable level.

Organization "B" policy may state:
- Management would proceed with caution with an activity with a low risk level ("L" for "Low").
- Management would not proceed until further control measures are included (ensure safeguards are adequate and implemented) for an activity with a medium risk level ("M" for "Medium").
- Management would not proceed with an activity with a high risk level ("H" for "High").

Different corporations may also adopt additional levels to further differentiate probability and consequence values, and may also have an increased number of risk categories. Thus our fundamental "3 x 3" matrix (with three levels each for consequences and probabilities, and three categories of risk (L, M, H) could be expanded to four or more categories of risk (Extreme, H, M, L, etc).

Risk Criteria: A Practical Example of Putting Theory into Practice

An organization has established the generic risk criteria table, shown below, based on their analysis of corporate data and reflecting their business context and related thresholds. Based on their analysis, the organization was able to describe varying degrees of impact on PEAP and categorized them as "High", or "Medium", or "Low". Similarly, the organization was able to describe varying degrees of probability and categorized them as "High", or "Medium", or "Low". With these data, the organization can build a 3x3 fundamental risk matrix. Consider this example:
- A management team including subject-matter experts could conceive of an activity in their facility that could escalate (loss of controls) to an unwanted incident. The team rates the incident opposite its probability and its impact on PEAP. For example, the management team selects the activity as the transfer of liquefied propane gas through a flexible transfer hose, conceives that this transfer hose could fail, and this results in an unconstrained leak of liquefied propane gas from an inventory of 10,000 kilograms through a 10 cm diameter hose.
- The team concludes that this incident could have a probability as "has been observed in similar circumstances", and could result in a disabling injury or fatality, a toxic release, high repair costs or damages to property >$100k, and loss of production for an extended period.
- Thus, the management team concludes that such an activity (the transfer of liquefied propane gas through a flexible transfer hose) has an Impact Rating of "High" and a Probability Rating of "Medium". The "risk" of such an event thus becomes "High" (select "H" if either one is "H"). This is a method for qualitatively categorizing the risk and testing for its acceptability.

A note on constructing the risk criteria table: By gathering and researching corporate data, the subject-matter experts and management team make their best, informed determination as to the ratings that reflect their business realities.

Risk Criteria Table

The following table shows two factors (Impact on PEAP and Probability) and several descriptions for each of the risk ratings. Management can use this table to determine the risk rating for an activity and any conceivable events that could arise (escalate) from that activity and can also use it to establish the acceptable levels.

Table 2.5 Example of a Risk Criteria Table.

Ratings	Impact on PEAP	Probability
High	High **P** Disabling injury, loss of body part or fatality. **E** Reportable violation, toxic release. **A** High repair cost (Typically > $100k). **Pr** Loss of function of facility for extended period, with business consequences, major quality deviation.	High • Repetitive event. • At least once per year • Several times in the life cycle of a project. • Has happened frequently in similar circumstances. • Greater than 50% chance of occurring.

Medium	Medium **P** Medical Aid injury. **E** Non-reportable spill, non toxic release. **A** Moderate repair cost (typically > $10k). **Pr** Short duration loss of function, serious quality deviation, medium business impact.	Medium • Infrequent event. • May only happen occasionally (less than once per year). • Has been observed in similar circumstances. • 10 to 50% chance of occurring.
Low	Low **P** First aid injury. **E** Minor lead, non toxic fugitive emission. **A** Low repair cost (typically <$10k). **Pr** Brief interruption or minor quality deviation or minor cost to correct.	Low • Unlikely event. • Never happened to date. • Has never been observed but is still felt to be a possibility • Less than 10% chance of occurring.

Legend: P = People; E = Environment; A = Assets; and Pr = Production

Corporate Policy, the Acceptable Level of Risk, and Management Direction

For the organization, the next step is to determine the levels of risk (acceptable or unacceptable) and the management directions *(management's instructions for what direction to take to resolve the risk or manage the risk, for a given level of risk)* for each of those levels. This becomes the policy of the organization (i.e. corporate policy). An organization needs to do this at least once to establish corporate policy; thereafter, the organization needs to periodically review it to affirm that corporate policy remains aligned with or exceeds society's and government's expectations for the responsible management of risk in the organization's operations.

In the "3x3" example, the risk of the activity (the transfer of liquefied propane gas through a flexible transfer hose) leading to conceived incident (failed transfer hose) was determined to be "High". Is "High" acceptable or unacceptable? It was earlier stated that "High is not acceptable", but where was it determined that "High" is not acceptable? Further, for an organization that is in the business of off-loading, storing, and loading LPG, and it has determined that the transfer has "high" risk, the organization is not going to abandon this activity as this basically means changing its business model. So, how does the organization set policy to continue with this core business activity?

It is responsibility of management to define all levels of risk including management directions for each of those risk levels and to set the acceptable level of risk. To do so, management is required to know and understand the laws and regulations, the corporation's financial concerns, the corporate values (these reflect the values of executive management and corporate directors), and the local community needs.

This is where corporate policies and rules, management system requirements, procedures, and to a certain extent, the values of management come into play. Policies describe the acceptable levels of risk and are intended to manage the risk of an organization's operations to within acceptable levels. For example, corporate policy could state that "no activity shall be undertaken if an event has happened in similar circumstances". (On a personal comfort zone, would you accept the risk of an activity that could be characterized as having a probability of "has happened in similar circumstances" and has potential impact on PEAP of fatalities and destroy your plant?)

Using corporate policy as the basis, this activity (the transfer of liquefied propane gas through a flexible transfer hose) has an unacceptable level of risk. Considering the risk management process, management's response must be to not proceed; that is, the organization must identify any additional risk reduction solutions to reduce the risk and re-assess the risk before resuming. In the example, a change from a flexible hose to rigid piping for transfers (and also to abide by government regulations prohibiting truck-to-truck transfers) reduces the risk to a level that now falls within the corporate policies, and the organization can proceed with the activity and manage the residual risks of the transfer of liquefied propane gas through rigid piping.

Note: A good management team will be watching for or alerted to an event at other plants (including competing organizations and non-related industries), study them, take the opportunity to learn from those other events, determine if there are weaknesses in their plant, and take any actions to address those weaknesses. This is the mark of an effective and very proactive risk management team.

ENGG404

Chapter 3:
The Risk Management Program

Section 3.1: A Model for a Risk Management

An effective risk management program consists of four elements: 1) an effectively implemented risk management system, 2) a risk management work process, 3) engineering controls, and 4) administrative controls (policies, procedures, checklists, etc.) and associated work practices. This chapter discusses the Risk Management System and the Risk Management Work Process, while Engineering and Administrative Controls are detailed further in Chapter 4.

Figure 3.1 The elements of an effective risk management program.

A **Risk Management Program** is the organization's overall risk management practice. It is the integrated approach to the continuous reduction of risk to people, environment, assets, and production/productivity (PEAP). It systematically applies management policies and procedures to identify, analyze, assess, evaluate, and manage (control) risk. The risk management program is driven by management direction with the purpose to control (i.e., mitigate, reduce, or eliminate) risks to an acceptable level and to prevent loss incidents involving PEAP. The risk management program involves such considerations and decisions as risk perception, acceptable risk, cost-benefit and resource allocation, and other value judgments.

The approach to risk management must always begin at the earliest stages of any endeavour, whether it be a new project or a retrofit project, a project-in-progress, or an ongoing operation. When leading an organization or operation, and in absence of a systematic approach to risk management, start the process regardless of any current activities to ensure thoroughness in managing risk in the operation.

A **Risk Management Work Process** is the systematic application of management policies, procedures, and practices to the activities of identifying, analyzing, evaluating, and managing the residual risk of activities that have been accepted by the organization.

A **Risk Management System** is defined as the integrated approach to the management of the continuous or ongoing reduction of residual risk to PEAP in the industrial setting. It is the documented set of management policies, procedures, and practices that enable the implementation of the risk management work process. It can consist of a number of elements, and sections within those elements.

Why is it Important to Me, the Engineering Graduate? Because:

- *You are going to be leaders, managers, and designers in your organizations during your career.*
- *Risk is inherent to your work, and you need to understand risk management processes.*
- *You need to understand what tools are available, their limitations, and how they work to successfully manage risk throughout your career.*

What is Important in a Risk Management Program?

Superior performance in safety and risk management is due to a robust risk management program. A survey of organizations with superior and continuing safety and risk management performance revealed a number of common characteristics of their programs. The following factors help build a successful, efficient, cost effective, safe and reliable operation:

1) Management is fully and visibly committed: their actions are always consistent with their words.
2) Wide and deep understanding of the importance of Safety and Risk Management;
3) Long-term commitment and undertaking by all employees, including management.
4) There is constant attention, a proactive program, and open two-way communication (always).
5) Safety and loss management is everyone's responsibility.
6) Non-negotiable procedures for critical jobs.
7) Safety and loss management is planned into each job with employees involved in this planning. Suggestions actively sought from all employees – including timely feedback.
8) Pride in performance at all levels. Positive reinforcement should play a continuous role.
9) Discipline plays a minor role - used as a last resort. Positive reinforcement should play a continuous role.
10) As a result of doing all of the above well, an effective Safety and Loss Management culture is developed and sustained.

It is not surprising that organizations will have significant similarities in the areas of emphasis within their respective risk management systems. Further, there is a significant amount of overlap between these focus areas and the standardized elements in a risk management system. Manufacturing organizations, industry associations, consulting organizations, and professional associations have built risk management systems that fit their needs based on data similar to the lists shown previously.

Section 3.2: The Risk Management Work Process

Recall that risk is a function of the probability of an event occurring (*How likely is it to happen?*) and the level of consequence, impact or severity (*How bad will it become?*) should that event occur. How do you analyze risk? Assess risk? Evaluate risk? Manage risk? These questions are answered in this section.

At first glance, risk analysis, risk assessment, risk evaluation, and risk management seem to be the same. However, these topics are unique. Risk management involves dealing with uncertainty.

- While hazards associated with an activity, or the consequences of an incident escalating from that activity, can be quantitatively or at least qualitatively determined in advance, there remains some uncertainty. *How bad will it become?*
- Similarly, the probability of an incident, by definition, is uncertain. *How likely is it to happen?*

Dealing with uncertainty makes the job difficult for a manager. However, risk management techniques turn uncertainty into tangible actions for preventing incidents. To apply these techniques, it is necessary to study and understand different concepts and approaches, their applications, and the merits and limitations of tools for managing risk. Familiarizing oneself with risk management techniques will enable a manager to reduce risks to an acceptable level, control residual risks, and ultimately prevent unwanted incidents that result in losses to PEAP.

There are many different processes to identify, analyze, assess, and evaluate the risks posed by operations or activities. While the words and processes may be different, they may be completely identical in purpose, methodology, and outcome. Unfortunately, like the words "incident" and "accident", there is no blanket uniformity in the field of risk management. This course content strives for consistent application of the terms.

Any activity has a risk and, to perform or execute that activity without incident, the risks associated with that activity must be managed (presumably before an activity is undertaken) as follows:

- The risks have been analyzed (i.e., the hazards identified and consequences and probability estimated);
- Some means or manner of safeguards or control measures to mitigate that risk has been determined;
- The level of risk for the activity has been evaluated and is acceptable to stakeholders; and

- The control measures have been or are intended to be implemented before and/or during the activity.

Now suppose the activity is repeated at some interval or is ongoing. Naturally, the associated control measures should always be in place whenever the activity is undertaken; this is the essence of “managing the residual risk”.

The Simplified Engineering Safety and Risk Management Work Process

The risk management process can be represented as a flowchart as shown below. It is based on a simplified **APEGA Guideline for Management of Risk in Professional Practice (Version 1.0, September 2006)**.

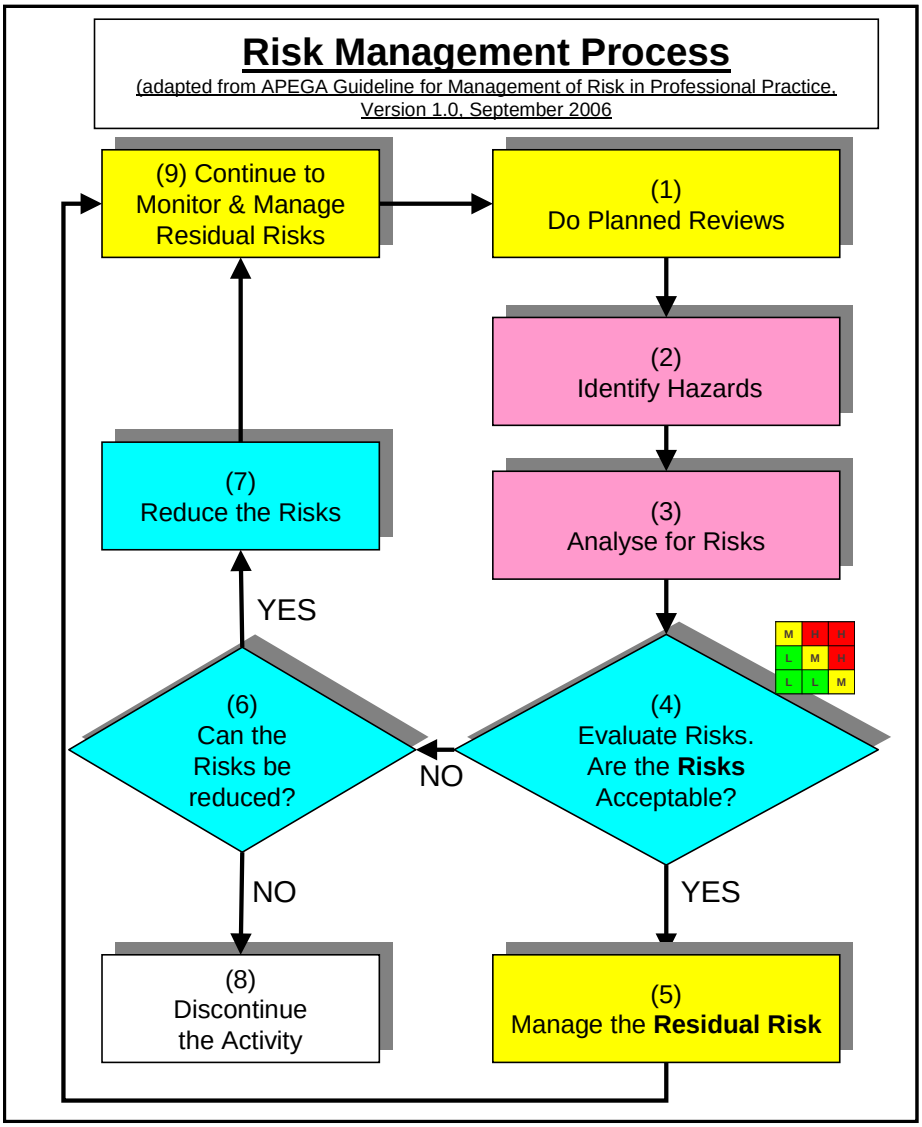


Figure 3.2 Adapted from APEGA Guideline for Management of Risk in Professional Practice, Version 1.0, September 2006

Key Management Activities and Steps in The Risk Management Work Process

Each of the boxes in the Risk Management Process flowchart in Figure 3.2 represents a step in the process, as described below. It is presumed that the risk management process is being applied for 1) a new project, 2) an existing facility where no risk management has been implemented, or 3) an existing facility where risk management has been and remains successfully implemented. In each of the three scenarios, there are different drivers. For a new project, risks have not been reviewed. In the second scenario, it would seem there has been a change in management, and the new management wants to start the process. For the third scenario, this step is part of an

ongoing process: the management system requires periodic reviews. In the discussions below, the term **activity** refers to the whole of a new project or an existing facility, or any of the activities that happen within them.

1) Conduct Planned Reviews

Key management activities:

- track organization actions versus alignment with policy
- ongoing analysis of the public's issues with respect to the type of business operation, including their perceptions of the risks with which they are concerned

The first step determines the requirements for risk reviews and defines when risk reviews are expected to be done and by whom. Reviews are mostly looking for, or at, effective management systems. For example, physical designs usually are done well if the engineer-design-build process is followed with appropriate reviews at various stages. Without reviews, hazards will not be found, and the manager may unknowingly put the facility at risk. The hazards must be reviewed and known to determine the risk. Regular reviews of varying types are conducted to find potential hazards in new designs or existing facilities.

Reviews should provide the data and information needed to monitor operations or new project designs. This information creates the database for monitoring as per the safety and risk management system. The database would include incident investigations, insurance organization reviews, third-party audits, internal audits, self-assessments, inspections, observations, regulatory activities (pressure vessel inspections, environmental reporting, asset renewal needs, changes to laws, code updates, etc.), as well as normal operating data collected on the business operations and maintenance activities. The manager needs to be proactive, and gathering good data and information is imperative for effective risk management.

Reviews need to be part of the ongoing management system. The manager of an existing facility must then mandate and drive these reviews. The manager and management team must monitor the operation for concerns and learn from industry activities in general through associations and the news. Through these means, potential concerns (e.g., possible hazards in the facility) are raised. The reviews can also include external reviews by such groups as the organization's insurance organization, industry associations, or government agencies. Effectively designing these reviews and having the right people to conduct them will yield valuable information that identifies possible weaknesses in the risk management system.

2) Identify Hazards

Key management activities include:

- look for, track, and analyze hazards and concerns that arise and that challenge policy
- raise public awareness and ensure accuracy and clarity of public perception

The management team will receive the planned review results which determine what needs to be further analyzed in terms of potential risk exposure. The next step is to identify the hazards related to the activity being studied. The process of hazard identification is a vital first step in the risk management process. If no attempt is made to identify hazards, then the assumption is there is no risk, and potentially significant risk exposures will not be managed effectively. That is why upfront hazard identification is so important.

If there has been a thorough attempt to identify hazards, and none of significance are found, then the integrity of the process is confirmed, and periodic reviews should be conducted to ensure that this is maintained.

There are many different tools to use to identify hazards, as presented in Chapter 2 **Hazards and Hazard Identification**.

3) Analyze for Risks: Determine Consequences, Probability, and Risks

Key management activities include:

- determine the risks that arise and that challenge policy

The third step is risk analysis. After identifying the hazards, then the risks of the activities are determined by determining: a) the consequences of an incident, and b) the probability of an incident. These analyses are designed

to quantify or categorize the risks by determining if existing or proposed safeguards and control measures reduce or mitigate the risks to acceptable levels. In other words, it evaluates the effectiveness of risk reduction solutions. The risk analysis methodologies required and the degree to which the risks need to be considered will vary.

Internal Step – Check for Control Measures
Before determining consequences and probabilities, the safeguards and control measures should be defined / identified, designed, developed, or already implemented. In other words, the risk estimations at this point in the process should consider the control measures that have been implemented or are intended to be implemented. Account for all known safeguards (i.e., designed into the new project or installed for existing facilities) and control measures when determining risks at this point.

Good designs, both new and existing, should be at or very near ALARP (As Low As Reasonably Practicable) for reducing risks (see Chapter 5 **The Fundamental Approach to Control All Risks**). If the designs are poor, or installed designs are deficient, this process will reject them on the basis of risk until improvements in the safeguards and control measures are made. After making improvements, risks can be recalculated to confirm they are acceptable.

Consequence, the first factor of risk, can be determined using many methodologies. The methodologies can be qualitative, semi-quantitative, or quantitative, depending on the hazards being analyzed. Quantitative consequences can be determined using complex tools such as gas dispersion modelling for a release scenario. In most cases, consequences are qualitatively determined by using a set of risk criteria (i.e., the consequences scale on a risk matrix or the consequences table that accompanies a risk matrix). These tools help to clarify the consequences so that the risk of the activities under study can be determined.

Probability, the second factor of risk, pertains to the failure frequency of systems, humans, equipment, machines, etc. Data are available generically, but the best data are in the operation's database, such as maintenance records and production records. Probability can be quantified, but requires a good amount of data and a good understanding of that data to be of value. In some cases, the long period between incidents does not yield sufficient information about the probabilities, and the judgment of risk management experts and senior management provide collective educated probabilities – leveraging data supports this approach. Probability is qualitatively determined by using a set of risk criteria (i.e., the probability scale on a risk matrix or the probability table that accompanies a risk matrix).

Risk Estimation
After consequences and probabilities have been determined, the following situations can arise:
1) In most cases, the qualitative determinations of probability and consequence can be derived from the corresponding scales on the risk matrix or the risk criteria. From these qualitative determinations, the risk is estimated using the risk matrix.
2) Some risk analyses may require explicit quantification of both potential consequence and frequency; this can develop into a complex engineering problem.
3) In some cases, an understanding of the potential consequences may be adequate to compel action and detailed analysis of frequency is not necessary (i.e., risk reduction solutions must be implemented). The assumption is either a) the probability is near 1 if the hazard exists (no controls on it), or b) the cost to eliminate or largely mitigate the hazard is relatively small.
4) In cases involving significant consequences, additional information on how likely the accident is to occur is needed. This is the most complex and most debated of topics when practiced in industry – how likely will the worst case occur?

At this point, the hazards have been identified, the activities analyzed for risk, the designed or installed control measures are noted, and the risks are determined considering the control measures.

4) Evaluate the Risks and Reduce Risk (through ALARP if Needed)

Key management activities include:
- assess the determined risks against the benchmark criteria for acceptability
- implement policy (make decisions) for acceptable risks
- determine and implement any actions to further reduce risks to acceptable levels
- continue to raise public awareness and ensure accuracy and clarity of public perception

The fourth step is to determine if the risks for the planned activities (with the control measures and safeguards in place), as identified in the previous step, are acceptable. The risk level of the activity, as determined in the previous step, is compared to a set of risk criteria, and management makes decisions based on the comparison. The formal term for this comparison is risk evaluation.

The risk of the activity must then be evaluated to see if it is considered acceptable. There are two basic approaches to evaluating risk against risk criteria:

1) The traditional approach is qualitative in nature and typically involves making judgments based upon standards. These standards evolve over time as a result of historical performance or experience. These standards are typically documented and communicated in the form of a risk matrix.
2) The second approach is quantitative in nature and involves comparing the risk of the activity with numerical criteria.

For the traditional approach, most corporations have developed risk matrices that describe what is considered low-level risk, medium-level risk, and high-level risk. These matrices can be based on policies and standards, but in some cases (e.g., new technologies), quantitative data may need to be researched or generated through studies to determine the acceptable and unacceptable levels of risk.

Of more importance, these matrices clearly communicate to employees what is acceptable (i.e., what they are allowed to do) and what is not acceptable. Low-level risks with existing / planned safeguards are usually acceptable without any further management involvement or risk reduction solutions, or design additions. Medium-level risk requires management involvement to ensure that additional risk reduction solutions are implemented to reduce the risk (i.e., acceptable with certain conditions). High-level risks are generally unacceptable: the use of safeguards and control measures does not reduce the risk to as low as reasonably practicable (ALARP). In most corporations, it is the most senior management that determines whether high-risk activities will proceed, and generally they do not approve such activities. It is worthwhile noting management engagement is critical, as they are assuming the direct responsibility for taking the risk.

When the risk has been appropriately reduced and determined to be acceptable with the safeguards or control measures, risk evaluation is complete, and the residual risk remains to be managed. If all conceivable control measures have been included in the risk estimation, and the risk remains unacceptable, then discontinue the activity. (This statement is the route from box (4) through box (6) and on to box (8) in the flowchart.)

5) Manage the Residual Risk, if Risk is Acceptable

Key management activities include:

- manage residual risks to ensure organization activities keep risks under control
- communicate these activities to stakeholders, including the public

Once a risk has been reduced to acceptable levels, the residual risk must be identified and managed. If not already done in the Step 1 (Conduct Planned Reviews), it is appropriate to ensure that appropriate and effective management systems are in place and that the residual risk is being monitored and controlled.

Recall that integral to Step 3 was that risk reduction solutions (control measures, etc.) were identified, defined, designed, or developed to reduce, mitigate, or eliminate the risks. Step 5 is where these solutions are further defined, designed, developed, and ultimately implemented, and their effectiveness checked to actively manage the residual risks.

The Risk Management System

Residual risk is managed by implementing a risk management system. This system consists of a number of elements (requirements) that must be executed to manage the risks in an acceptable way. **Once a risk is accepted, it does not go away.** It is there waiting to happen unless the management system is actively monitoring the operation for concerns, and management is ready, able, and willing to take proactive actions to correct potential problems (see **Risk Management System and Elements** later in this chapter).

This step heavily draws on the operation. Management must retain the resources to sustain the safeguards and control measures to maintain the residual risk levels at the intended risk levels (i.e., acceptable). Management is

now responsible for assuming and managing the residual risk, and for preventing incidents from happening. This due diligence is imperative, and many incidents have resulted when residual risk management lapses (see Chapter 6, **Due Diligence as Applied in Industry**).

6) Can the Risk be Reduced?

If the risk is initially determined to be unacceptable, methods of reducing the risk must be examined again and brought forward for evaluation. This is another internal step.

There are ways to reduce the risk, if a risk is initially determined to be unacceptable. Additional control measures (such as engineering controls, management systems and administrative controls, protective features and devices, personal protective equipment, or combinations of these) can be added to reduce or mitigate the risk to an acceptable level (see Chapter 5, **The Fundamental Approach to Control All Risks**).

If management is not prepared to accept those risks even after going through the process to determine all control measures and safeguards, then management must discontinue the activity. Also, if management is not prepared to provide resources for implementing the control measures, then management must discontinue the activity. To do otherwise, is irresponsible ethically (values) and professionally (legal).

If management does accept the risk (i.e., continues with the activity), they must ensure they manage the controls for those risks to keep the risks within acceptable levels.

7) Reduce the Risk, if it can be Reduced

If the proposed changes in control measures are reasonable and accepted by senior management, then make the necessary changes. When risk reduction steps are taken, hazard identification and risk analysis must again be completed to determine if any new risks have been introduced.

8) Discontinue the Activity, if Risk Cannot be Reduced

If the risk is unacceptable and methods to reduce the risk have been exhausted, then the activity creating the risk must be discontinued (stopped, not started, abandoned, etc.).

It is very important for management to recognize:

- when the risk is too high;
- when the residual risk cannot or can no longer be managed; or
- when the residual risk cannot be reduced any further (due to some constraint).

Management needs to be clear about discontinuing an unacceptably high-risk activity. Organization core values, ethics, objectives, etc. all come to play in this step. Challenging situations arise when it means lost profits, missed opportunities, professional set-back, stress, etc. This step is key because it asserts management will not undertake unacceptably high-risk activities (i.e., something that is unsafe and puts people at risk, pollutes, damages assets, risks your business needlessly, or negatively impacts the reputation of your organization).

The employees make conclusions on organization values based on the manager's actions, and their support for management decisions is dependent on management integrity. *Is what we are doing consistent with what we say?* Employees will watch you perform as a manager when tough decisions need to be made. This is another lesson in **The Engineer's Survival Guide**.

9) Continue to Monitor and Manage the Residual Risk

Note that when a change is made, the risk management process is once again used to evaluate possible new hazards and risks. Changes in processes can introduce risks or create potential problems upstream or downstream. Ensure your analysis of the change is done before the change is implemented to avoid creating unchecked hazards. Is one set of risks traded for another? If risks are not uncovered, the operational risk may go up unknowingly to managers.

Similarly, from Step 5, the process is once again used to check the risk management system and to search for unintended risk exposures. The risk management process is one that must continue to cycle.

More on Managing the Residual Risk

It is the manager's responsibility to minimize and control hazards to people, environment, assets, and production / productivity (PEAP). That is, it is the manager's duty to implement the actions and plans to **manage the residual risks** to ensure risks are kept under control, all with the goal to ensure an incident does not happen. The importance of managing the residual risk relative to the due diligence for a leader of an organization is discussed in **Due Diligence as Applied in Industry** (see Chapter 6).

A plan of action is drawn up from the risk management process to implement additional control measures. Typically, this plan consists of an action list, with completion dates and responsible persons, published and stewarded by senior management. Management must also provide the resources (i.e., people and money) to allow timely completion of the various tasks. In most organizations, risk management planning and action will be a continuous, ongoing activity (i.e., the plan is implemented and the actions checked to ensure that the actions are effective in managing the residual risks). Once the risk is determined to be acceptable, managing that risk (i.e., keeping the control measures effective) becomes the ongoing management challenge.

Managing the residual risk thus requires a **bias for action**. The application of the **Fundamental Management Process** (see Chapter 7) is key to managing the residual risk. Managers must constantly ensure that the safeguards and control measures, as determined in Risk Assessment, are being implemented and being maintained in order to keep the risks under control.

Managing the residual risk is the most critical of management activities, requiring constant vigilance and support. Successful managers possess a great deal of commitment, perseverance, and energy. Managers must uphold the standard (i.e., the minimum requirements as specified by government or by the corporate policies, whichever are more stringent), and typically work to go beyond those standards to improve and find better ways to manage the residual risk. Managers achieve this by conducting **safety reviews** (audits, inspections, and observations), as described in **Job Observations and Planned Inspections** (see Chapter 5).

Effective managers do not "let things slide" within their operations / their sphere of influence. Effective managers must plan their **inspections**, conduct the **inspections**, check that expectations are being met, and act accordingly. The discussion on how to uphold and improve on managing risk is complex and is more fully discussed in **Leadership, Motivation, Organizational Design, and Culture** (see Chapter 7).

Managing the Residual Risk of an Industrial Operation

The residual risk of an activity is that which remains after all safeguards and control measures have been implemented (or included in the intended design). These measures include **engineering controls** in the process operations as well as **administrative controls** in supporting work processes.

Success hinges on sustainably managing the residual risk – ensuring that the safeguards and control measures remain in place to limit risk to intended levels.

In summary, management must implement a proactive, systematic, and comprehensive risk management program that considers and addresses all consequences and probabilities, that sustains and maintains the safeguards and control measures. To limit the residual risk, and in so doing, avoids incidents and losses detrimental to sustaining the business activity.

Overall, key management activities in a risk management system are:
- analysis and assessments (to identify hazards and risks, and their control measures);
- active implementation (to carry out and steward to the management system for all requirements);
- incident investigations (to analyze and learn from incidents to prevent recurrence); and
- inspections and audits (to confirm that risk management system elements are being implemented).

Leadership in risk management is characterized by the fundamental management of the above key activities, as will be discussed in Chapter 7, **The Fundamental Process of Management: The Plan-Do-Check-Act Cycle**

(PDCA). PDCA is driven by management: leaders exhibit commitment by doing and checking, and by holding their people accountable.

Managers as Owners of Risk

A key activity of a manager is delegation: managers will be delegating some if not most of the decision-making on activities involving risk. Delegation means that the manager is assigning responsibility to their employees on the basis that the manager is assured they will make the right decisions. However, the manager must hold them accountable for their actions, and the manager remains responsible for and accountable for their decisions and actions. (Delegation does NOT mean abdication.)

Given that managers delegate work to their employees, and depend on their employees to do the work, they put great effort into hiring good, qualified people. Employees are assigned responsibilities for their work, along with the risks and means to manage the risks of that work. Successful delegation with respect to risk management requires managers to:

- have solid checks and balances in place to manage risk;
- educate and communicate clearly what level of risk is acceptable and what is not;
- ensure all employees understand their levels of responsibility and accountability for managing risk;
- ensure all employees understand when additional input to the decision-making process is needed (which will be explained in more detail in the MOC work process); and
- ensure all employees understand that when they deviate from the requirements for managing risk, they are putting themselves, their coworkers, the organization, the community, and the environment at risk.

The delegation of work applies to both the **core** workforce and the **contractor** employees.

- The core workforce employees perform duties and continually manage the risks of those activities within the boundaries of policies and procedures. Management has trained, certified, and authorized the employees to perform activities with risks, using the appropriate and required safeguards and control measures.
- Contractor employees are hired to perform duties, which may put the manager's operation at risk if management is not assured they will make the right decisions and take the right actions (i.e., manage the risks of their activities within the operation such that they do not put themselves, the operation nor the core workforce at risk).

Clearly, within line management, an owner (including shareholders and directors) or senior executive becomes accountable for everything employees do, including the consequences of a risk taken by them. If you were in this position, how would you manage risk? How would you make it clear to your employees what to do to manage risk? There is a need to clearly define what is acceptable and what levels of review and approval are required (especially in the face of change or when things deviate from the expected) to effectively manage your business.

It is important to realize the professional and ethical responsibilities around the ownership of risk. Although there are many available standards, regulations, guidelines, and policies to follow in the course of performing work, there are also many external pressures around costs, schedules, handling changes, etc. that can influence decisions and compete with priorities. **Leadership, Motivation, Organizational Design, and Culture** (Chapter 7) discusses how to handle these issues.

Vulnerability in Your Organization

Let's look more closely at the two previous points that managers are required to address:

- ensure all employees understand when additional input to the decision-making process is needed (described in the MOC work process); and
- ensure all employees understand that when they deviate from the requirements for managing risk, they are putting themselves, their coworkers, the organization, the community, and the environment at risk.

These two points are pivotal when one considers that many incidents are caused by decisions that were made without proper management involvement. These poor decisions in turn made the organization vulnerable to unintended and unacceptable risk exposure. These two points cannot be overemphasized.

Impact of Change on Risk (see MOC Section in this Chapter)

At the outset, it was stated that the Risk Management Process is a continuous and ongoing management activity, as is each of its components. Recall that a certain amount of risk has been determined, has been deemed

acceptable, and is actively being managed. However, it remains that something could change, that the risks will change, and that an unwanted incident could happen. Thus, management must be alert to any changes that may impact risk.

An area often overlooked, especially when it concerns change, is the area of competency in the wake of changes in the organization such as:

- extra staff on overtime to deal with changes in the normal operating state of a facility (i.e., during start-up or shut-down);
- rapid increase in staffing for temporary and short-term high workloads;
- organizational design change for efficiencies (right-sizing);
- individual career development;
- high turnover periods;
- technical changes;
- rapid expansion; and
- downsizing.

When Management Accepts the Residual Risk

When Management has accepted and is actively managing the residual risk, it is equally important that management do the following:

- Management must realize that not only is the frontline worker the most vulnerable to the risk exposure, but also the frontline worker is the one who is actually managing the risk of that activity daily. It is not the manager in the office who is managing the highly flammable compressed gas in the propane storage and handling facility; it is the hourly worker who has his or her hands on the tools and valves and hoses.
- Management must ensure all employees meet all requirements of all policies, operating and instruction manuals, and procedures to manage the residual risks. The requirements for all safeguards and control measures need to be documented, as well as how they are to be implemented to manage the risks of the activities. To ensure employees meet the requirements, managers must conduct safety reviews (i.e., internal and third-party audits).
- Management must ensure all employees understand the implications of not meeting all requirements:
  - laws (i.e., the judgment of what is acceptable and not acceptable legally);
  - societal morals /values (i.e., what is acceptable at this time);
  - the effects on people / public beyond consequences the law may impose;
  - the effects on environment beyond consequences the law may impose;
  - the effects on business beyond consequences the customers-under-contract may impose; and
  - the attitudes of workers and the public about the organization.

Risk Management is Proactive Management

The risk management program is proactive and is the barrier to preventing unwanted incidents. If there are weaknesses in the risk management program, then the latencies caused by these weaknesses represent a loss of control over the risks, which can lead to unwanted incidents. Two conclusions may be drawn:

1) effective systems with continuous improvement build a better barrier (or a defense) to preventing incidents; and
2) good incident investigations with follow-up to determine and address latent causes build a better barrier to preventing incidents.

A proactive, comprehensive risk management program addresses risks at all stages and during all stages of an operation or project. Proactive management is our defense and is the barrier to incidents. It supports the organization's goal which is the desired outcome of "zero" incidents.

Section 3.3: The Risk Management System (and Elements)

A Risk Management System is defined as the integrated approach to the management of the continuous or ongoing reduction of residual risk to PEAP in the industrial setting. It is the documented set of management policies, procedures, and practices that enable the implementation of the risk management work process. It consists of a number of elements, and sections within those elements, as follows:

1) Management Leadership, Commitment and Accountability
2) Risk Assessment and Management of Risks

3) **Community Awareness and Emergency Preparedness**
4) **Management of Change**
5) **Incident Reporting, Investigation, Analysis and Actions**
6) **Program Evaluation and Continuous Improvement.**
7) **Design, Construction and Start-up**
8) **Operations and Maintenance**
9) **Employee Competency and Training**
10) **Contractor Competency and Integration**
11) **Operations and Facilities Information and Documentation**

Every organization is composed of a collection of people who are working towards, and contributing to, the broader objectives of the organization. (In most "for business" corporations, the broad objective is to make a profit, and as discussed, the avoidance of loss is all about making a profit.) People work towards the objectives of the organization by working within a (risk) **management system**. People follow policies, work processes, and procedures that are intended to guide or direct people to complete their duties and tasks, and meet the objectives of the organization. Of course, managers are people, too!

Recall that every organization has (or should have) a (risk) **management system** that:
a) defines how an organization is managed;
b) documents the policies, work processes, and procedures by which and through which people execute their tasks and fulfill their duties; and
c) has the objective of complying with requirements or regulations stipulated by governments, industry associations, or the organization's corporate policies.

There are many different types of management systems that can address all aspects of organizations, ranging from managing human resources, accounting and finances (including managing financial risks), quality, production, maintenance, manufacturing, and managing risks in occupational safety and in process safety.

As discussed earlier in this chapter, the Risk Management Work Process directs managers to identify hazards and risks, determine acceptability, define and implement the risk reduction solutions, and manage the residual risk to prevent incidents. However, the work process does not explain what is needed in order to effectively monitor and control these risks. This is the purpose of a Risk Management System.

In the engineering safety and risk management world, there are many different management systems, some with good overlap, some highly focused on a particular industry sector (nuclear, pharmaceutical, civil construction, mining), and some that apply more broadly (occupational safety, chemical / unit operations process safety, environmental protection). There are many sources of these management systems: governments and government agencies, non-governmental independent standards associations, professional and industrial associations, and corporations. These management systems are utilized around the world.

Simply, a risk management system is a guide or a framework for organizations, more specifically for managers in those organizations, to manage the residual risks (the hazards and concerns) in their workplaces. It requires a management system with various elements to monitor different activities to manage risk within the organization, as a means towards continually improving performance and to prevent incidents. A management system consists of the set of elements that encompass the perpetual (or ongoing) key focus areas which are necessarily relevant to the scope and purpose of the management system. These elements are (or should be) within the control of managers. These elements are the substance of the risk management system, and through application of these elements and the supporting work processes and procedures, provide the means to manage the risk you are willing to accept.

The Basics of a Risk Management System

In general, a proactive risk management system should ensure that:
- all potential loss exposures are identified;
- the risks in each exposure are evaluated;
- intervention plans are developed;
- the actions from the plans are implemented;
- progress is stewarded (monitored and controlled / responded to by commending / correcting); and
- management partakes in the process and is seen to do so by all employees.

A proactive risk management system is based on two concepts:
- that there is always the risk of a loss, and
- management policies, work processes, standards, and decisions are implemented to manage business at an acceptable level of risk, and thus limit both potential loss and the probability of an undesired event or incident.

Who is Responsible?

Most importantly, Line Management (not the subject-matter expert with functional expertise) is responsible for implementing the Risk Management System. Line Management must determine the risks associated with their operations and manage those risks.

What are the Risk Management System Elements?

A risk management system consists of a set of topics or **elements** that narrow the scope of risk management to that particular topic. For example, the aspects of management commitment and accountability have already been discussed. Obviously, some definition and direction that focuses on this topic would be beneficial for implementing a risk management system (hence, the **elements**). And among the many different management systems, the number of elements can range from as little as half a dozen to well over 20. It all depends on the extent to which an organization wants to subdivide the topics.

The elements of a management system enable managers to systematically understand the risks an organization has and to systematically manage their operations around these risks to prevent incidents. Having a risk management system in place with focused and defined elements provides management with the needed framework to effectively manage risk exposures on a sustainable basis.

The ENGG404 Risk Management System

In this course, the ENGG404 Risk Management System will be used as a basis for study and for application in the team project. It is representative of a general approach used to manage residual risk and identify new hazards that need to be managed. When presented with other management systems, take the opportunity to compare, identify, and align the system elements.

The ENGG404 Risk Management System has the following elements to focus your efforts so that your associated actions are effective. A list of activities for each of these elements is presented. Again, within an organization's risk management system, each element: is clearly defined with specific standards and objectives; forms the basis for design, construction, and operation of the organization facilities and assets; forms the framework for stewardship of performance of the organization; and establishes the foundation for due-diligence.

ENGG404 will have a particular focus on these elements (described in more detail in the next subsection):
1) management leadership, commitment, and accountability;
5) incident reporting, investigation, analysis and actions; and
6) program evaluation and continuous improvement.

Please ensure you understand these management system elements and why they are important. As you progress through this course, you will be learning to apply these elements in the management of risks for any activity and/or facility. These elements are the substance of the risk management system and, through application of these elements and the supporting work processes and procedures, provide the means to manage the risk you are willing to accept.

Element 1: Management Leadership, Commitment, and Accountabiity

- It is the most important element of any in the system.
- If this element is not strong, the system will fail or at best produce mediocre results.
- To ensure commitment is believed and understood, actions must be consistent with the words.
- The commitment must be for the long term, be given constant attention, and have a strong proactive thrust.

- Corporate vision / mission / policy statements are essential.
- Objectives and targets: Although each element will have its specific objectives and plans towards meeting their goals, management must ensure these are set because it provides a means to:
  - identify priorities to all employees;
  - effectively allocate resources; and
  - communicate to all employees the goals as well as the progress towards meeting those goals.
- Management applies the Plan-Do-Check-Act (PDCA; see Chapter 7) and plays the key role in planning, organizing, leading, and stewarding the risk control program. This should be integrated with all other organization day-to-day, mid-term, and long-term activities.

What Does This Mean to the Graduate Engineer? (Refer to the Engineer's Survival Guide, ESG)

- *ESG #2: "Understand your program." Know your responsibilities in the management system and fulfill them to the best of your ability.*
- *ESG #3: "When you make decisions, put safety ahead of any other objective." Make safety a value.*

What Does This Mean to the Graduate Engineer, concerning Management Leadership?

- *As you may become a leader in a short time, remember your responsibility to those reporting to you and that your employees will be watching you all the time. You need to be faithful to the organization requirements. You set the culture.*
- *Most first-class organizations expect engineers and business graduates to quickly understand the importance of safety and risk management, and to demonstrate commitment to associated safety / risk management activities, a key requirement before they can progress in their organizations. Average organizations are also coming to this conclusion, partly in response to public and government pressures and the impact of media detailing the results of industrial disasters around the world when leadership is lacking. Increasingly, corporate leaders are embracing core values that reflect care for people.*

What Does This Mean to the Graduate Engineer, Concerning Objectives?

- *As a manager you need to be looking forward at least one year ahead.*
- *Your objectives need to be clearly focused on priorities with a means to measure progress.*
- *Taking ownership of these objectives means accountability.*
- *You need to be "better than government"; stretch beyond minimum standards.*
- *As a manager you cannot lose sight of corporate values. Your employees are watching you, and you need to lead them by showing your commitment to these values.*
- *Leaders model the actions, and employees model their leaders. In other words:*
  - *If your employees see you looking the other way, then they will also look the other way and never meet your expectations.*
  - *On the other hand, if your employees see you doing what you expect of them, then they see your commitment and will find it difficult not to live up to your expectations.*

Element 2: Risk Assessment and Management of Risks

- The ultimate goal of risk management is to eliminate risks or to reduce and control risks to improve performance and prevent incidents.
- Risk management answers these questions:
  - If needed, what can be done to reduce or eliminate the risks?
  - What can be done to reduce the probability or severity of risks?
- This is clearly proactive: an approach to systematically analyzing the risks of activities posed to people, environment, assets, and production (PEAP) to prevent unwanted incidents.
- Use of the right tools and having the right people for:
  - setting policy on categories of risk;
  - risk assessment (hazard identification, risk analysis, risk evaluation);
  - determining the acceptable level of risk; and
  - managing the residual risk.

What Does This Mean to the Graduate Engineer?

- *ESG #2: "Understand your program." Know your responsibilities in the management system and fulfill them to the best of your ability.*

What Does This Mean to the Organization?

- *The Risk Management System needs to be "firing on all cylinders". The residual risk is managed by ensuring an effective risk management system is embedded throughout the organization, at all levels.*

Element 3: Community Awareness and Emergency Preparedness

In Alberta, it is the law that an emergency plan must be in place for handling hazardous incidents. The plan is hopefully never activated, but needs to be ready and current. This element requires a specific Disaster Management System based on "Prevention – Preparedness – Response – Recovery" (see below). It is the only reactive component in the management system, in terms of when it is activated. However, it is entirely proactive in terms of being prepared to respond to and mitigate incidents by:

- understanding the hazards, credible release scenarios, and worse case scenarios;
- understanding the consequences (impact on PEAP) of any adverse incident (onsite and off-site); and
- having resources in place, including trained personnel and dedicated equipment, and a protocol to enlist other "mutual aid" sources should the incident escalate.

What Does This Mean to the Organization?

- *Remember there is always a probability an unwanted incident will happen.*
- *Being prepared is a proactive approach to managing risk of an unwanted incident. It means having the ability to mitigate an incident to a lesser consequence.*
- *By planning for emergencies and practicing the response plan, the organization will be prepared.*
- *Always look for the worst realistic case, determine all the consequences, and develop the emergency preparedness and response plan to handle it.*
- *The first questions any responder will ask is, "Do we have enough people and resources to handle the incident? Are we putting our people at too high a risk?" If so they will not respond directly to the incident often protecting nearby businesses instead.*
- *Today, an organization requires a good working relationship with the community. In addition to handling emergencies, an organization needs to work with its community and stakeholders on an ongoing basis because the public can be a supportive if knowledge is shared with them.*

Additional Points to Consider:

- Potential emergency assessments develop the worst-case scenario(s).
- Emergency procedures and training are carefully developed for the worst cases and include regular dry runs as a means of training and testing the plan for weaknesses.
- Fire and rescue teams are put together to be prepared and provide the coverage needed.
- Security and access are necessary to reduce risk to non-essential people and ensure emergency forces are focused on just the incident at hand.
- Emergency equipment appropriate for handling all scenarios needs to be carefully selected and maintained.
- Medical personnel, either on-staff or contracted, are needed to ensure all eventualities can be handled quickly.
- Emergency coordination and leadership with a clearly defined organizational plan in place is needed.
- Coordination with municipal emergency services and mutual aid is important. The municipality does have jurisdiction, but with an organization's emergency plan in place, they will most likely support.
- Mutual aid-supporting resources (e.g., fire department, police department, medical services, occupational health and safety (OH&S) area inspectors; industry mutual aid).
- Plan emergency simulations and press releases / contact with media and public.

Disaster Management System: Prevention, Preparedness, Response, and Recovery (PPRR)

- It is a means to describe emergency planning.
- Incidents can be effectively mitigated by effective response.
- It is essential to practice the emergency response plan to ensure preparedness. Practice drills build competencies for a quick, effective response when necessary.
- A quick return to operation is needed after an incident; however, careful planning is necessary before resuming operation. The legal requirement for securing the scene may be triggered.
- Timely response to the regulatory agencies is necessary. Their direction, as a result of an incident investigation, can impact your operation.

Element 4: Management of Change

- The scope of this element addresses how an organization manages change. It should include definitions, activities, and responsibilities such as: what constitutes a change; who is responsible for reviewing the change, who is responsible for approving the change, who are the stakeholders, how it is communicated, and so on.
- Change is defined as any modification to or involving a task, a job, or an operation, in any of these types of activities: design, construction or installation, maintenance (trouble-shooting, repair, servicing), process operation (process constraints, procedures, sequence of tasks, introduction of new substances or change to different substances), change in suppliers, regulated operations, or even a change to the organization.
- Any change needs to be evaluated in terms of risk. This includes assessing the risk of new processes, activities, and facilities with particular emphasis on identifying any new risks that need to be managed as a result of the change.

What Does This Mean to the Graduate Engineer?

- *ESG #2: "Understand your program." Know your responsibilities in the management system and fulfill them to the best of your ability.*

What Does This Mean to the Organization?

- *Although the management of change has been viewed as bureaucratic, unknowingly taking on risks outside policy (i.e., beyond the acceptable levels of risk) is simply irresponsible.*
- *Managers must reinforce the expectations concerning the management of change.*
- *In the absence of good change management, the organization's employees may inadvertently take on more risk than the organization intended.*

Management of Change (MOC) Work Process

Management of Change (MOC) is just what it says. Change must be managed. Over time, organizations were finding they were repeating mistakes in design changes or were not picking up on important aspects of an organizational change or an operational change. As a result, unwanted incidents occurred. In fact, as people began to analyze the problems around "change", the picture quickly broadened to involve all business and operations aspects when "change" was involved.

Management needs to look at changes (of all kinds) in terms of risk and the consequences of a change. Does the change introduce a new or different risk (new or different hazard, new or different likelihood, new or different consequence)? Does the change affect the effectiveness of safeguards and control measures? Will the change alter engineering controls or require changes to existing engineering controls? Will the change alter administrative controls or require changes to existing administrative controls? Will changes to administrative controls be effectively and efficiently implemented through new or revised work practices? Are new work practices required and therefore new training materials and new or refresher training?

Consequently, MOC became a specific focus area with associated policies and procedures. Almost anything that was not a direct replacement ("like-for-like") was considered a change and subject to review and approval before the change could be implemented. Changes to raw materials, equipment, procedures, suppliers, customers, contractors, designs (additions and deletions), and organizational changes (such as a person moving into a role to replace another or job role changes) need to be managed.

It is an accepted fact of business that such changes can occur in all areas of an operation or an organization. Management must ensure their employees:

- understand that change is a normal part of operations;
- have the tools to clarify the scope of change and evaluate it; and
- understand the requirements for reviews and for levels of approval.

In the normal course of day-to-day ongoing operation of a facility, where the worker needs to have the ability to make process changes within clearly defined limits (i.e., within design specifications), a formal MOC process is cumbersome; therefore, changes within those clearly defined limits are acceptable without a formal MOC review. This flexibility of the operation within limits (or boundaries or specifications) is needed to ensure smooth running of the facility. However, if changes are outside these limits (or beyond boundaries or exceed specifications), the formal MOC process must be applied and formal reviews are required. The MOC process and required reviews ensure the level of risk is determined to be acceptable and is risk controls are not compromised.

An often-overlooked area is the operational procedures used to guide the way employees do work. Associated procedures have been developed to ensure tasks will not have a negative effect; these are based on operational experience and lessons from previous incidents. Without a process to analyze changes to these procedures, there is a significant danger of creating a higher risk. Any variance to an existing procedure needs to be reviewed for consequence and risk.

Change can be temporary or permanent. Managers need to be cognizant of this difference.

- Too often managers think "a temporary change" means something done inexpensively. The people involved with the Flixborough disaster of 1974 suffered the consequences of this misconception.
- Too often managers do not fully think through the risks of taking safety systems offline temporarily. The people affected by the Bhopal disaster suffered the consequences of mismanaged changes.
- Research and conducting experiments within operations are a type of temporary change, and these need to be managed as well. There are many examples of experiments gone wrong. The Chernobyl 1986 disaster happened because risk assessments were not done, secondary controls and backup systems were not incorporated, emergency plans were not considered, and communications throughout the organization were sub-standard.

Review all the case studies in this course. The consequences of these incidents are obvious. What management of change issues were prevalent in each incident? Would a review have been of value at the time? Could these incidents have been prevented if reviews for the changes were done?

Why Must All Changes Be Managed?

All changes must be managed to control all possible risks that may be introduced as a result of the change, in addition to:

- ensuring management and employees understand risk over a long period of time; and
- ensuring the review and management of policies, standards, and procedures in any engineering discipline or operation.

How Is Change Managed?

Change management is accomplished through policy, work process, and procedures with guidelines to assist in assessing the proposed changes to the activities.

The **Management of Change Work Process** flowchart (as shown later in this subsection) describes how most organizations manage change or should manage change. It is a management systems guideline, it includes specific requirements, and it defines the boundaries within which people must work. In the procedure, there are several points where decisions need to be made. Many involve a choice, which is not necessarily a black and white one. It is imperative that each one of these choices is thoroughly thought out. When in doubt, the conservative route is always chosen. Also implied in this work process is the need to use input from others. Including others for advice or, in more serious cases, incorporating expert advice may be required to obtain management approval.

The work process starts out with a change that triggers the start of the process. It may seem simple, but it is important. Associated change management guidelines may include general categories to define the type of change under consideration (e.g., process, design, organization, etc.) and make provisions for individual workplaces that identify hazards specific to that area. Clarity is critical to ensure that employees are clear on what is needed and do not skip some areas of concern. This first step, proposing a change, is usually initiated by the person who wants the change or who has been directed to initiate the change; this is the Change Owner.

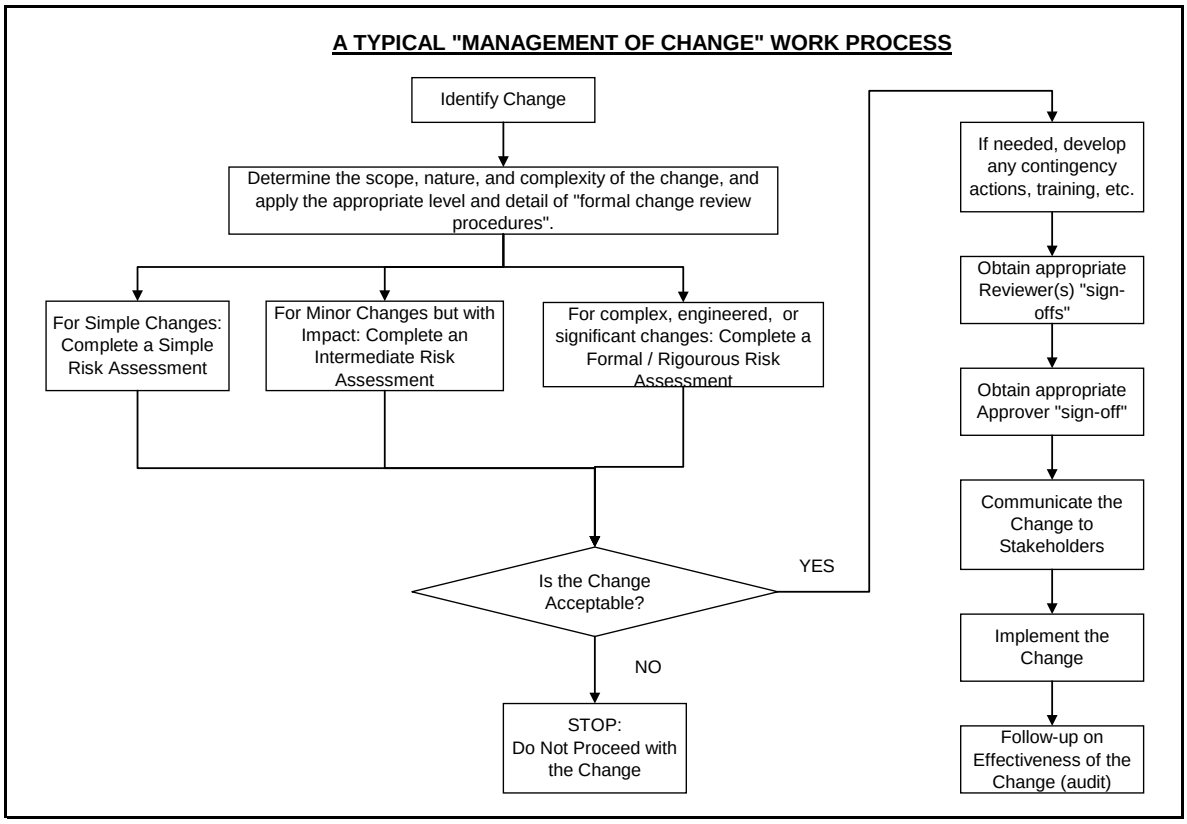
As the steps in the MOC work process progress, it can become very complex: sufficiently complex to require a detailed and documented procedure to guide the Change Owner and formalized training for employees using the MOC process. Given that the MOC process requires significant effort to complete, the involvement of associated personnel in periodic reviews or the development of the MOC process for their departments build commitment to the process. It also acts as a form of refresher training in the MOC process.

A Typical MOC Process

As can be seen in the flowchart below, there are a number of steps that are needed in the process above and beyond the four critical actions. As well, the degree or complexity (simple, minor, and complex) of the proposed change determines the extent (breadth and depth) of the risk assessment.

For risk assessments, the terms “simple, minor, and complex” are not defined here because these have different meanings for different industries. During scope definition of the change under consideration, the change will be categorized as simple, minor, or complex; the category of change will dictate the extent of risk assessment commensurate with the degree of change complexity. The intent is to show that risk assessment efforts need to be proportionate to the change complexity such that there is neither “overkill” nor gross oversights on risk assessments.

Management of Change Process:



The MOC Work Process: What needs to happen when making changes?

1) Identify and define the proposed change and its scope.
2) Understand the consequences of the change.
3) Understand the previous work that has been done.
4) Do risk assessments around the proposed changes.
5) Document the reasons for changes that were made.
6) Review and gain input of the proposed change by key stakeholders.
7) Revise or update the proposed change to reflect constructive input.
8) Finalize your proposed change and gain approval of key stakeholder(s).
9) Communicate your proposed change to key stakeholders.
10) Implement the change.
11) Check the effectiveness of the change and the effectiveness of how the change was managed.

The Responsible Roles in Management of Change

In MOC, there are several roles involved in managing the change. Each role becomes involved as the proposed change progresses through the work process.

- The Change Owner: the person who initiates and drives – "owns" – the change through to completion.
- The Stakeholders: broadly speaking, those who need to know about the proposed changes. Specifically:
  - Subject-matter experts need to review the proposed changes from the perspective of risk management in a wide number of areas (essentially opposite the management system elements) and specifically risk assessments on the proposed change.
  - Managers will "own" the change after it has been implemented (i.e., those who have responsibility and accountability in the area of the proposed change).
  - Representatives of those who may or will be affected by the change or subject to the change.
  - Representatives of those who will implement the change.
- Final Approver: the person who will approve the change. The approver is accountable for ensuring that the MOC policy, work process, and procedures have been followed.

Four Critical Actions for MOC

Although there are many steps in the MOC work process, as shown in a prior section and as can be seen in the graphical depiction below of the typical MOC work process, there are four critical actions in the MOC work process that the Change Owner must do:

1) Communicate the proposed changes to the stakeholders, before the change is finalized, and certainly well before the change is implemented. Specific actions may need to be completed to effectively do this on a case-by-case basis. The objectives are to communicate and to connect with those who can provide constructive input that may lead to an improvement in the proposed change.
2) Conduct appropriate reviews and risk assessments. Review the change with subject-matter experts and key stakeholders. The objectives are to gain constructive feedback / input from them, modify the proposed change based on feedback, check to confirm understanding, and finalize the change. The channels for communication and for approval (next step) also provide the opportunity for gathering additional input as part of the review process.
3) Seek final approval. It is essential to secure appropriate approvals for the proposed change before the change is implemented. After the Change Owner has finalized the change, the Change Owner must have it approved by the Final Approver (i.e., the manager responsible and accountable for the area in which the change is being proposed). It is not so much that the manager may be (but does not need to be) an expert in the subject matter of the change, but that the manager is accountable for ensuring that the MOC policy, work process, and procedures have been followed (i.e., that all appropriate assessments and reviews have been conducted). The senior level of management is ultimately responsible for the change.
4) Communicate and implement the change. The Change Owner is now ready to implement the change. It is essential to implement the change in the manner as documented in the approved change. Changes after approval (previous step) must be strongly resisted. If changes are needed, this re-sets the work process to the beginning. This should include: communicating the change to all stakeholders, training if needed, updating user-procedures, and any means of access to those procedures, and finally any commissioning and start-up of the equipment as may be needed. There may be many steps that are part of the entire change, and these may need to be implemented or executed in a logical order (i.e., operators need to be trained on new equipment before starting up the new equipment). This may sound straight-forward, but such critical activities have often been overlooked!

Simply, each of the above important steps in the MOC work process may require a detailed procedure as to how to do those activities. For example, a specific procedure or process is required for a formal or rigorous risk assessment. These specific procedures are unique to each organization.

Failure to Heed these Four Critical Actions

The roots of many incidents include:

- failure to communicate the change to essential personnel and stakeholders;
- failure to conduct appropriate reviews and appropriate risk assessments;
- failure to gain approval, or gain approval at the right levels within the organization; and
- failure to implement the change as agreed upon and approved by all stakeholders.

Documentation of Proposed Changes

Documentation of every MOC request and each step in every MOC request is good practice. Some firms have developed sophisticated online MOC databases (eMOC) to facilitate the MOC process and its requirements. Leading organizations require documentation of each MOC request. In some industries (e.g., aeronautics, pharmaceuticals, and food processing), documentation is imperative for due diligence and may be legally required. MOC documentation:

- generates a record of all proposed changes whether they were acceptable or not;
- provides a historical reference of the changes that have taken place in an operation as a resource for future use;
- serves as a resource for maintaining organization memory by preventing people from trying a change that did not work previously;
- is critical to auditing of the MOC policy; the documentation provides the record and data that auditors review to determine the soundness of the operation's MOC policy; and
- is essential for a due-diligence defense if something goes wrong with the change. The documentation for the particular change and how the organization manages change serves as the evidence. The documentation of risk assessments done as part of the MOC for the proposed change is especially important in this regard.

The minimum requirements of an MOC Policy include:

1) management systems must be in place for all departments to handle change;
2) opportunity identification means looking for changes, initiating the MOC work process to implement the appropriate risk reviews, and evaluate the potential outcomes before the change is made;
3) personal involvement means defining who needs to be involved and accepting all inputs;
4) training of employees on how to use the process;
5) effective communications to all people who need to know;
6) thorough and complete documentation;
7) regular audits of the MOC process;
8) incident investigations to evaluate MOC procedure validity;
9) performance measurement of the operations objectives, including the use of MOC; and
10) public involvement, if needed, when a risk to the public is identified.

Linking Two Management System Elements – MOC (Element #4) and PECI: (Element #6)
Management of Change (MOC) is intended to be the way that an organization manages changes within its facilities, its operations, or its activities. The question arises: how effective are the system, policy, work process, and procedures for managing change? To ensure a sound MOC process, there are three recommended practices:

1. Implement a formalized approach to audit the MOC process on a regular basis to ensure the MOC policy, work process, and procedures are being followed correctly. This is a macro-look at the MOC work process.
2. Implement a formalized approach to audit selected MOC requests to ensure that the changes and the associated procedures and risk mitigation strategies were fully and effectively implemented.
3. Address deficiencies when found.

In effect, the **Program Evaluation and Continuous Improvement** element of the management system is being applied to manage (PDCA) the **Management of Change** element of the management system. This is a "system audit" or a planned inspection at the organizational level.

Summary

Managing change is – and must be – an element of residual risk management fundamental to all organizations seeking performance improvement. Continuous improvement and innovation motivate constant change. The assurance that the changes happen with the correct thought, risk assessment, training, and communications is a more difficult task than it initially appears. Management diligence is required to receive all the value that is provided by this technique through assured compliance.

A robust MOC process is important, given that many investigations by government agencies look for this tool as a fundamental of organization practices. As indicated earlier, MOC offers many benefits:

- Ensuring the change is within the organization's acceptable risk criteria.
- Ensuring a change has no negative or unintended consequences on the other operational activities happening in your business.

- Keeping knowledge up to date and minimizing loss of critical skills on retirements.
- Ensuring employees are communicated with on all changes impacting them.
- It is a training tool.
- It is a means of ensuring due-diligence.
- It is a process which can be used for "any change" contemplated from hardware, to software, to people changes, to reorganizations, etc.

Element 5: Incident Reporting, Investigation, Analysis, and Actions

- A system or method for reporting of incidents of all types (with consequence (i.e., loss incidents) and without consequence (i.e., near miss events, unacceptable/sub-standard conditions, and unacceptable/sub-standard work-practices / at-risk behaviours)) must be part of an effective risk management system.
- The organization must create a culture, a non-threatening environment, where events are freely and openly reported and investigated. Avoid blame.
- The documentation, investigation, and analysis of incidents provide insight into the weaknesses of the management system (i.e., latent causes) and identify what needs to be addressed.
- Determining actions to address the latent causes and the effective implementation of such actions will prevent incidents. An organization requires good data to make decisions and to act on them.
- Checking the progress and effectiveness of actions demonstrates management commitment.
- Gathering incident data and analyzing it will help management focus on weak areas and allocate the right resources.
- Few incidents are truly isolated events. When a significant amount of data and a significant number of good reports are analyzed, emerging trends can be identified. Some related considerations for data analysis include: time frame (months, years); trades; plant areas; types of injuries (lost time, medical aid, first aid, near miss); type of injury contact; other similar plants, organizations, industry in general; and regulatory history.
- By applying thorough trend analysis, positive actions can be taken to prevent negative trends, accelerate improvements, and more importantly, prevent incidents.
- Successful processes for reporting and investigation are:
    - setting "trigger criteria" to initiate an investigation with some degree of formality and thoroughness (i.e., the more severe the incident, the greater the need to be more formal and thorough);
    - securing the scene, information/data, witness statements;
    - establishing a system for logging incidents and analyzing trends;
    - establishing a process for analyzing and communicating the findings / lessons learned; and
    - establishing a process for implementing the actions / recommendations from the analysis and for tracking progress on those actions.
- Successful processes for addressing actions, to gain credibility, and to demonstrate management commitment include:
    - prioritizing actions and allocating adequate resources to support effective implementation;
    - stating actions with a well-defined scope, due date, and clear ownership;
    - tracking progress and checking the effectiveness of the action in addressing the issue; and
    - communicating why any particular action taken is different than expected or why the expected action was not taken.
- Although after-the-fact, reactive management can contribute significantly to improvements in the management system, to the prevention of further incidents, and to overall performance improvements in the organization. Especially as it concerns loss incidents and the personal tragedies associated with those incidents, it is especially important for management to react (i.e., to investigate and analyze incidents, and to follow-up with effective, corrective actions to prevent future incidents).

What Does This Mean to the Organization?

- *Although incidents are a tragedy, the biggest tragedy would be to not learn from them.*
- *Unwanted incidents will happen. There is no guarantee they will not happen, even if the organization is within "statistical control limits". However, risk management systems should reduce incident probability and consequence to acceptable levels.*
- *Being prepared to learn from unwanted incidents demands an organized approach with a team ready to respond as the incident is underway. Reporting and investigating (gathering data) are key.*
- *Organizations rely on people to do their roles well; thus, understanding their needs and having them succeed is a management leadership responsibility. Creating and sustaining the desired work environment for a safety*

culture is critical. Incidents show the gaps in these efforts. It follows, then, that addressing these gaps will lead to an improved safety culture.

Element 6: Program Evaluation, Continuous Improvement, and Peer Review

- Continuous improvement of the management system and the performance within each of its elements is essential to maintain a competitive advantage, or at least maintain competitiveness, and to maintain sound stakeholder relations. If safety and risk are be managed effectively, all other aspects of the operation improve.
  - The employees are more satisfied in their jobs (safety needs are met).
  - The employees, as resources, are able to work on productivity gains and improvements, and not be diverted to loss incidents that consume costs in so many ways.
- Program evaluation works on many levels.
  - Third-party reviews (audits and inspections by independent reviewers) of the management system include: a) gathering evidence to confirm management system requirements are being met (or to find weakness); and b) providing the necessary feedback in order for management to determine priorities and act on them.
  - Similarly, peer reviews by people from within or close to the organization (i.e., internal audits and internal inspections) do the same. Care should be taken to encourage objective and thorough scrutiny of management systems under review. People might not audit themselves or their fellow workers as closely as a third-party auditor or inspector would. When internal audits are done well, third-party audits show "no surprises".
  - Effective leaders conduct in-the-plant or on-the-floor observations and interactions with employees. These can reveal concerns that need addressing. These can provide opportunities to recognize and reinforce acceptable work practices (behaviours) and acceptable conditions, and to intervene where sub-standard practices and sub-standard conditions (unacceptable behaviours and conditions) are not meeting expectations. Observations include field safety practices (wearing safety equipment, adhering to procedures, using field level risk assessments) and workplace conditions and housekeeping.
- Proactive management can contribute significantly to improvements in the management system, to the prevention of incidents, and to overall performance improvements in the organization.

Program Effectiveness

Program Effectiveness is a metric that measures the depth and breadth of the organization's policies, procedures, standards, manuals, training, and qualifications, etc., and the degree to which workers actually follow the rules and requirements in those policies, etc. (i.e., the effectiveness and compliance of execution). An organization must have both to attain superior program performance. No organization is 100% perfect. There is always room for improvement; thus, there is a need for an ongoing continuous improvement process.

What Does This Mean to the Organization?

- *An effective program evaluation based on third-party reviews, internal reviews, and reviews by leaders can lead to improved safety performance, which can lead to improved morale, improved productivity, and improved competitiveness. It means continuous improvement!*

Program Evaluation and Continuous Improvement (PECI)

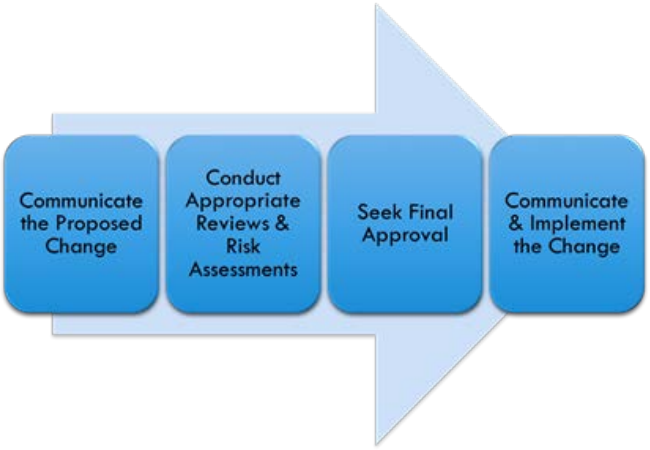
As the name implies, PECI is the element that defines what management must evaluate in their risk management program in order to improve on their program. It has the same tenets as Plan-Do-Check-Act (PDCA in Chapter 7): proactive and continuous improvement. PECI is essentially an audit of all parts of the risk management program.

The Audit

The Audit is a best practice. It finds deficiencies and weaknesses in the risk management system and program. Audits are driven by government regulations, industry association policies and standards (whether imposed or adopted), and corporate policies and standards. There are two types of audits: internal audits by people from within or close to the organization, and external audits by specially-trained third-party auditors who assess the facility. Audits test the implementation process at the organizational level: to see how well the RM program is effectively implemented (e.g., the MOC process; incident reporting, analysis, investigation, and action; training, etc.). An audit is a test at the organizational level (i.e., when the managers and the organization's management program are tested to determine the effectiveness of implementation).

Auditing the MOC (Element #4) Process

Recall the Four Critical Steps from the MOC Process:



These kinds of questions can be asked:

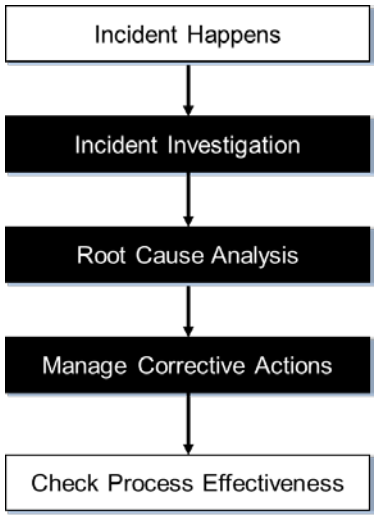
1) Were proposed changes communicated?
2) What kinds of risk assessments were conducted for the scope of change? Were they appropriate? Did they have the right mix of stakeholders and subject matter experts? Did these result in revisions to the proposed change?
3) Was final approval granted? Where is the evidence that confirms the final approver checked that the MOC process was fully applied for the change?
4) Was the change communicated prior to implementation? Were documents updated and training conducted prior to implementation? What evidence is there that these were done?

To answer the questions, the auditor must seek evidence. A database or dataset of records must exist for changes, include those that are: 1) proposed and in-progress; 2) proposed and abandoned, and 3) proposed and implemented. The records can be physical documents (i.e., paper trail) or virtual. Then, the auditor must:

1) select a number of records from the implemented changes;
2) check the recorded information in those records and compare them to the requirements of the MOC Process;
3) interview persons who have been a part of the MOC (their names should be on the records);
4) identify and record any deficiencies (e.g., a step was missed, a person did not receive the required training prior to the person using the implemented change); and
5) report findings, sometimes with recommendations, to the manager of the facility.

Audit on the Incident Investigation – Root Cause Analysis – Manage Actions (II-RCA-MA) Work Process

Similarly, an audit can be conducted on the Incident Investigation – Root Cause Analysis – Manage Actions (II-RCA-MA) work process (discussed further in Chapter 4).

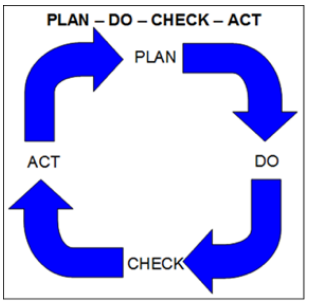


Questions that could be posed:

1) What is the threshold criteria for reporting?
2) What is the threshold criteria for investigating?
3) How thorough (breadth and depth) is the RCA?
4) Are latent causes identified and tested?
5) Were recommendations Specific, Measurable, Actionable, Relevent and Timely (SMART)?
6) Were the recommendations implemented? Did the recommendations address the problem (i.e., address the latent cause)?

Leading organizations include the PECI of the overall process. In fact, leading organizations test all elements of their risk management program… even PECI!

The Connection to the Fundamental Management Process



Through effective application, management system weaknesses can be discovered and deficiencies addressed: the overall program, and thus its performance, are on a continuous cycle of improvement (i.e., Program Evaluation and Continuous Improvement, or PECI).

PECI ensures the risk management program is effectively and robustly implemented. Leaders check that their risk management program is effective and, when found deficient, act to correct. PECI is PDCA practiced at the organizational level.

Element 7: Design, Construction, and Start-up

Throughout project planning, management, and execution reviews (from the conceptual stage to the handover and start-up stage) are critical. These activities are all outside of normal operations and inherently have more risk because more people are present, more energy forms are present, and sometimes it involves higher-than-normal energy states. Construction, maintenance turn-around, demolition, and plant operations start-up and shut-down are times where incidents are more likely to happen. Incidents are more likely to happen because the non-operational people involved may not be familiar with the hazards in the facility, with the safety culture, or the standard work practices (acceptable behaviours) in the facility (i.e., they arrive with their set of safety culture, values, and work practices, which can be difficult to change).

These stages sometimes have objectives that conflict or compete for limited resources. These can originate from project owner approvals, financial constraints, political climate, environmental approvals, public or stakeholder tolerance, cost control, schedules, communication, site safety, design, specifications, quantity estimates, procurement, construction management and contracts, and commissioning. An astute project manager will recognize the need for good and specific control strategies to manage these different objectives. Good risk management in a project leads to good project management, and attaining or exceeding project deliverables (i.e., no injuries; on time; on budget).

What Does This Mean to the Organization?
- *Effective risk management is required at any stage of a project or phase of operation of a facility.*
- *Effective risk management will enable the manager / organization to meet other project objectives.*

Element 8: Operations and Maintenance

- Organizations must monitor the operation in a proactive way to gather data to make informed decisions about changes in risk levels or changes in operations.
- The operation and maintenance of plant operations, equipment, and facilities must be within established criteria such as:
  - limits on process operating conditions as set by the process engineers;
  - limits on safety systems such as pressure relief valves, fire protection systems, and process equipment shut-down logic and tripping mechanisms, including computers and software used for automated process control; and
  - manufacturer's specifications.
- The monitoring and recording of operational and maintenance conditions, and the analysis of operational records and maintenance records will reveal deteriorating or deviating conditions that need to be addressed, thus, proactively preventing an incident.
- Equipment and specification limits must also be maintained. Where changes are necessitated, the Management of Change (MOC) process must be applied.
- Dedicated efforts must be made to prevent sub-standard conditions (i.e., the condition of safety equipment or the alteration of parameters outside the well-established limits). Otherwise, normalization of deviation (i.e., organizational complacency) may creep in and ultimately result in an incident.

What Does This Mean to the Graduate Engineer?
- *ESG #4: "Pay attention to failures in safety systems and take action."*

What Does This Mean to the Organization?

- *Processes must be in place for ensuring established criteria are maintained.*
- *Dedicated effort must be made to prevent the normalization of deviation.*

Element 9: Employee Competency and Training

- Effective employees are an asset for any organization. When leaders care about and support their employees, employees respond with superior performance. One key to supporting employees is enabling them to be fully competent in their job. Training and re-training / refresher training are the means to support the employees. Another key to supporting employees is the ability to gauge their performance and provide effective feedback.
- Training is an effective method for setting expectations: it ensures the expectations have been communicated to employees, that they understand the expectations, and that they have demonstrated competency in those expectations.
- Managers are responsible for ensuring their employees are properly trained and certified / qualified. This means the trainer has approved them as being properly trained, tested, and having exhibited all the skills and knowledge necessary to perform the job (i.e., they are competent).
- Training policies, training materials, and training records must be kept up-to-date. Commensurate with updating training materials, it is an opportunity to update records (see Element #11).
- Managers must also provide resources (i.e., competent trainers are utilized; suitable training facilities and practical in-house materials; access to external expertise such as Alberta Workplace Health and Safety) and include training on regulatory requirements (e.g., Alberta Occupational Health & Safety; Transportation of Dangerous Goods, Workplace Hazardous Materials Information System (WHMIS), etc.).
- Managers must have systems in place to check the effectiveness of the training and retention of that training.
- Managers must have systems in place to carefully select candidates in job competitions.
  - The first set of considerations includes: skills and knowledge; competencies; achievements, accomplishments and past performance; and certifications, qualifications, credentials, apprenticeships, and formal education.
  - The second set of considerations includes: their interpersonal and communication skills, their leadership skills, their employment history (work ethic and work culture), and their work experiences.
- Mangers must have systems in place to carefully assess employee performance, to provide feedback to employees, to provide recognition and reinforcement (and reward), and to apply progressive discipline as may be necessary.

Types of Training: There are many types of worthwhile educational and training methods employed by industry to continuously improve their safety and risk management performance. These are normally focused on all employees throughout the organization, with a matching of methods and content to the various job and professional levels. Some of the areas covered are:

- new employee orientation / integration and job-specific training;
- skills, competencies, and knowledge; apprenticeship, certifications / qualifications, and specialized training;
- safety basics: Workplace Hazardous Materials Information System (WHMIS), Job Safety Analysis (JSA), Field-Level Risk Assessment, personal protective equipment; and
- organization-specific risk management programs.

What Does This Mean to the Organization?

- *Competency of personnel, who are expected to carry-out tasks, is assured.*
- *It is important to note that if leaders / managers do not know what is required, how can they recognize sub-standard work practices, sub-standard performance, or unacceptable behaviours?*
- *Training is a form of due diligence. Training records can demonstrate due diligence.*

Element 10: Contractor Competency and Integration

Today, organizations cannot be productive without contractors. Contractors with many varied skills are an integral part of business. When a contractor arrives at an organization's job site to do work, the risk to the organization immediately increases. Contractors cannot be expected to know the organization's organization and culture; thus, contractors are not enabled to manage risks to the organization's level of expectation. Therefore, it is essential to select contractors with the right competencies not only in the skills they provide, but also on their sensitivity to the organization's risk levels and on their abilities to manage risks. Organizations must select contractors with a history

of success and ensure the contractor is fully integrated with the organization to ensure they understand and manage the hazards.

Key performance indicators for selection of contractors:
- capacity to perform the work;
- past performance, not just on costs, but especially on safety performance;
- injury rate and severity rate: contractor versus organization; contractor versus their industry; and
- compliance to regulations, codes, and standards.

What Does This Mean to the Organization?
- *Look at every contractor on site as someone who increases the organization's level of risk well above what the organization considers to be acceptable.*
- *The organization must pay extra attention to contractors and must have a process for selecting contractors. The organization must provide special training, supervision by the organization, and administrative controls to drive the risk level back to an acceptable level, all before the contractor starts the job.*

Additional points to consider:
- Influence the reduction of incidents involving contractors by employing competent contractors that work within the parameters of an effective safety program. The contractor must either use the organization's safety program or an acceptable contractor program.
- Competent contractors are those who are properly trained, well equipped, and effectively supervised. They should be screened before awarding the contract. Performance standards must be built into this contract — failure to do so will end up costing more in the end.
- Contractor organizations and their employees are not exempt from meeting applicable legislation and regulations, or your organization's requirements. If they fail to meet legislations and regulations, your organization (i.e., you) may also be held accountable by authorities. Hiring a contractor to do your work does not insulate you from the consequences of failure to meet regulations.
- Contractors should be treated with the same respect, must meet requirements at the same standard, and must be managed as efficiently as the host organization's own employees. If they are not, contractors may become the weak link in the project or operation. Many disasters in the industrial setting have demonstrated this weakness.
- For many organizations, the organization safety performance records now include contractors. To manage safety and loss management effectively, it is necessary to include contractors. Contractors are being used more frequently and they usually consist of highly trained technical personnel with specific expertise.

Element 11: Operations and Facilities Information and Documentation

- Information (data) is only as valuable as its accuracy and its ability to be readily accessed.
- Systems must be implemented to identify the information that requires monitoring, collecting / gathering, and storing / archiving for any purpose (i.e., as necessary for an incident investigation). There are two types of information: static and dynamic.
  - Static information relates to the initial generation or creation of a record (a piece of information) that remains accurate until it is changed at some future time. Policies, procedures, business plans, training records, equipment specifications, and any engineering design information fall under this umbrella.
  - Dynamic information includes real-time data relating to processes and machines that change continually, in some cases almost continuously, based on the operational characteristics of the process equipment or machinery.
- The information can be used for tracking trends on performance in any key area such as: safety (overall safety, number of sub-standard practices observed in a month), environmental performance (emissions to atmosphere, performance of monitoring equipment), assets (process equipment and machinery such equipment records, maintenance records, efficiencies of machines, expected life of machines) and productivity (operational details, process parameters, and production / through-put).
- Managers can use the information and performance trends and indicators for further analysis, and for making informed decisions.
- Static and dynamic information are critical for incident investigations and for applications of risk analysis and risk assessment.
- One specialized area is the documentation relating to changes of static information, as specified in the **Management of Change (MOC) Work Process** earlier in this Chapter.

What Does This Mean to the Organization?

- *Planned processes and systems are required for collecting, storing, and retrieving information.*
- *The capability for data analysis (sorting, filtering, calculations, etc.) is required.*
- *Managers must implement appropriate policies and procedures where workers are making decisions based on the information.*

Comparison of the ENGG404 Risk Management System to Other Systems

It is not the intention in this course to provide a rigorous and detailed risk management system; however, a brief review of other models demonstrates that management systems are not new and not limited to risk management.

The ISO-9000 series of standards pertains to quality in a facility. This series of standards defines the requirements for a quality management system, with the intention of improving and sustaining quality and competitiveness in the manufacturing and service industries. Similarly, the ISO-14000 series of standards pertains to environmental management in a facility. Facilities can adopt and implement a management system based on these standards with the intention of meeting the specified requirements and attaining certification via a third-party auditor (e.g., “This plant is ISO-9001 Certified”).

The ANSI/ASSE/ISO-31000 series of standards pertains to risk management, but it is intended for application for any type of risk management, and does not define any specific operational requirements (i.e., it provides a generalized framework only).

Unlike quality and environmental management, there is no international parallel for engineering safety and risk management. An organization is tasked with developing its own risk management system based on internal requirements and the regulatory requirements. Having said this, some standards focus on process safety management, a sub-set of engineering safety and risk management. For example, the CsChE Process Safety Management Standard (1st Edition, 2012) refers to a risk management system for process safety. Many elements are common between this Standard and our Risk Management System.

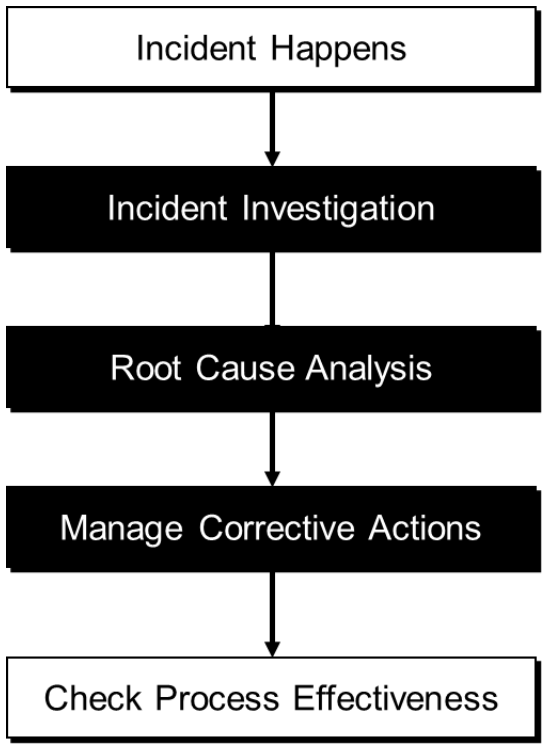
ENGG404

Chapter 4:
Incident Investigation, Analysis, Causation, and Action

Section 4.1: Incident Investigation, Root Cause Analysis, and Managing Corrective Actions

No matter how hard we try, no matter how many defenses are in place, incidents continue to happen, unfortunately. Managers need to investigate thoroughly to have as much information available, so that they can comprehensively analyze the incident to determine its causes.

This section presents the Incident Investigation, Root Cause Analysis, and Manage Corrective Actions work processes (II, RCA, and MCA, respectively) and the details of the macro-steps within these work processes. The process for investigating an incident is detailed here, whereas the process for conducting a root cause analysis and for managing corrective actions is presented in **Chapter 4.3: Root Cause Analysis of an Incident** and **Chapter 4.6: Tools and Process for How to Prioritize Actions**.



The Incident Investigation is a rigorous work process for assembling the investigation team and for collecting evidence relating to an event (i.e., the discovery and ascertainment of the facts of a loss incident).

The Root Cause Analysis of an incident is a rigorous work process for determining the causes of an incident. The analysis uses information learned from an Incident Investigation. The Root Cause Analysis is the process that answers these questions: How did it happen? What were the causes? Root Cause Analysis will be presented in **Chapter 4.4 Root Cause Analysis of an Incident.**

Manage Corrective Actions is a rigourous work process for determining and managing the corrective and preventative actions that address the latent causes identified in the RCA. Manage Corrective Actions (How to Prioritize Actions) will be presented in **Chapter 4.6: Tools and Process for How to Prioritize Recommendations.**

This section explains and relates the overall work process for Incident Investigation, Root Cause Analysis, and Manage Corrective Actions (II, RCA, and MCA, respectively).

Why Conduct II, RCA and MCA?

As managers, we must believe that all incidents are preventable. Remember we do not call these events “accidents,” because there is a connotation that an accident is not preventable. That is, we could not do anything to stop the incident from occurring. As leaders of organizations, we cannot believe that incidents are inevitable, nor can we allow a culture to develop that believes the same.

Fundamentally, managers need to investigate and find out what caused the incident to happen so changes can be made to ensure that same incident, or a similar one, does not happen again. The investigation also provides learning for all employees and acts as a means to reinforce management commitment.

Incident investigations and root cause analyses need to be perceived as learning experiences for all involved and where no one is to blame. Management must provide a free and open arena for discussion to get the best available information (complete and factual) and to get the fullest value out of the overall II, RCA, MCA work process. That is to say, managers must not lay any blame except at the feet of management. Having said this, people do need to be held accountable for their actions.

"Recently, I was asked if I was going to fire an employee who made a mistake that cost the organization $600,000. No, I replied, I just spent $600,000 training him. Why would I want somebody to hire his experience?" Thomas John Watson, Sr.

Are All Incidents Investigated or Managed Using this Overall Work Process?

It depends on the organization, its resources, and its level of discipline. Some organizations specify that the required level of investigation escalates with severity, or potential severity, of the incident. Other organizations may do nothing except the bare minimum as may be required by law. And of course, an investigation can only be initiated when an incident is reported.

Organizing an actual investigation means taking several people from their regular jobs to spend several hours or days in the overall process. This often is not possible; therefore, it is worthwhile to define criteria for which investigations will take place (i.e., the nature and/or severity of the incident that triggers an investigation) and include in those criteria the ability to do an investigation because knowledge may be gained.

Do not forget to include "near miss events" in the investigation decision process because valuable lessons can be learned without having suffered any consequences! And finally, there may be a need to proactively investigate the potential for an incident.

Who Leads the Overall II-RCA-MCA Work Process?

Generally, there is a need for an impartial leader (chairperson) who is familiar with the II and the MCA work processes, and who has credibility within the organization subject to the investigation. The impartial leader can also redirect supervisors and managers towards a non-threatening stance (see **1**) when emotions may become heated in the course of the investigation. The impartial leader must be skilled in sensing this situation and in coaching supervisors to "wait to see what the root cause analysis discovers" in the course of the investigation.

The leader assembles and leads a team consisting of:

- Four to six people for small incidents, growing appropriately for larger ones.
- Persons NOT directly involved with the incident.
- The line management / operational people responsible and accountable for the operation under investigation and who may have knowledge to contribute.
- Subject-matter experts and technical specialists, sometimes from an arms-length view to provide balance.
- One or more experts in the II, RCA, and MCA work process to provide balance and guide the other team members effectively through these processes.

As the organization progresses through the overall II-RCA-MCA work process, the members of the team(s) may change, depending on the mix of expertise needed and the stage through the overall work process. For example, the leader during the on-scene investigation (with expertise in securing the scene and collecting evidence) may not have the skills to lead the team through the root cause analysis. Similarly, the leader during the root cause analysis may transfer ownership to the facility leader who "owns" the facility and/or activity central to the loss incident, and is therefore responsible for the effective implementation of actions and recommendations to prevent recurrence.

At All Times During the Investigation, Set A Comfortable, Non-Threatening Atmosphere

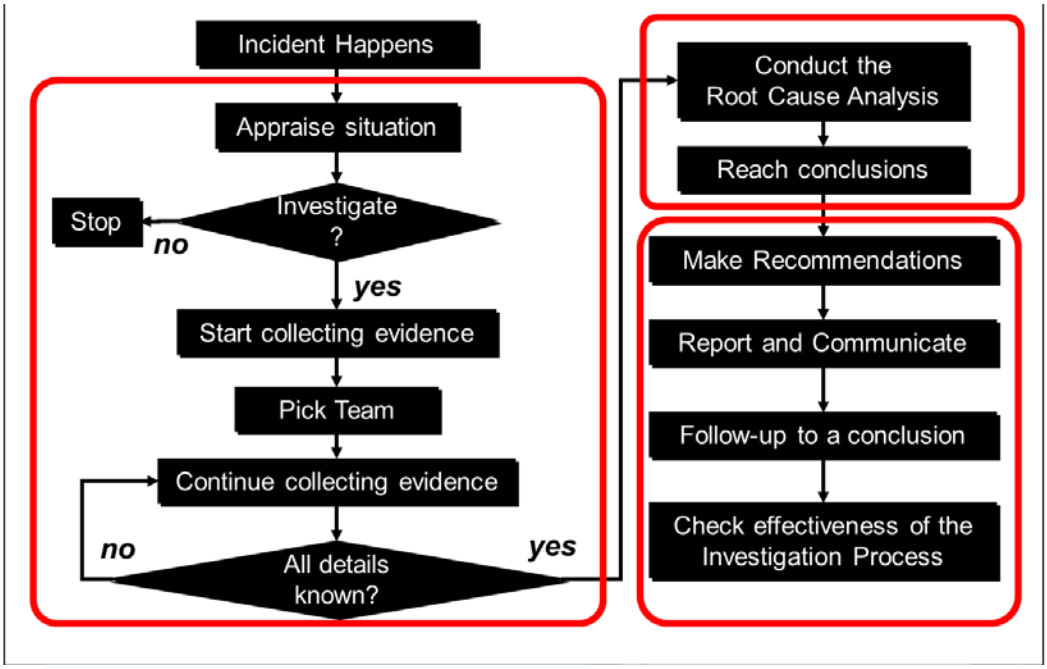
It is important to know how to manage people's experience with the incident, that is, how management treats people during an investigation and root cause analysis. These processes are not intended to point the blame at someone or determine it was their fault. The fundamental belief is that the management system failed the employee, and the fault is in the management system, not the employee. Recall one of the synonyms for latent cause is management system failure. It is the role of supervisors and managers to set this tone; however, the impartial leader can redirect supervisors and managers if needed, as described above.

Simply, treat people fairly, and with dignity and respect during the investigation. If an employee feels otherwise (that they will be mistreated or be blamed), then the employee will feel like they are in the hot seat and may attempt to protect themselves by withholding information or distorting the facts; this information is crucial to the investigation.

The Incident Investigation (II) Process

What is not reported cannot be investigated. What is not investigated cannot be changed. What is not changed, cannot be improved, and therefore will happen again. The II Process, as depicted below, can be described in a

number of steps, with each step having a number of detailed steps within each. The steps and their details are not exhaustive – this process is a framework which can guide and lead you and your team through the II process. The II process flowchart is presented below.



The II process steps explained:

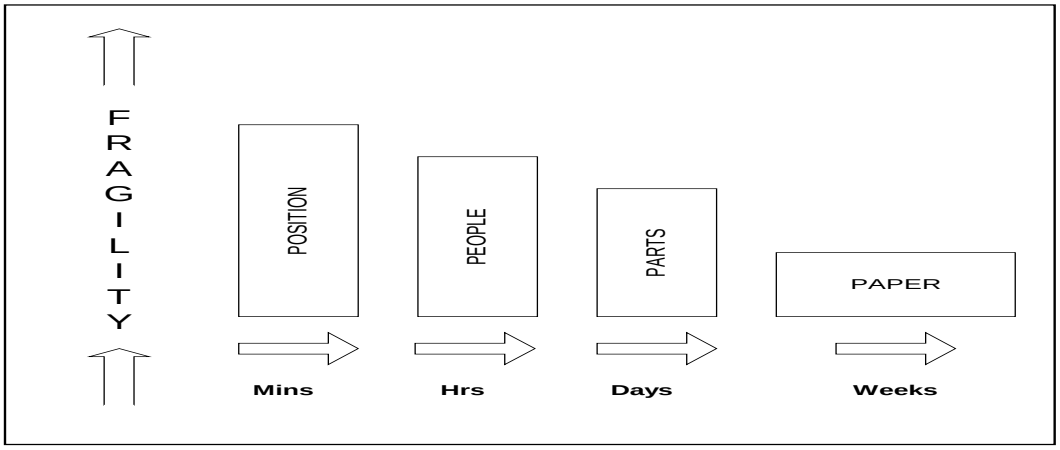
1) Appraise what happened

It will be necessary to determine if an investigation needs to be conducted or not. A good incident reporting policy, along with a good safety culture, supports workers in reporting all kinds of incidents (i.e., those without consequence (near miss events) as well as those with consequence). If an investigation is warranted, obtain a description of the incident and establish the scope of the investigation.

2) Secure the scene and immediately start gathering evidence

The scene of the incident should be secured (in some jurisdictions, the scene must be secured for gravely serious or fatal incidents) as soon as possible. Managers should train and direct the workers to secure the scene and protect evidence. Organizations should adopt stringent methods similar to those that police services take for securing the scene of a crime.

a) If not already done so, secure the scene of the incident (i.e., rope it off with appropriate ribbon tape). It is important to secure the incident area immediately so people do not disturb evidence while attending to the emergency. This activity should be underway within an hour. Evidence is fragile and must be protected and gathered quickly / carefully. Gathering evidence is a crucial step in a thorough investigation, but is often a challenge. Planning and care is critical to gathering the necessary evidence. Many organizations have detailed procedures and have trained staff that specialize in securing the scene, collecting evidence, and investigating the incident.



b) Collect positional evidence within a few hours, as the evidence can be easily disturbed. Make drawings, sketches, photographs, and video images of the scene. Record any radio communications.
c) Document the key people to contact. List people working in the area and emergency response people in attendance. The positions of people need to be recorded quickly. People can quickly forget where they were.
d) Interview people before they can talk to others as this may influence their story. Ask anyone as to what they saw, heard, smelled, felt, etc. If time is not available, distribute witness / observation statement forms without delay and request witnesses to write down their description of what happened. Follow up as quickly as possible with an interview and keep notes. When interviewing, use open-ended questions as much as possible.
e) Go out to incident site and observe situation.

3) Organize the investigation team

Identify what is going on and who is doing what (i.e., who is on the investigation team, who is contacting external agencies (if necessary), who is securing the scene, who is involved in emergency response, who is starting the recovery process, who authorizes clearance to the incident site, to whom does the lead investigator report?). Another question to ask is whether confidentiality need to be exercised. In Alberta, the Freedom of Information and Privacy Act must be respected.

a) Select appropriate team members to start the process and convene the Investigation Team.
b) Establish Ground Rules for the Investigation Team and gain the commitment of each member (e.g., unplanned and extended hours, travel from home, etc.).
c) Ensure Investigation Team members inform their families. Some investigations may require unplanned and extended hours; if there is news of an incident, team members should let their families know that they are OK.
d) Give the list of Investigation Team member names to security personnel (police, agency authorities) for access privileges.
e) Determine the Incident Description (for the starting point on the root cause analysis). This may take time. Start with the people directly involved. You may find you do not have all the right people taking part initially. This means possibly gathering additional evidence too.

4) Continue to gather evidence

a) **People evidence:** Record witness statements (i.e., their recollection of the event). Early witness statements are necessary to get a true picture of what happened, as stated in Step 2 above. Witness statements must be made within hours of the event. The more time that people have to think about what happened, the more likely their memory will be distorted. If they discuss it with anyone, they might have doubts and change their views. Written witness reports can be compared and provide corroborating evidence (i.e., look for commonality and for discrepancies). Ensure you set a comfortable atmosphere of no fear so witnesses can write freely.
b) **Parts evidence:** Mechanical parts or pieces from damaged equipment that are pertinent can be collected later, but need to be recognized as items not to be thrown out. Pictures will help to identify where they were. Often these parts have forensic value in that they can describe the sequence of events, temperatures, pressures, mechanical impact, electrical discharge, corrosion, etc. Analyze location of parts and condition quickly although this can take days.
c) **Position / visual evidence:** Maps / grids, drawings / sketches, videos, photographs, measurements, and positions of parts, structures, vehicles, people, etc. (i.e., anything involved in or destroyed by the incident).
d) **Records evidence:** Collect and secure any relevant paperwork, and make copies as necessary: these documents are the paper trail (i.e., the paper that documents the work-in-progress relating to the incident, such

as work permits, sign-in/out logs, procedures, check-sheets, log sheets, field level risk assessment cards, strip-chart recorders, etc.). Although paper will not deteriorate, it is surprising how paper documents are easily misplaced. These can contain valuable evidence that can ensure the true facts are used in the investigation. Thus, it is extremely important to gather and secure these documents immediately after the incident occurs.

e) **Computer data:** Collect the computer databases. Process unit operations data are monitored and logged by the process computers. These may log the data at some frequency: depending on the nature of the process, this could be at 1/1000 of a second to 1 minute. These data will not deteriorate, but can be time sensitive because the data may be software averaged after some time period (i.e., the critical few minutes leading up to the incident could be lost). Later, semi-permanent data should also be collected such as operations manuals, operating log books, maintenance records, inspection records, training records, etc.

5) Organize and conduct the RCA

It is at this stage that team members may begin to formulate ideas for possible improvements and recommendations. This is an appropriate time to start thinking and contemplating about these, but should be deferred to the formal step in the process. Ensure you have an appropriate team to start the process (the process and the team composition are discussed in detail in a subsequent sub-section).

a) Determine the sequence of events both leading up to the incident and after the incident, and define the **Incident Description**. This is not an obvious statement and several iterations may be necessary, including gathering more evidence, preliminary investigation, and checking / consulting with other experts in the root cause analysis process. The sequence of events must be chronological (i.e., in the order that things happened) either time based or event based.
b) Re-enactments, simulations, and models of the incident may be beneficial for the investigation, as well as for communicating, post investigation, about what happened. There may be a need to develop computer simulation models. Some of the intermediate events may need a more detailed analysis, a computer simulation, or re-enactment in the workplace.
c) Ascertain the substandard conditions and/or substandard practices. These are identified from the logical flow / sequence of events. Also, determine how these conditions or practices developed (i.e., what were the specific conditions that existed to cause the sequence of events to occur (immediate cause)?).
d) Analyze the evidence using the root cause analysis starting with the **Incident Description**. This starts with the incident description and goes “backwards” in time (i.e., works logically backwards). Do this by asking a series of “why” questions (e.g., A pipe broke, why? There was external corrosion, why? Corrosion management system was not maintained, why? …).
e) Drill down from the **Incident Description** through immediate and basic causes, to the latent causes (i.e., the points where control was lost). It is important to err on the conservative side to ensure no item is inadvertently missed.
f) Thoughtfully consider what contributed to each loss of control. In most cases, this exercise points to failure of management systems. In some cases, it points to poor design or construction. Be open minded.
g) The team should ask itself: Are we comfortable with the causes found? Is the depth and breadth of the investigation appropriate? Are the key stakeholders satisfied with the quality and thoroughness of the investigation and root cause analysis? The team members may need to re-group or perhaps consider a change in team members.
h) Develop the links between the latent causes and the management system weaknesses.

6) Reach a conclusion

Sometimes we know absolutely; sometimes we need to speculate. For our purposes in this course, the “most probable or plausible cause” is sufficient.

a) Team consensus is bolstered by the evidence and the appropriate and thorough application of the II and RCA processes. The evidence needs to be supportive each step of the way.
b) The key conclusions from the incident investigation and the root cause analysis are: i) the Incident Description; ii) the sequence of events; iii) the actual or most probable immediate and basis causes; and iv) the latent causes, the links between the latent causes, and the weaknesses in the management system.

7) Make recommendations

As the manager of the facility in which the incident occurred (or owner of the event), you are accountable for the event and the investigation. You must act decisively to follow-up on the investigation and work with your team to evaluate each of the recommendations, finalize and prioritize the selected recommendations, and assign people to the actions along with a due date / deadline. This is another example of the PDCA Cycle (see Chapter 7).

a) Recommendations are proposed actions for solutions to the problems.
b) The problems are the causes identified in the causal analysis.

c) There is a matrix of solutions such as: immediate, long term, temporary, permanent, corrective, preventative, and contingent.
   i) Corrective actions: Specific remedial actions that address the latent causes, both immediate and long term, to prevent this event from happening again due to the same latent causes.
   ii) Preventative actions: Specific remedial actions that address the latent causes, both immediate and long term, to prevent similar events from happening due to similar or other causes as may have been uncovered during the cause analysis.
   iii) Immediate: An action taken immediately. Often a temporary fix, but can be permanent.
   iv) Long-term final solutions will be far ranging.
   v) Contingent recommendations serve to reduce the impact should this incident happen again.
   vi) Note: "corrective" and "preventative" are differentiated as a) stopping the same event from happening again, and b) preventing a similar event from happening in a similar manner. Sometimes, an investigation finds weaknesses that have not yet resulted in an incident.
d) Some actions address immediate causes, some address basic causes, and some address latent causes. You must ensure that your actions address the management system failures.

8) Report and communicate

a) This is a key step because the stakeholders want – and need – to know the progress of the investigation and analysis, and that the management system weaknesses are being addressed.
b) The communication report needs to be well thought out, showing who took part, the process used to arrive at the conclusions, supportive evidence along the way, and logical reasoning for the recommendations.
c) Recommendations need to be clear, achievable, realistic, and written in a way such that they can be acted upon. The basis for priorities must be shown as well.
d) Communication should be done with all interested parties / stakeholders. In addition to management and the regulator, organization workers (either directly impacted or not), the public, and the media are other stakeholders to consider. You need to provide facts and an account of what you have done, along with what will happen in the future. Special care is required when engaging with the media to ensure that information is accurately presented.

9) Follow up to a conclusion

This is the final step in concluding an investigation and is ultimately part of the control step. This is also called validation of the actions.

a) This is a management responsibility to ensure all recommendations are completed to their satisfaction. Were the selected actions completed and were the actions effective? An action register to log progress and completion is essential.
b) All documentation relating to the investigation and follow up is thorough, comprehensive, and complete, and is appropriately filed or archived.
c) All impacted materials like operating drawings, design changes; equipment files, training packages, etc. need to be updated.

10) Check the effectiveness of the process:

Looking back at the Fundamental Management Process, this overall work process is overlaid with the Plan-Do-Check-Act Cycle.

a) For some investigations, depending on the severity of the event and investigation, management will take a more thorough and rigorous second look at the application of the work processes for the investigation and the actions implementation.
b) The purpose is to determine how effectively the organization: a) conducted the investigation; b) identified the causes (really drilled down); c) identified and prioritized actions; and d) implemented the actions.
c) This is a check (or control) on the stewardship of the overall work process. It answers the question, "How well did management investigate, analyze, act on, and follow-up on this incident?"
d) This process is one type of management system analysis and aims to sustain and improve the "Incident Reporting, Investigation, Analysis, and Actions" element of the management system, and is fulfilling the purpose of the "Program Effectiveness and Continuous Improvement" element.

Summary and Concluding Notes

The II and RCA processes will be effective only if:

- complete and factual data are used in the investigation;
- the RCA process identifies the cause (immediate, basic, and latent);
- strong links between the latent causes and the weaknesses in the management system are made;

- recommendations are turned into actions;
- actions are “actionable”;
- personnel responsibilities identified – who “owns” the action;
- action tracking system put in place;
- frequent review of action log by leadership / management;
- leadership ensures completion on timely basis; and
- leadership checks effectiveness after the actions have been implemented.

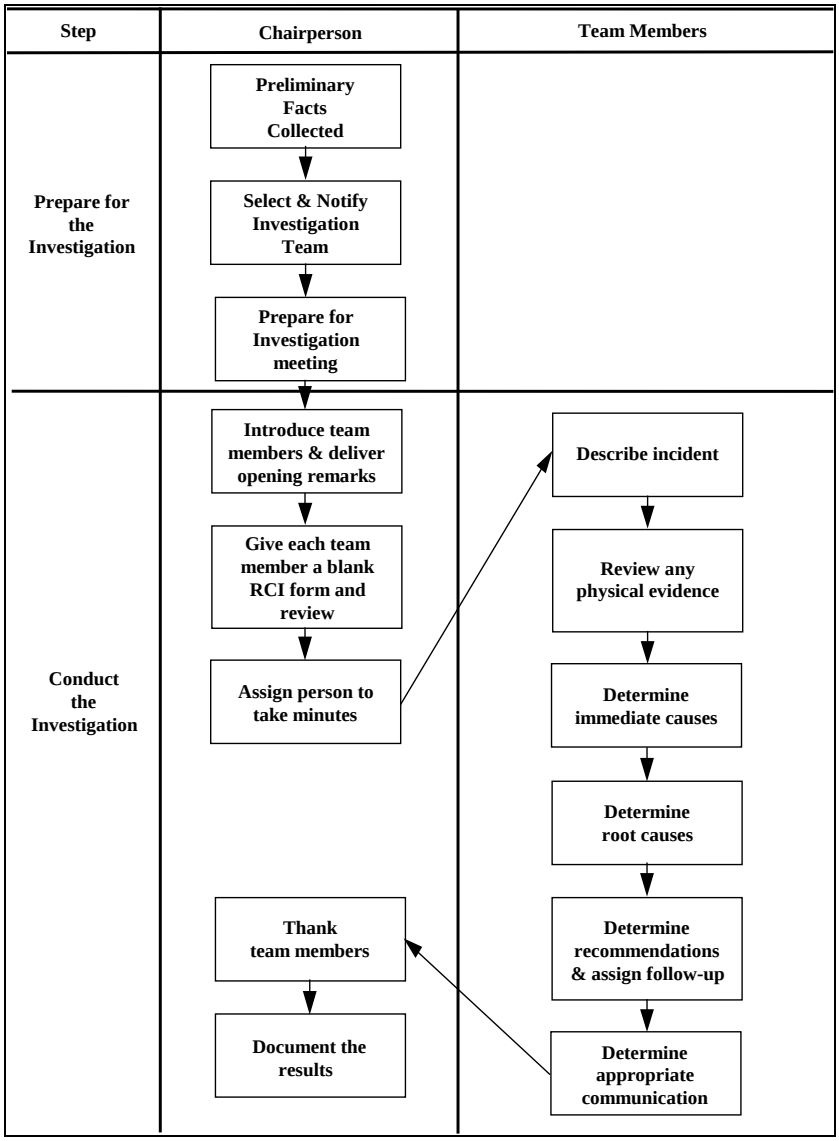
An investigation should be viewed as a learning experience for all people involved. By learning from mistakes, managers can learn. Management must commit to providing the people, resources, time, and processes to complete the investigation and analysis. Above all, management must support the people undertaking the investigation and analysis. This shows management commitment, and breeds commitment in the employees.

By using all available resources (i.e., the people in the organization), a manager stands the best chance to solve the problem and make the right corrections. The result is an efficient and effective process. When managers show their commitment, by giving this support and acting decisively to implement the corrective actions and preventative actions, employee commitment will rise as well.

For this reason, it is important to ensure employees do not get the impression this is a process for finding fault. It is paramount to ensure they feel safe in their jobs. As has been demonstrated in industry, a good manager can convey to the investigation team that: *In the root cause analysis, put the incident description at the top and put my name at the bottom, because I am responsible for the management system failure. Your job is to find everything in between.*

An Industry Model of the II and RCA Processes

A common industry practice includes a division of responsibilities as shown in this flowchart. Although this organization uses the term Root Cause Investigation (RCI), the intent of this process is the Root Cause Analysis (RCA). This diagram is an example of ambiguity in the real world where words have different meanings.



Section 4.2: The Cause and Effect Model for Incident Analysis

This section explains how to use the Simple Cause and Effect Model and the Detailed Cause and Effect Model as related to a loss incident. Either of these models can be used to:

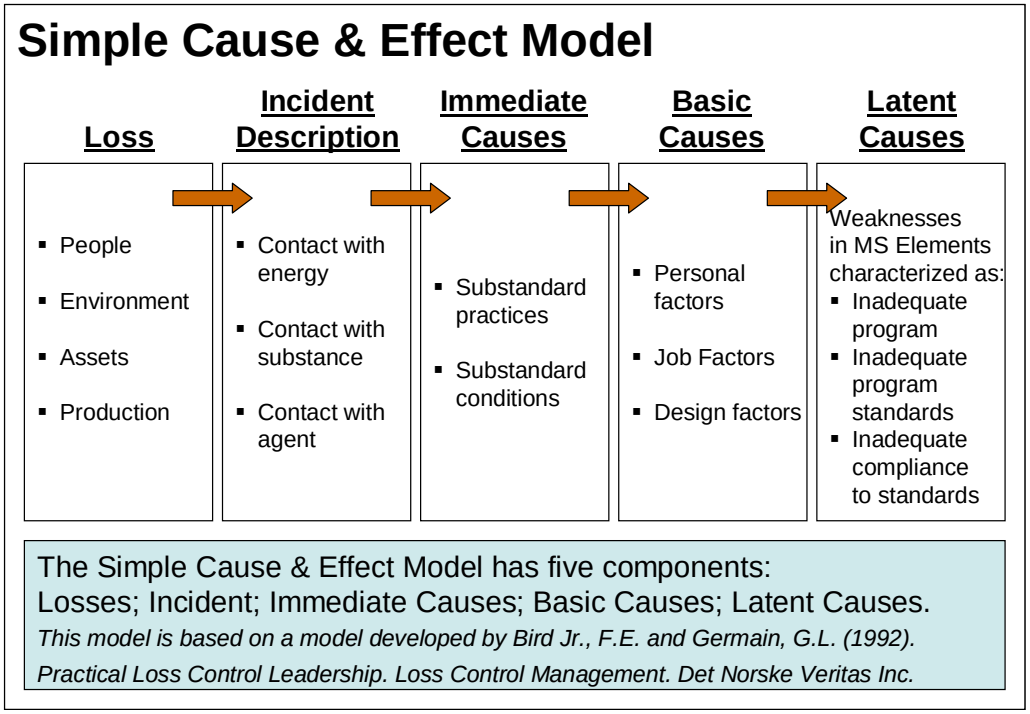
- Categorize and summarize the facts and information of the incident (overview or detailed);
- Communicate the nature of an incident and its causes in a structured manner that is readily understood;
- Further the II process after the RCA (i.e., check for thoroughness of the RCA towards understanding cause and preventing recurrence);
- Check that the II and RCA processes have drilled down to latent causes (i.e., management system failures) and are sufficiently broad to identify all potential causes.

There are two models that can be used to analyze and categorize the information learned from an RCA: the **simple model** and the **detailed model**. Both models categorize the information using five simple components:

- Loss or Impact on PEAP
- Incident or Incident Description
- Immediate Causes or Technical Causes
- Basic Causes or Human Factors
- Lack of Control, Inadequate Controls, Latent Causes, or Management System Failures

The approach is essentially the same for both models, other than the level of detail. The simple model is more suited for broad communication of an incident and the results of an incident analysis. The detailed model can be

used for checking depth and thoroughness of an RCA, and provides an easy tool to identify the latent causes or deficiencies in the management system elements. (Note: Other sources may refer to these models as a Causal Summary or an Incident Analysis Summary).



The template for the **Detailed Cause and Effect Model** is shown at the end of this section.

Incidents: The Causes and Effects

Consider the **causes** and **effects** of an incident. When characterizing an incident to determine the causes, it is easy to become confused between the incident, the effects, impact, and consequences of an incident, and the causes of the incident. It is also easy to jump to the obvious as the cause of an incident, such as an explosion, a mechanical failure, an electrical short, a computer failure, or a corroded pipe, etc. The point is do not jump to conclusions. It is critical that one keeps an open mind to understand the real cause in a structured manner and hence the solutions to prevent recurrence. Managers want to address the cause so the incident does not happen again. Being careful at the start of any investigation to define the losses and an appropriate incident description is crucial. Although the Incident Description can be tentatively identified immediately after an incident, or during the preliminary or early stages of an investigation, it is best to agree on a statement of the Incident Description at the start of the formal RCA. After the incident description has been defined, the branches or roots in the analysis leading to the latent causes become much clearer.

It is also important to understand that good incident investigations are not done to assign blame or find personal fault. Consider the response of the president of the MMA Railway to the 2013 Lac-Mégantic Derailment disaster, where he indicated that the disaster was because the train engineer failed to set the brakes on the train. While this may be a cause, it is not the latent cause. By firing or suspending this worker, will this action prevent another incident? The analysis of an incident using these methods will reveal if any such actions have drilled down to address the true latent causes, which are the management system failures.

The Components of a Cause and Effect Model

As seen from the previous figures, the following are important components of a cause and effect model: **Loss; Incident Description; Immediate Causes; Basic Causes; Latent Causes**. Each component is further developed and may require a return to the Detailed Cause and Effect Model.

Loss: The detailed description (quantitative and/or qualitative) of the consequences or impact of an event or incident on PEAP, where applicable.

Incident Description: A summary of the unplanned, undesired event that is the focus of the investigation that will identify the causes of the event towards preventing its reoccurrence. It is simply a brief description of the incident and the loss. While succinct, it must contain sufficient detail to describe the unintended event and all of its impacts.

- Inferior example: "Train derailment"
- Comprehensive: "Train derailment, 2 injuries, oil spill leads to groundwater contamination, $100K property damage, rail-line out of service for 3 days"

As the investigation team progresses through the incident analysis, it will be revealed whether the incident description was appropriate (of the right breadth and depth) or not. The incident analysis process then begins with carefully determining the **Incident Description**. In almost all cases, the incident description must be supported by evidence. In some cases, the incident itself has destroyed much of the evidence and being able to clearly state the incident description is not easy. In this case, careful speculation or deduction based on sound technical understanding is a reasonable approach. Uneducated guesses are potentially destructive. Please be aware that without a thoughtful incident description, the incident analysis may miss some causal factors and, without corrective actions, the activity is subject to having elements of the same incident happen again, due to the unsolved causes.

Immediate Cause (Technical Factors): When an investigation team convenes, there will be a number of opinions, positions, thoughts, and inputs on the possible causes of an event from within the team and external to the team. Although there will be speculation about multiple immediate causes soon after an incident and during the preliminary or early stages of an investigation and analysis, the formal RCA will identify true immediate causes and link other speculations and observations in a logical framework. It is important to ensure that the right subject-matter experts and stakeholders are assembled for the team.

- Immediate causes are circumstances that immediately precede an incident and can be determined by asking the question, "What caused the incident?" or by phrasing the question as "The Incident was caused by …?" The answers to these questions are the first level of causes, sometimes referred to as the first branch in the RCA.
- The first level of immediate causes is usually quite apparent, easy to identify, and logical based on the technology involved. The immediate causes generally include substandard practices / acts / behaviours, and/or substandard conditions which were evident at the time of the mishap. There must be at least one immediate cause (sometimes two or three, but rarely more in that first level). For example, an explosion may result when a leaking line and an ignition source occur simultaneously. The two immediate causes might be a gasket failure (defective equipment) and the presence of an ignition source in the area (fire and explosion hazard; see the Immediate Causes table below). The process continues with carefully determining the causes of those causes.
- Immediate causes consist of two categories, as shown in the following tables:
  - **Substandard practices** may be referred to as unacceptable behaviours or at-risk behaviours.
  - **Substandard conditions** may be referred to as unacceptable conditions.

Substandard Practices – detailed lists

Use of Protective Defenses (assumes in place) • Improper use of proper Personal Protective Equipment • Not using Personal Protective Equipment • Disabling guards or warning systems (safety devices) • Servicing, operating non-isolated or energized equipment • Lack of knowledge of hazards • Equipment not secured	***Use of Tools or Equipment (good equipment available)*** • Using equipment improperly • Using tools improperly • Using Defective equipment (aware) • Using Defective tools or materials (aware) • Servicing equipment while in operation
Following Procedures (assumes they exist and they are sound) **General:** • Not following safety standards or guidelines • Not following proper operating procedures or methods • Not following proper maintenance procedures or methods **Specific:** • Operating equipment without authority • Taking improper position or posture • Improper placement • Overexertion of physical capability • Improper mixing of chemicals • Improper loading • Working at improper speed • Conscious risk taking (by group) • Conscious risk taking (by individual) • Horseplay	***Inattention/Lack of Awareness (operators not focused)*** • Improper decision making or lack of judgment • Distracted • Inattention to footing and surroundings • Under the influence of drugs or alcohol

Substandard Conditions – detailed lists

Hardware • Defective equipment • Defective tools • Inadequate equipment • Inadequate tools • Improperly prepared equipment • Improperly prepared tools **Possible Reasons:** • Wear/Tear • Corrosion • Other	***Condition of Defenses*** • Inadequate guards/protective devices • Defective guards/protective devices • Inadequate Personal Protective Equipment • Defective Personal Protective Equipment • Inadequate warning systems • Defective warning systems • Inadequate isolation of process of equipment
Process Exposure • Exposure to fire and explosion • Exposure to noise • Exposure to energized electrical system • Exposure to radiation • Exposure to temperature extremes • Exposure to hazardous chemicals • Exposure to mechanical hazards	***Workspace Hazards*** • Great heights • Inadequate or poor housekeeping • Inadequate layout, clearances, congestion or protrusions • Inadequate illumination • Inadequate ventilation

Basic Causes (sometimes referred to Human Behaviours): Basic causes describe the reasons why the substandard acts occur and substandard conditions exist, and are difficult to identify. Often, they are not evident until after an incident has been thoroughly researched, investigated, and analyzed using an RCA; thus, probing and questioning throughout the process is required. Basic causes are the underlying factors that allowed, and perhaps even invited, the immediate causes to develop. It should be noted that each cause needs to be verified by evidence; this factor alone brings strength to the investigation process. As stated earlier, the incident may have destroyed the evidence so deduction based on sound technical understanding is a reasonable approach. Avoid speculation when no facts are known. During the formal process, several questions can be asked to determine the basic causes in the same manner as for determining the immediate causes:

1) Why did that substandard practice occur? Basic causes help explain why people perform substandard practices (i.e., their unacceptable behaviours). Logically, a person is not likely to follow a proper procedure if he or she has never been taught that procedure, or if that procedure is poorly written, or non-existent.
2) Why did that substandard condition exist? Basic causes help explain why substandard conditions exist. Equipment and materials, which are inadequate or hazardous, will be purchased if there are not adequate standards and if compliance with standards is not managed (pressure of cost and schedule).
3) What failure in our supervisory/management system permitted that practice or condition? This question actually begins to explore the latent causes.

The tables below help guide the user in categorizing the various details of the incident including the immediate and basic causes.

Engineering & Design Factors *(can apply to structures, equipment, tools, i.e. any engineered system)*	**Job Factors**	**Personal Factors**
• Inadequate technical design • Inadequate ergonomic design • Inadequate assessment of loss exposures • Inadequate standards, specifications and/or design criteria • Inadequate monitoring of construction • Inadequate assessment of operational readiness • Inadequate monitoring of initial operation • Inadequate evaluation and/or documentation of change • Inadequate inherently safe design	• Inadequate maintenance • Inadequate job procedures • Error-inducing conditions • Organizational factors • Incompatible goals • Inadequate training • Inadequate communication	• Inadequate physical / physiological state / capability to do the work • Perceived inadequate mental / psychological state / capability to do the work • Physical or physiological stress • Perceived mental or psychological stress • Improper risk taking / improper motivation • Lack of knowledge / lack of skill

Job Factors – detailed lists

Inadequate Maintenance *Encompasses underlying conditions that impact on the maintenance system.* • *inadequate preventative maintenance* • *inadequate reparative maintenance* • *excessive wear and tear of equipment* • *improper extension of service life* • *abuse or misuse of equipment* • *inadequate inspection/ monitoring* • *inadequate assessment of needs* • *other (please specify)*	***Inadequate Job Procedures*** *Factors affecting the structure of a job.* • *inadequate/absent safety regulations and/or procedures* • *inadequate reference documents, directives or guidance manuals* • *lack of initial orientation* • *inadequate work standards* • *lack of or inadequate job safety analysis regarding hazardous activities* • *inadequate shift handover procedures* • *inadequate identification and evaluation of loss exposures* • *negative reporting (meaning: if not told otherwise, assume all is well)* • *inadequate tools and equipment* • *poor regulations for Personal Protective Equipment use* • *Other (please specify)*
Error Inducing Conditions *Conditions existing in the work environment conducive to committing errors or violations* • *environmental stress* • *noise* • *atmospheric conditions* • *oxygen deficiency* • *task-related stress* • *repetitive/monotonous job task* • *confusing demands* • *extreme concentration or perception demands* • *physical / physiological demands* • *fatigue due to mental task load or duration* • *fatigue due to sensory overload* • *other (please specify)*	***Organizational Factors*** *Refers to systems or programs within the organization.* • inadequate work planning • unclear or conflicting reporting relationships • unclear or conflicting assignment of responsibility • improper/insufficient delegation • inadequate audit/inspection program • inadequate incident reporting/investigation system • inadequate purchasing • inadequate job placement (wrong person on the job) • inadequate performance measurement, evaluation and feedback • inadequate leadership / supervision • lack of supervisory / management job knowledge • inadequate or lack of safety meetings • inadequate safety promotion (visibility, acceptance) • inadequate control of change system • *other (please specify)*
Inadequate Communication *Includes the tools for communication and the process of communication.* • giving unclear or incomplete instructions • inadequate communication of safety and health data, regulations or guidelines • inadequate communication tools • inadequate horizontal communication (i.e., between peers) • inadequate vertical communication (i.e., between supervisor to peer) • inadequate communication between different organizations • absence or misuse of standard terminologies and phraseologies • other (please specify)	***Inadequate Training*** *This section pertains to organization-provided training.* • *inadequate training provided by organization; poor trainers, poor training materials* • *lack of training by organization* • *training requirements not identified as part of job description* • *training is ineffective (boring, lack of incentive to learn)* • *job requirements and training do not match* • *other (please specify)*
Incompatible Goals *Chosen when the conflicting goals originate from different management systems. A change in these conditions generally impact on the management philosophy.* • *system goal vs. safety goals* • *personal goals vs. safety goals* • *system vs. system goals*	

Personal Factors – detailed lists

Physical Capabilities • Substance sensitivities or allergies • Vision deficiency • Hearing deficiency • Other sensory deficiency • Respiratory incapacity • Other permanent physical disabilities • Temporary disabilities • Limited ability to sustain body positions • Restricted range of body movement • Other (please specify)	***Physical Stress*** Physical conditions specific to the individual that are: 1) Conducive to committing errors; or 2) Render the individual more susceptible to injury or illness. • Injury or illness • Fatigue • Blood sugar insufficiency • Drugs or alcohol • Other (please specify)

Improper Risk Taking / Improper Motivation Chosen when the conditions are specific to or impact directly on the individual. Recommendations generally fall under the control of the supervisor and employee. • Improper performance is rewarding • Proper performance is criticizing • Lack of incentives • Improper supervisory example • Inadequate identification of critical safe behavior • Inadequate reinforcement of critical safe behaviors • Inappropriate aggression • Other (please specify)	***Lack of Knowledge or Skill*** Conditions usually specific to an individual, but may be common to a peer group. • Lack of experience • Inadequate initial instruction • Infrequent performance • Lack of coaching • Inadequate practice • Misunderstood directions • Other (please specify)
Perceived Mental State • Irrational fears • Emotional disturbance • Inability to comprehend • Poor judgment • Memory failure • Poor coordination or reaction time • Other (please specify)	***Perceived Mental Stress*** Perceived mental conditions specific to the individual which may be: 1) Conducive to committing errors; or 2) Render the individual more susceptible to injury or illness. • Frustration • Conflicting demands • Preoccupation with problems • Confusing directions • "Meaningless" or "degrading" activities • Other (please specify)

Latent Causes: Latent causes may also be referred to as the lack of control, loss of control, inadequate control, inadequacies or deficiencies in the management system, root causes, management system failures, management system weaknesses, or the euphemistic management system improvement opportunities. Recall, Control is part of the fundamental management process: Control (Steward) or Act, as discussed in handbook **Chapter 7.4: The Fundamental Process of Management**. Almost always the latent causes will reflect inadequacies in the management system, and those reflect on the elements of the management system.

Latent causes are the fundamental or underlying causes behind the basic causes, and ultimately to the incident itself. The RCA process is an effective and efficient method for arriving at the latent causes and will provide the right guidance for identifying effective changes to the management system that are intended to work well into the future to prevent incidents.

In most cases, an organization or any part of an organization fails acutely or chronically because of lack of control. To make the necessary improvements to prevent incidents in the future, adjustments to the management system will be needed (thus, the need to find the management system failures). Leaders / managers must drive the RCA process to effectively find the latent causes; thus, when identified, these permit meaningful management action and management control.

Latent causes are the weaknesses in the Risk Management System Elements (more details on the RMEs can be found in **Chapter 3.3: The Risk Management System and Elements**).

12) Management Leadership, Commitment and Accountability
13) Risk Assessment and Management of Risks
14) Community Awareness and Emergency Preparedness
15) Management of Change
16) Incident Reporting, Investigation, Analysis and Actions
17) Program Evaluation and Continuous Improvement
18) Design, Construction and Start-up
19) Operations and Maintenance
20) Employee Competency and Training
21) Contractor Competency and Integration
22) Operations and Facilities Information and Documentation

Latent Cause Categories

There is no universal set of categories for the latent causes. Instead, one must relate the basic causes to the latent causes. This requires a bit of reverse logic in that one needs to express each of the Risk Management System Elements as a failure and then compare each of these failures with the basic causes. This is where the latent cause is – the management system element that failed – and how the basic causes are linked to latent causes.

The Risk Management Program is the all-encompassing set of policies, standards, and procedures for each of the Risk Management System Elements. Latent causes are failures in the Risk Management System Elements, which can be categorized in three ways. Note that each latent cause can be assigned to only one of these three categories. The latent cause categories are as follows:

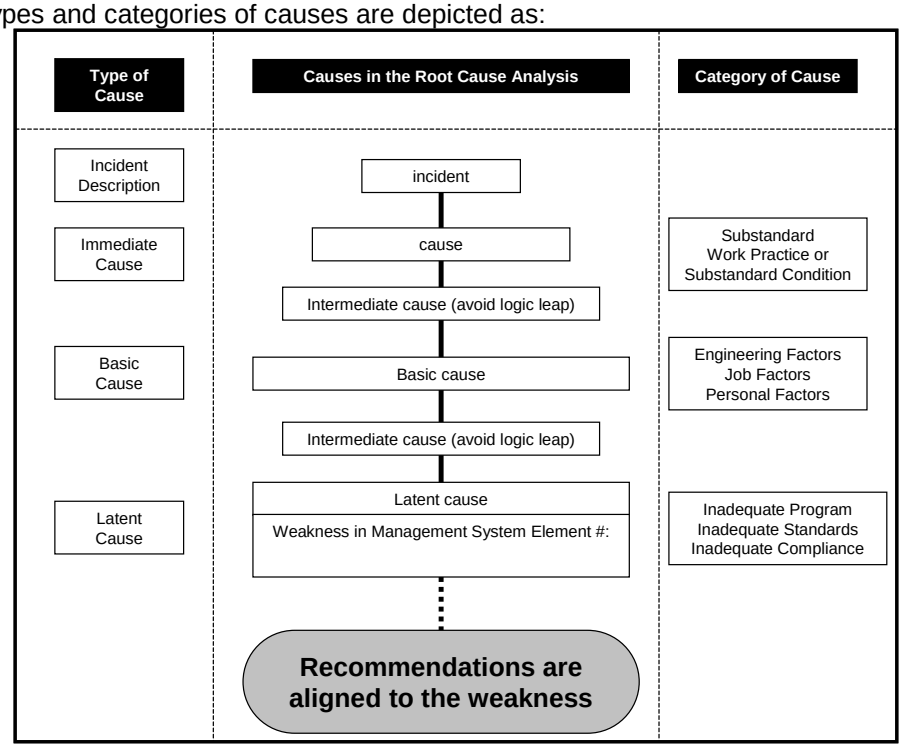
- P = Inadequate Program**:** The Risk Management Program is either non-existent or is lacking in many of the necessary Risk Management System Elements.
- S = Inadequate Program Standards**:** The Risk Management Program exists and all Risk Management System Elements are present; however, the policies, standards, and procedures necessary to implement, maintain, and sustain the Program are either non-existent or inadequate (it could also mean employees do not understand the existing standards or procedures)
- C = Inadequate Compliance with Standards**:** The Program and supporting standards and procedures exist, but work practices are not meeting the requirements as laid out by the standards and procedures (it could also mean employees do not have access to existing standards or procedures)

What does "Inadequate Compliance with Standards" mean?

Compliance with the standards means that the work practices are completed effectively or are executed in an effective manner so as to meet the stated objectives, aims, purposes, intents, and requirements of the Risk Management Program (i.e., to comply with the standards and procedures). When work practices are not completed, or not effective, or executed in an ineffective manner, then there is "Inadequate Compliance with Standards".

The Cause and Effect Model and the Root Cause Analysis Structure

The alignment to types and categories of causes are depicted as:



This relation and the alignment to types and categories of causes as defined in the **Cause and Effect Model** are depicted as **Intermediate Causes**. Intermediate causes are used to link immediate to basic, and basic to latent causes to avoid logic leaps. This is discussed further in **Chapter 4.3: Root Cause Analysis of an Incident**.

Intermediate causes are used to link immediate to basic, and basic to latent causes to avoid logic leaps. Consider these two contrasting examples using a propane explosion loss incident:

1) *Thousands of residents evacuated; caused by undertaking an illegal truck-to-truck transfer.*
2) *Thousands of residents evacuated; caused by potential escalation of fire and thick, dense smoke; caused by major propane fire at near-by propane distribution facility; caused by large, uncontrolled release of liquefied propane gas; caused by rupture of transfer hose; caused by defective transfer hose; caused by using transfer hose for truck-to-truck transfer; caused by lack of inspection / lack of suitable rating for truck-to-truck transfer; caused by undertaking an illegal truck-to-truck transfer.*

The connection between the evacuation and the illegal truck-to-truck transfer is not apparent. The connections between each link are made all the more obvious in the second example. Always check your logic by asking, "Was *X* caused by *Y*?" (see the **Template for a Cause and Effect Model**).

Summary Conclusions

Incidents that impact PEAP are caused and have causes rooted in the weaknesses in management systems. These incidents do not "just happen". There are exceptions: natural events such as earthquakes, tornadoes, tsunamis, etc. Some insurance contracts describe these as "acts of nature". And even for these natural events, proactive engineers design and build their physical systems (structures, mechanical machinery, pressure vessels, electrical distribution systems, pipelines, bridges and roads, telecommunications systems) to limit consequences where practical. If the latent causes result in deficiencies in design, or fabrication, or construction, or installation, or operation, or maintenance of such physical systems, then the management system weaknesses may cause greater impact on PEAP than the designers had in mind. Other considerations:

- The **Cause and Effect** model categorizes the causes under various general descriptors and sub-descriptors.
- When using the Incident Analysis Summary tools, it is not that important to align causes with the groups. It is important to be able to recognize in which group a cause is categorized. It is most important to drill down and identify all causes, especially the latent causes.
- After having identified all causes, and specifically the latent causes, the link or relation to lack of control or inadequate control can be made.
- Each latent cause can be aligned with one or more specific management system elements; thus, one can begin to make recommendations to correct the weaknesses in the management system, eliminate the latent causes, and prevent incidents.
- A **Template for a Cause and Effect Model** with two categories of latent causes is shown here:

Detailed Cause and Effect Model:

Losses	Incident	Immediate Causes	Basic Causes	Latent Causes		
Type	Type	Type	Type		Categories	
				Weaknesses in System Elements	P	C
Injury / Illness	**Body Motion:**	**Substandard Work Practices**	**Engineering & Design Factors:**	1) Management Leadership, Commitment and Accountability.		
First Aid	Struck against	Use of Protective Defenses (assumes in place)	Inadequate technical design	2) Risk Assessment and Management of Risks.		
Medical Treatment	Struck by	Use of Tools or Equipment (good equipment available)	Inadequate ergonomic design	3) Community Awareness and Emergency Preparedness.		
Lost Time	Fall to lower level	Following Procedures General: (assumes sound & exist)	Inadequate assessment of loss exposures	4) Management of Change.		
Fatality	Fall on same level	Following Procedures Specific: (assumes sound & exist)	Inadequate engineering/technical standards, specifications and/or design criteria	5) Incident Reporting, Investigation, Analysis and Actions.		
	Caught in	Inattention / Lack of Awareness (not focused)	Inadequate monitoring of construction	6) Program Evaluation and Continuous Improvement.		
Environment	Caught on		Inadequate assessment of operational readiness / completeness of construction	7) Design, Construction and Start-up.		
spill / release <25 kg, no adverse impact	Caught between		Inadequate monitoring of initial operation	8) Operations and Maintenance.		
spill / release >25 kg, no adverse impact	Overexertion		Inadequate evaluation and/or documentation of change	9) Employee Competency and Training.		
spill / release >25 kg, adverse impact	Overstress		**Job Factors:**	10) Contractor Competency and Integration.		
regulatory exceedance			Inadequate maintenance	11) Operations and Facilities Information and Documentation.		
off-plant adverse impact	**Contact with:**		Inadequate work standards / job procedures			
	Environmental Heat		Error-inducing conditions			
Assets	Environmental Cold	**Substandard Conditions**	Organizational factors			
Minor <$5,000	Hot surface	Hardware	Incompatible goals			
Serious $5,000-$50,000	Cold surface	Condition of Safeguards	Inadequate training			
Major $50,000-$500,000	Fire	Process Exposure	Inadequate communication			
Catastrophic >$500,000	Electricity	Workspace Hazards	Inadequate equipment and tools for the job			
	Chemical - corrosive	Process Hazards	**Personal Factors:**			
Business Interuption *	Chemical - toxic		Inadequate physical / physiological state / capability to do the work.			
Minor <$5,000	Noise		Perceived inadequate mental / psychological state / capability to do the work.	***Categories of Latent Causes:***		
Serious $5,000-$50,000	Pressure		Physical or physiological stress.	***P = inadequate program and/or standards***		
Major $50,000-$500,000	Radiation		Perceived mental or psychological stress.	***C = inadequate compliance with program and/or standards***		
Catastrophic >$500,000			Improper risk taking / improper motivation			
** measured as conversion cost of lost production plus any wasted / lost materials*			Lack of knowledge / lack of skill.			

This model is based on a model developed by Bird Jr., F.E. and Germain, G.L. (1992). Practical Loss Control Leadership. Loss Control Management. Det Norske Veritas Inc.
Adapted by ESRM Program at The U of Alberta, including the APEGA Model for Management System Elements.

Section 4.3: Root Cause Analysis of an Incident

The RCA process is the logical breakdown or analysis of an actual incident to identify the causes. During an RCA, all types of causes are determined, including the immediate causes, the basic causes, and the latent causes due to weaknesses in the management systems. It not only identifies the actual causes of the incident, but also can be used to identify possible, probable, or conceivable causes. It can also reliably describe the sequence of events leading up to the incident (i.e., all circumstances (conditions, actions, behaviours, etc.)).

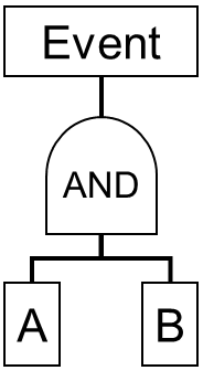
The RCA process is intended to drill down to the latent causes. It is here that the weaknesses in the management systems are revealed. The starting point is the **Incident Description** which is the unplanned event, the focus of your investigation. After the latent causes are known, then the weaknesses in management system elements can be addressed through improvements in the management system elements. In other words, the recommendation should address the management system element or its sub-elements. Benefits of an RCA include:

- It can focus on one specific cause at one time;
- It identifies all causes through brainstorm thinking, which then can be supported by evidence, and then linked in a logical framework;
- It provides a picture of the incident in a clear and logical way; and
- It can be qualitative or quantitative in nature.

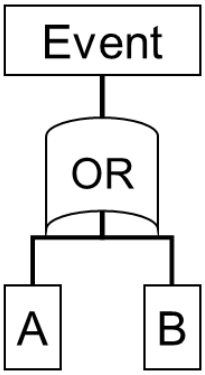
Nomenclature and Symbols for an RCA

Behaviours, activities, operations, and conditions come together to cause an incident. Different symbols are used in the analysis to describe these and bring a logical interpretation of the RCA. A rectangular box describes a behaviour, activity, operation, or condition. The **AND** and **OR** gates are used to describe combinations of actions, behaviours, activities, operations, and conditions that caused the event.

AND Gate



OR Gate



AND Gate

- One possibility is a combination of activities that must happen (e.g., Activity A AND Activity B)
- Another possibility is a combination of conditions that must be present (e.g., Condition A AND Condition B)
- Another possibility is a combination of activities that must happen and conditions that must be present (e.g., Activity A AND Condition B or Behaviour A AND Operation B).

OR Gate

- One of several activities must happen (e.g., Activity A OR Activity B)
- One of several conditions must be present (e.g., Condition A OR Condition B)
- One of several activities must happen or conditions must be present (e.g., Activity A OR Condition B)

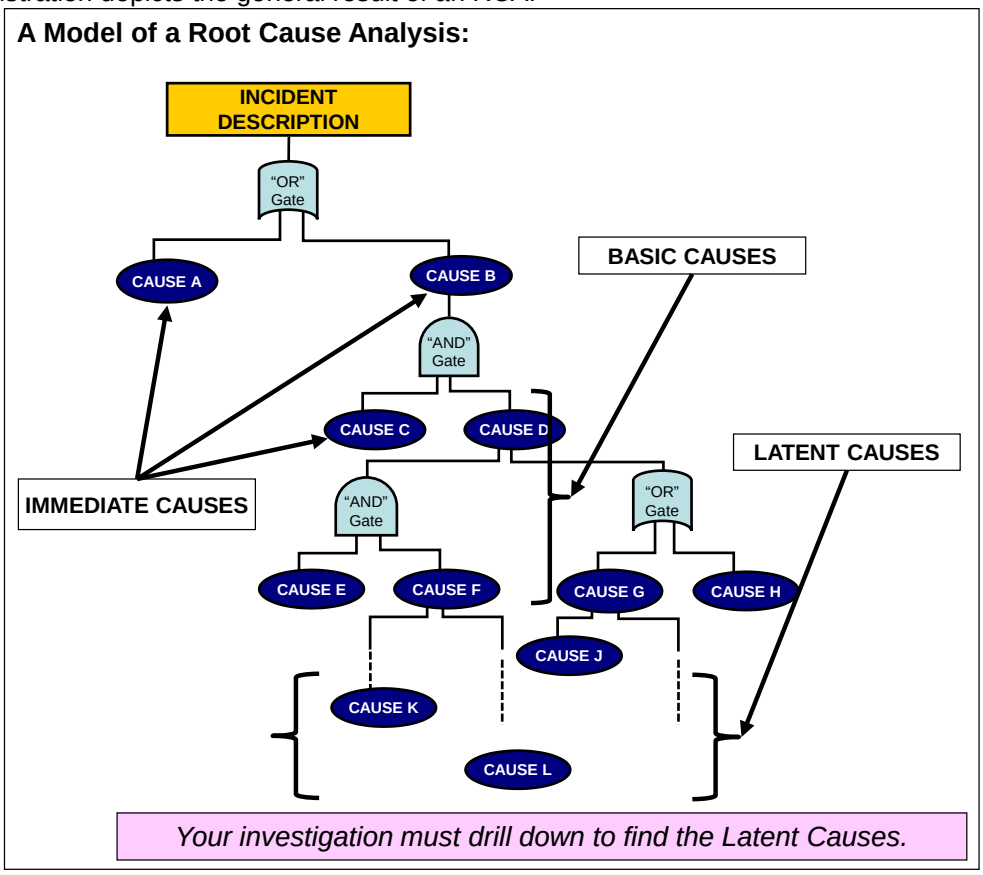
How to Conduct and Construct an RCA

Before starting an RCA, it is absolutely necessary that as many facts of the incident are known (i.e., what happened, when, where, the impact on PEAP, and especially the sequence of events leading up to the major incident). Much time and effort can be saved by avoiding the debate as to details of what happened. This information should have been determined during the course of the II process. Of course, questions will arise during the RCA that will require seeking more information.

1) Define and state the **Incident Description**.

2) After the team has agreed upon the **Incident Description**, ask the question "why?", and the answer will fundamentally be the "**Incident Description** was caused by Cause A or Cause B", as shown in the model RCA below. It could also have been answered as the "**Incident Description** was caused by Cause A and Cause B".
3) For each cause found in the levels working down, ask the same question, and the fundamental answers will be "Cause B was caused by Cause C and Cause D", for example, and so on.
4) The analysis will find technical causes and human factor causes at the initial levels and in the deeper levels as the analysis is drilled down. These will need to be addressed as part of setting recommendations, but it is necessary to continue to drill down until the latent causes have been reached; that is, where there was loss of control caused by the weakness in the management system.
5) Ultimately, a point will be reached where the latent causes are found.
6) Avoid "logic leaps".

The following illustration depicts the general result of an RCA.



Breadth and Depth of the Scope of Your RCA: The scope of an RCA has at least two dimensions: breadth and depth. In many cases, the investigators will most likely find that the initial breadth of the scope of the RCA is either too wide or too narrow.

Breadth of the Scope of Study: To determine if the breadth is too wide or too narrow, look a little forward in the root cause.

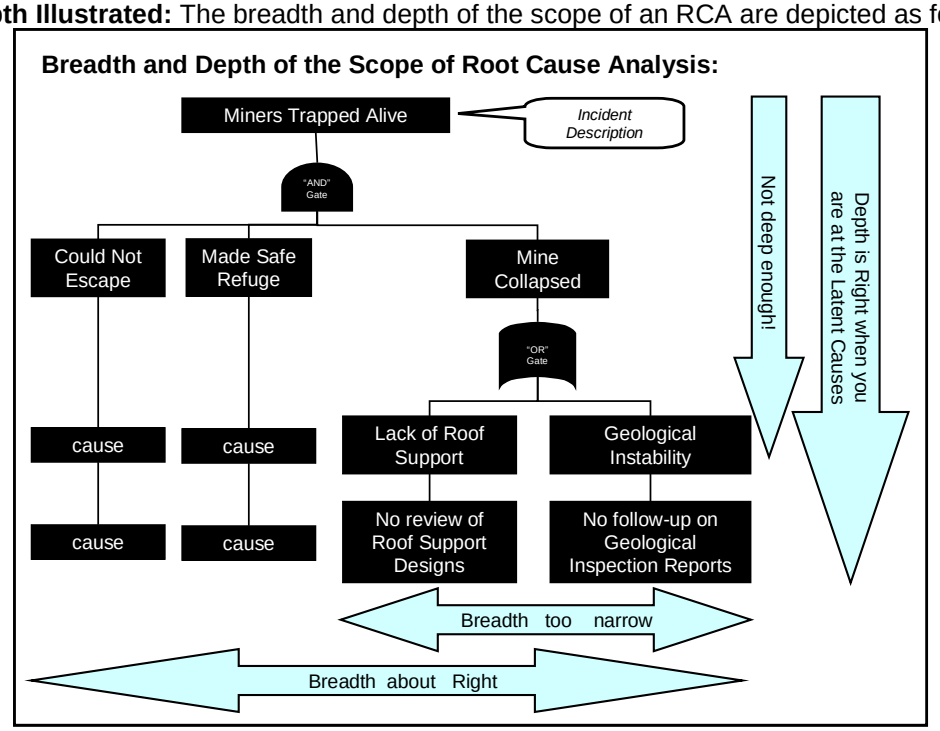
- To determine if the analysis is too wide, check whether the causes are outside the influence or control of the management's operation (e.g., people consumed contaminated water because the city failed to issue a boil-water advisory is too broad for analyzing the causes of a spill from the manager's chemical processing plant). *NOTE: Ordinarily, all of the Elements in the Risk Management System must be addressed. For purposes of the course, coverage of fewer elements is acceptable.*
- To determine if the analysis is too narrow, the RCA team cannot state one way or another if the analysis has examined all of the elements of the management system or verified that those elements are immaterial.
- Consider the incident of 33 Chilean miners who were trapped for 69 days in 2010:
  - In the root cause, is the **Incident Description** "Mine Collapsed" or "Miners Trapped Alive"?

- If the analysis starts with “Mine Collapsed”, then all management elements relating to how and why the miners were trapped, how and why they stayed alive, how and why a rescue was undertaken, are excluded. There are too few of the Risk Management Elements examined. Breadth is too narrow.
- So, for this case, it is more appropriate to start with “Miners Trapped Alive” as the **Incident Description**, and enough of the Risk Management Elements should be addressed to be thorough in the analysis.

Depth of the Scope of Study: The depth of the analysis (i.e., how deep the analysis drills) must get to the latent causes or the losses of control. These are the management system failures that directly relate to the Management System Elements.

- Use detailed causes (small steps) when going deeper so that causes are not skipped over.
- When the lowest level of cause in a root is obviously and readily aligned with one of the Risk Management Elements, the right depth of that root has been reached.
  NOTE: Ordinarily, all of the Elements in the Risk Management System must be addressed. For purposes of the course, coverage of fewer elements is acceptable.
- Consider the previous example of the 33 miners trapped alive for multiple days. In the root cause starting with the **Incident Description** “Miners Trapped Alive”, a string of causes (without regard to other AND or OR causes) could be generated as follows:
  - miners trapped alive caused by
  - escape route blocked caused by
  - heavy equipment in the way caused by
  - heavy equipment abandoned caused by
  - heavy equipment failed caused by
  - heavy equipment not maintained caused by
  - no qualified maintenance staff caused by
  - need for staff not recognized caused by
  - heavy equipment operational performance not measured caused by
  - **no policy to maintain equipment or measure performance**.
- This last cause is a latent cause – the link to a management system element is clear.

Breadth and Depth Illustrated: The breadth and depth of the scope of an RCA are depicted as follows:



Developing and Validating the Causes:

The Immediate Cause is the set of circumstances that immediately precede the incident and cause the incident in a physical, real sense. They usually can be sensed or seen, and they leave evidence. Most often, there is only one

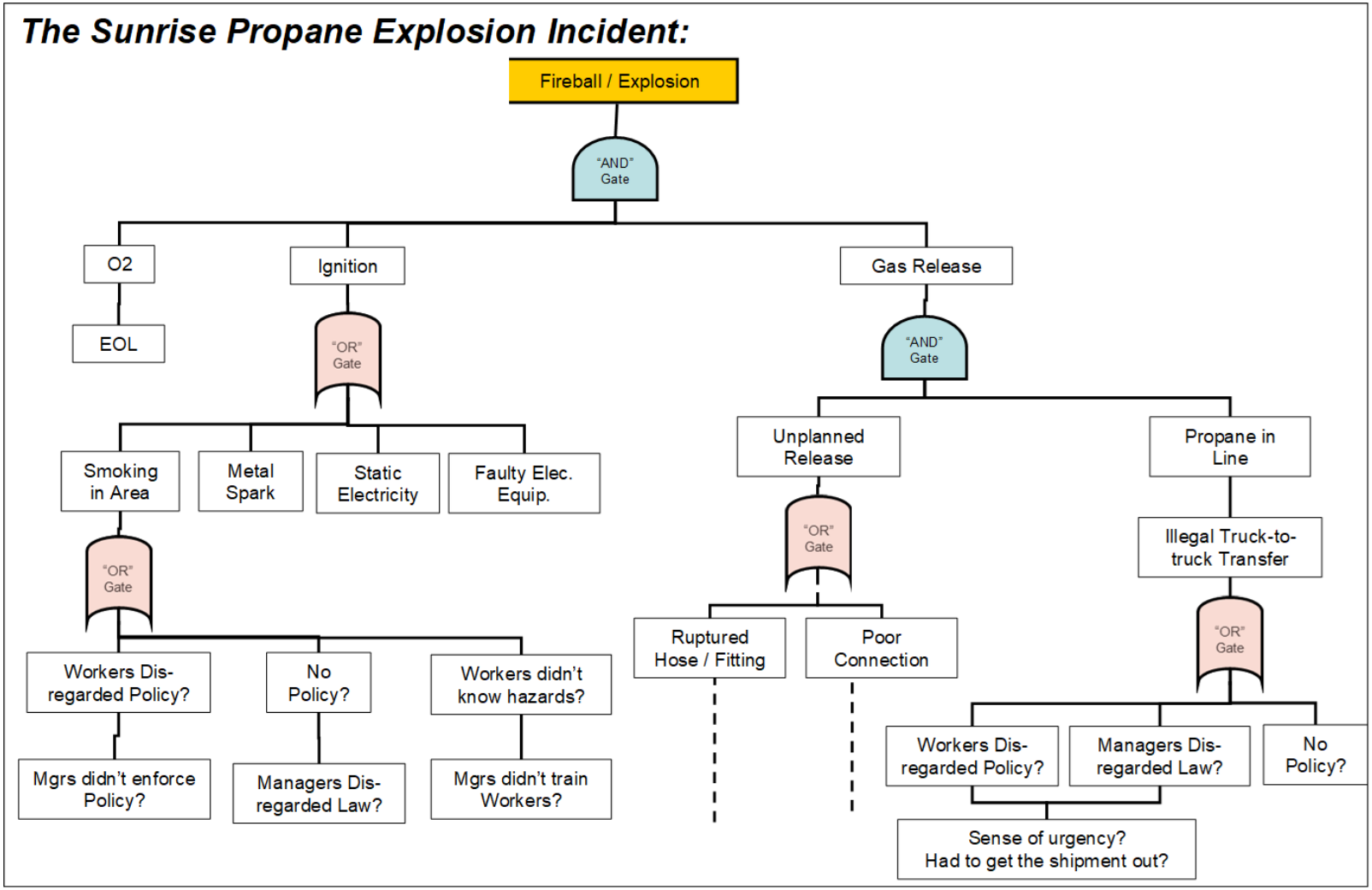
immediate cause, but there have been examples where more than one immediate cause have happened. To determine the basic and latent causes, ask the questions as noted in **How to Construct a Root Cause Analysis**.

Once you think you have completed your RCA and you think you have identified all actual causes, take time to verify by looking for hard evidence for each cause. This should include all of the causes: immediate, basic, and latent. Review and confirm your conclusions with your workplace colleagues. This activity validates the actual causes and will be supportive and valuable for determining recommendations and action items.

Summary

- Incidents that impact PEAP are caused and have causes rooted in the weaknesses in management systems. These incidents do not just happen.
- The latent causes of incidents can be determined and corrected (the control is restored) using the RCA process.
- After having identified all causes and specifically the latent causes, then the link or relation to lack of control or inadequate control can be made.
- The weakness in the management system can be aligned with one or more specific management system elements; thus, after having identified the latent cause (i.e., management system failure), then recommendations can be made to correct the weaknesses in the management system and eliminate the latent causes that lead to incidents.
- Incidents have causes rooted in management system weaknesses (i.e., latent causes). Latent causes can be determined and corrected (the control is restored) using the RCA process. After identifying latent causes, the link to lack of / inadequate controls can be made. Lack of control resides within, by, or through a weakness in the management system – the two are equivalent.
- Latent causes are synonymous with weaknesses in the management system and can be aligned with one or more specific management system elements; thus, one can begin to make recommendations to correct the weaknesses in the management system and eliminate the latent causes that lead to incidents.
- A draft RCA is noted below for a propane explosion incident.

The Sunrise Propane Explosion Incident:



Section 4.4: Latent Causes and The Swiss Cheese Model

A number of different terms have been used to describe the same thing. This is not meant to create confusion, nor is it because there is lack of consensus on terms. Much like, Energy = Heat:

Latent Cause = Root Cause = Loss of Control

Latent Cause = Management System Failure = Weakness in a Management System Element

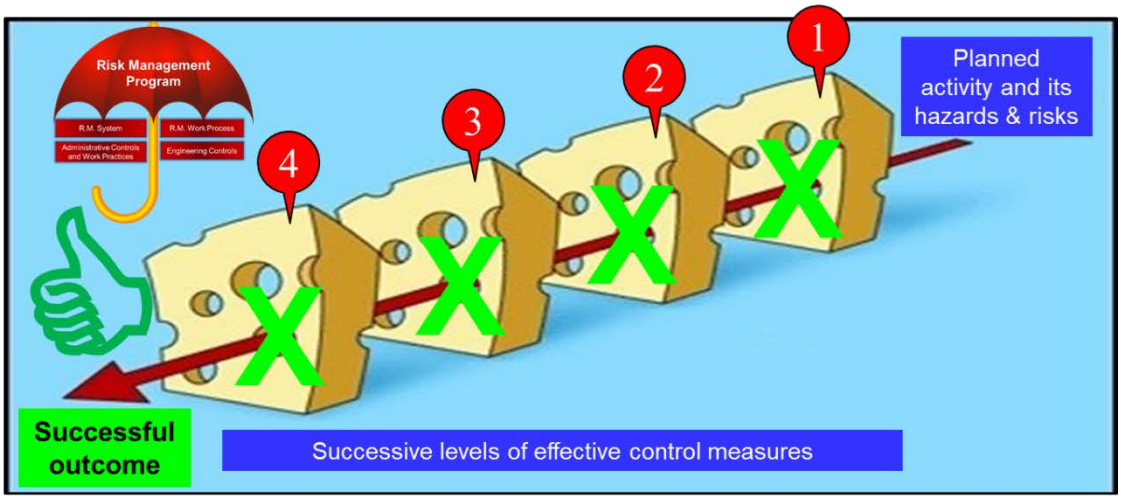
These mean the same thing, but for different stakeholders, the phrases bring more meaning.

The Swiss Cheese Model is another model that provides a means to see the causal factors of an incident. The model was originally proposed by Dante Orlandella and James T. Reason (University of Manchester) and has since gained widespread acceptance. This discussion uses the term "Swiss Cheese Model" not in the sense and categories as offered by Orlandella and Reason, but in terms relative to this course.

All organizations perform activities to add value to the enterprise and to fulfil the vision and mission (purpose) of the organization. To do so, some kind of activity is planned, with its inherent hazards and risks, and with the intention of a successful outcome of that activity. Various working components of the risk management program are implemented so as to control the hazards and reduce risks to prevent an incident. These components, as depicted by the slices of cheese, are the risk management system (RMS) and work processes, the engineering controls and safeguards, the administrative controls, and the work practices. All are managed by the risk management program through the execution and implementation of the elements of the RMS.

A Fresh Perspective: The Block of Swiss Cheese and the Slices in the Block

Levels of risk management are applied (1,2,3,4) to control the hazards and reduce the risks associated with the planned activity to an acceptable level, where: 1) RMS; 2) Engineering Controls; 3) Administrative Controls; and 4) Work Practices. Please see Chapter 7 for more information on this model.



Chapter 3.3: The Risk Management System and Elements defines and specifies all responsibilities and activities within an organization to control hazards and reduce risks to acceptable levels. The RMS is typically interpreted as the first slice. Holes of this type are created when there is an inadequate program: the system does not adequately define or specify all responsibilities and activities within the organization (i.e., the administrative controls are non-existent). When responsibilities and activities are not well defined, there are breakdowns in the subsequent controls, as represented by the slices of cheese.

Engineering Controls, a type of engineered system, are typically interpreted as the second slice. Holes of this type are created when:

- the design of engineering controls is deficient;
- the fabrication, construction, or installation of the engineering controls is defective;
- the operation or maintenance of the engineering controls is sub-standard; or through

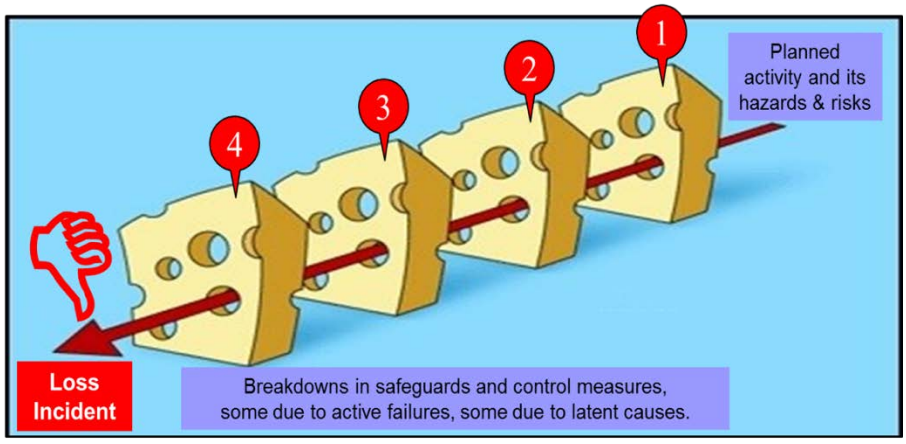
- any combination of the above.

Administrative Controls, the set of (documented) policies, rules, and procedures of an organization, are typically interpreted as the third slice. Holes of this type are created when there are inadequate program standards (i.e., the administrative controls are deficient). When documented policies are not well defined, there are breakdowns in the work practice (i.e., workers are not certain of the exact requirements of their duties and may perform or execute their jobs inadequately, and usually without knowing so).

Work Practices, as depicted by the fourth slice, are the actual implementation or execution of the work activity as defined and/or specified in the administrative controls. These apply not only to the immediate work at hand, but also to the maintenance and operation of the installed engineering controls, to the training and competency verification of workers, and to any other activities as may be required by the risk management system. Holes of this type are created when there is inadequate compliance with program standards (i.e., the work practices are sub-standard even in presence of sound administrative controls).

When the risk management program is effective (i.e., all control measures (engineering and administrative) are working), then there is a successful outcome to the planned activity, and loss incidents are prevented. The implementation of a Risk Management Program (system, work processes, policies, etc.) maintains the effectiveness of all control measures. In other words, when all management system elements are effectively implemented within a risk management program (i.e., all barriers are working), loss incidents are prevented. The Swiss Cheese Model in this case depicts that there are “no holes”.

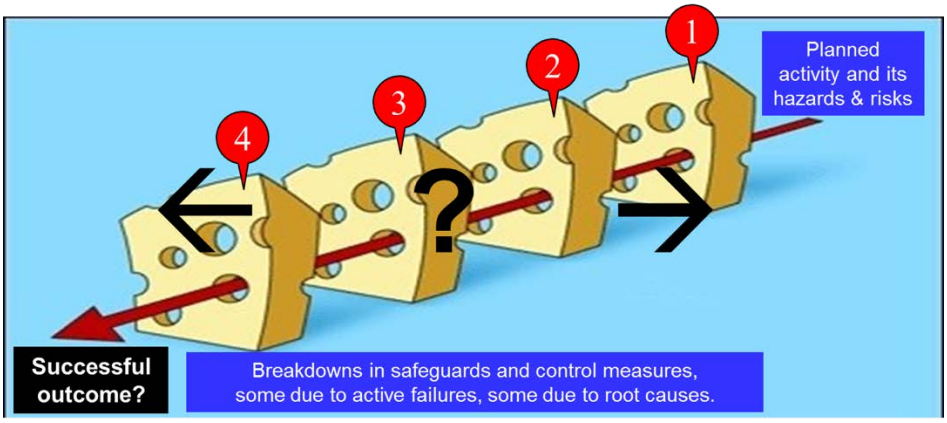
When there are weaknesses in the Risk Management System (i.e., the program implementation is defective or ineffective), then there are breakdowns in the engineering controls, the administrative controls, and the work-practices, as represented by the holes in the cheeses slices. These ineffective or defective components are depicted by “holes in the slices of cheese”, hence the name “Swiss Cheese Model”. It is only a matter of time (probability, likelihood, chance, luck) before all of the breakdowns in the engineering controls, administrative controls, and work practices happen at the same time – these holes align – and a loss incident happens.



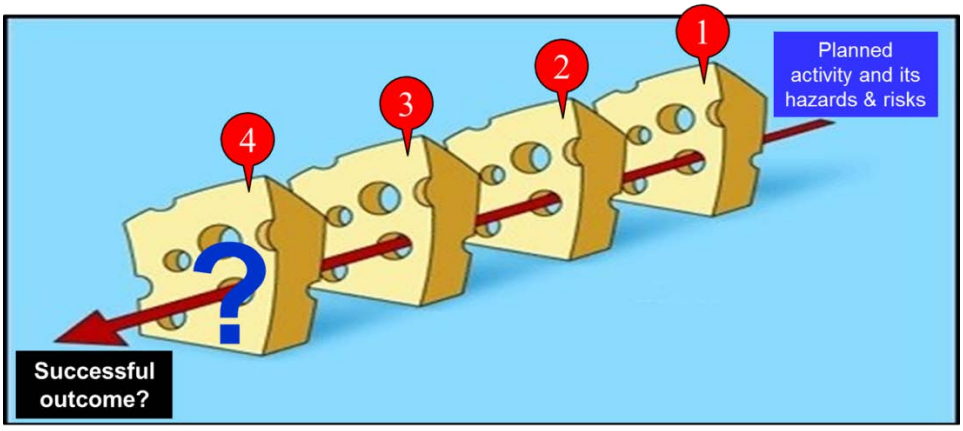
After the root cause is completed and the recommendations that address the root cause(s) are effectively implemented, then the effectiveness of the implementation of the Risk Management Program is restored, and planned activities can be undertaken with successful outcomes.

When there are deficiencies in the management system controls, these can lead to deficiencies in the engineering controls and administrative controls. When circumstances align (i.e., the “holes line up”), an incident occurs. Deficiencies in the management system are the latent causes. Barriers are not foolproof, and there is a real probability that they can fail. They are dependent on humans to maintain; thus, work practices, the “human factors”, form the last line of defense to prevent a loss incident. The discussion of human factors is explored in handbook section **Chapter 7.8: Individuals - Human Error, Risk Perception, And Motivation of Safe Behaviour**.

Linking Root Causes to the Swiss Cheese Model
Consider this case where the management program is ineffective and allowed the engineering controls and the administrative controls to degrade. How could a loss incident be prevented?



Analysis of an Event as Explained Using The "Swiss Cheese Model"
Consider the case where a worker intentionally pays particular attention to their activity (task, job, etc.) because … and what happens when …

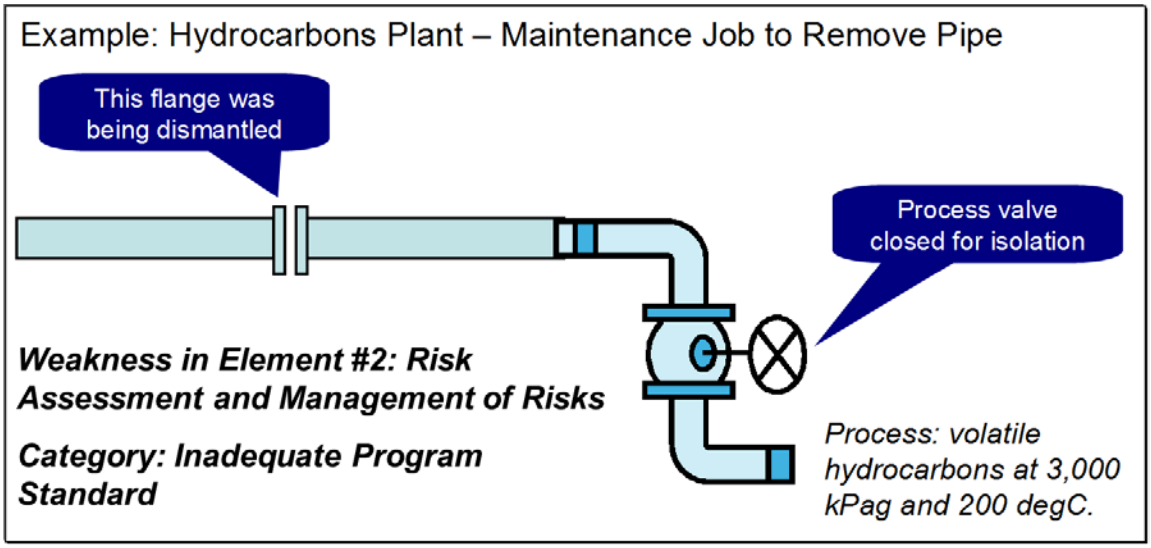


Example: Hydrocarbon Plant – Maintenance Job to Remove Pipe:

This example demonstrates how a latent cause leads to an incident when other causes align.

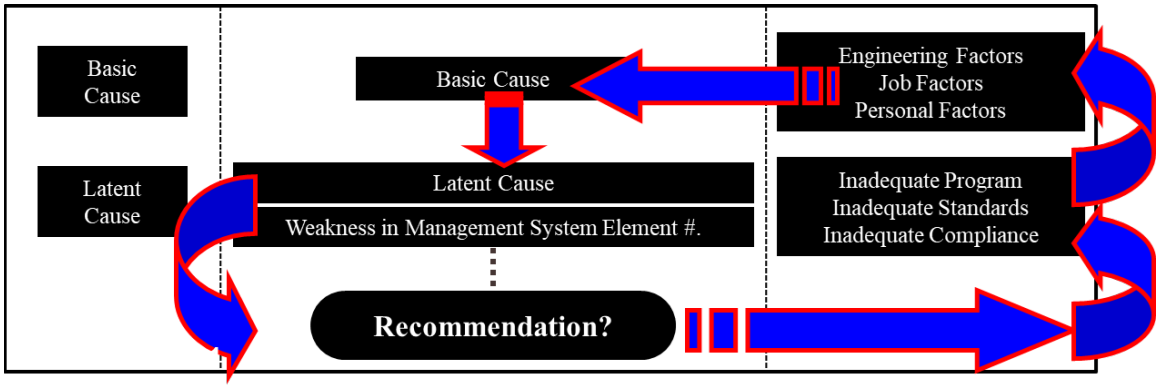
- Workers were tasked with removing pipe on a light hydrocarbon service.
- The isolating block valve did not seal tightly between the point of dismantling and the pipe that remains in service (under pressure with a flammable hydrocarbon gas) (i.e., a small amount of gas was able to leak through the closed valve).
- This job had been performed knowingly and successfully many times in the past with the same set of conditions. It was confirmed that workers were taking additional actions to overcome the deficiencies in the management system.
- On one occasion, while dismantling the pipe, the gas was ignited, and there was a small fire. Were it not for other contingent control measures that were in place to mitigate the possibility of ignition, there was a real possibility that this incident could have escalated.
- Upon investigation, there are many immediate and basic causes; however, the latent cause of this event was allowing the workers to dismantle pipe down-stream of an isolating block valve that was leaking. When saying "allowing", it is meant that there was no management system control in place to deny the workers the authorization under the unacceptable conditions. That is, the management system allowed the workers to work in unsafe conditions.
- It was only a matter of time before the right conditions aligned with the latent cause, and a fire resulted. In this case, the good work done by workers when this job was previously completed was not done by a second set of workers because these workers were not informed of the additional actions to overcome the deficiencies in the management system.
- Simply, there was no process or procedure in place to check the necessary conditions before authorizing the work. This is an example of an **inadequate program standard**, which is a category for a latent cause. The latent cause relates to **Element #2: Risk Assessment and Management of Risks**.

- If there was a standard to assess the risks for this specific condition of isolation (e.g., a valve that did not seal tightly), the task to assess would have been elevated to a higher level among management. Management action would have been triggered to assess the risk of the job (working downstream of the defective valve) and determine additional safeguards to reduce the risk to an acceptable level before proceeding with the activity.



Section 4.5: Linking Latent Causes to Recommendations for Actions

Recall the concepts of different types of causes as introduced in **Cause and Effect Models** and in **Root Cause Analysis**. These sections demonstrated how to drill down through immediate and basic causes to determine the latent causes. The relation and the alignment to types and categories of causes are depicted as:



This section explains how management can pin-point specific improvements to elements and identify actions to address the management system weakness(es), thus enabling management to make sound, effective decisions towards improving the risk management program and preventing loss incidents.

Linking Latent Causes to Actions

After the RCA has been fully developed in the II process, the latent causes become known. The next step is to identify recommendations for actions.

To do so, the latent causes should be expressed as weaknesses in terms of the organization's management system elements and then identify if there is a weakness in the program, in the associated standards, or in compliance with the standards. This is an iterative process and will involve some additional work on the part of the

investigator and leadership to question and fully understand the relevant management system element and the category of the latent cause. This may involve re-visiting the category of the basic cause to further refine the statement of the latent cause. The line of questioning follows:

- Which element of the RMS is relevant to or relates to the latent cause? Re-check the category of the basic cause to express the latent cause more accurately and more precisely.
- What is the nature / category of cause (i.e., was it inadequate compliance to a well-documented management system standard, an inadequate standard to document management activities, or an inadequate program)? This effort will reveal the appropriate action to take to address the latent causes.

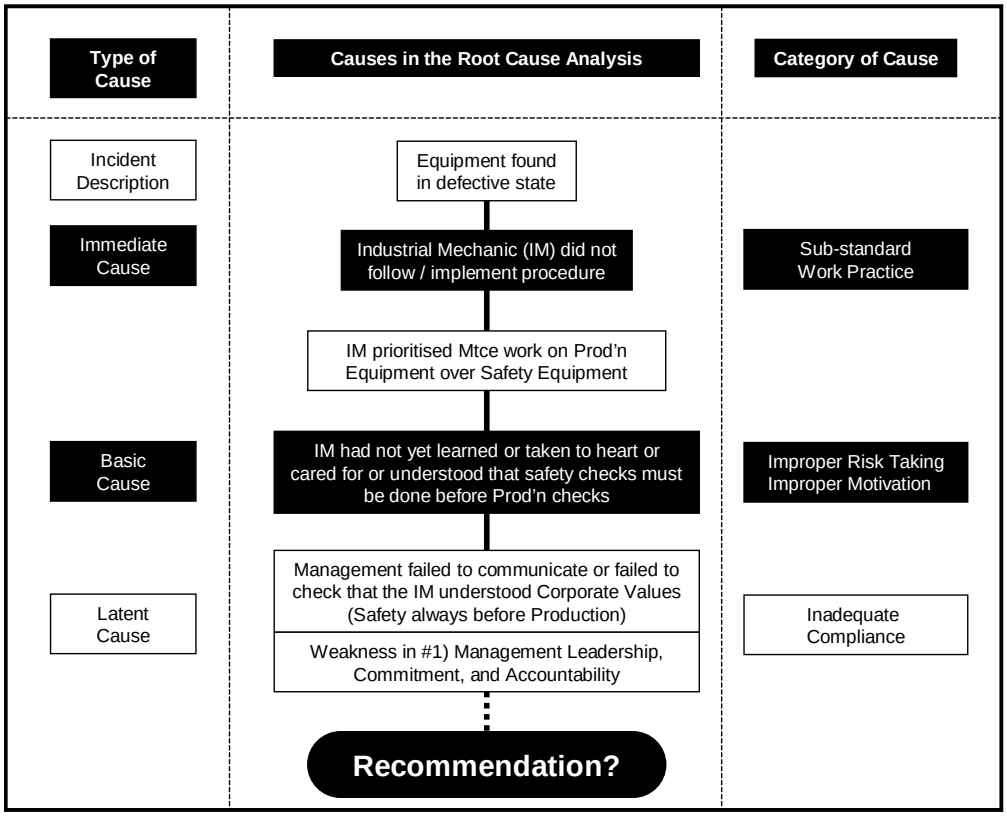
An Example of One Root Path in an RCA

One path of an RCA has been fully developed as shown below. For clarity and focus, the complete RCA is not shown. It can be seen in the example that the investigator has fully drilled down to a latent cause and has expressed the identified latent cause in terms of a weakness in a management system element.

With this clarity in the analysis, the action specific to the management system element becomes much more obvious, especially after some effort to determine:

- The latent cause (i.e., was it Management Commitment, Leadership, and Accountability (leadership and communication) or Employee Training and Competency?); and
- The category of cause (i.e., was it inadequate compliance to a well-documented management communication standard, an inadequate standard to document management activities, or an inadequate program (no management communication program))?

In this case, using the table on the next page, an appropriate recommendation could be stated as: *"Communicate Corporate Values to all employees during new employee orientation and on a bi-annual retraining basis, including a test for understanding of Corporate Values."* Can other possible and appropriate recommendations be stated?



Use the **Cause and Effect Model** as an aid if there is a need to revisit the basic causes when refining the statement of the latent cause.

Basic Causes		Latent Causes			
Type	No.	System Elements	P	S	C
Engineering & Design Factors:		1) Management Leadership, Commitment and Accountability.			
inadequate technical design		2) Risk Assessment and Management of Risks.			
inadequate ergonomic design		3) Community Awareness and Emergency Preparedness.			
inadequate assessment of loss exposures		4) Management of Change.			
inadequate standards, specifications and/or design criteria		5) Incident Reporting, Investigation, Analysis and Actions.			
inadequate monitoring of construction		6) Program Evaluation and Continuous Improvement.			
inadequate assessment of operational readiness		7) Design, Construction and Start-up.			
inadequate monitoring of initial operation		8) Operations and Maintenance.			
inadequate evaluation and/or documentation of change		9) Employee Competency and Training.			
		10) Contractor Competency and Integration.			
Job Factors:		11) Operations and Facilities Information and Documentation.			
Inadequate maintenance					
Inadequate job procedures					
Error-inducing conditions					
Organizational factors					
Incompatible goals					
Inadequate training					
Inadequate communication					
Personal Factors:					
Inadequate physical / physiological state / capability to do the work.					
Perceived inadequate mental / psychological state / capability to do the work.					
Physical or physiological stress.		P = inadequate program			
Perceived mental or psychological stress.		S = inadequate standards			
Improper risk taking / improper motivation		C = inadequate compliance			
Lack of knowledge / lack of skill.					

Section 4.6: Tools and Process for How to Prioritize Recommendations

Synonymous Terms:
In the context of this discussion on tools for prioritizing actions, recommendations are derived from the findings of the risk assessments or RCA.

- "Findings" are the "possible ideas" or the "possible risk reduction solutions" that can be identified from the risk assessments or from the RCA.
- The findings or possible risk reduction solutions are evaluated opposite certain criteria, ranked in order, and the top findings are selected to become the "recommendations" (i.e., recommendations are a sub-set of the findings).
- "Recommendation", "action", "recommendation for action", and "a risk reduction solution" are synonymous.

Many risk management activities (reviews, analyses, assessments, inspections, audits, engineering design studies / projects, incident investigations, and root cause analyses, to name a few) will generate a number of conclusions, a number of findings, or possible risk reduction solutions, and ultimately a number of recommendations. The recommendations usually draw management's attention because these will require resources and time, and there are limits to those resources.

Thus, management must carefully evaluate the findings to determine which ones are practicable, can be effectively implemented, and be effective when implemented; thus, turning possible risk reduction solutions into recommendations (i.e., any and all recommendations must have been validated, prioritized, and appropriately assigned as actions to make things happen). A method or means to prioritize the possible risk reduction solutions and select recommendations for implementation (actions) is needed, especially when there are quite a number of recommendations and limited resources.

Many tools and methods are available, ranging from the simple with few parameters and minimal scoring (on each parameter) for characterizing each of the possible risk reduction solutions, to very complex with numerous parameters and detailed and intricate scoring. A popular tool consists of three parameters: 1) speed (slow or fast); 2) quality (poor or good); and 3) price (cheap or expensive). With three parameters, and two scores for each parameter, one can quickly determine that there are nine (9) possible rankings. The lowest priority (and therefore most undesirable) possible risk reduction solution would have a ranking of "slow to deliver, poor quality of the finished item, and at high price". The highest priority (and therefore, the most desirable) recommendation would have a ranking of "quick delivery, the best quality available, and at the lowest price". While such a model may be quite suitable for scoring and ranking which mechanic will make repairs to your automobile, it is not suitable for ranking recommendations pertaining to risk management.

Three tools and one work process are presented for turning that long list of possible risk reduction solutions into a short and prioritized list of recommendations (i.e., actions to implement / risk reduction solutions):

1) **The Simple Effort vs. Gain Tool**
2) **The Complex Effort vs. Gain Tool**
3) **The Severity vs. Frequency Tool**
4) **The Work Process to Create a Key Set of Recommendations.**

1) The Simple Effort vs. Gain Tool for Quickly Prioritizing Actions

Consider the relation of **Effort versus Gain** as shown in the graph below. When evaluating and prioritizing a number of corrective and preventive actions, "pick the low hanging fruit" that "get the biggest bang for the buck" (i.e., the most gain for the least effort). The best solutions are those that are:

- Easiest to implement;
- Lowest cost to implement;
- Quickest to implement; and
- Reduce the risk the most (the most practicable and effective solution).

Effort and Gain are two simple criteria that can be used to quickly evaluate all recommendations. Other and more complex criteria can be used. For example:

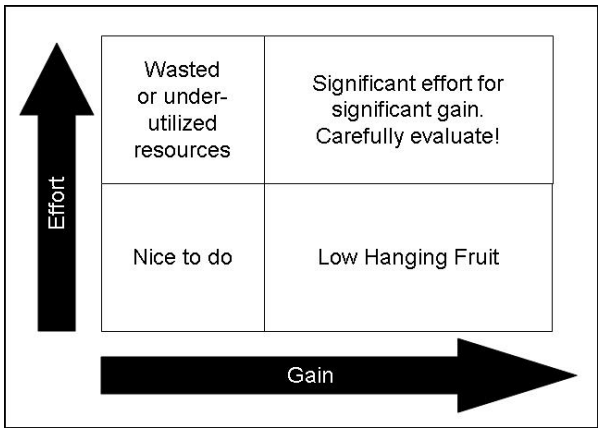
- **Effort** can be easily categorized as:
  - low effort = high priority;
  - high effort = low priority.

- **Effort** can be further described in reference to its **practicability** (which is not the same as practicality):
  - simple or known technology = high priority;
  - difficult / challenging / develop new technology or apply complex technology = low priority.
- **Effort** can be expanded to include:
  - costs (cost to implement, the cost to maintain the solution); low cost = high priority
  - time and duration (the time before the action can be implemented, the duration the solution must be maintained); quickest to implement = high priority
- **Gain** refers to:
  - The effectiveness of the solutions in reducing the residual risk.
  - The solution that reduces the risk from an unacceptable level to an acceptable level (i.e., the greatest reduction in risk level).
  - Or a combination of the above.
- To determine **Gain**: Typically, the persons with expertise and knowledge of the incident, the technology, the causes, and the scope and nature of the fix can make the best judgment on the effectiveness of the risk reduction solutions.

Low Hanging Fruit: The recommendations that are most effective for the least effort should rise to the top of the list of actions to implement.

Significant Effort for Significant Gain: Those recommendations that are most effective, but require significant effort should also be on the list of actions. First carefully evaluate to ensure that the costs to achieve the gain are acceptable; otherwise, management may choose to discontinue the activity (and eliminate the risk).

The Two Remaining Quadrants: The recommendations that remain are in either of the two remaining quadrants. Nothing should motivate a manager to waste money on minimal gain, although other motivators besides gain may come into play for the nice-to-do recommendations.



2) The Complex Effort vs. Gain Tool

The Complex Effort vs. Gain Tool is a refinement of the Simple Effort vs. Gain Tool in that it consists of discrete sub-factors that can be semi-quantitatively or quantitatively segmented for both Gain and Effort

The **Gain Index** of the complex tool is dependent on the effectiveness of a recommendation.
- Higher indices reflect recommendations with the ability to: a) address latent causes and prevent the incident; or b) attain the greatest risk reductions (largest reduction in risk level) (i.e., to eliminate the hazard / risk).
- Lower indices reflect recommendations with the ability to: a) reduce the impact of (mitigate) the loss incident; or b) attain lower risk reduction levels (i.e., reduce the impact of the hazard / risk).

In the Complex Model, Gain has four ratings. To determine the Gain Index, describe the effectiveness of the recommendation in terms relative to the technology base under study (i.e., what do Gain ratings of "1, 2, 3, and 4" mean, and then score the Gain as "1, 2, 3, or 4").

Gain Index	Gain Index Criteria (any one of or combination of)
4	➢ Addresses latent causes. ➢ Eliminates hazards or has the greatest reduction in risk levels. ➢ Eliminates initiating events.
3	➢ Addresses basic causes. ➢ Reduces risk levels to a lesser extent than "4". ➢ Prevents incident by eliminating subsequent condition splits. ➢ Eliminates impact in overall PEAP despite having an event.
2	➢ Addresses immediate causes. ➢ Reduces risk levels to a lesser extent than "3".

	➢ Minimizes impact significantly in overall PEAP (i.e., mitigates the consequence of an incident).
1	➢ Minimizes impact slightly in overall PEAP (i.e., mitigates the consequence of an incident). ➢ Does not address any cause. ➢ Reduces risk levels to a lesser extent than "2" or not at all.

The **Effort Index** of the complex tool is based on an overall scoring for the sub-factors of cost, timeline of implementation, duration of implementation, etc. In this Complex Model, Effort has six discrete sub-factors:

- Practicability: Solutions that are easy to implement, easily resolve or fix the issue, or where simple or known technology is applied reflect lower effort. Solutions that are difficult, challenging, or where new technologies (the technology does not exist / must be developed), or novel or complex technology are applied reflect higher effort.
- Initial Cost: Solutions that have a low initial cost reflect lower effort, whereas solutions that have high initial cost reflect higher effort.
- On-going Costs: Solutions that have low on-going costs reflect lower effort, whereas solutions that have high on-going costs reflect higher effort.
- Timeline (the amount of time before the action can be implemented (e.g., planning, communication, etc.): Solutions that can be implemented immediately reflect lower effort, whereas solutions that require a long lead time before implementation reflect higher effort.
- Duration (the amount of time it takes before the action addresses the relevant latent cause (e.g., training plan, Management of Change program, etc,): Solutions that take a short time to effectively address the latent cause reflect lower effort, whereas solutions that take a long time to effectively address the latent cause reflect higher effort.
- Frequency (how often does the action need to be repeated): Solutions that are one time only or have a low frequency of implementation reflect lower effort, whereas solutions that have a high frequency of implementation reflect higher effort.

	1 (high effort)	2	3	4 (low effort)
Practicability	difficult / challenging / develop new technology	apply complex technology	apply simple technology	**the solution is not technology**
Initial Cost	> $2M	$1M - $2M	**$0.1M - $1M**	<$100,000
On-going Costs	> 100,000 per year	$100K > cost per year > $10K	**<$10,000 per year**	no additional on-going cost
Timeline (the time before the action can be implemented)	implemented more than one year	can be implemented within 1 year	can be implemented within 3 months	**can be implemented immediately**
Duration (the time it takes before the action addresses the relevant latent cause)	**requires more than 3 months**	requires less than 3 months	requires less than one month	requires less than one week
Frequency (how often does the action need to be repeated)	once per month or more often	once per quarter	**once per year**	one-time

Applying the Complex Effort vs. Gain Tool

Typically, the persons with expertise and knowledge can make the best judgment as to the criteria indices and the scores for the Gain and Effort of a recommendation. Expertise and knowledge include the incident or the process technology under study, the findings of the investigation or risk assessments, and the scope and nature of the recommendation.

Indices and scoring each of those indices can be defined for the two factors (Gain and Effort), and the criteria for each of the indices for the sub-factors can be modified to suit the user. Using the tables above, consider any possible risk reduction solution.

- The Gain of the possible risk reduction solution may be scored as a "4: Eliminate initiating events and / or addresses root causes."
- The Effort of the possible risk reduction solution is scored on the six sub-factors, as denoted by bold text in the table above, and has a total Effort score of 18 (4+3+3+4+1+3).

- The total score for this particular possible risk reduction solution is 72 (4 x 18).
- Note: The suggested brackets for these sub-factors may not be sufficiently sensitive and may need to be adapted to the user's purposes. For example, suppose all of the possible risk reduction solutions are under $500,000 for Initial Cost. The current table would score these as either a 3 or a 4, which may not sufficiently differentiate the possible risk reduction solutions for ranking. In response, change the brackets on Initial Cost to something a little more sensitive (e.g., >$500,000; $200,000 - $500,000; $20,000 - $200,000; <$20,000). The description of the adaptation(s) and the rationale should be documented along with the criteria table.

The following table indicates the scoring for all six sub-factors of Effort. Conceivably, a set of risk reduction solutions could have a range of scores from 6 (1 x 6) to 96 (4 x 24). To differentiate between a 24 of "Low Effort" and a 24 of "High Effort", consider the Gain score. This ambiguity in scoring could be rectified by changing the scoring for Gain from 1, 2, 3, 4 to 1, 2, 4, 9, respectively.

3) The Severity vs. Frequency Tool

This Severity vs. Frequency Tool is adapted from *Industrial Accident Prevention* by H.W. Heinrich, Dan Petersen, and Nestor Roos (McGraw-Hill Inc., 1980). In almost all cases, recommendations are made to prevent, stop, control, or otherwise mitigate a hazard that could lead to a loss incident. It makes sense to evaluate a recommendation based on the risk it addressed. In consideration of the two factors of risk (consequence and probability), a recommendation can be evaluated: 1) on the extent to which it mitigates the hazard; and 2) on the frequency of a loss incident resulting from the uncontrolled hazard.

The first part of this tool consists of two parameters and four scores for each parameter: Severity (negligible, marginal, critical, and catastrophic) and Frequency (extremely remote, remote, reasonably probable, and probable).

The MIL-STD-882 standard, a US standard for safety system programs, quantifies severity with four parameters. Expressions relating to engineering safety and risk management are presented as follows:

- Negligible: will not result in personal injury or process / equipment / asset / environmental damage
- Marginal: can be counteracted or controlled without injury or major damage
- Critical: will cause injury or major damage, or will require immediate corrective action to prevent injury or major damage
- Catastrophic: will cause death or severe injury, or complete loss of asset or irrecoverable release / spill to the environment.

Similarly, frequency can be quantified as:

- Extremely Remote: a failure is expected in a timeframe of more than ten years
- Remote: a failure is expected between in one year to ten years
- Reasonably Probable: a failure is expected between one month to one year
- Probable: a failure is expected within one month

It can immediately be seen that the quantitative meanings of each score can lead to debate; thus, the team that evaluates the recommendations must agree upon the quantitative meanings of the scores before beginning to score and rank each of the recommendations.

Score Your Recommendations to Determine Positive Impact: As with the Simple Effort vs. Gain Tool, it is necessary to understand the potential for positive impact of the recommendation. To understand the potential for positive, apply the severity and frequency scores.

With four possible scores for each parameter, there are 16 possible rankings. Compare this with the four possible rankings from the Effort vs. Gain Tool: more complex tools require more precise definitions of each parameter and more detailed understanding of the impact of the recommendation as it pertains to the severity and the frequency.

The team, having gained or estimated these details to the best of their ability, scores each of the recommendations to arrive at a set of preliminary rankings. The ranking for each recommendation is simply a detailed method for quantifying the gain of an action. The upper part of the graphic below illustrates the ranking of recommendations on frequency vs. severity.

Determine the Immediacy of the Recommendations: To effectively move recommendations to actions, one must determine the immediacy of the action (i.e., when it must be initiated and completed). This is the second part of this tool, that is, the timeframe in which the action must be addressed and implemented. A simple guideline can be “do immediately” and “do within three months”. This may be adequate for “low hanging fruit” types of actions, but is inadequate for complex recommendations which may require engineering projects or long-range studies. A more suitable set of guidelines to manage a broader scope of actions is defined as:

- Drop it: Forget the action because the action is not worth doing. The issue is so negligible and so extremely remote that to address it is a waste of resources.
- Long range study: Submit to an engineering group for project design or for long-range study.
- One-year Correction: Establish a plan to complete the action within one year.
- Three-month Correction: Establish a plan to complete the action within three months.
- One-month Correction: Immediately initiate a plan to complete the action within one month. If a shutdown of the operation to effect repairs is required, then a shutdown of the operation within the month is required.
- Immediate Correction: Immediately initiate repairs to complete the action as soon as possible. If a shutdown of the operation to effect repairs is required, then shutdown the operation immediately.

As with the quantitative meanings of severity and frequency, the immediacy of actions is characteristic of the organization and the risks to which the organization is willing to be exposed. Team members must agree upon the set of guidelines for managing actions before determining the immediacy of those actions. Team members are directed to consult their organization’s corporate policies for guidelines on assigning timing of actions. These are in the form of policies and practices for occupational safety, process safety, construction project management, or maintenance turnaround management. The timeframe for completion may also be set by government regulations or agreements.

The Hazard-Action Table: After having determined the Severity-Frequency score for a recommendation, the “Immediacy” of that recommendation can be determined using the following Hazard-Action Table. An example best explains how to apply this table.

1) A recommendation has a scoring of “catastrophic” and “probable”. Find this point in the upper section.
2) Look in the lower section to find the indicated black box: therefore, the immediacy for the “catastrophic and probable” action is “Immediate Correction”.

HAZARD - ACTION TABLE				
	SEVERITY			
FREQUENCY	Negligible	Marginal	Critical	Catastrophic
Extremely Remote				
Remote				
Reasonably Probable				
Probable				
ACTIONS	ASSIGN IMMEDIACY TO THE ACTION			
Drop it				
Long-range Study				
1-Year Correction				
3-Month Correction				
One-Month Correction				
Immediate Correction				

Comments on Ranking Actions: As stated previously, team members are directed to consult their organization's corporate policy for prioritizing the immediacy of actions. However, there may be other stakeholders that influence priorities (typically to drive these actions to completion sooner rather than later). Personal experience and bias of managers may drive actions to completion sooner than corporate policy may direct. For example:

1) A recommendation has a scoring of "critical" and "remote".
2) Corporate policy, as may be illustrated by the above table, may dictate immediacy for this action as a "Three-Month Correction".
3) However, the operations manager may be biased (for any number of reasons, including personal experience in his or her professional career) to want to drive the action to completion sooner and may direct personnel to complete the action within one month.

As future employees of organizations, you must learn the corporate policies as well as understand any other influencers on those actions. Undertake appropriate reviews of the ranking of actions with your leader(s) to ensure stakeholder reviews and inputs.

Paralysis by Analysis: A Pitfall of Ranking Tools

The three models presented here ("Simple Effort vs. Gain", "Complex Effort vs. Gain", "Severity vs. Frequency") demonstrate that models can range from simple to complex. Indeed, there are innumerable tools for scoring, and each can be highly refined and quite specific for a particular organization, a particular problem, or a particular work process. One pitfall that can arise with ranking tools, and especially with complex tools, is "paralysis by analysis". This can occur at two points of the overall process.

1) Members of the team continue to select and refine a particular ranking tool in hopes of driving to a purely quantitative and objective ranking tool.
2) The team excessively spends time and energy to ensure the scores for "effort and gain" or "severity and frequency" for the recommendations are precisely and accurately known.

In both cases, the team the team defers action or fails to take action to address the issue and reduce the risks. This is known as "paralysis by analysis". Always check your team's activity and progress to avoid this trap.

While detailed analysis may reduce the risk of making a wrong decision about turning recommendations into actions, the time and energy may be more wisely expended on implementing the action. Of course, more complex methods are justifiably needed for evaluating high-cost recommendations; thus, more time and expertise are needed. "Value Engineering" and "Cost–Benefit Analysis" are two widely known methods, but are beyond the scope of this section.

Process to Create the Set of Key Recommendations

The set of key recommendations is derived from the findings (i.e., the latent causes as identified from an RCA or the process hazards as identified from the applied risk assessments). Recommendations should be actionable,

tangible, realistic, achievable, measurable, and written in a way that is clear with no doubts or ambiguities. Use the ESRM Program Elements or the set of process hazards as a guide for your recommendations. Note that many risk reduction solutions can be grouped in a manner to create a key recommendation, as described below (i.e., a recommendation in broad terms with specific deliverable actions or executable actions). This process consists of these major steps:

1) Generate the Preliminary Recommendations.
2) Prioritize the Recommendations.
3) Characterize Each of the Recommendations.
4) Do a "Reality Check".
5) Document the Recommendations.
6) Summarize the Recommendations.

Note: Steps 1) through 4) are "work in progress" and do not necessarily need to be formally documented.

1) Generate the Preliminary Recommendations

The findings are the possible risk reduction solutions as identified from either: a) the RCA that address the latent causes; or b) one or more applied risk assessment methodologies that address the process hazards and risks. To generate the preliminary set of recommendations:

- Take all of the possible risk reduction solutions identified previously and group these using a suitable common factor such as "by latent cause", "by management system element", "by process hazard", "by process unit operation", or other common factor.
- Group the detailed risk reduction solutions under a common and comprehensive recommendation.
- State the comprehensive recommendation in actionable terms. Describe what it is, how it is done, and what it addresses. These comprehensive recommendations with the detailed risk reduction solutions are the preliminary set.

2) Prioritize the Recommendations

The following process is used to prioritize the preliminary set to create a prioritized list of the key practicable recommendations (from highest to lowest):

- Characterize each of the recommendations using any of the three tools described above. The indices of the **Complex Effort vs. Gain Tool** are used here as an example.
- For due diligence and documentation to support recommendations, it is recommended to state the tool used to score and the criteria for scoring (i.e., the rationale for scoring the set of recommendations).
- Typically, the persons with expertise and knowledge of the incident, the technology, the findings of the risk assessments / investigation, and the scope and nature of the fix can make the best judgment as to the Gain and Effort of a recommendation.
- Determine the Gain Index and Effort Index (according to the tool selected).
- Determine the Total Score (Total Score = Gain Index multiplied by Effort Index).
- Rank your recommendations from highest to lowest using the Total Score. Ranking is the process to determine the priority (i.e., rank = priority; therefore, a ranked list is the same as a prioritized list and should be numbered and ordered starting with the highest priority).

3) Characterize Each of the Recommendations

Further characterize each of the key practicable recommendations, depending on the nature of the study:

- Nature of the Fix: Such a description helps managers more fully understand the scope.
  - Permanent one-time;
  - Permanent on routine / on-going basis for life-of-project or life-of-operation; or
  - Temporary until a Permanent fix is made.
- Latent Cause(s): For an II and RCA, state the specific latent causes that this recommendation is intended to address and the appropriate Management System Element(s).
- Process Hazards: For a risk assessment, state the specific process hazards that this recommendation is intended to address and the appropriate Management System Element(s), if applicable.
- These characterizations (nature, latent cause, or process hazard) are not used the ranking process.

4) Do a Reality Check

After the set of recommendations has been ranked, do a "reality check" on the order of the recommendations. Consider these questions, depending on the nature of the study:

- Will these really address the latent causes and prevent a loss incident?
- Will these really address the process hazards / risks and prevent a loss incident?
- Does the order of recommendations make sense?

- Iterate the previous steps as needed (i.e., re-score and re-rank if necessary).

5) Document the Recommendations
Document each of the key practicable recommendations in the final priority order including any necessary information, such as the scores and the characterizations (i.e., the list should be numbered and ordered from highest to lowest).

6) Summarize the Recommendations
Create a summary table of the key practicable recommendations in actionable terms, as shown below, depending on the nature of the study:

For an Incident Investigation and Root Cause Analysis

Rank	Recommendations	Gain Index	Effort Index	Total Score	Nature of Fix	Latent Causes Addressed	Alignment

For a Risk Assessment

Rank	Recommendations	Gain Index	Effort Index	Total Score	Nature of Fix	Hazards Addressed

Test the Risk Reduction Solutions

Much has been stated about selecting, prioritizing and managing recommendations and actions, but this effort is wasted if the risk reduction solutions are not effective. Risk reduction solutions should be tested against the risk studies (i.e., the II and RCA or the risk assessment) to determine the degree of risk reduction. It may be necessary to research the proposed solution to determine how successful or effective it is when implemented. This will determine the expected effectiveness of the action and will feed into the prioritization process as the Gain. Also, as already stated, a cost / benefit analysis should also be completed. This will feed into the prioritization process as the Effort.

Considerations for Evaluating and Selecting Risk Reduction Solutions

In risk studies, a number of actions (the risk reduction solutions) have been determined: these actions can form an action plan. Should all recommendations for risk reduction be implemented? What criteria are used to determine which ones, if any, should be implemented, versus simply discontinuing the activity? Who is involved in prioritizing, selecting, and implementing the solutions? How are risk reduction solutions implemented?

1) Criteria for Selecting Risk Reduction Solutions
Risk reduction solutions should be tested against risk studies to determine these factors:
- The simplicity or complexity of the solution: how easy is it to implement? Where feasible and known to be effective, simple and straight-forward solutions, besides being lower cost, do not introduce the possibilities of other hazards and risks that can be associated with complex solutions. Simple solutions (as long as they are effective) are preferred over complex solutions.
- The cost (people and resources) of the solution, not only in terms of initial cost (capital or initial large start-up expenditure), but also for on-going “expense” costs for people and/or materials and/or purchased services. A cost / benefit analysis may be necessary. In industry, it is not uncommon to discontinue an activity (permanently shut down a facility) because the costs to implement solutions to manage the residual risk outweigh the economic productivity of the facility. Lower cost solutions (as long as they are effective) are preferred.
- The effectiveness of risk reduction: how effective is the solution? You may need to research to determine prior success (e.g., compare the effectiveness of solutions implemented at other facilities, whether the same industry, related industry, or different industry) and, in some cases, undertake pilot-plant scale or lab-scale operations to test the effectiveness. Risk reduction solutions that substantially reduce risk are preferred over solutions that marginally reduce risk.
- The timeliness of implementation: can the solution be implemented within the short term or will it require extensive planning and execution before the solution is fully implemented?

2) Engaging Key Stakeholders

The decisions concerning the appropriate risk reduction solutions should include key stakeholders as much as possible and in far in advance. Management must reasonably engage key stakeholders in the decisions concerning the appropriate risk reduction solutions. The decision-making process includes prioritizing, selecting, implementing, and checking the effectiveness of the risk reduction solutions. In the early stages of selection, stakeholders can include senior management, the public, and government. This ensures that all key, high profile issues are being addressed in a manner consistent with corporate policy and public (government) policy. In the latter stages, (design, implement, and use / apply) key stakeholders must include the Manager, the Designer, and the User. This strives to make this a team effort and to obtain "buy-in" at the working level.

One group of stakeholders that must be considered and involved in the processes is those who are exposed to the risks. What might seem acceptable to the decision-makers (in terms of the risk of the activity or the risk reduction solutions) may not necessarily be acceptable to these stakeholders. The evaluation of risk levels and the selection of risk reduction solutions should include these stakeholders.

3) Implementing Risk Reduction Solutions

Recommendations and actions (i.e., the action plan), have their potential value truly realized when those actions are effectively implemented. To move from a list of risk reduction solutions to an effective and action plan, an owner must be identified for these risk reduction solutions. With rare exception, it is the head manager of the organization in which the actions will be implemented who is identified as the action plan owner. An effective manager exercises ownership for their action plan with these tasks:

- List actions by priority (and category, if meaningful).
- Assign owners (e.g., the person responsible for completing the action).
- Assign a realistic due date by which the action is completed and implemented.
- Ensure the action plan (i.e., the list of actions) is communicated to appropriate stakeholders.

An effective manager has a bias for action. He or she regularly checks the status of progress on all actions. Are the action item owners making progress? Have they met any hurdles or barriers where they may need help? As the reader can no doubt sense, the term “owner” means they are responsible for that action, getting it completed and implemented effectively, by the due date, and within budget (if funds have been budgeted).

For major studies, there can be many actions required. These actions can have different priorities for completion with short-, mid-, and long-term end dates, and should be assembled into an overall completion plan including bar chart, arrow diagram, project planning system, etc. Highly complex action plans may require a project manager, and progress may be reviewed / stewarded with senior management. The effective project manager should anticipate this, should provide regular updates to senior management, and open communications immediately if major issues arise that impede progress. The priorities of the actions and action plans must fit into the priorities of the operation, and this is the most effective way to reduce overall risk.

As with any plan, action plans can change: priorities, owners, due dates, resources needed or resources available, and even the scope of the action may change. Thus, communication of the changes to all involved is important, so as to ensure the stakeholders are well-informed and can re-evaluate earlier decisions. For example, senior management may take action to influence or affect those changes (i.e., make more resources available or even decide to stop the plan altogether and discontinue the activity associated with the risk reduction solutions). As well, each change should be reviewed for risks before implementation (**Chapter 3.4: Management of Change**).

ENGG404

Chapter 5: Tools for Risk Management

Section 5.1: Tools that Support Leadership in Risk Management

Recall these two definitions:
- **Hazard**: A potential source of serious harm to people, environment, assets or production (PEAP).
- **Risk**: The possibility of injury, loss, or environmental incident created by a hazard. The significance of risk is a function of the probability of an unwanted incident and the severity of its hazard (i.e., the consequence).

Within the field of engineering safety and risk management, several methodologies (processes, tools, methods, and approaches) are widely practiced with the intent to identify, analyze, and assess the hazards and risks associated with activities in industrial, commercial, and institutional operations. The overarching purpose of these is to:
- identify risks that are at unacceptable levels;
- generate risk reduction solutions that are intended to reduce risks to acceptable levels; and
- implement the most optimum risk reduction solutions to manage risks (risks that are associated with activities) to PEAP so as to prevent an incident or mitigate the consequences should an incident transpire during the course of that activity.

By using the methodologies to conduct these planned reviews, management can make informed decisions about the risks associated with their operation's activities and ultimately prevent a loss incident.

The tools and information presented in this chapter are meant to enable students to become leaders in risk management: to enable them as future managers / leaders in the workplace to talk to people (the workers), to interview them about their safety concerns (i.e., hazards in the workplace), to demonstrate how to use these tools to improve the workers' effectiveness in using these tools, and to coach the workers on how to manage risks in their jobs. Hence, course learners need to have a good understanding of the tools presented herein.

The implementation of these tools at the coaching level trains managers to be effective as leaders in risk management. It also raises the visibility of the manager in a useful and productive manner and thus demonstrates management commitment. Note that **Root Cause Analysis** and **The Cause and Effect Model for Incident Analysis** are missing from the list. These are causal analysis tools of loss incidents to determine latent causes (see Chapter 4); it does not assess risks (probability or consequence) either qualitatively or quantitatively.

Section 5.2: The Fundamental Approach to Control All Risks

A standardized, fundamental approach to control all risks is termed as **Risk Reduction Solutions**. Risk Reduction Solutions is a hierarchy of controls (i.e., an order of effectiveness for identifying, evaluating, and selecting risk reduction solutions). Note that this is an order of effectiveness and not an order of priority.

The approach to control any risk is to seek possible risk reduction solutions in order of effectiveness. This order of effectiveness is leading practice in industry because the higher the order of effectiveness, the lower the probability that human factors will come into play. Moving down the list of industry practices (numbered 1-5, as shown below) introduces more human factors and the possibility of the risk being mismanaged increases.

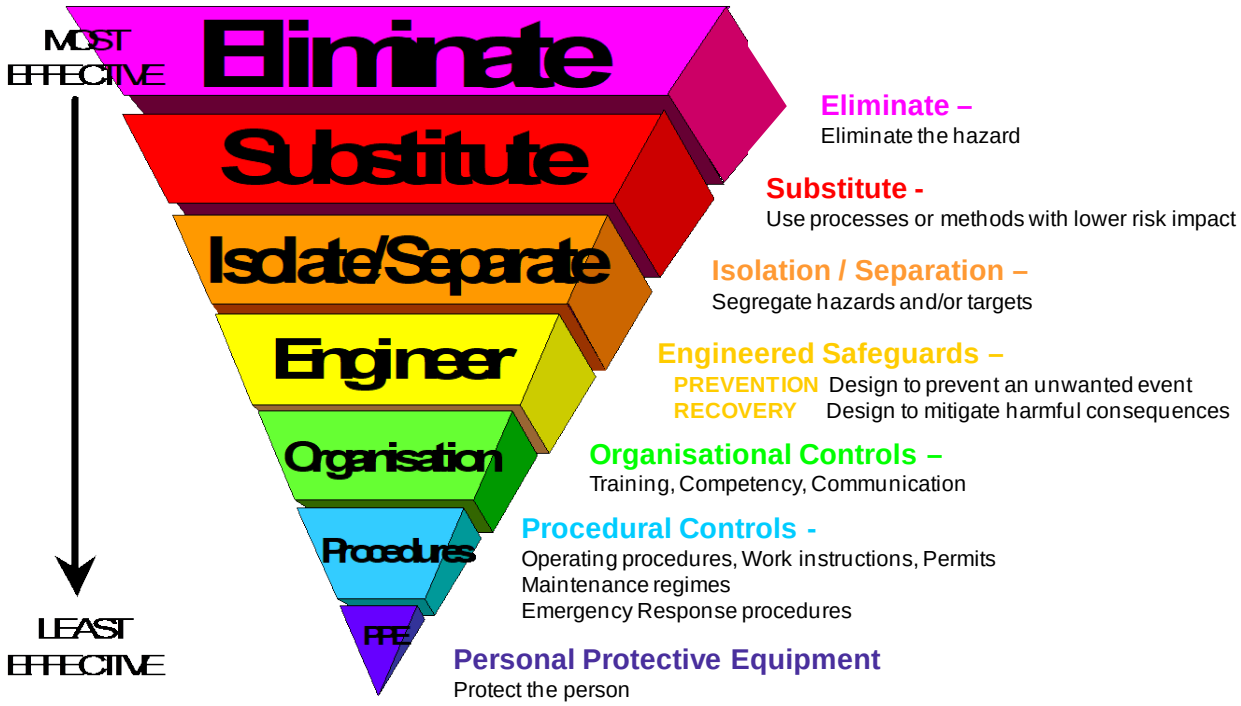
The Alberta Occupational Health and Safety Code, Part 2 Hazard Assessment, Elimination, and Control, Section 9, specifies the order of effectiveness. Industry practices generally align with or exceed the requirements with these widely practiced measures:

1. **Eliminate** the hazard. This solution is the most effective measure and can be done by removing the hazardous substance or stopping the hazardous activity. Some principles of Inherently Safer Design can achieve the same objective.
2. **Apply Engineering Controls**. If the hazard cannot be eliminated, then apply engineering controls to control the hazard. Engineering Controls can include the elimination of the hazard or applying the remaining principles of **Inherently Safer Design** (moderation, substitution, and simplification). The aim is to "design out" the hazard (thus, no risk) or include designed controls as part of the package. Some examples:
   - Contact can be prevented by using enclosures, machine guards, and worker cages.
   - Exposure can be prevented by using enclosures, ventilation systems, or reducing the quantity or concentration of the harmful substance in the work area.
3. **Apply Administrative Controls and Work Practices to Reduce the Exposure**: Control the hazard through administrative controls (policies, standards, procedures) and work practices. These measures are the next least effective and should only be used if the previous solutions are not feasible. One means to minimize exposure is to reduce the number of times the hazard is encountered. Consideration might be given to modifying steps

which are hazardous, changing the sequence of steps, or adding additional steps (such as locking out energy sources).
   - Administrative Controls can include policies, standards, procedures, permits, education and training, communications, organizational controls, and auditing.
   - Work Practices involve the execution or application of the Administrative Controls. To be effective, the work practices must comply with requirements of the Administrative Controls. These activities can include meeting standards of skilled trades know-how, following work procedures, good housekeeping, proper labeling, proper storage, personal / industrial hygiene, rules compliance, and reinforcement of work practices.
4. **Use Personal Protective Equipment**: Protect people from the hazard using personal protective equipment (PPE). PPE is typically not considered to be anything more than contingency protection: it is the last line of defense and should not be considered the sole or primary means to prevent an injury. The reliance on these measures should only be used if the previous solutions are not feasible. Where the use of appropriate personal protective equipment is required, emergency facilities (such as eyewash stations and safety showers, automatic defibrillators) should also be provided to reduce the severity of an incident should one occur.
5. **Use combinations**. A combination of the above is acceptable where and when a greater level of worker safety is provided.

Applying the Risk Reduction Hierarchy – Inherent Safety Principles:

What more can be done *to further reduce the risk?*
Are these risk reduction measures ***reasonably practicable****?*



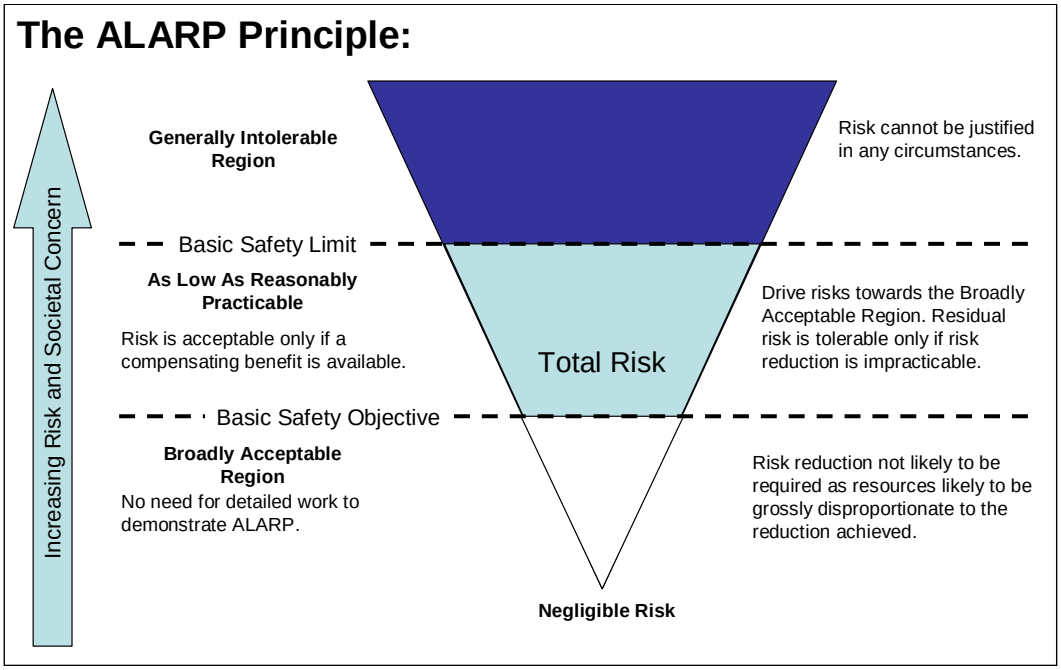
Graphics courtesy of E. Wakley & T. Humbke, Shell Canada.

Reducing Risks to As Low As Reasonably Practicable (ALARP)

In selecting risk reduction solutions, the manager's goal is to reduce the risk to as low as reasonably practicable (ALARP). The ALARP principle considers the practicality of an action, and the costs and benefits of action or inaction. While ALARP is not a true cost / benefit analysis, the notion of knowing that the action is worthwhile (or not) must enter into the decision-making process. The thorough application of ALARP requires:

a) a detailed cost / benefit analysis (e.g., the costs for the risk reductions solutions must be estimated within a reasonable range (+/- 10%, +/-25%, or other ranges, depending on the stage of the project and the method applied for estimating the costs) and the potential or expected savings as a result of those risk reduction solutions must also be estimated within a reasonable range); or

b) empirical estimates based on historical performance within the organization. The cost / benefit analysis need not always be a positive return (as there are other non-tangible benefits of risk management such as "social license to operate") to proceed with a project, but management must be aware of the costs and the benefits to make an informed decision. The exploration of the cost / benefit analysis is not within the scope of this chapter.



Adapted from APEGA Risk Management Guidelines, Ver. 1, September 2006.

Section 5.3: Field Level Risk Assessment (FLRA)

The Field Level Risk Assessment (FLRA), as the name implies, is used by workers who are about to perform work, in the field. The "field" is the job-site or work-site (i.e., the place where workers are about to do their work). There are three key purposes of the FLRA:

1) It is for workers to assess hazards and to eliminate or control those hazards before starting work (the job at hand).
2) It is used to share and communicate the nature of the job and the hazards associated with that job when working on a crew / team / group.
3) It is used to ensure understanding of the control measures to eliminate or mitigate the hazards when working on a crew / team / group.

In some uses, probability is a factor; however, the underlying assumption is that if there is a hazard, then there is a probability an incident will occur, so action must be taken to address the hazard. For example, an electrical extension cord is running along a busy walkway and poses a tripping hazard. It is assumed that someone will trip on it in the foreseeable future (i.e., probability is 1).

- An effective control measure: eliminate the tripping hazard by removing it, re-routing it, or covering it.

- An ineffective control measure: place a placard or flagging near it to alert a worker or to broadly communicate to everyone to “watch out for extension cords on the walkways”.

The FLRA is for “the here and now” of the job (in real time) and can supplement a Job Safety Analysis (JSA) and/or a Standard Operating Procedure (SOP). It is intended to address hazards and risks that may not have been anticipated when the JSA or SOP was written. The FLRA provides an additional level of care and control for unanticipated hazards, so that work can proceed safely nonetheless. However, it is the last proactive step to manage risk exposure in the workplace to prevent injuries.

The Basic Steps to Create an FLRA

1) Identify the job and job scope.
2) Determine the macro-steps or major tasks of concern in the job. (Note: The FLRA can also be used as a rudimentary job planning tool if all steps or tasks of the job are noted.) If a JSA/SOP is being used, identify tasks and hazards that are not identified in the JSA/SOP.
3) Identify the hazards of each of those tasks.
4) Determine the risk for an incident to happen associated with each of the hazards for each of the steps. (Some FLRA methods do not document this step in practice.)
5) Identify suitable control measures for each of the identified hazards.
6) Re-assess the risk after these control measures are included as part of the job execution. Answer the question: “Is the risk acceptable or are more control measures needed?”
7) Most importantly, communicate / share the FLRA with co-workers.
8) Implement control measures, and do the job (i.e., execute or perform the sequence of steps or tasks).
9) Continually re-assess risk throughout the job (especially if conditions change).

Note that the FLRA provides an additional level of detail on tasks, and care and control for unanticipated hazards, so that work can proceed safely nonetheless. If the risk from these hazards cannot be satisfactorily addressed via the FLRA owing to factors beyond the worker’s control, work should be stopped and a formal JSA analysis conducted to formalize more robust controls.

There are many variations of an FLRA (e.g., the 3-column and 5-column versions as seen below). Examples from industry are shown in the following pages.

Job Scope:		**Workers:**	
#	**Task or Step:**	**Hazards**	**Control Measures**

Job Scope:		**Workers:**			
#	**Task or Step:**	**Hazards**	**Risk**	**Control Measures**	**Risk**

Date: ____/____/____ **Work Order #**_____ **N/A** ☐ **Company:** _____

Job Description _____

Pre Task Analysis must be completed at Job Site

Pre Task

Permits

- ☐ Obtained Required Permits
- ☐ Permit Receiver Confirmed Job Isolated
- ☐ Meet all Permit Conditions/Discussed with Crew
- ☐ Signed on to Exempt Job List
- ☐ Signed into Block/Unit
- ☐ Confined Space/Temporary Enclosure

Emergency

- ☐ Know location of Nearest Communication System
- ☐ Know location of Nearest Safety Shower/Eyewash
- ☐ Working Alone Requirements Met
- ☐ Know location of Nearest Assembly Point
- ☐ Know Evacuation Route/Alarms
- ☐ Know Wind Direction

PPE

- ☐ Available
- ☐ Trained in Use
- ☐ Inspected/In good condition
- ☐ Additional PPE Required

General

- ☐ Discuss Job Hazards with Crew
- ☐ Review Job Package
- ☐ Follow Procedure Use Policy
- ☐ MSDS/Labels Reviewed

Pre Task Triggers

Overhead Work

- ☐ Barricades
- ☐ Signage
- ☐ Workers in Area
- ☐ Flagging

Tools/Equipment

- ☐ Correct Tools for Job
- ☐ Tools/Equipment Inspected
- ☐ Qualified to use Tools/Equip.
- ☐ Tool Potential to Slip
- ☐ Tool Potential to Fall

Ergonomics

- ☐ Awkward Body Position
- ☐ Over-extension
- ☐ Sustained Position
- ☐ Repetitive Motion
- ☐ Twisting Motion
- ☐ Pre Task Stretch/Warm Up
- ☐ Reaction Forces

Elevated Work

- ☐ JLG/Mechanical Lift
- ☐ Scaffold/Ladder Use
- ☐ Gin Wheels (Pulleys)
- ☐ Hoisting Tools/Equipment/Materials

Environmental

- ☐ Spill Potential
- ☐ Waste Handling Plan Required
- ☐ Waste Containers Available
- ☐ Gasket Disposal
- ☐ Containers Labeled

Lifting/Pulling/Pushing

- ☐ Manual Lift/Pull/Push
- ☐ Assistance Required
- ☐ Mechanical Lift (Crane, Chain Fall)
- ☐ Condition of Equipment
- ☐ Correct Rigging Practice
- ☐ Excessive Force
- ☐ Crane Lift/Checklist

Electrical

- ☐ Extension Cord Inspection
- ☐ Work On/Near Energized Equipment
- ☐ Procedure Required
- ☐ GFCI Test
- ☐ Qualified
- ☐ Voltage _____

Housekeeping

- ☐ Aisleways/Walkways Clear
- ☐ Trash Containers Available
- ☐ Congestion
- ☐ Loose Debris/Materials
- ☐ Hoses Coiled/Correctly Stored

General

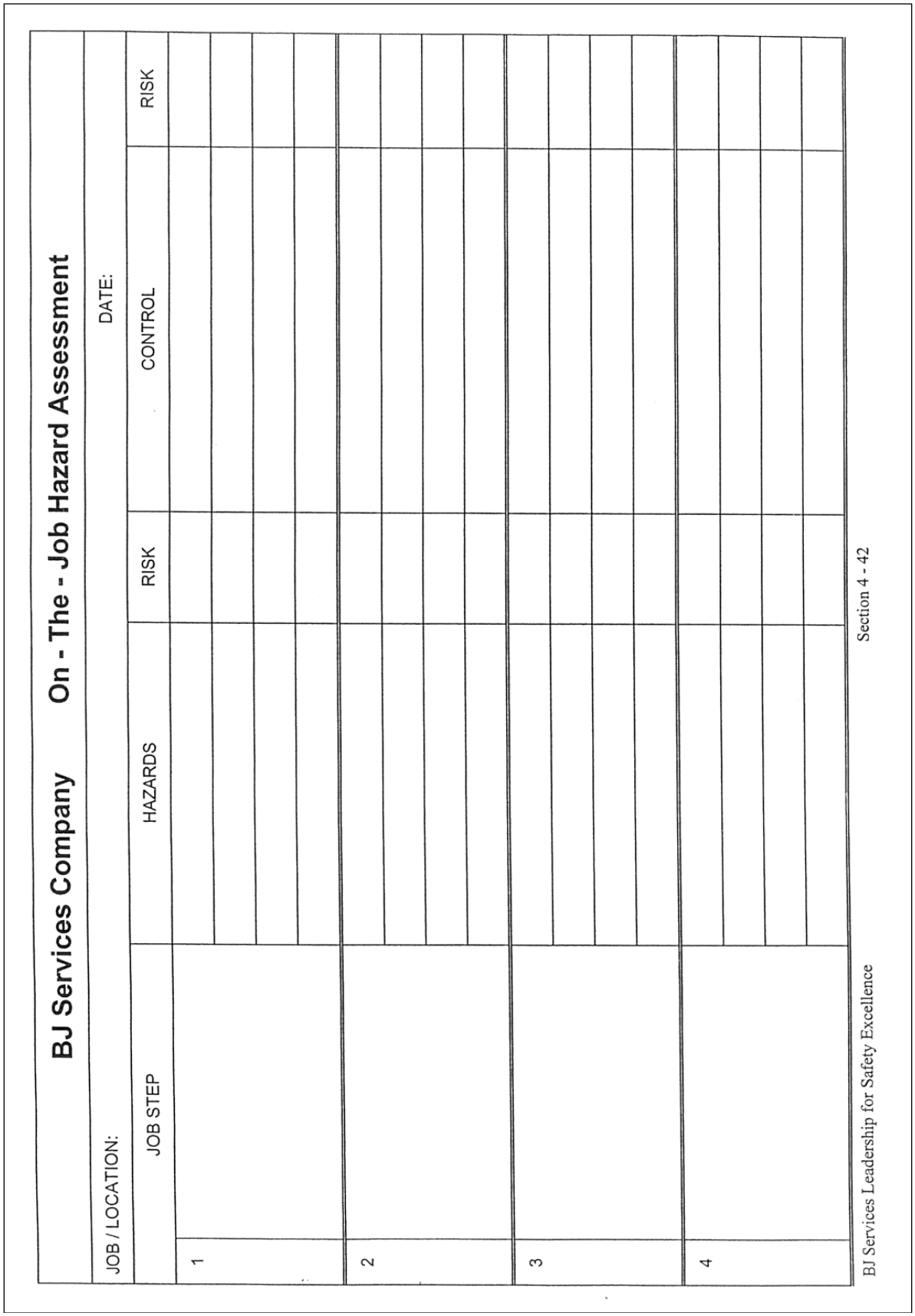
- ☐ Hot/Cold Surfaces
- ☐ Procedure Available
- ☐ Pinch Points
- ☐ Slip Potential
- ☐ Trip Potential
- ☐ Fall Potential
- ☐ Sharp Objects
- ☐ Tight Clearances
- ☐ Reactive Chemicals
- ☐ Industrial Hygiene
- ☐ Rotating Equipment
- ☐ Pressurized Lines/Equipment
- ☐ Weather Conditions
- ☐ Adequate Lighting
- ☐ Access/Egress

Name(s) _____
Please Print Names of All Crew Members

Sign On: _____
Have Participated in the PTA Discussion/Analysis

Post Job Checklist	Yes	N/A
Job Cleaned Up	☐	
Permit Signed Off	☐	☐
Job Package Feedback Completed	☐	☐
Job Package Returned	☐	☐
Signed Out of Block/Unit	☐	☐

Example FLRA Form



BJ Services Company On - The - Job Hazard Assessment

JOB / LOCATION: DATE:

	JOB STEP	HAZARDS	RISK	CONTROL	RISK
1					
2					
3					
4					

BJ Services Leadership for Safety Excellence

Section 4 - 42

Section 5.4: Semi-Quantitative Risk Assessment

The Semi-Quantitative Risk Assessment is a method that combines the risk analysis and risk assessment steps into one seamless but iterative process. It is sometimes referred to as the Simple Risk Assessment. It is important to note that a semi-quantitative method compares an estimated risk level with the benchmark risk level, with both being determined using the same basis (i.e., the same Consequence Scale and the same Probability Scale (the axes on the Risk Matrix or accompanying risk table)).

The method is based on the fundamental risk function of probability and consequence. A risk is determined before (or without) control measures. The risk is compared to the organization's risk standards (as may be documented in a risk matrix): if the risk is not acceptable, additional control measures are planned for implementation, and the risk is assessed again to determine if these planned changes will further reduce the risk. This cycle may be repeated until the residual risk is reduced to within acceptable level.

Management makes the decision to proceed if satisfied with all of the additional control measures and is agreeable to implementing them to achieve the desired residual risk level. If management is neither satisfied nor agreeable, or if all studies have exhausted all possible control measures and the residual risk is not acceptable, then the decision must be to not proceed. The semi-quantitative risk assessment table captures this iterative process, as shown further below.

How to Conduct a Semi-Quantitative Risk Assessment

This method is almost always done by a multidisciplinary team. This team should have a combined and complete understanding of the system to be reviewed. The team must reach agreement on the following:

- a statement of objectives;
- a clear definition of the system(s) to be analyzed;
- design and operational details of the system;
- a listing of principal concern categories;
- a listing of all known assumptions and constraints;
- the time constraints which govern the risk assessment; and
- the personnel required (and available) to support the risk assessment at various stages.

The team must also have management's support and commitment to implement key recommendations that evolve from the study. Once a risk is identified, management has an ethical responsibility to reduce the risk to an acceptable level before proceeding with the activity. (*Professional engineers and geoscientists also have a professional responsibility.*)

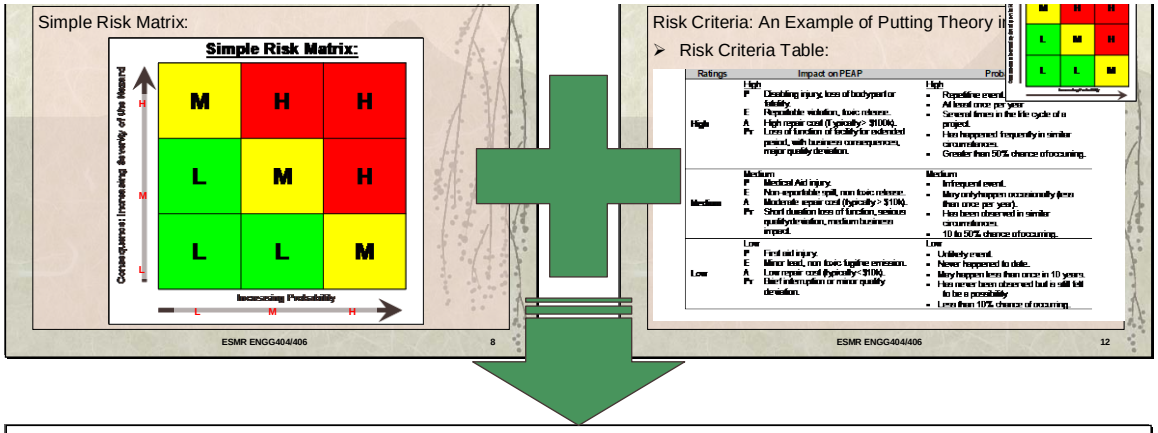
The assessment is done using a tabular form. The risk assessment is done on a particular activity within and under normal operations, before any particular incident. It addresses the scenarios that could potentially happen, their impact, and their probability. It also describes the level of risk involved, the recommended controls, and estimated residual risks to manage after controls have been implemented.

While conducting a Semi-Quantitative Risk Assessment, consider:

- These fundamental questions:
  - What could go wrong?
  - How could it affect me?
  - How likely is it to happen?
  - What can I do about it?
- The following specific to the procedure:
  - Identify activities and hazards
  - Assess hazard (consequence)
  - Assess probabilities (frequency)
  - Assess risks
  - Determine precautions
  - Assess residual risk (the risk that you are willing to accept and now need to manage)
  - Decide follow-up actions
- Consider the Risk Acceptance Criteria (The Risk Matrix)
  - Unacceptable risk (therefore, risk controls required)
  - Acceptable risk (some risk controls will be needed and justified by this process)
  - After assessing the risks, precautionary actions are identified. It is important to note that precautionary actions may bring more risk, which needs to be carefully reviewed, per the Management of Change process.

- Risks associated with the new actions are determined, and associated follow-up activities are carried out. Any change can add risk.

Recall that the Risk Matrix and Risk Criteria Table are integrally used in the Risk Assessment. Note: Impact is the same as “Consequence” in the following examples.



Generic Semi-Quantitative Risk Assessment Table Template:

Event Key Factors	Deviations	Prob-ability	Impact	Risk Before Control Measures	Control Measures / Safeguards	Change in Prob-ability	Chang e in Impact	Residual Risk	ProceedY /N?

Examples of Different Semi-Quantitative Risk Assessment Templates

There are many different versions of the Semi-Quantitative Risk Assessment (SQRA) table as shown in the four blank templates and the examples below. Although each has been tailored by the users to meet their specific needs, the fundamental steps of determining the risk of an activity before and after controls are evident. These are a sampling of the wide variety used by corporations, government agencies, and by risk management specialists. Note: Impact is the same as consequence in the following examples.

Item	Concern	Impact Rationale	Impact	Probability Rationale	Probability	Risk Before Control Measures	Control Measures & Safeguards	Change in Probabilty	Change in Impact	Residual Risk

Event Key Factors	Deviations	Probability	Impact	Risk Before Control Measures	Control Measures & Safeguards	Change in Probabilty	Change in Impact	Residual Risk

Event Key Factors	Deviations	Probability	Impact	Risk	Controls	Change in Probabilty	Change in Impact	Residual Risk

Event Key Factors	Deviations	Probability	Impact	Risk	Controls	Residual Risk

Note: Impact Rationale is the same as Consequence in the following example.

Semi-Quantitative Risk Assessment Example: "City Centre Power Failure"

FAILURE OR LOSS SCENARIO	EFFECT	CONSE-QUENCE	PROB-ABILITY	RISK	RISK CONTROL	RESIDUAL RISK
Loss of light in offices	Reduced work productivity	M	L	M	Provide backup power Reschedule work hours Add lighting	L M L
No traffic lights	Increased traffic congestion Major Traffic accidents Minor traffic accidents	L H M	H L L	M H L	Traffic officers Traffic officers No change needed	L M L
Difficulty while inside buildings	Injuries	H	M	H	Emergency lighting warnings	M-L
Fire occurs during outage	No smoke detectors Difficulty getting to fire	H H	L M	M H	Extra staff Battery back-up Position trucks at key locations	L M
Reduced people controls	Crime	H	M	H	Increased security	M

An Example of the SQRA as Applied in the Oil Sands Industry

This SQRA is a risk assessment worksheet for a propane-filling depot under normal operations. This was done before any particular event.

Item	Concern	Impact Rationale	I	Probability Rationale	P	Risk	Controls	Residual Risk
Propane Tank	Leak	Loss of inventory or small fire	L M	Highly unlikely since tanks is code built and tested	L	M	Leak test system before commissioning	L
	Catastrophic failure	Explosion and fire causing injuries and property destruction	H	Tank is protected from over pressure by relief valve. Fire or external impact could damage tank	L	M	Provide security barrier around tank. Post evacuation notices in even of fire.	L
Piping	Flow restriction	Inconvenience to user. May present fire hazard	L	Debris or corrosion products in line. Possible ice plug	M	M	Regular maintenance. Provide heat trading on line to prevent freeze-up. Develop filling procedures.	L
	Leak	Loss of inventory. Small fire	H	Piping subjected to abuse may develop leaks at connections	M	H	Regular lead testing. Erect "no smoking" signs and remote isolation valve.	M
	Rupture	System depressured. Large flash fire possible, involving the tank.	H	Highly unlikely if quality piping system installed. External object could strike piping	L	M	Install bracing and shield around piping. Design regulator to quick shut-off if downstream pressure drops rapidly.	L
Metering	Calibration error	Customer overcharged. Poor public relations	M	Not likely, given the frequency of refilling the storage tank	L	L	Keep accurate records and calibrate system on a regular basis.	L
	Valve may freeze open	Cannot shut off system causing spill	H	Unlikely if system is designed properly	L	M	Trace circuit. Install emergency shut-off	L
Customer	Spill propane on ground or on hot surface	Fire or explosion	H	Possible but not likely	L	M	Post-operating instructions and hazards warnings. Install quick shut-off.	L

Legend: I = Impact; P = Probability; (L = Low, M = Medium, H = High). Source: Syncrude Canada Ltd.; used with permission.

Section 5.5: The Canadian Centre for Occupational Health and Safety (CCOHS) Job Safety Analysis Model

The Canadian Centre for Occupational Health and Safety (CCOHS) provides a method and template for developing a job safety analysis (JSA). A JSA is a procedure which helps integrate accepted safety and health principles and practices into a particular task or job operation. The CCOHS method and template are available at: http://www.ccohs.ca/oshanswers/hsprograms/job-haz.html

The CCOHS JSA Model has been revised and adapted for use within ENGG404. Although heavily based on the CCOHS Model, some terms have been re-phrased to align with terminology in ENGG404, as well as to expand its application for use in any hazard assessment plan, whether it be a **Field Level Risk Assessment** (the details of the "here and now"), a **Job Safety Analysis** (how do I perform this job or this type of work), or a high-level project overview. It should be noted that a JSA can be used to create and document **Safe Operating Procedures** (SOPs).

Why do a Job Safety Analysis?

It is important to diagnose potential hazards in your workplace before they become a problem. There are methods to conduct a job safety analysis and minimize / eliminate hazards so they can be avoided. JSAs, also called a job hazard analysis or a job task analysis, use a systematic approach to identify hazards related to a job (a set of tasks) and to determine the appropriate control measures. It demonstrates:

a) that the employer has properly planned the work (an efficient job plan and/or procedure);
b) that workers can do the work safely (job can be executed with risk of injury minimized);
c) due diligence when practiced (a job plan / procedure is documented and suitable for training, checking, and qualifying competency, and for execution of work); and
d) effective change management (for managing changes in equipment, personnel, materials, and the procedure itself).

The application of a JSA (and SOP) is one of the best injury prevention tools that exist.

What is a Job Safety Analysis?

A JSA is a procedure that helps integrate accepted safety and health principles and practices into a particular task or job operation. In a JSA, each basic step of the job is to identify potential hazards and to recommend the safest way to do the job. Other terms used to describe this procedure are job hazard analysis or job hazard breakdown. To be effective, a JSA must cover all aspects (the major tasks or steps) of a particular job. A particular scope of work or project may require several jobs, and thus several JSAs (i.e., one for each job). A JSA can be modified for a specific job (e.g., build scaffold can be modified for work in a warehouse or for work in a petrochemical plant).

Some individuals prefer to expand the analysis into all aspects of the job, not just safety. This approach is known as total job analysis. The methodology is based on the idea that safety is an integral part of every job and not a separate entity. In this document, only health and safety aspects will be considered.

The terms job and task are commonly used interchangeably to mean a specific work assignment, such as operating a grinder, using a pressurized water extinguisher, or changing a flat tire. JSAs are not suitable for jobs defined too broadly (e.g., overhauling an engine) or too narrowly (e.g., positioning car jack). Think of a job as a set of tasks or major steps and a project as a series of jobs. Overhauling an engine is a project, whereas hoisting an engine and removing a crankshaft could be two of a number of jobs in the project. Parallels could be drawn for work in laboratories.

What are the benefits of doing a Job Safety Analysis?

One of the methods used for carrying out a JSA is to observe a worker actually performing the job. The major advantage of this method is that it does not rely on individual memory and that the process prompts recognition of hazards. For infrequently performed or new jobs, observation may not be practical.

Another approach is to have a group of experienced workers and supervisors complete the analysis through discussion. An advantage of this method is that more people are involved in a wider base of experience and promoting a ready acceptance of the resulting work procedure.

Initial benefits from developing a JSA will become clear in the preparation stage. The analysis process may identify previously undetected hazards and increase the job knowledge of those participating. Safety and health awareness is raised, communication between workers and supervisors is improved, and acceptance of safe work procedures is promoted.

A JSA, or better still, a written work procedure based on it, can form the basis for regular contact between supervisors and workers. It can serve as a teaching aid for initial job training and as a briefing guide for infrequent jobs. It may be used as a standard for health and safety inspections or observations. In particular, a JSA will assist in completing comprehensive incident investigations.

What are the Basic Steps to Conducting a JSA?

The following basic steps apply when conducting a JSA of any type.

1) **Select the job** / job scope / nature of work to be analyzed.
2) **Identify job steps:** Break the job down into a set of major tasks or sequence of steps; write the steps in the job.
3) **Identify hazards:** Identify potential hazards or potential incidents associated with each step.
4) **Assess risk:** Determine risk posed by each hazard before control measures / safeguards are implemented.
5) **Identify control measures / safeguards** for each hazard: Determine the control measures / safeguards and/or preventive measures and/or critical work practices (workplace behaviours) to eliminate / minimize / overcome / mitigate each of the hazards.
6) **Re-assess risk:** Determine risk posed by each hazard after control measures / safeguards are implemented.
7) **Review and discuss the JSA** with the workers; set the expectation that the workers will follow the JSA (i.e, to implement control measures).
8) **Execute the Work.**

What do you need to know when Selecting the Job for JSA Analysis?

Ideally, all jobs should be subjected to a JSA. In some cases, there are practical constraints posed by the amount of time and effort required to do a JSA. Another consideration is that each JSA will require revision whenever equipment, raw materials, processes, or the environment change. For these reasons, it is usually necessary to identify which jobs are to be analyzed. Even if an analysis of all jobs is planned, this step ensures that the most critical jobs are examined first. Factors to be considered in setting a priority for analysis of jobs include:

- **Incident frequency and severity**: jobs where incidents occur frequently or where they occur infrequently but result in disabling injuries.
- **Potential for severe injuries or illnesses:** the consequences of an incident, hazardous condition, or exposure to harmful substance are potentially severe.
- **Newly established jobs:** due to lack of experience in these jobs, hazards may not be evident or anticipated.
- **Modified jobs:** new hazards may be associated with changes in job procedures.
- **Infrequently performed jobs:** workers may be at greater risk when undertaking non-routine jobs and a JSA provides a means of reviewing hazards.

How do I Identify Job Steps (i.e., break the job into basic steps or tasks)?

After a job has been chosen for analysis, the next stage is to break the job into steps tasks. A job step or task is defined as a segment of the operation necessary to advance the work. Care must be taken not to make the steps or tasks too general. Missing specific steps and their associated hazards will not help. On the other hand, if they are too detailed, there will be too many steps. A rule of thumb is that most jobs can be described in less than ten steps. If more steps are required, you might want to divide the job into two segments, each with its separate JSA, or combine steps where appropriate. As an example, the job of changing a flat tire will be used in this document.

Each step is recorded in sequence. An important point to remember is to keep the steps in their correct sequence. Any step which is out of order may miss serious potential hazards or introduce hazards which do not actually exist. Make notes about what is done rather than how it is done. Each item is started with an action verb. Job steps are recorded in the left-hand column, as shown below:

Sequence of Events	Potential Incidents or Hazards	Control Measures
Park vehicle		
Remove spare and tool kit		
Pry off hub cap and loosen lug bolts (nuts)		
And so on...		

This part of the analysis is usually prepared from knowledge or by watching a worker do the job. The observer is normally the immediate supervisor. For a more thorough analysis, have another person (preferably a member of the joint occupational health and safety committee) participate in the observation. Key points are less likely to be missed this way. The job observer should have related experience and be capable of carrying out all parts of the job. To gain cooperation and participation, the reason for the exercise must be clearly explained. The JSA is neither a time and motion study, nor an attempt to uncover individual unsafe acts. It is the job, not the individual, that is being studied in an effort to make it safer by identifying hazards and making modifications to eliminate or reduce them. The worker's experience contributes in making job and safety improvements.

The job should be observed during normal times and situations. For example, if a job is routinely done only at night, the JSA review should also be done at night. Similarly, only regular tools and equipment should be used. The only difference from normal operations is the fact that the job is being observed. When completed, the breakdown of steps should be discussed by all the participants (always including the worker) to ensure that all basic steps have been noted and are in the correct order.

How do I Identify Potential Hazards?

Once the basic steps have been recorded, potential hazards must be identified at each step. Based on observations of the job, knowledge of incident and injury causes, and personal experience, list the things that could go wrong at each step. A second observation of the job being performed may be needed. Since the basic steps have already been recorded, more attention can now be focused on each potential hazard. At this stage, no attempt is made to solve any problems which may have been detected.

To help identify potential hazards, the job analyst may use questions such as these (not a complete list):

- Can any body part get caught in or between objects?
- Do tools, machines, or equipment present any hazards?
- Can the worker make harmful contact with moving objects?
- Can the worker slip, trip, or fall?
- Can the worker suffer strain from lifting, pushing, or pulling?
- Is the worker exposed to extreme heat or cold?
- Is excessive noise or vibration a problem?
- Is there a danger from falling objects?
- Is lighting a problem?
- Can weather conditions affect safety?
- Is harmful radiation a possibility?
- Can contact be made with hot, toxic, or caustic substances?
- Are there dusts, fumes, mists, or vapours in the air?
- Causes of past injuries?
- Legislation or regulatory requirements?
- Employer-imposed requirements?
- Manufacturer’s specifications, instructions, or procedures for equipment and materials?
- Other work in progress near the work area?
- Changes in conditions at the work area such as weather, lighting, noise, other activities, increase / decrease in number of people / traffic volume, working surface conditions, working at elevation?

Potential hazards are listed in the middle column of the worksheet (example below). Again, all participants should jointly review this part of the analysis.

Sequence of Steps	Potential Hazards	Control Measures
Park vehicle	a) Vehicle too close to passing traffic b) Vehicle on uneven, soft ground c) Vehicle may roll	
Remove spare and tool kit	a) Strain from lifting spare	
Pry off hub cap and loosen lug bolts (nuts)	a) Hub cap may pop off and hit you b) Lug wrench may slip	
And so on...	a) ...	

How do I Identify Control Measures?

The final stage in a JSA is to determine ways to eliminate or control the hazards identified. Each hazard identified in the previous step needs a control measure or preventative measure. The measure explains how the worker will control or eliminate the hazard, and significantly reduce the risk of injury.

The fundamental approach to control hazards utilizes a hierarchy of actions, starting with hazard elimination followed by other control measures listed in order of their strength or effectiveness:

- Elimination
- Engineering Controls
- Administrative Controls and Work Practices
- Personal Protective Equipment

These generally accepted measures are further explained in **Section 5.2: The Fundamental Approach to Control All Risks**.

In listing the control measures, do not use general statements such as "be careful" or "use caution". Specific statements which describe what action is to be taken and how it is to be performed are preferable. The recommended measures are listed in the right-hand column of the worksheet, lettered to match the hazard in question. For example:

Sequence of Steps	Potential Hazards	Control Measures
Park vehicle	a) Vehicle too close to passing traffic b) Vehicle on uneven, soft ground c) Vehicle may roll	a) Drive to area well clear of traffic. Turn on emergency flashers. b) Choose a firm, level parking area. c) Apply the parking brake; leave transmission in PARK; place blocks in front and back of the wheel diagonally opposite to the flat.
Remove spare and tool kit	a) Strain from lifting spare	a) Turn spare into upright position in the wheel well. Using your legs and, standing as close as possible, lift spare out of truck and roll to flat tire.
Pry off hub cap and loosen lug bolts (nuts).	a) Hub cap may pop off and hit you b) Lug wrench may slip	a) Pry off hub cap using steady pressure. b) Use proper lug wrench; apply steady pressure slowly.
And so on...	a) ...	a) ...

How should I make the information available to everyone else?

A JSA is a useful technique for identifying hazards so that workers can take measures to eliminate or control hazards. Once the analysis is completed, the results must be communicated to all workers who are, or will be, performing that job. The side-by-side format used in JSA worksheets is not an ideal one for instructional purposes. Better results can be achieved by using a narrative-style communication format. For example, the work procedure based on the partial JSA developed as an example in this section might start out like this:

1. Park vehicle.

a) Drive vehicle off the road to an area well clear of traffic, even if it requires rolling on a flat tire. Turn on the emergency flashers to alert passing drivers so that they will not hit you.

b) Choose a firm and level area for parking. You can jack up the vehicle to prevent rolling.

c) Apply the parking brake; leave the transmission in PARK; place blocks in front and back of the wheel diagonally opposite the flat. These actions will also help prevent the vehicle from rolling.

2. Remove spare and tool kit.

a) To avoid back strain, turn the spare up into an upright position in its well. Stand as close to the trunk as possible and slide the spare close to your body. Lift out and roll to flat tire.

3. Pry off hub cap; loosen lug bolts (nuts).

a) Pry off hub cap slowly with steady pressure to prevent it from popping off and striking you.

b) Using the proper lug wrench, apply steady pressure slowly to loosen the lug bolts (nuts) so that the wrench will not slip, get lost, and/or hurt your knuckles.

4. And so on.

A more fully developed JSA for the above job is provided below for reference purposes only.

Some points to consider

- The analysis and assessment of risks is an iterative process and can be “co-mingled” (this is the same for the re-assessment of risks).

- The JSA and SOP models can be applied to a task, a minor job, to a complex job, or even to a project involving quite a number of jobs.
- As with any complex process involving risks and involving people, it is preferable to engage as many stakeholders as possible in the creation, review, and approval of a JSA.
- The JSA/SOP is a sharply focused application of the very broad Risk Management Process.

Form for Job Safety Analysis Worksheet

Job Safety Analysis Worksheet		
Job Scope / Scope of Work / Nature of Work:		
Analysis By:	Reviewed By:	Approved By:
Date:	Date:	Date:

Potential General Hazards	**Control Measures & Critical Work Practices**

Major Tasks of Job or Sequence of Steps	**Potential Hazards or Potential Accidents**	**Control Measures & Personal Critical Behaviours**

Example: Let's Change a Flat Tire

Job Safety Analysis Worksheet		
Job Scope / Scope of Work / Nature of Work: **Remove Wheel Assembly with Flat Tire from Vehicle; Replace Spare Wheel Assembly**		
Analysis By: JRC	Reviewed By: GW	Approved By: SK, PhD
Date: 20130407	Date: 20130408	Date: 20130409
Potential General Hazards	**Control Measures & Critical Work Practices**	
a) Pinch Points, Abrasions, Sharp Edges b) Strains c) Being Struck d) Exposure to traffic	a) Wear hand protection (work gloves). b) Use proper lifting technique. Push down when possible. c) Keep clear of vehicle. Push away from face or keep face clear when pulling. d) Space or warning signs.	

Major Tasks of Job or Sequence of Steps	**Potential Hazards**	**Control Measures & Critical Work Practices**
Park vehicle.	a) Vehicle too close to passing traffic. b) Vehicle on uneven, soft ground. c) Vehicle may roll.	a) Drive to area well clear of traffic. Turn on emergency flashers. b) Choose a firm, level parking area. c) Apply the parking brake; leave transmission in PARK; place blocks in front and back of the wheel diagonally opposite to the flat. d) Use flares or reflective warning triangles if in unavoidable traffic area.
Remove spare and tool kit.	a) Pinch points between spare and vehicle. b) Strain from lifting spare.	a) Wear hand protection (work gloves). b) Turn spare wheel assembly into upright position in the wheel well. Using your legs and standing as close as possible, lift spare out of truck and roll to flat tire.
Pry off hub cap and loosen lug nuts (or bolts on some vehicles) by ½ to 1 turn.	a) Hub cap may pop off and hit you. b) Lug wrench may slip.	a) Pry off hub cap using tool with steady pressure. b) Use proper lug wrench; apply steady pressure slowly. Push down; do not pull up as this may strain your back.
Place jack on firm ground and at specified position on vehicle for jacking.	a) Jack may sink or vehicle is unstable on soft ground. b) Jack may damage underside of vehicle.	a) Use a wooden board or metal plate under jack. b) Check owner's manual for exact position.
Begin jacking vehicle until tire is clear of ground, allowing for flattened tire as well.	a) Vehicle is unstable and may shift off jack. b) Jack may "kick-back".	a) Keep body and limbs clear of underside of vehicle, and clear of jack.
Loosen lug nuts / bolts.	a) Wheel assembly may fall from hub. b) Falling wheel may destabilize vehicle.	a) Steady wheel assembly. b) Keep body and limbs clear of underside of vehicle, and clear of jack
… and so on …		

Section 5.6: Checklists for Executing Work

A risk management leader must become familiar with the basics and variety of checklists that are used for the execution of work to check for compliance, as will be discussed in **Job Observations and Planned Inspections**. The checklist is a basic tool for checking conditions and work practices, and readiness to perform work prior to commencing that work. It provides a list of questions and issues that are used to gather data and identify concerns to be resolved. The checklist also provides a way for a person to identify specific hazards and risks associated with the activity or operation, and implement control measures to reduce the risks to associated levels.

The development of the checklist is best done with a team of experienced people. The items on the checklist are developed or created by an expert (or an expert team) in the particular system undergoing the checks; the expert(s)

has determined specific practices and conditions (or parameters) that must be met or satisfied to maintain / reduce risks to acceptable levels for acceptable (safe) operation. Naturally, these control measures are the expected practices and behaviours before and during the execution of work. Simply, when work is being executed that satisfies or complies with the necessary control measures, then the risk levels of that work activity are brought within acceptable levels. Deviations from acceptable work practices, parameters, and conditions are unacceptable and are hazards. Those hazards generally spring from deviations or deficiencies in the day-to-day conditions of the facilities and installations or their surroundings. The scope of possible hazards includes chemical, mechanical, electrical, weather and climate, housekeeping, etc. Of course, once a hazard (i.e., a deviation from acceptable conditions or work practices) has been identified, actions can be taken to address the hazard.

Checklists can be developed for any objective, but need to be done with much care and thought. A checklist can take too narrow a look at the activity or facility and may miss some important points. Checklists should be routinely reviewed during their use to ensure they cover your needs and are up to date with any changes in the operation or management priorities, or even changed regulations.

Checklists can be categorized into two broad groups: 1) the use of checklists prior to and during the execution of work, as discussed in this section; and 2) the use of checklists to check for compliance, per **Job Observations and Planned Inspections** (see Chapter 5).

The Use of Checklists Prior to and During the Execution of Work

Employees using checklists are searching for deviations that can increase the risk level associated with the work about to be performed or during the work. The classic example: The pre-flight checklist that is used by commercial airline crews checking the critical functions on the aircraft before take-off. If there are any deviations found, the aircraft is grounded until the problem is solved.

Checklists can be created that complement or mirror the requirements of a safety rule (a corporate safety policy or safety procedure, or a safety regulation) to aid the worker in using and executing that safety rule, etc. For example, the Permit-to-Work (PTW) is a critical checklist used in the safety procedure to check for hazards and control measures before “giving permission” to start work on a job within a facility and also during the performance of that work.

It is relatively easy to train new employees on a basic checklist, although checklists for leadership activities and advanced technologies require specialized training. Because checklists are very specific, they do have limitations and drawbacks:

1) Checklists do not cover everything, can never be entirely complete, nor meet the needs of every situation. If one is not carefully observant, hazards or areas not on the checklist can be overlooked. Management has to ensure that further hazard identification and risk analysis are carried out.
2) Checklists can become long and getting through them may be difficult for some, especially when used repeatedly, to a point where people cover items in a perfunctory fashion (so-called “checking off the boxes”) and may overlook hazards that should otherwise be flagged when items are carefully considered.
3) Checklists with highly repeated use and lack of support (leadership does not check / audit to ensure compliance) could fall into lax or relaxed use. In other words, employees become complacent about the need for the checklist and the hazards and control measures that are specified in the checklist. Recall the tracking and use of the PTW in the Piper-Alpha loss incident.

Checklists are only the beginning of a risk assessment and are only as good as the number and quality of items, the depth of understanding of the checklist itself, and the scope and intent of each check item. Checklists should only have succinct information points and checkboxes, and should have a stand-alone procedure that describes what each check is for, how to check, and what to do when a deviation or deficiency is found. Checklists without this disciplined approach can fall into disuse or misuse (i.e., workers can become complacent about the need for, and use of, the checklist).

There are many other types of checklists that can be used prior to and during the execution of work such as: Permit-to-Work; Hot Work Permit; Confined Space Entry Permit; Work on Energized Electrical Equipment Checklist; Pre-lift / Pre-hoist Checklist; Piping Break-in Checklist; Tools, Vehicles, and Equipment Checklists; Plant Operations or Plant Equipment Checklists; Technically- or technology-specific Checklists, and so on. These support engineering safety and risk management within facilities. However, beyond basic familiarity, the detailed discussion of these is not within the scope of ENGG404.

An Example of a "Permit to Work Checklist for Piping/Vessel Break-in"

1) JOB SCOPE:

Work LIMITED to the following:
(Job Scope/Description/Tasks & Area/Equipment & Boundaries):

Date: _____
Time: From _____ AM/PM to ____ AM/PM

_____

_____

The Scope of work includes the following (additional Permits and/or Checklists/Forms needed):

☐ Breaking Into Piping Systems (complete Break-in Checklist; template also available)

(here, insert checks for other kinds of work – hot work, confined space entry, etc.)

2) SAFETY ORIENTATION:

All people working under this Permit to Work have the necessary Site / Facility / Work Group Indoctrinations and Orientations?	[ ] Yes	[ ] N/A
Emergency procedures and alarms, locations of assembly points and evacuation routes and the location of emergency equipment, including; nearest safety shower, eye wash, fire extinguisher and telephone and/or intercom have been reviewed and are understood?	[ ] Yes	[ ] N/A
The scope and boundaries of any other work in the area that could impact this permitted work has been reviewed and is understood?	[ ] Yes	[ ] N/A
Other workers in the area have been notified that this permitted work could impact their work, including the locations of any barricades?	[ ] Yes	[ ] N/A
All equipment to be worked on has been properly prepared, identified and is ready to work on?	[ ] Yes	[ ] N/A

3) ENVIRONMENTAL IMPACT & HOW TO ADDRESS IMPACT:

Piping system normally contains:

Method for emptying / purging / venting / flushing / cleaning the piping system:

Method for directing line contents to safe point for recovery / venting / scrubbing / flaring:

Method for disposing of wastes:

4) ON-SITE INSPECTION

☐ Pre-job On Site Inspection Complete? Person who completed pre-job inspection (name): _____

☐ Additional inspection needed during job? If yes, describe scope: _____

☐ Post-job On Site Inspection Complete? Person who completed post-job inspection (name): _____

5) HAZARDOUS SUBSTANCES / CHEMICAL HAZARDS:

See MSDS(s) for review of safety & health hazards.

List the Chemicals contained / previously contained in the piping system:

Hazards: [ ] Flammable [ ] Toxic [ ] Corrosive [ ] Reactive [ ] Inhalation [ ] Skin Contact [ ] Other:

List the Chemicals specific to the job:

Hazards: [ ] Flammable [ ] Toxic [ ] Corrosive [ ] Reactive [ ] Inhalation [ ] Skin Contact [ ] Other:

6) PHYSICAL HAZARDS:

List the hazards of the area, the work, and the equipment for the specific task

[ ] Sharp Edges	[ ] Pinch Points	[ ] Flying Debris	[ ] Dust	[ ] Asbestos / RCF
[ ] Falling Objects	[ ] Pressure Extreme	[ ] Heat Exposure	[ ] Flash Fire	[ ] Inert Atmosphere
[ ] Working at Elevation Falls ____ < 1.8 metre ____ > 1.8 metre	[ ] Electrical Flash / Switching High Voltage / Work on Energized Electrical Systems	[ ] Thermal Burn Contact with Hot / Cold Surfaces	[ ] Noise (>area requirement)	[ ] Radioactive Sources / Radiation [ ] Other: _____

7) PERSONAL PROTECTIVE EQUIPMENT:
Protection required for hazards: Specify the PPE, precautions, and safeguards to protect against the process related hazards / break-in to piping systems, and the specific job/task-related hazards per the Client's PPE Grid.

Body / Clothing:	***Head:***
Breathing / Respiratory:	***Face / Eyes:***
Elevated Work / Fall Protection:	***Hearing:***
Barricading / Warning Signs:	***Arms / Hands:***
Additional Requirements:	***Foot / Leg:***

Workers have specialized training as required [ ] PPE Use [ ] Asbestos / RCF [ ] SCBA [ ] Fall Protection [ ] Elec. Flash Protection [ ] Other: _____ [ ] N/A

Ergonomic Concerns and Safeguards: [ ] N/A

8) COMMUNICATION: Responsibilities communicated to PTW Acceptor:

[ ] Crew accountability and addressing workers' concerns
[ ] Conditions for Work Stoppage
[ ] Reporting Changes that Affect Job Safety
[ ] Managing PTW Over Crew Change / Shift Change
[ ] Reporting a change in the Permit Acceptor
[ ] Requirements for Close-out of PTW

The person accepting the permit will ensure that all workers: **Initials of Permit Acceptor:** _____

A. Understand the hazards of the area, equipment and work and the safeguards in place.
B. Understand potential environmental impact and procedures for addressing this.
C. Understand and follow Personal Protective Equipment requirements.
D. Have the necessary skills and knowledge to do the permitted work safely.
E. Know emergency procedures, alarms and assembly points.
F. Know the location of and how to use emergency equipment.
G. Know the scope of other work that could impact this work.
H. Understand the scope of this permitted work.

9) BREAKING INTO PIPING SYSTEMS: Complete this Section for Breaking Into Piping Systems: Doesn't Apply [ ]

Describe exact location(s) of break-in(s):

Describe method for identifying break-in location(s); see item 4) above.

Describe status of the piping system i.e. methods for depressurizing and clearing of contents, per item 3) above:

Describe methods for verifying that isolation devices are holding i.e. sealing tightly:

Radiation sources closed, controlled, & confirmed closed? [ ] YES [ ] N/A

Barricading needed? [ ] YES [ ] N/A
If yes, describe method:
If yes, describe area to be barricaded:

Is temporary grounding or grounding-continuity of piping system needed? [ ] YES [ ] N/A
If yes, describe method:

Can PPE requirements per item 7) above be relaxed at some point after the initial break-in? [ ] YES [ ] N/A
If yes, describe point when it can be relaxed, and describe the level of relaxed PPE:

See previous sections for Environmental Impacts, Hazardous Substances / Chemical Hazards, Physical Hazards, and Personal Protective Equipment.

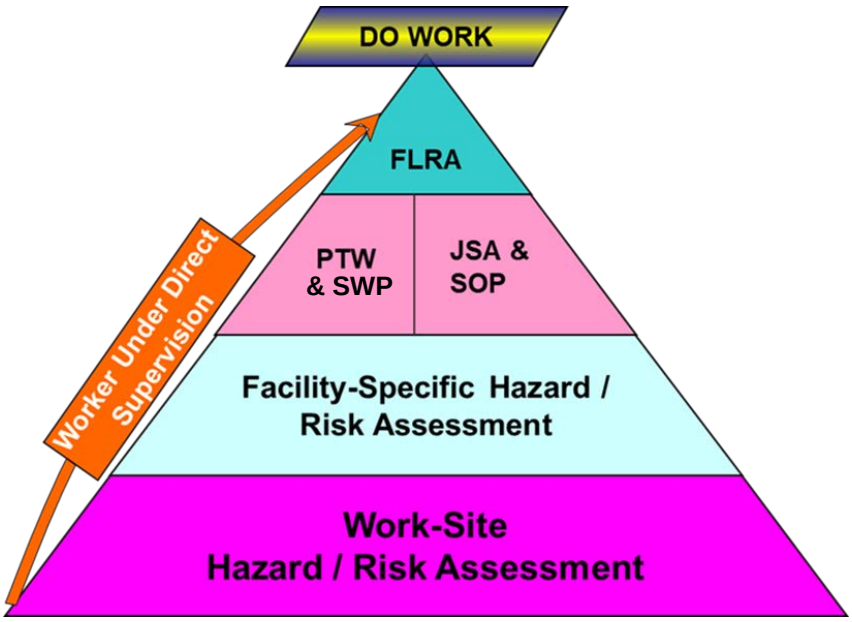
Section 5.7: Putting the Tools Together – A Multi-Layered Approach to Hazard / Risk Assessment

A leading organization in the petrochemical processes manufacturing industry applies the basic approach of the CCOHS JSA at several and different levels of job planning and job execution. This application at different levels allows workers to build up layers of information concerning the assessments (hazards / risks and control measures) in the areas where they will be stationed and for the nature of the work they will be performing. Referring to the layered triangle below, for each of the planned and successive steps that a worker experiences between arriving at the work-site through to "Do Work", a hazard / risk assessment forms a part of each step. The assessment includes the identification and the mitigation of hazards for the work being performed and the workplace. This approach exceeds the requirements of **Alberta OH&S Code Part 2, Hazard Assessment, Elimination, and Control**.

A Depiction of the Multi-layered Approach to Hazard Assessment

The worker progresses from bottom to top. Each of the assessments is methodical, thorough, documented, dated, available to the worker, and engages the worker in risk management. Each of the layers is described in the next section. Below is a list of acronyms:

- FLRA: Field Level Risk Assessment (a qualitative risk assessment methodology)
- PTW: Permit to Work (a special type of checklist)
- SWP: Safe Work Permit (a special type of checklist)
- JSA: Job Safety Analysis (a qualitative risk assessment methodology)
- SOP: Safe Operating Procedure (a qualitative risk assessment methodology and checklist)
- LCP: Life-Critical Procedure or Life-Saving Rule (part of the work-site risk assessment)



Steps in the Multi-layered Approach to Hazard / Risk Assessment

These requirements apply to all workers – core employees and contractor employees – that perform work at the work-site. Beginning at the bottom of the triangle as depicted in the diagram above:

1. **Work-Site Hazard / Risk Assessment:** Soon after the worker arrives on site for the first time i.e. a new employee, the worker will receive the work-site hazard / risk assessment i.e. some of the general hazards of and rules for working on site. This is typically part of a new employee's indoctrination or orientation to the organization or organization. Life-critical procedures or life-saving rules are included as part of this assessment.
2. **Facility-Specific Hazard / Risk Assessment:** For larger organizations, a new employee may be assigned to a work area, or a project, or department, or unit within the larger organization i.e. a specific facility. The new employee will receive the hazard / risk assessment for that specific facility within the larger organization. This is typically part of a new employee's indoctrination or orientation to the specific facility.
3. **Job Safety Analysis (JSA) / Safe Operating Procedure (SOP):** The worker will be assigned work and will perform the assigned work using their set of core job skills (training and work practices), sometimes in

conjunction with a Job Safety Analysis (JSA) or a Safe Operating Procedure (SOP). The JSA and SOP will have a hazard / risk assessment embedded within.

4. The worker requires "authorization to proceed with the work" or "permission to do the work". Authorization or permission can be given in three possible ways depending on the policies of the organization, and/or the scope and nature of work, and/or the nature of the job site (the location where the work is actually being performed). A **Permit to Work (PTW)** is a highly-specialized check-list. A "permit to work" (PTW) or "safe work permit" (SWP) is issued to the worker(s) by the authorizer (i.e. a facility work coordinator), at which time hazards of and control measures for the job, as well as the job site, are discussed.
5. **Field Level Risk Assessment (FLRA):** Immediately before starting work (especially effective when preparing to do the work), the worker completes a Field Level Risk Assessment (FLRA). This addresses tasks, conditions, and hazards not anticipated when the JSA/SOP was written, or when the PTW was discussed and permission granted, and for hazards in the work area with which the worker is not familiar.
6. **Do Work:** After having considered and addressed all hazards to the best of the worker's and the system's abilities, the worker can perform the work.

Visitors are a special case. They receive the initial work-site hazard assessment, and are then fully escorted at all times; thus fulfilling the requirement for a non-competent person to be under the direct supervision of a competent person at all times.

Section 5.8: Job Observations and Planned Inspections

Recall that checklists can be categorized into two broad groups: 1) the use of checklists to conduct a planned inspection to check for compliance; and 2) the use of checklists prior to and during the execution of work (i.e., the checklist aids the worker in meeting requirements for the execution of work, as per **Chapter 5.6 Checklists for Executing Work**).

The Planned Inspection method goes by several names such as: **Planned Inspection of the Workplace**, **Manager's Safety Review**, **Job Audit**, **Integrated Audit**, and **Hazard Assessment Audit**. Words such as "inspection", "review", "assessment", and "audit" carry negative connotations, so some organizations soften this by calling these methods a **Field Observation of Risks** or an **Observation / Interaction / Intervention**, or a **Safety Review**. The phrase **Planned Inspection** meets our purposes here.

The manager's **Planned Inspection** is a formalized method intended for use by managers. There are two different types of planned inspections: 1) at the individual / team level; and 2) at the organizational level. Both of these check for compliance with requirements; however, the former checks the people for compliance with the program standards, and the latter checks the organization for compliance of the standards and the programs (i.e., checks the effective implementation of the risk management program).

The Purpose of the Planned Inspection at the Individual / Team Level

The manager's **Planned Inspection at the Individual / Team Level** is a formalized method that is intended for managers to use in the facility to interact with workers. Almost any formal risk assessment tool (such as hazard assessments, safety inspections, safety reviews, inspections, or safety audits) can be adapted and used to conduct an inspection, and this takes on the form of a checklist for a Planned Inspection. The use of a checklist greatly aids the manager in conducting a planned inspection because it is methodical, thorough, and documented.

This type of Planned Inspection aids the manager in their risk management activities within the facility such as checking for compliance (i.e., the specified requirements (work practices and conditions) are being met). As will be learned, the manager is accountable for ensuring compliance with requirements within the facility, and with that accountability comes the responsibility to actively check (an audit or planned inspection) that requirements are met, and to take action when requirements are not being met (sub-standard work practices and conditions). Requirements are defined in:

- legislative acts, regulations, and codes (e.g., The Alberta OH&S Code);
- the manufacturer's specification in the assembly, use / operation, maintenance, etc. of any material or equipment; and
- a corporate risk management program which includes the risk management system, standards, rules, policies, procedures, work processes, etc., as well as the previous two sets of requirements.

The purpose of this type of **Planned Inspection** is to enable managers to get out into the workplace to talk to workers, to interview them about their concerns about hazards in the workplace, and to coach them on how to manage risks in their jobs; hence, the need to understand and apply checklists, per **Checklists for Executing Work**. No matter what the Planned Inspection is called, the manager's main purposes are:

- To demonstrate they care about workers;
- To observe and interact with workers;
- To determine if there are sub-standard conditions in the work place and to check for compliance with requirements;
- If there are sub-standard practices being performed, to take steps to address those sub-standard conditions or work practices to come into compliance (i.e., intervene and coach the worker towards successful application of risk management); and
- If practices and conditions are acceptable, to commend the workers for successfully implementing risk management (i.e., for practicing acceptable-risk behaviours).

Naturally, these actions reinforce the expected practices and behaviours in the workplace before and during the execution of work. Recall from **Section 5.6: Checklists for Executing Work**, when work is being executed that satisfies or complies with the necessary control measures, then the risk levels of that work activity are reduced to acceptable levels.

Managers gain great value when they observe and interact with workers as the workers perform work. This is a means for managers to "Manage by Walking Around" or "Walk the Talk" and is effective for maintaining leadership visibility. As well, it is a **planned inspection** and is an application of the fundamental function of management – **Plan-Do-Check-Act** as will be discussed in **Chapter 7.4: The Fundamental Process of Management - The PDCA Cycle**. This type of Planned Inspection is an application of the PDCA at: a) the individual level (one-on-one) when the manager is interacting with one individual; and b) the team level when interacting with two or more workers (e.g., a foreman / crew leader and crew).

The Means of the Planned Inspection at the Individual / Team Level

To conduct a **Planned Inspection at The Individual / Team Level** effectively, the manager is required to know the work area in which the manager is making the observation, needs to have some knowledge of the trade and the nature of the work being performed, and needs to know the applicable requirements of the work underway (i.e., know the applicable checklist). This knowledge is needed such that the manager can understand the technical nature of the job and work, and can ask or answer informed questions. This interaction provides:

- The workers with an opportunity to communicate with a manager face-to-face;
- The manager with an opportunity to engage the workers in addressing safety issues and managing risks; and
- The manager with an opportunity to coach the workers for safety success.

Managers need to be trained to observe (i.e., have the ability to see actions and conditions that may create a hazard and result in an injury). Recall the Discovery method for finding hazards (e.g., energy sources, line-of-fire, lack of safeguards, triggering event, etc.). Experienced operations and maintenance personnel use 1) their senses (sight, sound, smell, feel) to observe the conditions and for potential deficiencies; and 2) their insightful trade and industry experience to observe the work practices for potential problems.

Managers also need additional training and practice in social skills with workers for effective observations, communication, interactions, and interventions to reinforce or correct the desired acceptable behaviours. This is because these techniques involve in-depth interactions (e.g., an interview during an audit) wherein the key imperative is to interact with or interview the worker in a non-threatening manner. Approaching and interacting with a worker in a non-threatening manner avoids the situation where workers take a defensive stance when asked about their work.

Managers should also learn to ask open-ended questions to guide the workers to the solutions to resolve their concerns. The skill in asking open-ended questions allows the worker to think for themselves and have a positive interaction, instead of being told or scolded on what to do, which can be a negative experience. This focused training followed by mentoring on these three skills (observation, social skills, ask open-ended questions) ensures that managers will be successful in their interactions with workers. The theory and practice for interacting with others is discussed in **Leadership, Motivation, Organizational Design, and Culture** (see Chapter 7).

Key Steps in The Planned Inspection

A Planned Inspection at the Individual / Team Level can involve management from level and from any function such as operations, maintenance, or other functional expertise role. The planned inspection method uses a formal, highly disciplined, thorough, and methodical approach for managers; it includes these specific steps:

1) Introduce yourself with a brief explanation as to why you are there;
2) Observe the conditions in the workplace and determine if these are acceptable or sub-standard;
3) Observe the work practices (worker behaviours) being performed by the workers, and determine if these practices are in compliance (acceptable or sub-standard / at-risk);
4) Interact to reinforce the desired behaviours (i.e., commend your workers to reinforce their activities that maintain acceptable conditions and are consistent with acceptable standards of practice);
5) Intervene when sub-standard work practices (unacceptable practices / at-risk behaviours) are observed and take steps to address those sub-standard conditions or work practices;
6) Coach users on how to look for and address hazards;
7) Ask the workers if they have any safety issues or concerns;
8) Take any concerns that workers may have that they cannot resolve themselves and act on those concerns / see them through to resolution. This point has the most value for workers.

The Planned Inspection as a Means to Maintain Leadership Visibility and Combat Complacency

Often, workers will become accustomed with the operations, facility, equipment, policies, and work processes. This comfort can lead to complacency, the gradual decline in the standard of work practices, and the acceptance of sub-standard conditions and work practices. Management can ensure the standards they expect are maintained by actively taking part in these risk assessments, thus ensuring that complacency does not set in. Management also has a face-to-face opportunity to coach workers to be empowered in taking action to correct sub-standard conditions and intervene to address at-risk behaviours, thus positively influencing culture with the end result of improved safety performance.

Thus, the **Planned Inspection at The Individual / Team Level** is an effective method for maintaining leadership visibility on a regular basis and for combating complacency in the workplace. In addition, this type of planned inspection – the interaction between the manager and the worker – is sometimes the only link between the workers and management, and may be the only way for workers to connect with and communicate to management. When performed properly, workers will value these interactions because their concerns are heard and addressed.

Example of a Planned Inspection that Maintains Leadership Visibility and Combats Complacency

The Hazard Assessment Audit Process is a process for a specialized planned inspection that pertains to the **RMS Element 2) Risk Assessment and Management of Risks**. Its intent is to check the implementation of all requirements pertaining to management of risks in the execution of work. The manager uses the checklist to ensure that all requirements are met (i.e., to check that work practices and conditions are in compliance). Inherent in this process is the direction to take corrective action when any sub-standard practices and/or conditions are noted. This completes the PDCA cycle at the Individual / Team Level: the manager plans the inspection, does the inspection, checks for deviations in work practices and conditions, and acts to correct those deviations.

The Planned Inspection at the Organizational Level (Audit)

This type of **Planned Inspection** is a means to audit the effectiveness of the risk management program (the system, policies, procedures, etc.) at the Organizational Level. It is the actual means to implement the requirements of the **RMS Element 6) Program Evaluation and Continuous Improvement**.

As described in the previous section, the Hazard Assessment Audit Process is designed to check for and take action on deviations or deficiencies at the Individual / Team Level, but it is also designed to investigate why there were deviations or deficiencies at the Individual / Team Level that have causes within the organization (i.e., management). This drives management to investigate the risk management program and system (i.e., it is looking for latent causes (weaknesses in the management system)). The manager should learn the cause of deviations or deficiencies at the Individual / Team Level, as these deviations are signals that something is not quite right in the risk management program (i.e., there are weaknesses). It could be a simple oversight of a worker involved in that work of the day or it could be the result of a gap in the risk management system (i.e., a latent cause).

Continuing with the example as described in the previous section, the **Audit Process** could also reveal weaknesses in how hazards and risks are identified and/or controlled (e.g., there is a flaw or inadequacy in the PTW checklist that the workers are using for their assigned work. Any deviations found through this manner can then be corrected, thus completing the PDCA cycle at the organizational level.

A planned inspection of this type is not limited to **RMS Element 2: Risk Assessment and Management of Risks**. A planned inspection of this type could be created and implemented that checks the implementation of any risk management system element (e.g., a planned inspection that checks the requirements pertaining to Management of Change, thus checking **RMS Element 4: Management of Change** at the organizational level). The **Planned Inspection at the Organizational Level** is a management activity that is driven by the fundamental PDCA process. The manager applies the PDCA cycle to check for deviations from or deficiencies in the policies and systems, and acts to correct those weaknesses, thus addressing latent causes in a proactive manner.

A Planned Inspection at the Organizational Level encompasses these similar steps and key points as well as the review of applicable documentation (policies and records) and the execution of responsibilities of management. For example: i) How diligent are managers in executing the MOC work process? ii) How thorough are managers in thoroughly investigating and analyzing a loss incident?

Planned Inspections and Types of Causes

The **Planned Inspection at the Individual / Team Level** is intended to check for deviations or deficiencies at the individual / team level (lack of compliance). The manager discovers sub-standard causes and conditions (these are immediate causes), and the manager's actions are to coach for compliance (i.e., initiate immediate action to correct).

The **Planned Inspection at the Organizational Level** dives deeper to understand why there were sub-standard causes and conditions (i.e., to discover latent causes in the organization). This type of planned inspection is proactive because it discovers and addresses latent causes before a loss incident occurs.

- When an organization has a robust program and a set of robust standards, the latent cause can be characterized as *"C: Lack of compliance with program and standards"* . In other words, the worker was not meeting explicitly stated requirements.
- When an organization lacks a set of robust standards, the latent cause can be characterized as *"S: Lack of a set of standards"*. In other words, the set of standards did not reflect the expectations of the risk management program and/or did not adequately state or describe what the worker should do.
- When an organization lacks robust program, the latent cause can be characterized as *"P: Lack of a program"*. In other words, the program was inadequate in describing the overall expectations or was non-existent.

A successful **Planned Inspection** program will deliver on improved workplace conditions and acceptable / superior work practices, and ultimately an improved safety culture and improved safety performance. But to be successful, the **Planned Inspection** program must ensure that:

a) managers are competently trained in the techniques for observation, interaction, coaching, and intervention, (visible and effective). This is important because it trains managers to be effective and visible. Visibility demonstrates commitment and accountability, and that influences the safety culture of the organization in a positive manner with a positive outcome;
b) any concerns identified by workers are being addressed, and
c) any latent causes are addressed. The latter two are especially important because it demonstrates management commitment.

Section 5.9: Reporting and Correcting Sub-standard Conditions and At-Risk Behaviours

Definitions:

- **Sub-standard Conditions** and **Unacceptable Conditions** are synonymous.
- **At-Risk Behaviours**, **Substandard Behaviours**, **Sub-standard Work Practices**, and **Unacceptable Work Practices**, and **Sub-standard Practices** are synonymous.
- **Near Miss (Near Hit)**: Any event or action which under slightly different conditions or circumstances could have resulted in injury or illness to one or more people, equipment or property loss, harm to the surrounding environment, a reactive chemical or process safety event, or a motor vehicle / mobile equipment incident. This is an event without consequence (i.e., no impact on PEAP).
- **Near Miss Prevention**: The act of taking remedial steps when observing an unacceptable condition or an unacceptable practice to prevent the condition or practice from escalating to a loss incident of any magnitude on PEAP, including real losses and near miss events.

The Impact of Addressing Sub-standard Conditions and Work Practices in the Workplace

As will be discussed in **Building A Safety Culture and The Incident Pyramid** (see Chapter 7), the pyramid is supported on a base labelled as "sub-standard conditions and work practices". By addressing these, safety culture can be positively influenced and improve safety performance. As with the other methods, tools, and processes presented in this chapter, this is another proactive approach that addresses sub-standard conditions and work practices, all towards preventing loss incidents. It is a non-planned inspection (unlike FLRA, SQRA, JSA, Checklists, and Inspections / Audits which are all planned) triggered by observations in the workplace. One method is to report sub-standard conditions and work practices; industry refers to this method as the **Near Miss Prevention Program**.

Simply, preventing a near miss incident is the act of taking remedial steps when observing a sub-standard condition or practice, to prevent the condition or practice from escalating to a loss incident. By extension, this also prevents a loss incident. If no action is taken, these sub-standard conditions and practices could lead to further deterioration in workplace conditions and practices, and thus a gradual decline in the ability to manage risks appropriately. This ultimately leads to a loss incident. Consider the Piper Alpha Loss Incident and the work practices concerning the PTW. The value of near miss prevention is ingrained in the opportunity to mitigate hazards before consequence and to prevent an event that may result if the condition or practice were not addressed.

Method

This method can be practiced by anyone in the organization (with suitable training), thus fostering safety leadership at all levels within the organization. It empowers any worker at any level to take action to correct the sub-standard condition or practice. The method involves observation and intervention on an opportunistic basis (i.e., a non-planned inspection; during the course of normal work activity, a person makes an observation and takes action). The basic steps of this non-planned inspection method include:

1) A Person Observes an Unacceptable Condition or Practice / At-Risk Behaviour:

- This step occurs frequently and is simply where people see a condition or a practice that does not meet either the requirements or expectations of the organization, the business, the site or the facility.

2) A Person Takes Immediate Action to Correct:

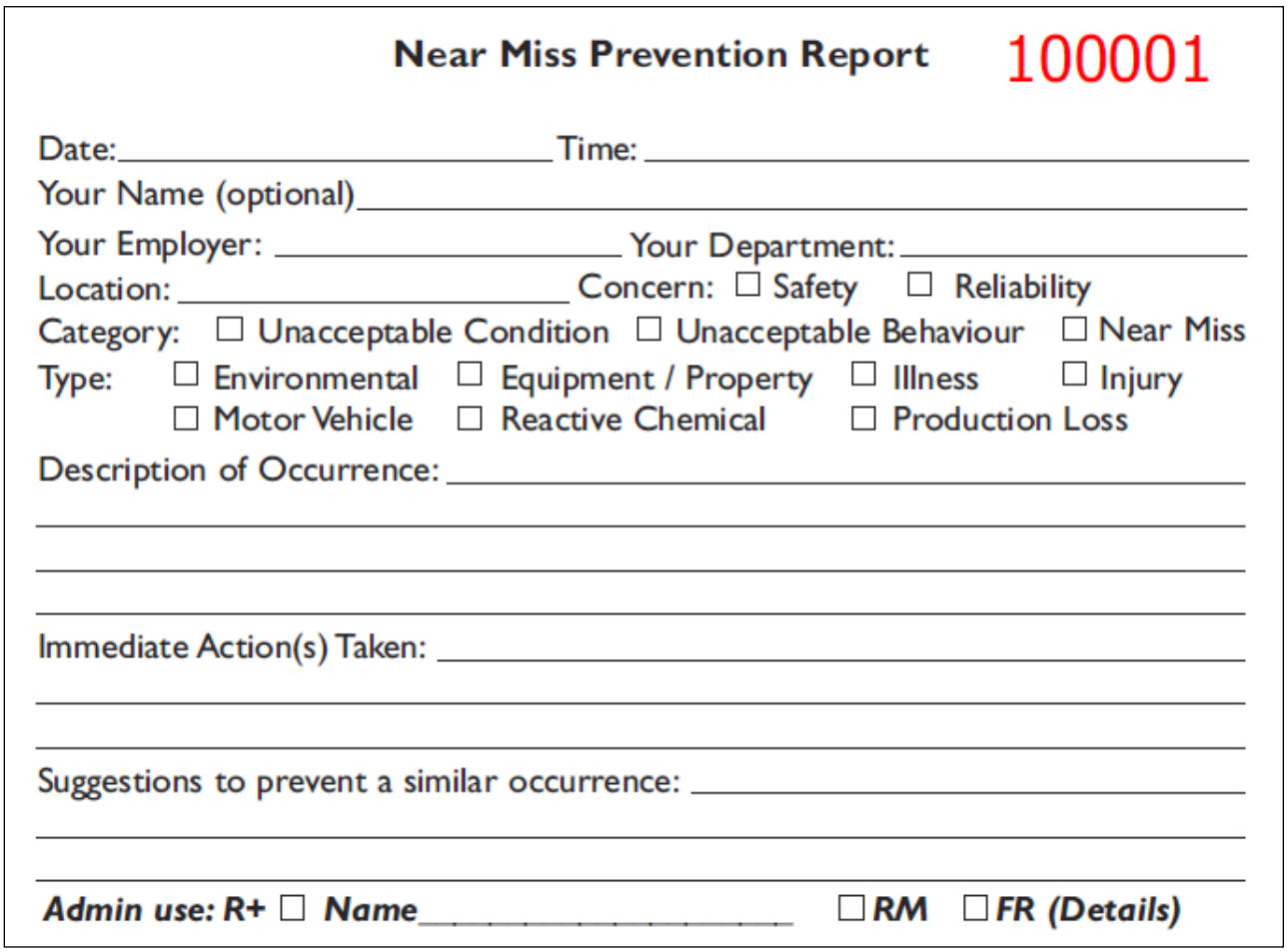
- The person must take immediate action to address the unacceptable condition or unacceptable practice.
- For unacceptable conditions, the person must act to eliminate the hazard or control the hazard. Where the hazard is potentially life-threatening, the person may need to personally guard others from the hazard if safe to do so.
- For unacceptable practices, the person must coach for success, intervene, and correct.
- The success of this system is critical to the person acting immediately to intervene and correct the condition or the practice before it escalates into a more serious event.
- There is no benefit gained when no immediate action is taken. A lack of action may put someone at risk.

These two steps significantly influence culture when practiced by all persons (especially the workers because they are closest to the hazards, are managing the risks directly, and are in the best position to intervene with their co-workers). In short, workers are empowered to address safety issues as they perceive them.

Reporting and Tracking

A simple form can aid the user to record the details. Subsequent steps can include documenting, reporting, tracking, and communicating of the observed sub-standard condition or at-risk behaviour. These forms refer to such

an observation as a “near miss prevention report”. The data from these forms can be entered into a database for additional analysis such as looking for any deteriorating trends in ongoing facility activities.



Near Miss Prevention Report 100001

Date:_____ Time: _____

Your Name (optional)_____

Your Employer: _____ Your Department:_____

Location: _____ Concern: ☐ Safety ☐ Reliability

Category: ☐ Unacceptable Condition ☐ Unacceptable Behaviour ☐ Near Miss

Type: ☐ Environmental ☐ Equipment / Property ☐ Illness ☐ Injury
☐ Motor Vehicle ☐ Reactive Chemical ☐ Production Loss

Description of Occurrence: _____

_____

_____

_____

Immediate Action(s) Taken: _____

_____

_____

Suggestions to prevent a similar occurrence: _____

_____

_____

Admin use: R+ ☐ ***Name***_____ ☐ ***RM*** ☐ ***FR (Details)***

ENGG404

Chapter 6:
Risk Management in Industry

Section 6.1: Process Safety Hazard and Process Management Overview

The following two definitions are based in part on those of The Canadian Society for Chemical Engineering:

Process hazard or **process safety hazard** can be characterized by four components:
1) The asset: "a physical situation in a facility / plant / operation / installation (i.e., the assets where the activity is underway);
2) The potential impact: with a potential for human injury, damage to property or the environment;
3) It occurs through the release of energy via a trigger or triggering event (sub-standard conditions and at-risk behaviours can be process safety hazards); and
4) The release of energy: in the form of fire, explosion, toxicity, corrosivity, mechanical energy (momentum, dynamic, destabilized static), chemical energy (thermodynamic, kinetic / reactive / run-away reaction, release to the environment as a leak or a spill), nuclear energy and wastes, and electricity.

Process safety hazards can include:

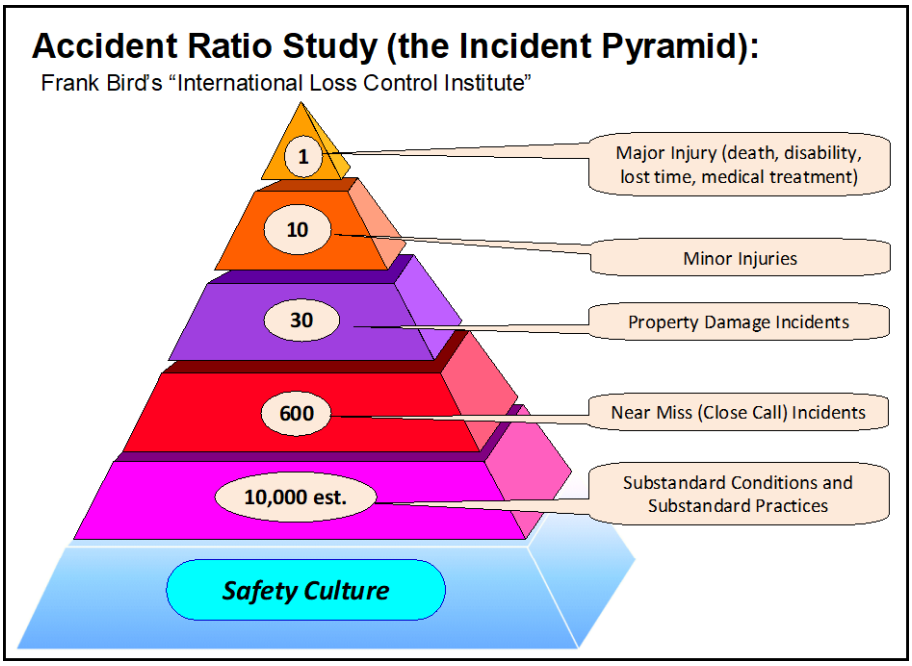
➢ Pressure: high / low / very low (vacuum) / differential; vessel rupture / collapse ➢ Temperature: high / low / very low / cryogenic ➢ Flow: high / low / no / back / reverse ➢ Heat flux: radiant / conductive / convective ➢ Reactions: combustion, exothermic, reactive, unstable, pyrophoric ➢ Flammability / fire / flame speed / deflagration / explosion / detonation ➢ Slow exothermic / self-heating reactions without a heat sink lead to accelerated exothermic reactions ➢ Alloys and chemicals: incompatible materials of construction, hydrogen embrittlement / temperature embrittlement ➢ Solutions, suspensions, mists, dusts, dispersions ➢ Toxic, noxious materials; asphyxiants	➢ Kinetic energy – moving equipment, rotating, revolving, reciprocating ➢ Mechanical failure – machine failure, structural collapse, vibration ➢ Potential energy – gravity, liquid heads, granular materials slopes, voltage, differential pressure; ➢ Electrical classification, hazardous areas, ignition sources ➢ Electricity: electrocution, static, DC, AC, arc flash, ground faults, reverse polarity, non-synchronized switching ➢ Radiation / radioactivity: naturally occurring radioactive material; nuclear reactions, radiation – alpha, beta, gamma ➢ Erosion / corrosion ➢ Noise and sound intensities ➢ Persistent, bioaccumulative, toxic (PBT)

Process Safety Management is the disciplined development and application of management principles and systems, hazard / risk assessment methodologies, and the most effective technology to the identification, understanding, and control of process hazards. This is done to prevent and mitigate process-related unplanned events (e.g., fires, explosions, mechanical and electrical losses, and chemical releases) to prevent process-related injuries and loss incidents. The chemical and petrochemical industries have been the focus for much of the development of Process Safety Management systems.

As a result of several significant incidents, various regulations (particularly in the USA, Holland, Great Britain, and Germany) are in place around the world. These regulations have also affected other industries. However, the chemical and petroleum industry remains the leading edge in development of management systems for process safety. For this reason, two noteworthy risk management systems are presented in **The CSChE and US-OSHA Models for Process Safety Management**. *Note: Some jurisdictions and organizations may refer to* process safety management as process hazard management*.* In addition, corporate ethics can be modelled on **The CIAC Responsible Care ® Model** for member organizations in Canada.

Process Safety Loss Incidents and The Injury Pyramid

In **Chapter 7, The Importance of Culture to the Organization** there is a brief discussion introducing process safety in **Frank Bird's Incident Pyramid**. It has been observed (anecdotally through data observations, not a comprehensive nor broad study) that a pyramid comparable to Frank Bird's Incident Pyramid can be made for process safety incidents. This comparison is made in the following two figures. Note the parallels in the corresponding layers of the pyramids.



Bird, Frank E., and Loftus, Robert G., Loss Control Management, International Loss Control Institute, 1976.

Process safety incidents can also be categorized based on the cost of the loss as well as the impact to the environment. Some jurisdictions and some corporations have strict and detailed definitions for classifications of process safety incidents. A set of suggested classifications for value-loss is given in the Process Safety Incident Pyramid (although these could easily be another magnitude higher, depending on the nature of the industry). Some examples of sets of loss brackets are:

Catastrophic Loss	Major Loss	Minor Loss
Loss > $500,000;	$500,000 > Loss > $50,000	Loss < $50,000
Loss > $2,000,000;	$2,000,000 > Loss > $100,000	Loss < $100,000
Loss > $5,000,000;	$5,000,000 > Loss > $1,000,000	Loss < $1,000,000

There are several practical applications of process safety engineering:

- to integrate safety in engineering for all life cycle stages of a plant: design, construction, commissioning, start-up, operation, maintenance, turn-round / shut-down, and ultimately decommissioning / demolition;
- to implement policies and programs to evaluate risks and to develop risk management plans; and
- to establish and follow Engineering Design requirements for robust designs of all independent layers of protection.

Leading organizations in process safety performance have innumerable policies, standards, engineering design requirements, and loss prevention principles for process safety that define the most effective technology for process design and equipment including safety-instrumented systems.

Section 6.2: Due Diligence as Applied in Industry

The following three statements are excerpts from the University of Alberta's **Earth and Atmospheric Sciences' The Safety Information Site** (http://safety.eas.ualberta.ca/node/74).

What is due diligence? Due Diligence simply means taking all reasonable steps to protect the well-being of employees, co-workers, students, and visitors. To comply with the standard of due diligence, all reasonable precautions must be taken, even to the point of exceeding generally accepted practices. Due diligence requires the identification of hazards and the implementation of specific preventative measures to protect employees from loss, injury, illness, and disease.

Why should you practice due diligence? In the event of an accident or injury, there is the potential for liability against individuals as well as corporations and institutions. The liability for environmental, health, and safety losses

or offenses is based on common law principles, and ignorance of the law is no defense (e.g., Occupational Health & Safety Act; Alberta Environmental Protection and Enhancement Act). Due diligence requires proactive management and corporate and individual accountability.

What are the Benefits? Practicing due diligence means providing reliable, serviceable, and maintained protective equipment and materials appropriate for the hazard. It also means ensuring that the employees and students are competent for the tasks they are required to perform and that they understand all instructions, information, and supervision. Records should be kept of all training, inspections, safety meetings, equipment maintenance, incidents, and investigations. Written policies and procedures need to be developed and a job demands analyses need to be conducted before designing any training program.

Legal Definitions

Some legal definitions are listed herein for ready reference. These definitions are useful for understanding what due diligence is, where and why a due diligence defense would come into play, and where it will not. The intent is to provide general information on what to do before something go wrong: your decisions as engineers and managers may be questioned or scrutinized should something go wrong.

- **Criminal Offence or Crime:** "An act or omission which is prohibited by criminal law and punished, usually by fine or imprisonment" (http://www.duhaime.org/LegalDictionary/C-Page5.aspx). In other words, in terms as what is prohibited by law or required by law, you did something you were not supposed to do, or you did not do something you were supposed to do.
- **Absolute Liability:** "An offence in which it is not open to a person to avoid liability on the ground that she or he acted under a reasonable mistake of fact which, if the facts had been as the accused believed them to be, would have made his act innocent" (http://www.duhaime.org/LegalDictionary/A.aspx). It is an obligation or command to do something or not do something. You do not have a choice; you must do it. In other words, there is no explanation for going through a stop sign; you are guilty and must pay the fine.
- **Strict Liability:** An offence following from "tort liability which is set upon the defendant without need to prove intent, negligence or fault; as long as you can prove that it was the defendant's object that caused the damage" (http://www.duhaime.org/LegalDictionary/S-Page3.aspx). It is the express possibility of right to choose to do something or not do something. You have the option of deciding if you do or do not proceed based on the situation and circumstances. You did something (or did not do something) with the best intentions in mind, taking care at each step, and some unforeseeable adverse event happened; something went wrong, and it is contrary to a regulatory law. You have committed an offence, but you have an opportunity to explain yourself; here is where "due diligence" comes into play.
- **Due Diligence:** "Reasonable verifications and precautions taken to identify or prevent foreseeable risks" (http://www.duhaime.org/LegalDictionary/D-Page3.aspx).
- **Defense of Due Diligence:** It is an organization's or an individual's means to defend itself by explaining that all reasonable precautions were taken during the course of work and, by providing evidence in the form of records and documents, that all reasonable precautions were in fact taken. In assessing a defense of due diligence, several factors are considered. These factors may be expressed in the form of the question: "Did the organization exercise its responsibility by taking all reasonable precautions and by verifying the effectiveness of those reasonable precautions so as to identify and prevent foreseeable risks?" Due diligence can be used as a legal defense under trial in a court of law. The defense of due diligence is described in law as a possible basis of an organization's or an individual's defense should they need to prove they were proper in their decisions. The defense of due diligence requires the defendant to prove his/her innocence versus the court having to prove one's guilt.

The Practical Application of Due Diligence

For the employee, due diligence means fulfilling the employee's duties according to the organization's policies, procedures, etc., for jobs and tasks in which the employee is competent. The employee's duties may include documenting the completion of those jobs and tasks. For the employer, due diligence means:

- providing accurate policies, procedures, etc. that meet or exceed minimum requirements as dictated by law (e.g., appropriate hazard / risk assessments and control measures);
- ensuring employees are trained and competent in their roles and jobs (e.g., training on procedures and work practices);
- ensuring employees are fulfilling the requirements of their roles and jobs (e.g., checking work practices); and

- documenting that all such activities have been done, as well as documenting what actions were taken when such activities were not done (i.e., when employees are not fulfilling the requirements of their roles and jobs).

Note: When employees fulfill their duties in accordance with organization policies, procedures, etc., the employees may not be looked upon as liable, and the employees may be insulated from any legal action. If such is the case, the investigation turns to those who are responsible and accountable for the policies, procedures; such action has led to charges against organization officials / senior executives. The opposite is true: employees who do not follow policies, procedures, etc. with due diligence leave themselves open to personal liability.

Due Diligence in Context of Risk Management

Due Diligence in the context of risk management means:

IF	THEN
If an organization has defined action plans to mitigate (eliminate, or reduce and control) the risks of an activity and decides to proceed with the activity,	Then the organization must implement the action plans and ensure that those actions are, and remain, effective in mitigating the risks.

Specifically, the organization must:

- understand the hazards and risks in the workplace and associated with any work activities;
- take all reasonable precautions and measures to protect PEAP;
- train their employees sufficiently and confirm that their training is effective;
- confirm (audit, check, inspect) that all reasonable precautions and measures are effective;
- where and when those precautions and measures are found ineffective (i.e., sub-standard conditions and work practices / at-risk behaviours), the organization must take steps to correct; and
- Document as appropriate.

The Importance of Documentation for Due Diligence

Recognizing our responsibilities under the Professional Engineers Act is one thing, but having to show we did what we determined as correct is another. There may be times when one is questioned / scrutinized as to how one arrived at a decision in the design of a machine or an installation, or around the operations of the business. This is where it becomes important to understand the concept of due diligence.

As discussed in this section, due diligence is supported by good documentation of the decisions made, actions taken, and work practices carried out, including: policies, procedures, and records (the supporting documents that are evidence that the actions were undertaken such as checklists, logbooks, and equipment records); training materials, competency tests, and training records of employees; performance / personnel files of employees; documentation showing change management of policies, procedures, etc.

The previous list also includes the management decisions: the need to clearly and comprehensively record management's decisions with sufficient background information. For many organizations, their policies, procedures, etc. describe how decisions are made and how to document those decisions; however, a record (a diary or journal) would be appropriate and prudent for individuals.

Should something go wrong, the documentation and records provide the evidence that the organization and employees were fulfilling their duties using the work practices as directed, instructed, or guided in the policies, procedures, etc. and that these duties were being fulfilled by competent employees. An inspector or investigator from the regulatory agency can demand these records. In the absence of these records, the employer organization cannot prove it has taken all reasonable verifications, precautions, and steps to identify or prevent foreseeable risks to protect the well-being of employees. In such a case, the employer may be fully liable for the consequences of any incident.

A Reminder About What's Important

This discussion is not so much about how a manager or an employee can protect themselves. It is really about how managers and employees are legally obligated to undertake their activities to protect people, the environment, etc. and, in legal terms, how to undertake their activities.

Section 6.3: The Business Case for a Risk Management Program

While the discussion in this section is primarily focused on the business impacts related to occupational safety, the concepts will equally apply to process safety and to impacts on all aspects of PEAP (environmental incidents, public safety and health, asset protection, business protection, and security).

Given the previous, incidents related to failures in process safety management are especially applicable because: a) the impact of these incidents can impact more than one person (possibly dozens and in some cases hundreds of people); and b) the costs involved for the follow-up of a major incident can easily reach into the millions of dollars. By adopting ESRM programs complete with expert resources, management efficiencies are made, and the potential Return on Investment (ROI) for having a strong risk management program increases substantially.

Why Do We Need to Build a Business Case for Risk Management?

Simply, it is hard to justify investment if there are no incidents. If funds are allocated to safety to prevent incidents, it is hard for management to see the fruits of doing this (i.e., ROI). Yes, their incident statistics should show success, but knowing the correct level of management focus and funding is difficult.

Most projects and priority initiatives are looked at from a value improvement basis. That is, if a new project is built, many factors can be determined, including meeting the customers' demands, improved quality of product, helping the organization image in the community, or reduced costs, among many things. The factor that is most often front and centre in any new project or priority initiative is the ROI (note: ROI is defined as the profit the project is expected to produce over several years and how long it will take to pay down the initial capital investment needed to build the project).

So, how does one do a similar analysis for paying out funds for a risk management program that is intended to prevent or mitigate incidents, or any installed capital project that is a risk reduction solution (a control measure)? This question is one that has not reached all businesses, as it should. Too often organizations look at risk management as a cost of doing business, instead of looking at it as an investment in the business.

The increase in public pressure to reduce workplace incidents furthers the need for presenting a good case for risk management. As can be seen in the next figure, steady progress has been made in reducing injury frequencies over time: These impacts are not just taking place in Alberta, but across North America and the rest of the world. The topic of risk management and its field of practice are becoming a sustainable development issue; more than ever, it is a means to remain viable and competitive.

The parallel is also seen in environmental protection, and here the business case is increasingly apparent. A business cannot simply decide to open shop (i.e., build a refinery, build a pipeline, start mining oil sands). It must have government sanction (approval), and thus it must have public support. This is the *de facto* license to operate. If an organization does not get it, or loses it, it is out of business (and cannot make a profit). Some examples where public opinion has significantly influenced proposed developments include: nuclear power in northern Alberta, the Northern Gateway Pipeline, Keystone XL, Alberta Industrial Heartland developments, oil sands development, and new well production techniques (such as hydraulic fracturing).

Cost of a Safety Program versus the Cost of Loss Incidents

Costs are incurred whenever an incident happens. Consider the costs to PEAP (i.e., injuries to workers and to the general public; environmental impacts; loss of assets; and loss of productivity (business output)). As has been demonstrated in many loss incident cases, those costs can be quite dramatic. Most analyses of the actual costs of injuries acknowledge that there are costs related to human suffering, but no attempt is made to quantify those costs. The only times that these costs are quantified on a regular basis are in various courts of law when lawsuits are resolved. Of course, the costs can be quantified for environmental clean-up, fines for violating occupational and/or environmental regulations, the costs for loss of assets and reputation, and for business interruption (loss of productivity or loss of business output).

Costs are also incurred when a program is implemented and managed to prevent incidents, known as the Cost of a Safety Program. This could include training, additional personnel, systems to gather data, protective equipment, procedure development and management, audits and inspections, etc. It also includes changes to designs or added mitigation features to a project as a result of proactive project reviews. These added features or design

changes eliminate incidents that might have happened, but will never be known. So how does one estimate these costs?

A distinction must be made between the cost of a safety program and the cost of loss incidents. While the difference may appear quite obvious, there are characteristics of each which must be understood. One particular characteristic of interest is the level of certainty of the occurrence of the cost of a safety program as compared to the uncertainty of the occurrence and cost of a loss incident. This is perhaps the single major difference that exists between these costs that so drastically influences managers. In addition, the uncertainty associated with a loss incident means that the potential savings of avoiding a loss incident are usually not included in a detailed financial analysis for purposes of hard investment of funds. The potential savings through loss avoidance must be carefully treated in the financial analysis.

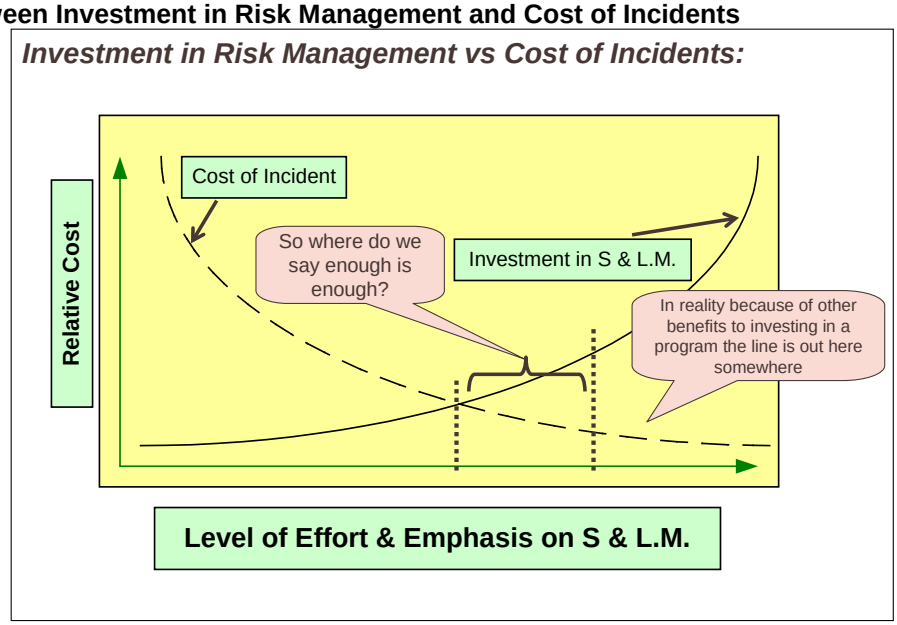
Certainty versus Uncertainty

In the face of uncertainty, organizations often grapple with the following questions: 1) if we do not have incidents, are we spending too much on a risk management program; and 2) how much is the "right amount" to spend on Engineering Safety & Risk Management?

The costs associated with injuries consist of the direct and indirect costs of injuries. These will be described in greater detail later. Nonetheless, these are costs that are incurred as a consequence of the incidents in which injuries are sustained. In other words, in the absence of injuries, there are no injury costs. This is a certainty. What is not certain is whether or not there will be an injury.

On the other hand, the costs of safety are those which are incurred as a result of an emphasis being placed on safety, whether it be in the form of improvements to facilities, upgraded equipment, training, alcohol/drug testing, safety incentives, staffing for safety, personal protective equipment, safety programs, etc. These are costs that are a certainty for any implementation of some facet of the safety program. The dilemma, on the surface, is that safety efforts will cost a given amount of money while the costs of injuries are incurred only if there is an injury. Thus, should funds be spent on safety when there might be no injuries even if there are not expenditures on safety? This is a game of probabilities.

Relationship Between Investment in Risk Management and Cost of Incidents



Hinze, Jimmie W., Richard J. Coble, Theo C. Haupt, "Incurring Costs of Injuries versus Investing in Safety" in Construction Safety and Health Management, 2000. S & L.M.: Safety and Loss Management

The above figure illustrates the relationship of the cost of incidents and the cost of a risk management program. The hypothesis is that incident occurrences (and consequently, the incident cost) will be high when there is a low emphasis on risk management, and incident occurrences will be low when the emphasis on risk management is high.

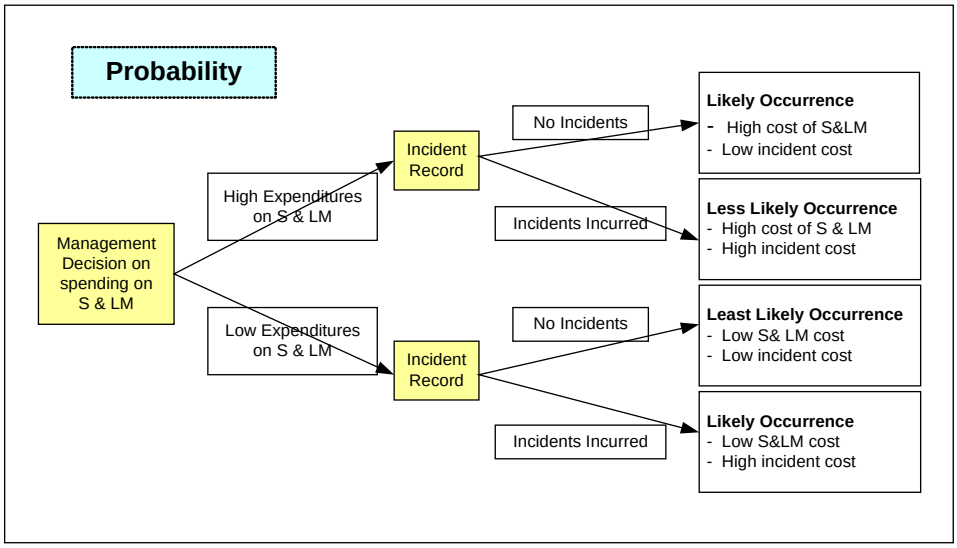
From an economic perspective, there appears to be an optimal level of emphasis to be placed on risk management. But, from a practical point of view, this level is rarely achieved with the emphasis generally being far below the optimal. This is because of the uncertainty. The dollars spent on risk management cannot be directly measured against the incidents that did not occur. Perhaps some modeling effort could generate a likely number of incidents in the absence of risk management expenditures. Even then, there will be tremendous or gross approximations that will need to be made to estimate the costs of the incidents that might have occurred.

These are all uncertainties that make it difficult to sell the need to make expenditures on risk management on a purely economic basis. It is important that an emphasis on risk management be recognized or even be accepted as being a principal means by which incidents can be reduced. If this is not accepted, the allocation of funds to the ESRM effort may fail to produce results simply because there is insufficient commitment to the effort.

The commitment of management to the concepts of a risk management program is crucial. This is the decision point, and if management believes in the risk management program and support its funding, the right things will happen. In the long run, their vision should see the results for which they are looking.

Likelihood: Relationship of Emphasis on ESRM to Incident Occurrence

The likelihood of an incident happening can be shown as in the figure below. Looking at it this way, management support for a risk management program should see the cost of incidents as low in comparison to the non-supportive management view. Incidents will happen, but with a program in place, the numbers and the impact of indirect costs will serve to reduce the overall loss. This is an application of a business probability model.



Hinze, Jimmie W., Richard J. Coble, Theo C. Haupt, "Incurring Costs of Injuries versus Investing in Safety" in Construction Safety and Health Management, 2000. S & LM: Safety and Loss Management

Cost of Injuries

Consider worker safety and the economic impact of injuries. Depending on how the economic impact of injuries is examined, a variety of ratios can be determined. All show that the uninsured costs drive the costs higher. For example, uninsured and indirect costs include:

- medical needs of the worker and their family members;
- possibility that the worker may be less productive, temporarily, after returning to work;
- the workers who responded to help in the emergency took time from their jobs;
- the workers involved or who were observers will not be as productive;
- the productivity of the injured worker's co-workers may be negatively impacted;
- the cost for a replacement worker to perform the job, including the training needed;
- the replacement worker will require time in the job before reaching similar productivity;
- the supervisor's time will take them away from other work, as more supervision will be needed;

- damage to facilities, equipment, or products;
- compliance officer inspections, recommendations, reports etc. will require management attention; and
- public meetings, media needs, and other issues.

These costs will add up and far exceed the actual cost (insured cost) directly incurred as a result of the injury incident.

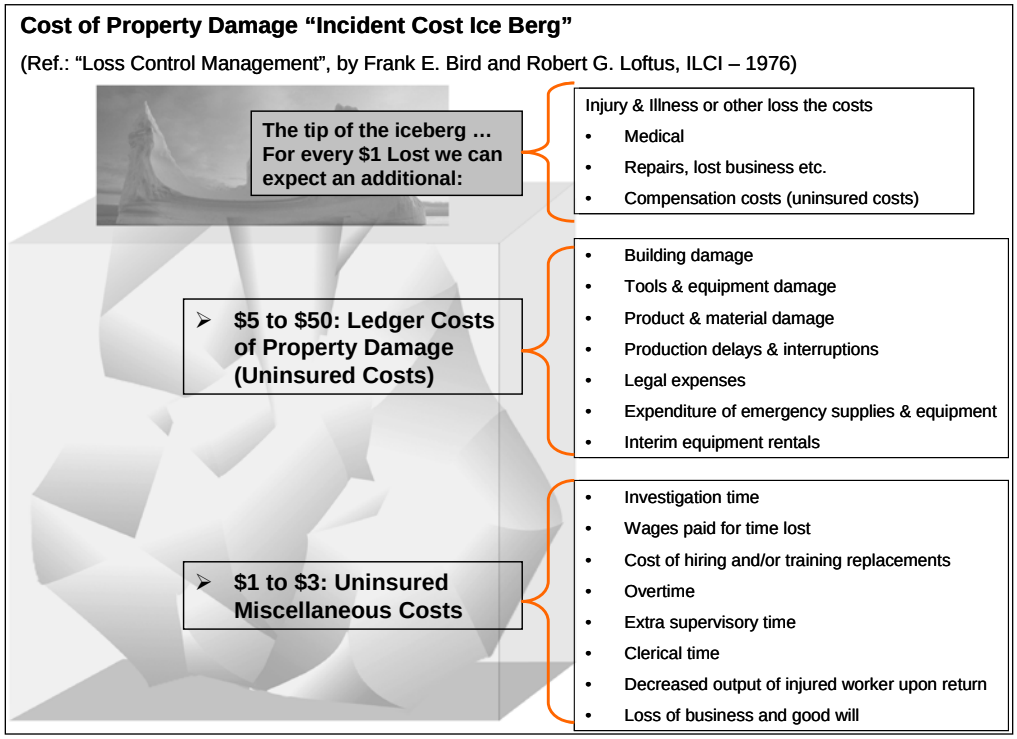
Summary of Indirect Costs Related to Medical Case Injuries

Not all types of costs will be incurred for every medical case injury. Furthermore, the costs will vary a great deal. An overview is given below:

1. Injured Worker:
   - Productive hours lost on the day of the injury
   - Productive hours lost subsequent to the day of the injury
2. Transporting the worker:
   - Productive hours lost on the day of the injury
   - Vehicle time and mileage
3. Crew costs:
   - Hours lost from reduction of crew
4. Workers idled by watching:
   - Other workers' time
5. Damages materials/equipment:
   - Worker time to repair the damage
   - Additional time to restore conditions
   - Money to replace damaged materials / equipment
6. Replacement worker:
   - Lost productivity per hour worked
7. Supervisory time:
   - Hours to assist injured worker and respond to the situation
   - Hours to investigate the incident
   - Hours to complete reports
8. Other impacts:
   - Hours working with safety compliance officers
   - Hour working with media personnel

The Incident Cost Iceberg

Similar relationships can be seen when looking at the Incident Cost Iceberg with respect to property loss incidents that may result from a process safety incident. Here, the costs due to environmental cleanup, replacement of damaged assets, lost business, and litigation by those whose lives and livelihood have been impacted escalate to higher levels. The argument for "loss avoidance" becomes much stronger.



The above Incident Iceberg breaks down the cost of a property loss incident where there is injury or illness to show the uninsured costs an organization can incur. Such costs are significant and by no means can be ignored while making the Business Case for having a Safety Program in place. Although Bird's study was conducted in 1976, the relative ratios remain the same.

Benefits of Risk Management, The APEGA Viewpoint

(From the APEGA Guideline for Management of Risk in Professional Practice – September 2006):
For some industries and in some jurisdictions, risk management is a regulatory requirement. However, for those who must be convinced of its utility, there are numerous benefits of risk management to a professional practice including the following:

- The control of risks is improved by identifying and minimizing the associated probability and severity of consequences.
- The explicit consideration of risk improves return on investment and allocation of resources by helping the professional practice to avoid harm, minimize losses, and save time. Risk management may indicate that the professional practice should back out of risky projects.
- The use of a comprehensive, documented, transparent approach to risk management demonstrates due diligence.
- There are fewer surprises. Risk management may help to uncover hidden risks in situation that appear straight forward at first glance.
- Risk management and communications promotes two-way dialogue with stakeholders regarding new operations, products, policies, or decisions, allowing them to understand and be part of the process.
- Investors, lenders, insurers, clients, and customers are increasingly drawn to professional practices that are able to manage risks effectively.

Benefits of Risk Management, The US Chemical Industry (AIChE) Viewpoint

The chemical industry has generally been the focus of most activity around risk management; however, like most programs, they are not sustainable if management fails to support the program. Economic data can be used to determine the ROI for expansions, debottleneck projects, etc., but the return on risk management programs is difficult to quantify.

A safety program requires allocating resources. If the program is successful, then injuries will be low. As demonstrated above, the cost of injuries can easily justify a program. Several organizations, through short-term goals, have forgotten the value of supporting risk management programs and have reduced resources resulting in an increase in incidents and costs.

In response, the CCPS of the AIChE (the Centre for Chemical Process Safety of the American Institute of Chemical Engineering) has developed some rationale for building the business case for risk management. The membership of the institution identified more than 50 benefits of having a program, and from these, four broad themes were identified that support sustainability:

1) **Corporate Responsibility** (includes social responsibility and product stewardship): Corporate responsibility builds positive and lasting relations with customers, suppliers, local community, the public, government agencies, and employees. Being responsible alleviates any safety-risk concerns of investors and improves relationships with financial institutions. Customers are assured of a secure supply. A safe workplace supports employees. The organization enjoys an improved reputation in the marketplace. Insurance premiums are lower.
2) **Freedom to manage and operate your business** (self determination): The sustainability of the organization is more assured with sound risk management programs in place. It assures that the organization will retain its license to operate with the full support of the public, community, and other stakeholders. Organizations must be responsible if they want to retain their social license. An organization's future can be severely impacted by a major incident.
3) **Loss Avoidance:** As demonstrated in many of the cases studies, incidents result in the loss of hard dollars. Losses include damage, business interruption (usually higher in cost and often 4 times the cost of damaged assets), regulatory fines, litigation costs (up to 5 times the regulatory fine cost), and finally loss of customer confidence and reduced sales. The incurrence of incidents means investigations, reporting, and following up, all of which draw on an organization's resources. This reactive response does not create new value. Organizations can demonstrate that effective process safety management programs have helped prevent major losses.

   It is also noted that major incidents within an industry have an effect on all organizations in that industry. This ripple effect ranges from the impact on regulations and to sales of products. Corporate executives are now being held accountable for loss incidents and are being charged for lack of due diligence in safety and risk management. Employees, managers, officers, and board members of organizations are then at personal risk beyond their jobs by not having an effective process safety management program.
4) **Creating Positive Stakeholder Value:** Good risk management avoids losses. Risk management improvements in process safety can lead to productivity improvements such as improved yields, higher through-put rates, higher reliability, less down time, and lower maintenance costs. Improved corporate reputation means acceptance by the community, stronger stock valuation, lower capital cost, a good market image, and positive impact on sales. Process safety management allows the organization to achieve substantial increases in revenues and profits.

The AIChE gathered the following data from several large chemical and petroleum organizations. These data demonstrate improved performance in a number of areas as a direct result of having a process safety management program (*Source: American Institute of Chemical Engineering, Center for Chemical Process Safety, "The Business Case for Process Safety", 2001*):

- 5% increase in productivity, primarily due to increased reliability of equipment.
- 5% reduction in maintenance costs.
- 3% reduction in production costs.
- 1% reduction in capital budgets.
- 20% reduction in insurance premiums.

Potential savings can be determined using the AIChE ratios above and the organization's operations data; thus, a positive ROI and a positive business case can be made for having a good risk management program in place based on improvements in productivity and lower costs in key areas.

This is an empirical approach based on the AIChE ratios. To apply this in an actual facility, you would require actual cost data and ratios more pertinent or specific to your facility or operation, which may require some data collection and analysis to determine those ratios. The **Before Implementation** vs. **After Implementation** should be analyzed to quantify and validate the actual improvements to further develop the model for the organization. This analysis can be done using the template at the end of this section.

A Preliminary Approach to a Financial (Cost / Benefit) Analysis

Financial analysis is a methodology for evaluating or assessing a project to determine the net value of it on the basis of cash flows. Cash flows include the initial investment, a decrease or increase in periodic expenses, and a

decrease or increase in revenue streams (i.e., the costs and the benefits). For an investment for profit, the investor has an expectation that the net financial value is positive (the threshold of which may not be simply "greater than zero") and if so, will proceed with the investment decision. Typically, such an analysis uses rigourous "time value of money" calculations (e.g., Future Value, Net Present Value, etc.) and values of costs and savings which are known to have a high degree of certainty (i.e., more precise and more accurate estimates).

The preliminary approach as described below is used to assess a) the costs of any improvement to reduce risk of a loss incident; and b) the cost avoidance of that loss incident. This is a preliminary assessment of a cost/benefit analysis because all information is not known or not known to a high degree of certainty / estimate (i.e., the values have a degree of uncertainty ranging from low to high). The methodology for this preliminary assessment is:

a) Determine the **Cost Avoidance of a Loss Incident**; this is typically the monetary value of the PEAP losses for a similar loss incident (injury costs, lost time worker costs, environmental clean up costs, asset and infrastructure costs, production losses, etc).
b) Estimate the **Initial Costs of Improvements**. Use actual values (if known to a high degree of certainty) or use the upper limit of the bracket when using the Complex Effort vs. Gain Tool.
c) Estimate the annual **On-Going Costs of Improvements**. Use actual values (if known to a high degree of certainty) or use the upper limit of the bracket when using the Complex Effort vs. Gain Tool.
d) Calculate the **Total Costs of Improvements** over the life of the project. In industry, the typical life of a project is 30 years. Therefore:

   Total Costs of Improvement = Initial Costs plus 30 times On-going Costs.

e) Calculate **Annual Risk Exposure (ARE) without any Improvements**. This ARE_1 is determined as the likelihood of a loss incident happening during the life of the project, where likelihood is the annual fraction of the life of project (i.e., one-thirtieth). Therefore, the ARE_1 without improvements is the Cost Avoidance of a Loss Incident times the likelihood of a loss incident or:

   ARE_1 = Cost Avoidance of the Loss Incident x 1/ 30.

f) Calculate **Annual Risk Exposure with Improvements**. In this case, the improvements reduce the likelihood of a loss incident by one to three orders of magnitude. To simplify, the likelihood is one one-thousandth (33.3 x 30). Here, the ARE_2 with Improvements is the Cost Avoidance of a Loss Incident times the likelihood of a loss incident or:

   ARE_2 = Cost Avoidance of the Loss Incident x 1/ 1000.

g) Calculate the potential **Gross Benefit**: This is determined as the Annual Risk Exposure without any improvements minus Annual Risk Exposure with improvements or:

   GB = $ARE_1 – ARE_2$

h) Calculate the potential **Net Benefit**: This is determined as the potential **Gross Benefit** minus the **Total Costs of Improvements**.

Two case studies are presented in the table below to illustrate the application of this preliminary approach. As stated, this is a preliminary analysis and is not intended to support nor drive the final financial decision. Further work must be done to increase the degree of certainty on likelihoods of the loss incident; improve certainty / accuracy of the cost estimates; improve certainty / accuracy of the savings estimates; consider and quantify other factors which may provide additional benefits; improve certainty / accuracy of the annual risk exposures; improve accuracy of the life expectancy of the project; and finally, consider the time-value of money. This detailed analysis must be performed using the accepted rules and guidance of the organization, and must meet the organization's investment threshold (i.e., a minimum ROI) before making a final decision to proceed (or not proceed) with the investment in the project.

Table: Preliminary Approach of a Financial (Cost / Benefit) Analysis

	Case 1	Case 2
Cost Avoidance of a Loss Incident	$ 1,000,000,000	$ 1,000,000,000
Initial Costs of Improvements	$ 10,000,000	$ 2,000,000
Ongoing Costs of Improvements per Year	$ 1,000,000	$ 100,000
Life of Project	30	30
Total Cost of Improvements	$ 40,000,000	$ 5,000,000
Annual Risk Exposure without Improvements	$ 33,333,333	$ 33,333,333
Annual Risk Exposure with Improvements	$ 1,000,000	$ 1,000,000
Gross Benefit	$ 32,333,333	$ 32,333,333
Net Benefit	**-$ 7,666,667**	**$ 27,333,333**

Business Case for Investing in ESRM Program for Company X:					
	Current Values	**Estimated Gains, % (per AIChE Ratios)**	**Improved Values**	**Net Gains**	**Units**
Production Rate:	Mkg/yr	%	Mkg/yr		**million kg per year increase**
Maintenance Costs:	$/yr	%	$/yr		$ per year maintenance cost savings
Production Costs:	$/yr	%	$/yr		$ per year production cost savings
Capital Costs:	$/yr	%	$/yr		$ per year capital cost savings
Insurance Premiums:	$/yr	%	$/yr		$ per year insurance premium savings
Incident Cost Savings:					$ per year in incident cost savings
			Total Potential Savings:		$ per year total savings
			Estimated Costs for ESRM Program:		$ per year of the ESRM Program
			NET POTENTIAL SAVINGS, ESTIMATE:		$ per year net savings, estimate

Section 6.4: Professionalism, Ethics and Equity, Integrity, and Conflict Of Interest

Without due care and diligence, your professionalism and ethics could be called into question, and no one wants this to happen in their careers. For example, the media reported on corruption within the City of Montreal management offices, with police investigations ensuing (2012-2013). These corruption cases have lead to investigations and charges against professional engineers within the municipal offices for alleged corruption crimes. Such actions are far from the standards of professionalism, ethics, integrity, and avoidance of conflict of interest that the public and our profession demand of its members. (The Quebec Corruption Inquiry, CBC News, https://www.theglobeandmail.com/canada/article-quebecs-anti-corruption-crusaders-have-been-swift-to-arrest-but-slow/)

Your reputation, your credibility, your career, and your ability to work in the profession is at stake. In this section, we discuss what it means to be an upstanding and outstanding professional engineer.

Professionalism and Ethics

We are professionals and have a responsibility under the Professional Engineers Act to perform our roles appropriately. (Note: Although course focuses on Alberta, each provinces across Canada has similar legislation.) The guidelines of The Association of Professional Engineers and Geoscientists of Alberta (APEGA; http://www.apega.ca/pdf/Guidelines/Professionalism.pdf) describe a profession as a calling that requires:

- specialized knowledge;
- intensive preparation;
- high standards of achievement;
- high standards of practice;
- ethical conduct;
- continued study; and
- public service (duty to the public).

The Canadian Council of Professional Engineers has defined the "Practice of Engineering" as:

> "The practice of professional engineering means any act of planning, designing, composing, evaluating, advising, reporting, directing or supervising, or managing any of the foregoing, that requires the application of engineering principles, and that concerns the safeguarding of life, health, property, economic interests, the public welfare or the environment."

This definition finds its way into the provincial legislation in each province as to how we must act as engineers. Note the words … "safeguarding of life, health, property, economic interests, the public welfare and the environment."

The parallel to PEAP is obvious:

- In this context, safeguarding means protection (i.e., the protection of life…).
- Consider the meaning of economic interests. The many cases we have studied demonstrate that Assets and Production / Productive Capacity clearly fall under this aspect, but look from the perspective of the recent news of corruption in Quebec. It should be readily apparent that we are talking about the funds and resources (and this includes confidential information and confidential data) entrusted to us by our employers, whether it is a government agency, or an enterprise.
  - The manner in which we manage those resources and the decisions we make concerning those funds are fundamentally based on our values, and some of those values are ethics, trust, honesty, and rightful ownership of property.
  - Suppose you are a petroleum engineer. Your employer organization is involved in well surveys and well servicing. A report comes across your desk that indicates much higher than expected reserves in an existing production zone. You recognize that this information is valuable to someone. What decisions and choices will you make? What are your values on which you base those decisions? Professionalism and ethics means that your decisions as a professional engineer must fall within the meaning of professional engineering.

The Practice of Engineering:

- **is technologically complex:** It is a specialization applying scientific principles from a multitude of different fields towards delivering safe and reliable products to our society.
- **has a large contribution to society:** Engineering achievements have contributed to the advancement of society. People greatly benefit from fresh potable water, reliable power and transportation, streets, bridges, buildings, and the consumer products we buy and use everyday.

- **has ethical obligations** to the public, employers, clients, and the profession: As discussed in this section, our responsibility is to the public, but of equal significance is our relationship with employers, clients, and the profession.

As professional engineers, our practice and actions are founded on these fundamental principles:

- Have proper regard for safety and protection of the environment
- Be a faithful agent of your employer (corporate loyalty)
- Respect confidentiality
- Provide factual representation of competence
- Understand what constitutes proper acceptance of professional responsibility to the public for engineering work (signing and sealing)
- Be honest and impartial
- Treat others with respect, fairness, and good faith

Professional Bodies

An engineer practicing anywhere in Canada is subject to the regulations and oversight of the provincial association which regulates the profession. In Alberta, the Association of Professional Engineers and Geoscientists of Alberta (APEGA):

- Administers the Engineering, Geological and Geophysical Professions Act of Alberta
- Publishes guidelines for professional practice and ethics
- Self governs: the Professions Act authorizes and empowers the association to govern its members without oversight or intervention by the provincial government.
- Serves the public interest
- Ensures high standards of practice
- Enforceable code of ethics
- Ensures only properly qualified people are allowed to practice
- Students in the Faculty of Engineering are student members of APEGA and "shall conform with the Code of Ethics"

Another professional body is the Canadian Council of Professional Engineers (CCPE), also known as Engineers Canada. Its purpose:

> "Engineers Canada exists in support of the constituent associations, to advance the engineering profession and its self-regulation in the public interest at a cost that is justified by the results."

CCPE also publishes a set of guidelines for professional practice and ethics. It is not the intent to review the content of these guidelines, rather to inform you that they exist and why they exist.

Public Expectations of Professional Engineers

The public, meaning anyone who engages a professional engineer for their services, has expectations:

- Competent and cost effective service
- Regulation in the public interest
- Protection of public safety
- Practitioners who keep up-to-date
- Ethical practice

Ethics in Engineering

Ethics in engineering is the study of the moral issues and decisions confronting individuals and organizations involved in engineering. The study of moral issues is the study of right (acceptable) and wrong (unacceptable) actions, behaviours, work practices. The decisions we make – whether "right or wrong" – are based on our values. The study deals with voluntary actions specifically taken by an individual with sufficient knowledge of the options available to him or her.

Code of Ethics

As professional engineers, and because we are a self-governing profession, we must live by a code of ethics to ensure we can meet the expectations of the public. We are governed by the Engineering, Geological and Geophysical Professions Act as administered by APEGA, including engineering students. The code of ethics:

- represents a consensus among engineers about the standards that should govern their conduct;

- provides guidance;
- does not necessarily provide a definite answer on how to handle a particular ethical issue;
- is a set of dynamic principals guiding conduct and way of life;
- helps us avoid conflict of interest; and
- teaches us that our actions should enhance the dignity and status of the profession.

Areas of Potential Ethical Problems

As professional engineers, we may find ourselves in positions where certain information entrusted to us is sensitive and could give an unfair advantage to one party over another. This unfair advantage could be unethical or illegal, and thus our decisions about using that information or decisions based on that information must adhere to our principles and our ethics. Consider these possible situations:

- Conflict of interest
- Conflict of Values
- Responsibility for public and worker health and safety
- Corporate loyalty
- Trade secrets, confidentiality, and proprietary information (technical or financial)
- Gifts from contractors or others
- Honesty in research and testing
- Treatment of others

One day, you may find yourself in a compromising situation where there is a potential conflict of interest. But if you give careful thought, make decisions based on the appropriate set of positive values, and set your standards accordingly, you can manage yourself through obstacles like these with little difficulty and gain the respect of your fellow workers.

Integrity and Ethical Behaviour

Here are two thoughts on integrity:

1) Doing the right thing at the right time. This is very easy to do if it is a positive, pleasant, or popular choice. It is not an easy thing to do when it is not positive, pleasant, nor popular.
2) Doing the right thing at the right time even when nobody is watching.

Which one do you think has the higher degree or is a more ideal example of integrity? Remember, that the right thing is what people perceive to be the right thing. So, imagine having to explain yourself and consider these questions:

- Will my decision / action pass a review on the court house steps?
- Will I be proud, embarrassed, or ashamed of my decisions / actions?
- How would my friends and family react to my actions when reading about it in the paper the next day?

Ethical behaviour is doing the right thing at the right time, even when nobody is watching. Ethical behaviour is the desirable path even when faced with challenges. It is not necessarily an easy path, a popular choice, skirting the law, skirting corporate values, nor inconsistent with corporate values. Even when the outcome of the decision is negative (i.e., challenging, difficult, costly, or damaging to your organization), the negative outcome should have no bearing on the decision.

The Decision to Make: Stay the Course of Ethical Conduct or Acquiesce?

You will be faced with challenges in your careers such as peer pressure, pressure from superiors, conflicts of values, conflicts of interests, and temptation (e.g., temptation of offers from those who inordinately or unfairly benefit from your decisions and/or your position of influence in the decision-making process, or temptation to unfairly profit or benefit from exclusive or “insider” information).

Will you have the courage to make the right and ethical decision when there is pressure to compromise? Or will you give in to pressure or temptation, or take the “easy” path because it is less of a struggle? A series of questions can guide you through this:

a) What is the situation or circumstance? This is the description of the reference concerning the possible choices and the possible choices that could be made.

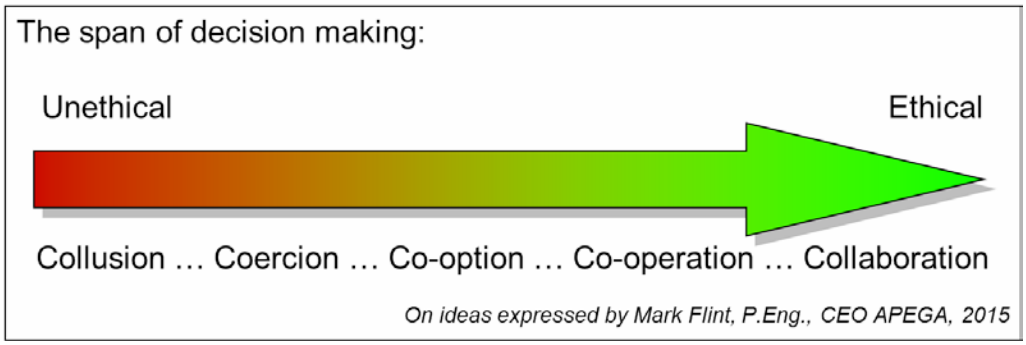
b) What is the issue or concern with that situation or circumstance in terms relative to ethical conduct? This can be best described by the issue or concern of the (unethical) choice being considered; the consequences of that choice in terms of impact on PEAP; and a notion about management’s awareness of the

issue or concern as it relates to legal requirements, statements and policies on corporate values, and/or professional ethics. What is the hazard (process or occupational), the risk of that hazard becoming uncontrolled under the current deficiencies, and the notion about management's awareness of the issue or concern as it relates to the select Key Point?

c) **What did you do (or what should you have done), again, in terms relative to ethical conduct?** Describe the decision made, its status (ethical or unethical), and the justification for this ethical decision (or lack of justification for this unethical decision).
d) **What was (or would have been) the final result or outcome?** Describe the outcome of the decision and the outcome of the activity.

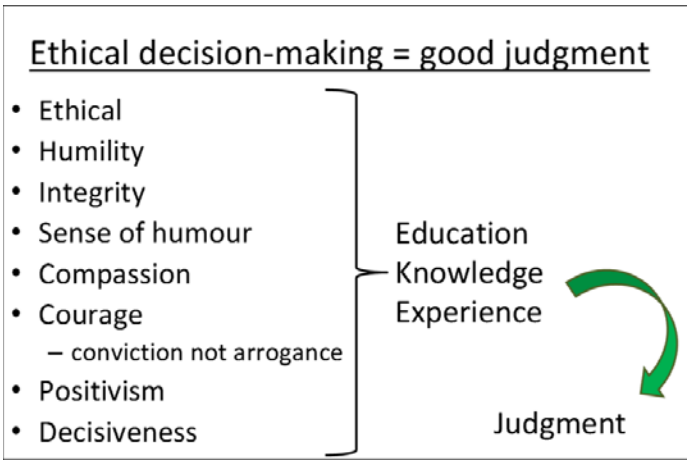
Ethical Behaviour, Leadership, and the Decision-Making Process:

The idea of leadership has been explored in several chapters. Here, leadership is further explored within the scope of ethical behaviour. Certainly, leadership involves a decision-making process, a process that more often than not involves other stakeholders (i.e., the employees that report to the leader, the employees affected by the decision, and the employees that implement management decisions). The manner and process in which those decisions are made characterize the degree of ethical behaviour. Below is a scale of conduct that ranges from most ethical to unethical: collaboration, co-operation, co-option, coercion, and collusion.



The Component Values of Ethical Decision-Making

Ethical-decision making is equivalent to exercising good judgment. Good judgment results when a person uses a set of positive values (e.g., an understanding of and belief in ethics, possessing a sense of humility, possessing integrity in a commitment to fulfill the spirit of the law and corporate policies, possessing personal traits of compassion, courage (conviction, not arrogance), being positive, and being decisive) in combination with his / her education, knowledge, and experience.



The Predicament: How Will You Manage Apparent Contradictions and Ambiguities?

What happens if you find yourself in a predicament? The actions of the organization seem to contradict the values of the organization or the organizational values seem to contradict your sound set of risk management principles and values?

- Your situation: You, a new graduate and just starting in your career, have a new set of values to support sound risk management practices, and you are hired by an organization.
- Your predicament: You find that the actions of the organization seem to contradict the stated organizational principles and values, or the organizational values seem to be, or actually are, contrary to sound risk management principles as taught in the ENGG404/406 courses.
- Your choices:
  - Do you degrade your values?
  - Or do you leave the organization in search of an organization with compatible values?
  - Or undertake the initiative to change the practices to align with sound values or change the set of principles and values of the organization. In other words, do you decide to undertake the challenge of changing the culture of that part of organization under your influence?
- Your ultimate decision depends on your position and level of influence, and why you were hired into that position.
- Fast forward: What happens if you find yourself in a similar predicament later in your career? In this case, it may be why you were hired into that new role: to change the culture. You should note that you may face the predicament at other departments or units within the same organization.

The Dilemma: Work with Your Organization or Whistleblow?

You may find yourself in a position where it seems your professional responsibilities and professional ethics are in conflict with your organization's actions. This can be an extremely complex issue to tackle in your career, with so many variables, unknowns, and circumstances specific to the case.

Recall the discussion on the relationship between you and your supervisor from Chapter 7 (Workplace Relationships: You and Your Direct Supervisor). Your first steps should be to work with your organization (i.e., to seek clarity and understanding of your organization's position), because the first possibility is a misunderstanding or miscommunication.

Should you find that there is no misunderstanding or miscommunication, your second step should be to work with the oversight groups (i.e., higher levels of authority, human resources, corporate accountability office, corporate ombudsman, etc.) and within your organization's corporate policies and procedures to resolve the issue. Of course, your position, authority, and influence in your organization can have a direct impact on the outcome.

Ultimately, you may find you cannot resolve the apparent conflict, and you are motivated to seek external avenues of inquiry (e.g., report to government authorities or professional associations) as a last resort. This action is termed "whistleblowing". **The act of whistleblowing is not a trivial action.**

Although there are some protections in some jurisdictions and by some professional bodies for the whistleblower, the process does call into question the integrity and ethics not only of the organization under scrutiny, but also of you, the whistleblower. The whistleblower's personal motivators may come into question: is it a grudge or an honest and factual concern driving this person? Factors that can affect the process and ultimately its outcomes include:

- perceptions of the individual and of the organization;
- the relationship between the individual and organization;
- opinions and positions of third-party bodies; and
- the personal feelings and emotions of the persons involved.

It is only through the fair and balanced investigation process of the authorities or professional bodies that a truthful outcome will be found.

.

ENGG404

Chapter 7: Leadership, Motivation, Organizational Design, and Culture

Chapter 7: Leadership, Motivation, Organizational Design, and Culture

Most people consider engineers to be professionals embodying attributes such as specialized knowledge, attention to detail, thoroughness, high standards of practice, continuous learning, and public service. These attributes represent an aspiring number of ethical expectations that we place on professionals in our society. Ethics is about "doing the right thing", and of paramount importance is the health, safety and welfare of the public. We have an obligation to provide safe workplaces and projects and there is an expectation to report on conditions that constitute a material, immediate threat to safety, health, welfare or the environment. Professionals also have a responsibility to lead by example, a requirement that incentivizes an engineer's efforts to be seen as a safety champion. Thus, from an ethical standpoint, safety takes precedence over all other considerations and it follows from the previous treatment that safety is simply "the right thing to do".

Safety champions are professionals that see safety as a moral imperative. The ripple effect of having an organization with engineers, managers, and senior leaders committed as safety champions means lives saved, harm prevented, the environment protected and organizations spared from tragic business loss. Organizations that are ultimately successful in achieving safety performance require safety leadership at every level of the organization. This means moving from compliance (something you have to do) to a commitment (a personal choice to support) where safety is integral to the job. Good safety is not achieved by an individual alone, but through a team effort. We know that, by themselves, folks may experience errors such as forgetting an important step, misreading a situation, or being unaware of an impending risk exposure. As a team empowered by agreement among members to observe and intervene, people look out for each other and responsibly self-correct variances when safety is challenged. It means "making everyone is a leader in safety". This high level of engagement is the hallmark of organizations achieving safety performance excellence.

In this chapter, we will consider factors that affect safety leadership at an individual, team and organizational level. What are the responsibilities of a manager in establishing a safe work culture? What principles enable a leader to gain the motivation and commitment of his/her employees? How do team behaviours and organizational culture affect the safety of everyday operations in an organization?

Section 7.1: The Importance of Culture – Making Everyone a Leader in Safety

The Merriam-Webster Dictionary defines culture as *"the set of shared attitudes, values, goals, and practices that characterizes an institution or organization"* (from http://www.merriam-webster.com/dictionary/culture accessed 24-April-2017).

Every organization has a culture. Every organization has sub-organizations, and therefore sub-cultures. An organization's culture directly determines its performance. Simply defined, culture is "how we do work here": it is something an organization *has* and *is*. Culture is manifested in organizational features such as structures, controls, reward systems, symbols, language, ideology, rituals, myths, human resource practices, performance criteria, location of authority, legitimate bases of power, decision making orientation, styles of leadership, compliance, evaluations and motivation (Schein 1985). Note that the sharing of attitudes, values and goals, and practices among the individuals within an organization define the culture of that organization.

Next come some defining questions. How do people see their leaders and how do those leaders define the culture within the organization? Let's examine a few examples. Bryan is all about keeping production moving. Mark is the leader that constantly talks about cost and budget performance. Gale is yet another leader with an unwaveringly focus on schedule, whether it be for that last maintenance outage or that next project milestone. In short, how do people see their executives, supervisors, general managers, and other senior leaders in the organization? What do these influential and respected individuals wear as a brand when it comes to corporate performance? How does a leader become a champion for safety?

These insightful observations and queries provide for sober reflection and may inspire a different mindset as leaders set about to navigate through the demands of their corporate responsibilities. To move as a leader from where people perceive they are today to where they need to go as a safety champion requires a large measure of courageous change at the personal level. Our leaders are very talented people and by now have mastered proven skills and strategies in their career path. However, to now integrate a new value set into a time proven capability that has served them so well in the past can be a challenging transition.

Once the organization's safety declarations are made and the safety presentations are given, our leader moves on to address other pressing business needs. A day in the life of an executive or senior leader can be interesting indeed, moving directly from the aforementioned safety work straight into a production meeting, conducting a project review, carrying out a stakeholder consultation, and the list goes on. However, beyond the previously specified safety work, safety is now a focus in all the business activities listed thereafter. In these beginning stages, this continuous and relentless focus on safety is accomplished by a leader personally demonstrating to the organization that safety support must move beyond words to becoming a way of doing business.

While our leader embraces personal change, becoming an emerging safety champion for the organization, it is in tandem with engaging the balance of organization leadership and teams towards promoting and encouraging safety leadership at every level. Business meetings to review performance now begin with safety and loss management as the first agenda item. Project management reviews begin with a focus on safety and loss management performance up-front. Every corporate board meeting begins with a stewardship on safety and loss management performance. Safety themed presentations are given at team meetings. Stakeholder meetings share the organization's efforts in safety leadership. Personal contacts with employees seek to explore if safety is being supported.

With each ongoing activity wherein safety is brought to bear as a focus, it becomes exceedingly clear to people that the move towards a higher performing safety culture is real, and over time is appreciated as something in the best interests of all affected. The care of executive leaders for peoples' safety builds a positive momentum on performance that spills over into all business dimensions as will be seen later.

Having safety as part of every conversation may seem daunting and perhaps artificial at the start, until leadership and the workforce shift in their understanding that the move to a safety culture is important and enduring. Senior leader perseverance in delivering the safety message at every opportunity and enrolling support through time is the imperative that will shape organization culture and the corporate DNA. When a safety culture is lived, it is evident to all of those within and external to the corporation. When a safety culture is prevalent, then on the occasion of corporate sessions when the question is posed, "how do we do work here?", the answer always is "we do it safety!".

As the safety journey continues, there will also be an important transition. When the CEO, Vice President or another senior leader enters the room, the attendant employees will tell you that that person is all about safety. The 'safety branding' of the organization is now clear. Safety is the norm, and it comes first. And when the brand promise is safety, it communicates a care for employees beyond any traditional measure, in that everyone understands their own personal safety and well-being come ahead of all other considerations.

As the corporate safety culture matures, safety may not even be explicitly mentioned in a particular conversation, but everyone knows that safety never takes a backseat to any other goal, objective or work activity. Most importantly, everyone understands the role they play is important to the total safety effort, and that for success "everyone must be a leader in safety". It goes beyond compliance (something you have to do) and becomes a commitment (a personal choice to support), and it underscores the importance of a team effort to succeed. Where an individual may have a lapse or unintended risk exposure, a caring team has the increased capacity to monitor each other's work with the intent of protecting folks from these variances (a simple cross check can reduce risk exposures by a factor of ten).

As everybody becomes a leader in safety, it is heartening when, at a particular juncture where safety may not have had the right airtime or consideration, it is the people and teams themselves that identify this potential departure, and leaders are supported to ensure that safety always comes first. It really is a team effort.

Building A Safety Culture and The Incident Pyramid

Risk is unavoidable. The everyday actions of individuals have inherent risk, regardless of whether the risk is considered high or low. This risk can be amplified with the actions of multiple individuals within an organization and can affect the operations of the organization and safety of its employees. Successful leaders of risk management understand the **Three Tenets of Risk Management**. These tenets are the base on which we create our values, influence individuals and teams, and shape the culture of our organizations.

1) **Incidents occur and are regularly reported in the media.** People are injured or killed. Leaks and spills affect the environment adversely. Facilities / equipment are damaged or destroyed. Services and/or production and productivity are interrupted. People's lives are disrupted. **These losses cannot be denied nor diminished.**

2) **Incidents are a source of learning, but incidents are a hard way to learn.** Incident investigations are not the way we want to learn! There are better and more proactive ways to improve. **Incidents are a tragedy, but the biggest tragedy would be NOT to learn from them.** Thorough incident investigations and risk reviews remain a critical skill in our risk management toolbox.

3) **All incidents are unacceptable and all incidents are preventable.** A leader's decisions and attitude toward risk directly affect the operations, maintenance and facilities of an organization and ultimately workers' lives, health and wellbeing. Our tolerance of conditions and practices that are substandard, or our intolerance of those, will define the culture of the organization that we lead and will determine the performance of that organization. **Our position and stature as a leader require us to espouse this tenet and diligently work towards preventing all incidents.**

The Incident Pyramid

The Incident Pyramid is based on the landmark Accident Ratio Study (Bird 1969) which found that for every major injury (death disability, lost time and medical treatment), there are 10 minor injuries, 30 property damage incidents, and 600 near miss cases. Industry opinion estimates another 3,000 to 10,000 instances of substandard conditions and substandard practices as shown in Figure 7.1.

Additional studies and observations propose ratios of the same order of magnitude where reporting protocols are similar. While Anderson and Visser (2013) has shown that these ratios are not applicable for all industries, **for our purposes, use the ratios (1 : 10 : 30 : 600 : 10,000)** as shown in Figure 7.1.

Incidents with Consequence vs. Incidents with No Consequence

Another important consideration to note is the differentiation between incidents with consequences and incidents with no consequences. The upper three levels of the pyramid in Figure 7.1 represent incidents with major consequences (i.e. incidents falling under the 1 : 10 : 30 ratio), while the lower two levels of the pyramid represent incidents with minor or no consequences, yet (i.e. incidents falling under the 600 : 10,000 ratio). Incidents with minor or no consequence can include:

- Non-first aids (e.g. a worker banged their knuckles when pushing on a pipe wrench).
- Near miss incidents (e.g. the pipe swung uncontrollably from the crane but did not strike anything).
- Substandard conditions (e.g. slippery floor caused by a spill).
- Substandard work practices (e.g. facility workers do not rigorously issue a safe work permit to trades workers).

Organizations with very good observation and inspection processes and reporting protocols will observe ratios of similar magnitude to the Accident Ratio Study.

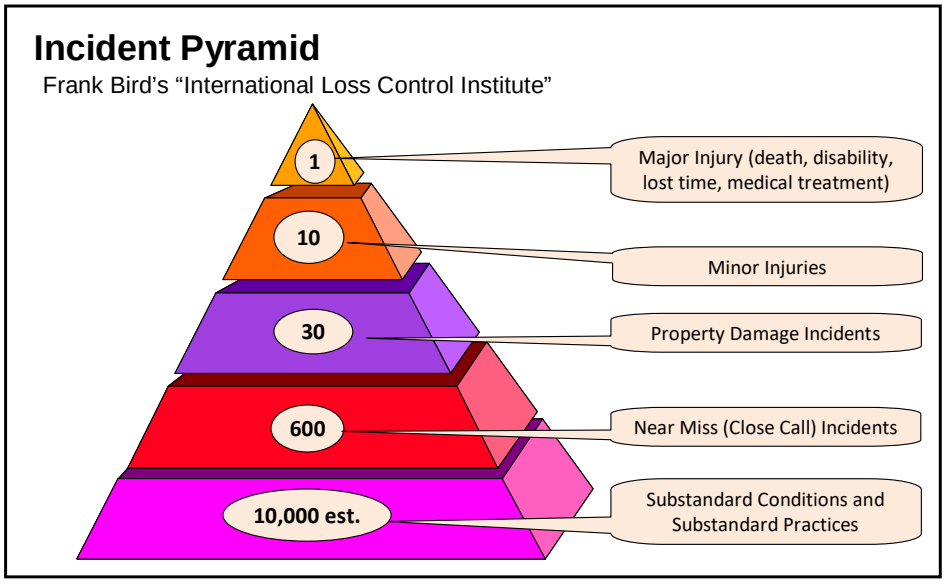


Figure 7.1 Bird, Frank E., and Loftus, Robert G., Loss Control Management, International Loss Control Institute, 1976.

It is important to note that the ratios are neither absolute nor fixed and do vary widely due to a number of factors. These factors can include, but are not limited to, the degree of observations and self-reporting on substandard conditions and substandard practices, as well as the extent of reporting major, minor and near miss incidents (close calls). Thus, statistics for different organizations may provide widely different incident pyramids. Intuitively, this makes sense: if an organization monitors and reports all incidents with minor or no consequence, then the base will be quite large.

Under-reported Incidents

Organizations with inferior observation and inspection processes or reporting protocols will observe skewed ratios versus the Accident Ratio Study. For example, where there is reluctance to report and correct the incidents with no consequences, the reported data will skew the shape to that of a pine tree as shown in Figure 7.2, where the actual number of incidents with no consequences are much higher. Quite likely, these incidents will go unresolved because they are not being reported and addressed.

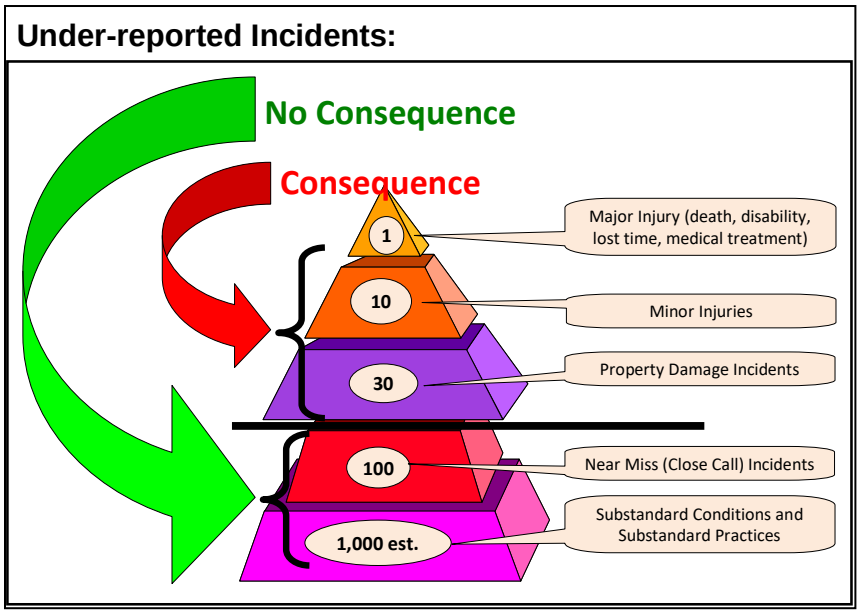


Figure 7.2 Under-reporting of incidents lead to a skewed pyramid. The black consequence line represents the separation of incidents with major vs minor or no consequence.

It is important to note that the extent of follow-up with corrective and preventative actions for all incident types in the pyramid will have the effect of reducing the number of serious injuries overall. **Superior-performing organizations have processes in place to observe, inspect, report, and correct all incident types**, both those with consequences and those with no consequences.

Proactive Action versus Reactive Response

Organizational personnel reactively respond to incidents with major consequences because it is after the fact: nothing can be done to change what has been impacted. What would happen if management addressed the many incidents with no consequences? The cumulative effect of learning from near miss incidents and reporting and acting on substandard work practices and conditions can prevent more serious incidents. **Superior-performing organizations take proactive action on incidents below the consequence line to prevent escalation to serious incidents and their consequences.**

Substandard Conditions and Substandard Practices

The incident pyramids suggest that a certain number of substandard conditions and substandard practices must be experienced (must accumulate) before a near miss event occurs, or that a certain number of near miss events must be experienced before a medical treatment case occurs, and so on up the pyramid. This is **not** the case.

These ratios are **not** wholly dependent on each other. It is more accurate to state that these ratios indicate a level of risk management and that these ratios are not a predictor of future events nor a predictor of the number of low-severity events that need to occur before a high-severity event occurs. Certain substandard conditions and substandard practices never, or with extremely low probability, lead to a severe loss incident (e.g. the substandard practice of leaving a filing cabinet open). However, other substandard conditions and substandard practices will, or with high probability, lead to a severe loss incident (e.g. the substandard practice of not anchoring one-self while working at elevation).

The challenge for management, who may be faced with limited resources, is to ensure that risk levels for activities and operations are continually monitored and ranked in order to focus efforts and resources on the right set of activities. Management must ensure that activities with higher risk exposure and/or increased risk reduction potential are done ahead of those with lower risk exposure. The action to continually monitor is a required step in the Risk Management Work Process, as discussed in **The Risk Management Work Process** (see Chapter 3).

The Link Between Safety Culture and The Incident Pyramid

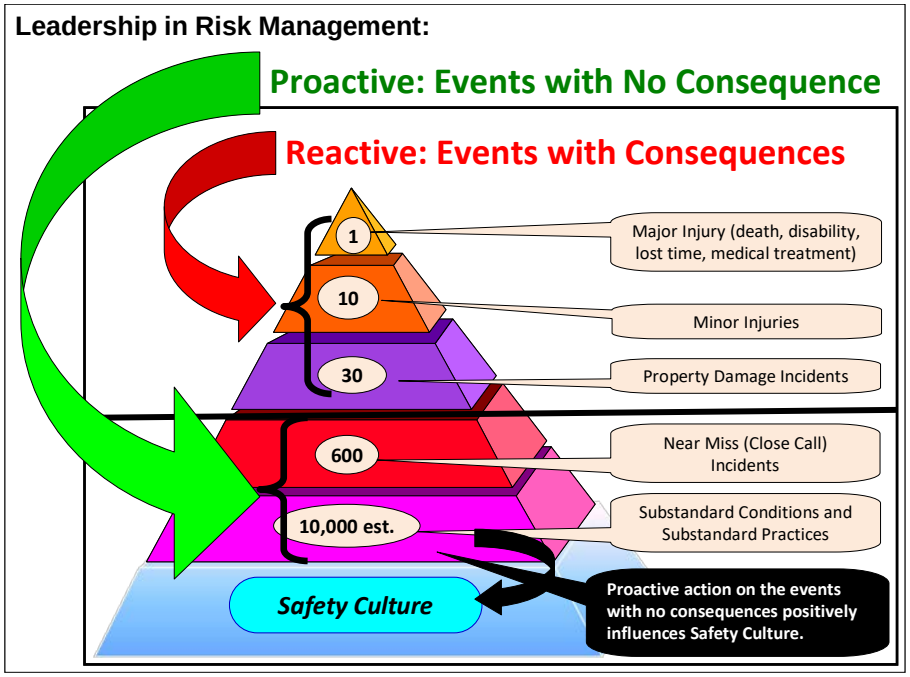


Figure 7.3 An organization's safety culture underlies how all incidents are dealt with.

The discussions on the Incident Pyramid are based on the premise that the number of near miss incidents and incidents with consequences increases with increasing occurrences of substandard conditions and substandard work practices. Since these substandard conditions and substandard work practices are subject to the underlying "culture" of the organization, it is vitally important to report and correct them in order to reduce near misses and incidents, as well as improve the culture of the organization.

Bird's (1969) model demonstrates the ratios of certain classifications of loss incidents over a very broad database. These ratios include loss incidents involving lapses in both workplace (occupational) safety and process safety for complex facilities. The discussion on process safety management, the related risks, and process safety loss incidents begins in **Risk Management in Industry** (see Chapter 6). The important point to note is that process safety incidents generally have a much greater potential to cause multiple injuries or fatalities.

The Link Between Safety Culture and the Performance of the Organization

Recall the incident pyramid. Why are the incident ratios (essentially, the shape of the pyramid) different for different organizations? Ratios are different because organizations have different safety cultures. When leaders work to improve their organization's safety culture, the performance will improve in all parameters – People, Environment, Assets, and Production (PEAP).

Work practices and workplace conditions are subject to the underlying culture of the organization and are the product of an organization's culture. Substandard work practices and/or workplace conditions will lead to unplanned incidents of varying severity in the workplace.

Given that the safety culture drives what happens in the organization and underpins the incident pyramid (see Figure 7.13), if a manager wants to improve performance, the manager must start by positively influencing the culture to routinely identify, report and correct substandard practices and conditions in the workplace (i.e. proactive management).

For example, the untidiness of a maintenance shop (extension cords, tools, equipment and materials scattered on the floor) is a substandard condition which can lead to an increased rate of tripping on or over those items. The untidiness is "accepted" – more accurately, tolerated – by the facility manager. This tolerance of untidiness is part of the culture that can lead to an incident. Conversely, our intolerance of such substandard conditions will define the culture of the organization that we lead and will determine the performance of that organization.

Creating a safety culture of recognizing and addressing substandard conditions is not the sole responsibility of one individual – the safety leader - but it is a collaborative endeavour which requires collective leadership towards safety and risk (Gray & Silbey 2011).

Section 7.2: The Power of Leaders to Influence Behaviour

The instinct to respond to/obey managers, leaders and authority figures is an important factor in human motivation and for understanding behaviour in the workplace. This factor underlines the vital role that leaders play in setting the culture of an organization or a team, and in shaping the behaviour of team members. If team members are willing to follow instructions from leaders, and have a deep sense of duty to authority, why is human error and at-risk behaviour such a problem in the workplace? Why can't we just put some good procedures in place and ask (tell) people to follow them? Is there more to workplace motivation than a strong drive to respond to the instructions of leaders and authority figures? These questions are explored in the following subsections.

Workplace Relationships

The Line Management Model plays a role in demonstrating the lens through which team members see an organization and their relationship with others in the line. Let's examine three key relationships in your career: 1) you and your direct supervisor; 2) you and your peers, the people with whom you work; and 3) you and the people that work for/report to you.

1) You and Your Direct Supervisor

While all relationships could be considered important, your immediate career success depends on the relationship you have with your direct supervisor. You can expect that your supervisor will set expectations for you in these forms: your area of responsibility, objectives and goals, policies and procedures, directions, jobs and tasks, and even "unwritten rules" of the organization culture.

Building a relationship with your supervisor is not a "one-time thing". It requires the right focus at the right period. It is critically important for you to understand your supervisor's expectations of you. Some challenges to expect:

- Too often the new employee will not ask questions for fear of looking stupid.
- ✓ Building the rapport early in the relationship overcomes this challenge.

- Too often the supervisor is not a skilled communicator, and the message they give is not clear.
- ✓ Take the time and make the effort to understand your supervisor's expectations.

- Too often the supervisor is busy with other duties and finds it difficult to have enough time to spend with the new employee, you, and does not see the long-term impact.
- ✓ Then briefly review with your supervisor to seek confirmation of your understanding

The start of any new job or role (or the case where your supervisor changes) is the time to begin building an effective relationship with your supervisor. Seek to understand what is expected of you through questions and discussions. This builds the rapport where it becomes natural to be open with your questions and your thoughts, not only in the short term, but also throughout the life of the relationship.

For the most part, supervisors like it when their employees directly ask them questions as this will confirm that their employees understand expectations. Ask questions until you understand and document answers to develop a set of your own references from which to work. As a new employee, you will be taking in a tremendous amount of information in a rather short period of time, and it is most difficult to memorize and recall all of it. In a fairly short time, you will be well into your job responsibilities, and there will be expectations on you to perform. Understanding expectations is a key success factor.

There will be a need to periodically update your supervisor on your progress. Your supervisor may initiate this, but if not, you need to make it happen by periodically giving your supervisor a progress report. In the early stages of building the relationship, a face-to-face meeting works best until a strong and comfortable working relationship has developed where the periods can extend, or progress can be shared by email or phone call. The progress report provides a means of interjecting comments, discussion of ideas, verifying that you are meeting expectations and managing your responsibilities such that there are "no surprises".

Recall what the Milgram experiment was about – the power of a position of authority (i.e. your supervisor) over you. When directions from your supervisor clash with ethics, values, norms, rules and/or policies, you need to be open and ask questions to verify your understanding. Communication is not easy. What might at first seem to be clashing or conflicting directions, may not at all be that. This also applies to seeking direction and clarifying expectations that your supervisor has of you. Your supervisor will want you to succeed, but your supervisor will also test you to determine how you react or respond to different tasks, situations, jobs or projects.

Finally, supervisors want solutions, not excuses, and not more problems. If things are not going as planned or expected in your area of responsibility, you will need help, and you will need to inform your supervisor. Do not let it go unreported until it becomes an unwanted surprise. Before doing so, make sure you have analysed and assessed the problem and have some possible solutions that you want to discuss for further direction. Better yet, have the right solution with all of the supporting information backing up that recommendation and ask for support.

While your immediate career success depends on the relationship you have with your direct supervisor, your long-term career success also depends on that relationship. By observing and applying the above over the long term, you will be able to sustain effective relationships with all of your supervisors over the course of your career.

2) You and the People that Work for You

Possibly earlier than you expect, you will be asked to supervise people. You will be the new person. You need to build the relationships with employees under your supervision, so you should take it upon yourself to apply many of the points listed in the previous subsection. Specifically:

- In the search for answers, your employee may feel that asking questions would be viewed as negative, so they won't for fear of "looking dumb". Your challenge is to create and maintain an organization where asking questions is viewed as and received as a positive experience.
- You need to make the effort and the time to initiate contact and interact with your employees. Developing respectful relationships right from the start is a key to success, and without a strong relationship, you could fail.
- You need to communicate clearly and always check for understanding.

No one has all of the answers, and everyone has different and complementary knowledge, experience and skill sets. Respect your employees for their skills and knowledge. Do not give them the impression that you know more than they do. Respect their knowledge and skills, and they will return that respect.

Building on the previous point, you have a "whole" person working for you, not strictly the skill set for which that person was hired. For example, suppose you hired an auto-mechanic for your fire brigade because (s)he was a volunteer community firefighter. This individual isn't simply an emergency responder or an auto-mechanic. To your pleasurable surprise, this individual quickly understands the risks associated with your mining operations and is extremely good at implementing appropriate control measures to manage those risks.

While you may have an area of expertise, your role as a supervisor is to guide and coach them to use their skills and knowledge to resolve issues and to support them when they do need help reaching resolution. Teams and teamwork are powerful engines for problem solving. Your employees are a resource for knowledge and information, which will help you make the right decisions. The collection of thoughts and expertise from all members will lead to better solutions, most likely different than your initial idea. Skills and knowledge are valuable so ensure you credit your employees for their contributions.

As the supervisor over other employees, you need to understand that people may blindly follow you (as was the case in the Milgram experiment). As critical as communication is, it is not easy, and you will be constantly challenged for clarity in your expectations / directions / instructions. Let your employees know in clear and certain terms what you expect, and if/when your expectations are confusing or conflicting, that you are open and welcoming to their questions to verify their understanding. Always respect the person who comes to you seeking clarity. Dignity, respect and integrity in your interactions with people are essential for building and maintaining effective relationships.

Finally, it is important that you not only set realistic expectations (or maintain the ones already established), but also that you "Walk the Talk". Never compromise the expectations you have of others. Your active visibility with your employees and your care for them will influence the culture in your organization. If your employees see that you are not following policy, they will see the double-standard and will not follow policy nor meet your expectations.

3) You and Your Peers

Be yourself, be comfortable, be open and be sociable. While this applies to all relationships, your peers want to know you. The relationship with your peers is mutual; it can be mutually rewarding because they need you as much as you need them. It may not be initially apparent, but you will become involved with them from time to time on your project or their project, or your career paths will cross. Be confident in your skills, but remain respectful of the skills and abilities of your peers.

Each of us is different. Because people perceive you through your actions and behaviours, you want your actions and behaviours to truly represent your honourable intentions. You are building relationships and associations for the future with your supervisor, with your peers and with your employees. You and your co-workers are part of a team, and all of you are there for the same overall purpose, working towards the same goal: contributing towards a successful organization.

What Makes an Effective Leader?

> "*Leadership is the use of power and influence to direct the activities of followers toward goal achievement. To accomplish this, a leader is entrusted with people and resources to add value to the business in a principled (legal, ethical, moral) way. A leader adds value by supporting their employees in a team or business unit so that they can do their jobs better.*" Gord Winkel, Chair and Industrial Professor, Engineering School of Risk Management and Safety.

A leader's values shape the vision and culture of an organization. A leader's values provide the foundation for an organization to define 'who we are' and 'how do we do things around here'. Leaders must understand their own values and those of the organization that, ideally, are aligned and serve as the standards for others. Having a set of values and adhering to those values are essential to effective leadership for the good of the organization and the good of the people in and affected by the organization.

Promoting an engaged safe team is helped by tapping into and promoting values that have meaning for team members and will encourage norms of safe behavior. Examples of values an organization and its leaders should promote to encourage a safe work place include, but are not limited to:

- Community: We have a sense of responsibility for the safety and care of colleagues.
- Accountability: We take responsibility for your actions.
- Collaboration: We work together.
- Empowerment: We respect and respond to everyone's need to show mastery and competence at what they do.
- Consistency: We respect and follow the safety policies, processes and procedures. Our work practices meet or exceed the documented requirements.

Being an effective leader is more than sharing an innovative, worthwhile, and achievable vision of the future of the organization. Leaders need to be approachable, trustworthy, knowledgeable and communicate effectively. Leaders need to be "system" thinkers, such that they can see the structures and processes that drive the organization's complex issues. By seeing the underlying processes within the organization, leaders can understand the mechanisms for changing the organization's response, while maintaining its values.

The Theory of Different Leadership Styles

Leadership is not 'one size fits all'. Different styles of leadership depend upon the time demands of tasks, stages of a project, levels of team development, ability and willingness of team members, and culture of the organization including the "global-ness" of the organization (i.e. international culture). There are three leadership theories that affect which leadership style one chooses: 1) individual motivation; 2) team behaviour; and 3) organizational culture.

1) **Individual Motivation:** Over the last 70 years we have seen work increase in complexity; people are required to apply deep skills and knowledge while machines, automation, and technology remove the requirements to complete simple tasks. This sophistication in work has been matched by more sophisticated theories of management and a deeper view of human nature.

   Self Determination Theory focuses on the degree to which an individual's behaviour is self-motivated and self-determined. The hypothesis is that people have three basic psychological needs: competency, relatedness, and autonomy. To motivate people to perform to the best of their ability we must look to provide environments where the following will flourish:

   - **Competency:** Whether it is fishing, sailing, skiing, or engineering, we have an innate need to learn, develop, and hone our skills. We will happily sit for thousands of hours to learn to play a musical instrument for no reward. Work can also provide opportunities to learn, develop, and hone skills so we can do our best and become valued employees.
   - **Relatedness (development and maintenance of relationships):** We are social and tribal by nature. Many people spend more time at work than with their families, thus having deep relationships of trust and respect is a vital aspect of an effective team. Where this is achieved, individuals will conform to the group norms and behaviours, and will be willing to make significant efforts to support team goals and objectives. It is important that those group norms include respect for safety rules and the achievement of the highest safety standards.

     Further, rather than just being a job that provides a wage, work can be an important source of meaning. We can be part of something that has a purpose and a contribution to the community, a great organization that is doing valuable things. An important element of this purpose can be pride in achieving excellence and being part of a work community that cares about each individual's safety and well-being.
   - **Autonomy:** Although we want to be part of a social group, and recognize the need for leaders, we also have a strong sense of our 'self' as an independent person – a person who cherishes the right to make decisions and choices that align with our interests and desires. Micromanaging, right down to telling workers when and for how long they can go to the washroom, will destroy all autonomy and will be deeply demotivating and alienating.

2) **Team Behaviour:** Social action theory has many applications, but when it comes to risk, this theory states that people take risks because of peer pressure or a general community perception that an activity is low risk. A person could be persuaded to engage in unacceptable (even unsafe) behaviour if "everyone else is doing it" or the community at large doesn't perceive an action to be unsafe. Leaders should create and/or influence the team environment so that teams or "work communities" do not have an informal culture of breaking the rules and taking risks. Leaders should encourage strong behavioural norms of low risk behaviours and compliance with safety rules and procedures.

Working in teams is a very effective and productive way to get work done. Tuckman's Model hypothesizes that as a team progresses from leader-directed to self-directed management, the commitment level of the team members increases. As leaders, we want increased commitment from our employees; thus, it is our job to put supports in place for self-directed, empowered teams to form and flourish. Leaders need to understand the capabilities of the employees under their supervision in order to set them up for success, not failure. Don't assume your work groups are empowered. Test their skills and knowledge using appropriate human resource policies and processes. If they are not capable of being self-directed and empowered (e.g. high turnover rate might be a factor), then you may initially have to give more direction. In absence of a fully-empowered self-directed team, the leader will need to step in to provide more direction.

3) **Organizational Culture:** Social control theory states that an individual's "connectedness" to an organization promotes behaviour conformity, which can have a positive influence on risk perception and encourage acceptable (safe) behaviours. Studies show that employee engagement through volunteer or safety programs tends to raise risk awareness and reduce risk-taking in the workplace. Being able to participate in hazard identification and contribute to workplace safety improvement builds affiliation with an organization and leads to safer work practices.

Organizational identification, or a connection to organizational goals and a collective work identity, is associated with fewer occupational hazards and greater safety participation. Employees with greater organizational identification are more likely to encourage coworkers to follow safe work procedures and take action to stop safety violations.

How to Unlock Discretionary Performance

This section explores the management of people: understanding what drives behaviours in the workplace and how to manage those behaviours. It includes managing the skills and knowledge of people (i.e. motivating people to use their set of skills to the best of their ability) to empower people in the workplace. It rests on an understanding of yourself and others in order to achieve shared responsibility and shared leadership. Being able to effectively engage people in the workplace is an important attribute of good leadership and healthy team environments.

The study of human motivation has a special focus because it builds the bridge between good management and good leadership. It provides the tools necessary for a leader to both manage and lead people effectively. To unlock people's discretionary performance, the single most important factor is to "engage" the workforce. "Work Force Engagement" is attained through the leader's actions at each stage of the model. These concrete actions enable a leader to engage the workforce:

- When a leader shares their expectations and values, workers feel safe and secure in their roles within the organization.
- When a leader provides workers opportunities to participate and contribute, the leader's employees feel that they control their own destiny – and do.
- When a leader encourages their employees to act on those opportunities, the employees feel that they are part of and belong to the organization.
- When the leader respects employees for their accomplishments and recognizes them for their accomplishments, the leader's employees build confidence and feel confident.
- The leader's ongoing efforts in these actions build and maintain workforce engagement and sustain the employees in a state of self-motivation.

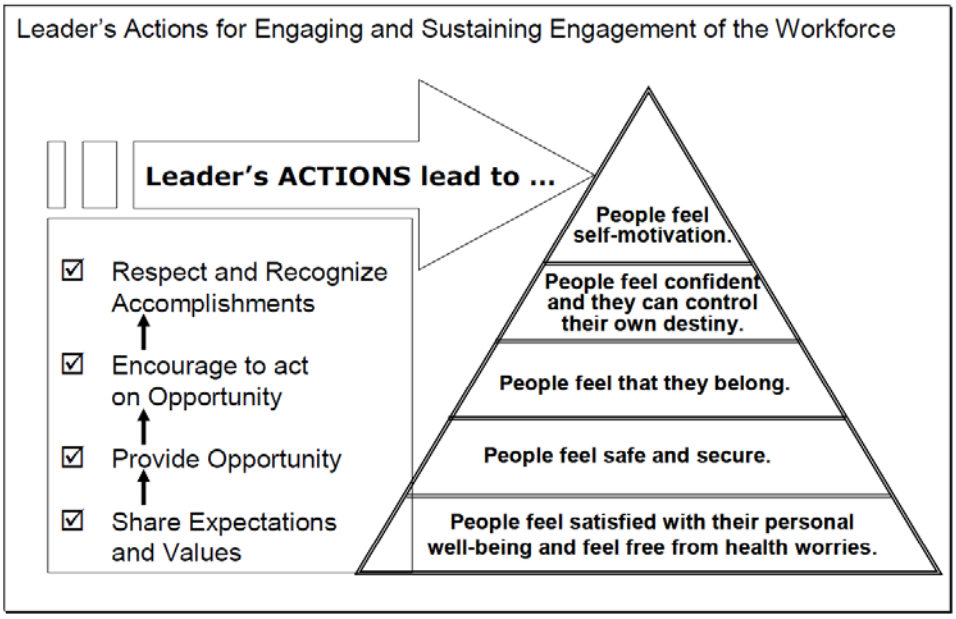


Figure 7.4 Leader's Actions for Engaging and Sustaining Engagement of the Workforce.

The Characteristics of Good Managers

Good managers have common characteristics in leading their organizations. When it concerns engineering safety and risk management, good managers:

- Provide the leadership and commitment to obtain and maintain first-class results in safety and risk management. This is the key to success.
- Must have a working knowledge of the fields of expertise and be able to critique intelligently.
- Know how to make the best possible use of the knowledge and skills of specialists in a team approach.
- Ensure that the whole organization is involved, not just the specialists.
- Ensure that a first-class, comprehensive safety and risk management program is installed and managed effective, and understand the benefits.
- Be able to view the long-term picture with a view toward continuous improvement in a cost-effective way.

When Leadership Fails: The Milgram Experiments

By Dr. Stanley Milgram, social psychologist, 1961 – 1962 at Yale University (Edited)

Experiments were run by a psychology professor named Milgram in which participants in the teacher role were willing to deliver continued, intense, and dangerous levels of shock to a kicking, screeching, pleading other person. Only one major aspect of the experiment was not genuine. No real shock was delivered; the Learner, the victim who repeatedly cried out in agony for mercy and release, was not a true subject but an actor who only pretended to be shocked. The actual purpose of Milgram's study, then, had nothing to do with the effects of punishment on learning and memory. Rather, it involved an entirely different question: when it is their job, how much suffering will ordinary people be willing to inflict on an entirely innocent other person?

The answer is most unsettling. Under circumstances mirroring precisely the features of the bad dream, the typical teacher was willing to deliver as much pain as was available to give. Rather than yield to the pleas of the victim, about two thirds of the subjects in Milgram's experiment pulled every one of the thirty shock switches in front of them and continued to engage the last switch (450 volts) until the researcher ended the experiment. More alarming still, not one of the forty subjects in this study quit his job as Teacher when the victim first began to demand his release; nor later, when he began to beg for it; nor even later, when his reaction to each shock had become, in Milgram's words, definitely an agonized scream. Not until the 300-volts shock had been sent and the victim had shouted in desperation that he would no longer provide answers to the memory test did anyone stop – and even then, it was a distinct minority who did.

These results surprised everyone associated with the project, Milgram included. In fact, before the study began, he asked groups of colleagues, graduate students, and psychology majors at Yale University (where the experiment was performed) to

read a copy of the experimental procedures and estimate how many subjects would go all the way to the last (450 volts) shock. Invariably, the answers fell in the 1 to 2 percent range. A separate group of thirty-nine psychiatrists predicted that only about one person in a thousand would be willing to continue to the end. No one, then, was prepared for the behaviour patterns that the experiment actually produced.

The explanation that subjects weren't scared of the potential physical danger to the victim was also examined in a subsequent experiment and found to be wanting. In that version, when the victim was instructed to announce that he had a heart condition and to declare that his heart was being affected by the shock – "That's all. Get me out of here. I told you I had heart trouble. My heart's starting to bother me. I refuse to go on. Let me out." – the results were the same as before: 65 percent of the subjects carried out their duties faithfully through the maximum shock.

Milgram is sure he knows the answer. It has to do, he says, with a deep-seated sense of duty to authority within us all. According to Milgram, the real culprit in the experiments was his subject's inability to defy the wishes of the boss of the study – the lab-coated researcher who urged and, if need be, directed the subjects to perform their duties, despite the emotional and physical mayhem they were causing.

The extreme degree to which subjects in Milgram's situation were attentive to the wishes of authority was documented in yet another variation of the basic study. In this case, Milgram presented the Teacher with two researchers, who issued contradictory orders; one ordered the Teacher to terminate the shocks when the victim cried out for release, while the other maintained that the experiment should go on. These conflicting instructions reliably produced what may have been the project's only humor: in tragicomic befuddlement and with eyes darting from one researcher to another, subjects would beseech the pair to agree on a single command they could follow: "Wait, wait. Which is it!?" When the researchers remained in disagreement with each other the subjects tried frantically to determine who was the bigger boss. Failing this route to obedience with the authority, every subject finally followed his better instincts and ended the shocks. As in the other experimental variations, such a result would hardly be expected had the subjects' motivations involved some form of sadism or neurotic aggressiveness.

To Milgram's mind, evidence of a chilling phenomenon emerges repeatedly from his accumulated data: it is the extreme willingness of adults to go to almost any lengths on the command of an authority that constitutes the chief finding of the study. There are sobering implications of this finding for those concerned about the ability of another form of authority – government – to extract frightening levels of obedience from ordinary citizens. Furthermore, the finding tells us something about the sheer strength of authority pressures in controlling our behaviour. After witnessing Milgram's subjects squirming and sweating and suffering at their task, could anyone doubt the power of the force that held them there?

The Milgram experiments detail how an instinct to respond to leaders and authority figures is an important factor in human motivation and understanding behaviour in the workplace. It underlines the vital role that leaders play in setting the culture of a team or organization and in directing team members' behaviour. It is important to remember your influence as a leader to guide others in building a safety culture.

In another case, on April 28, 2015, Brian Frederick Tomyn, aged 55, had been working with a backhoe operator, digging a trench on 123rd Street in Edmonton, Alberta. He was working to connect new water and sewer lines to a nearby home. The trench was not braced in any way and a wall collapsed, burying Tomyn alive. After a CCOHS investigation, the job site supervisor was sentenced to four months in jail, and his employer fined almost half a million dollars. According to the case judge, the accused 'exploited the vulnerability of a vulnerable worker at their own profit…They put their own interests ahead of any regulations." Yet another example of failed safety leadership.

Section 7.3: Causes of Safety Incidents: At-Risk Behaviours and Human Errors

There is no single cause of any incident, but research shows that human error typically plays a major part. Where technology stops, humans are the ones remaining to do the work, and as humans, we are not perfect and over time error can result.

However, when identifying human error as a cause, we must be careful to correctly identify the underlying (or **latent**) causes for the 'mistake' that has led to the incident. An error may be the result of substandard conditions and substandard practices, such as a poorly designed process or system, bad communication, a lack of training or management turning a blind eye to poor practices and behaviour. Simply categorizing any of these underlying factors as human error or mistakes runs the likelihood that the actual systemic causes are missed. As such, human errors are more correctly termed "human factors", which is a category of basic causes.

Habituated Action Theory

Even experienced team members may become complacent about risk. Habituated Action Theory argues that engaging in high-risk behaviour many times without a negative outcome often decreases the perceived risk associated with this behaviour. Those who repeatedly perform a high-risk action without an adverse consequence eventually become desensitized to the risk.

In a study of attachment to cell phones, it was found that those who habitually used a cell phone while driving had a lower risk perception than those who had a lower proportion of trips taken while using a cell phone. These studies show that risk taking can lead to a vicious cycle of more dangerous behaviour if negative consequences are not swiftly realized. Risk perception continues to decrease and risk tolerance continues to increase in this cycle. These insights have particular importance for the management of team members in high risk environments where experienced workers may become complacent and place themselves and their colleagues at risk.

Use the principles of the Self Determination Theory to consider how you could motivate experienced workers in high risk environments to respect safety rules and procedure.

Section 7.4: Leadership Models – Applying the Principles of Human Motivation to Lead Safety

Historically, incident prevention typically used additional administrative and engineering controls. Implementing more policies and procedures, and installing more engineered systems were often perceived as being easier than addressing the issues of unacceptable/at-risk behaviour.

Addressing unacceptable/at-risk behaviour is a challenge for many people and organizations because it involves a great deal of coaching, intervention and perhaps confrontation. It is especially difficult when people lack the skills or the motivation to handle these situations or if they do not appreciate the risk of not addressing these issues.

When you consider that most incidents have basic causes that are directly related to behaviour and motivation, then addressing these issues is an imperative for incident prevention and improved performance in safety and risk management.

What are common ways of dealing with these issues?

Leaders must deal with situations where people fail to fulfill their roles effectively and efficiently. People have responsibilities, and people must be held accountable for their decisions and actions when performing their job. When people make mistakes or perform substandard work, the leader must know how to manage their response.

Initially, under responsible management, this involves determining why the work was substandard: did the worker have the right job line-up, procedure, tools, training and/or instructions? This allows responsible management to look for and address latent causes, and guides the correction of the substandard work to an acceptable level. In very few cases, may this require addressing unacceptable behaviours. Leaders must take action to correct substandard work practices so workers are set up for success on future jobs. Leaders must address unacceptable workplace behaviours because they are accountable for their workers' decisions and actions. If a leader does not take action, the next-level leader must (and will!).

The following are common leadership models that can be used to inform strategies for developing strong safety cultures, thereby addressing substandard practices and conditions in the workplace:

- **Model 1: "Our Personal Iceberg" Model**
- **Model 2: The Line Management Model**
- **Model 3: The ABC Model**
- **Model 4: The Swiss Cheese Model**
- **Model 5: The Training and Learning Cycle Model**

For all models, we stress the importance of treating people fairly, equitably, balanced and with dignity and respect. Leaders should take the opportunity to recognize good behaviours and good work.

Model 1: "Our Personal Iceberg" Model – How Attitudes Shape Behaviours

People are complex, and we hardly ever see the “whole” picture of a person. In everyday work situations, a leader might see only the “surface” skills of a co-worker, but managers need to consider the “parts that make the person” (strengths, values, attitudes, etc. as shown in Figure 7.5) rather than just dealing with their demonstrated actions and behaviours.

All employees in an organization have a personal iceberg regardless of their position. An individual’s personal iceberg starts with their core strengths and works all the way up through to their opinions, all of which form their intent to act and forms how their intentions are translated into actions. It is the actions that people see, and this is how people perceive others.

Being able to effectively engage people in the workplace is an important attribute of good leadership and healthy team environments. For people to carry-out desired behaviours willingly, management must understand what drives the behaviours for each of their employees (i.e. what is below the surface) and support their employees in order to gain commitment. For example, rather than simply rewarding good and punishing bad behavior, leaders should aim to create work environments that meet the core needs of the individuals to influence their behaviour.

This model acknowledges and celebrates that all people are different and that leaders must work at understanding and valuing each team member as an individual with their own values and goals. Leaders should work at building a relationship with each team member where there is trust and understanding of these differences. This model also draws attention to the idea that individual motivation (i.e. values) can influence attitudes and beliefs, in this case towards safety, which will be an important part of building a safety culture.

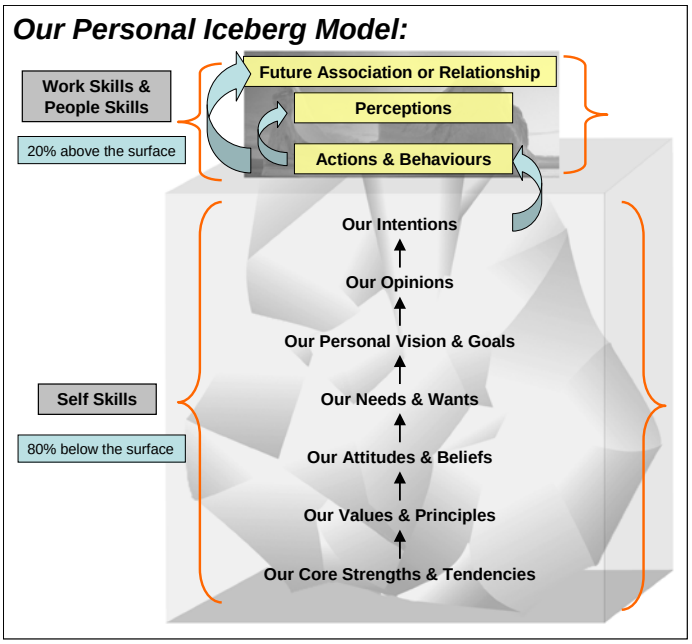


Figure 7.5 Our Personal Iceberg Model: Above the surface demonstrates visibly how people behave. Below the surface is the story behind the behaviour: the reason people act the way they do, what motivates them to act the way they do.

Model 2: The Line Management Model – How it Addresses “At-Risk” Behaviours

The Line Management Model describes an organization that produces goods and/or services through its workers, and although these workers exist at many different levels within the organization, it is the front-line workers who generally accomplish the productive output of the firm. Thus, the relationship between the front-line workers and their direct leader is very important to the effective and efficient productive output of an organization. This is not to discount senior leaders: they have the same responsibility as front-line supervisors to see that their teams function effectively in a healthy workplace culture.

The Line Management Model (Figure 7.6) characterizes the organization in two parts:

1) The relationship of the employees within the operations side of the organization (the left-most list) and the lines of management that exist. The output of the organization is done by the workers through effective and

productive action. The workers have a leader (the supervisor) and the supervisor has a leader (the managers) and so on and so forth up the line. Line managers are responsible and accountable for managing the risks of their activities and operations, not the persons in the functional expertise role.

2) The relationship of Line Management to the functional expertise side of the organization. The functional expertise roles are internal consultants or trained leaders. They have considerable expertise as a particular subject matter and work for the organization. Although they do have leaders, their fundamental role is to provide expertise to those in operations (i.e. those who actually produce the output of the organization).

One key requirement for leadership at all levels in the organization is to ensure that functional expertise in safety and risk management is linked or leveraged to support the line organization. It is especially important to recognize that front-line workers, by virtue of their direct exposure to energy sources and plant equipment, must be well supported by leadership to manage risk in the workplace.

Larger organizations employ a great number of experts in their field. These experts are leveraged (shared) to support all operations within the geographic area where the organization has operations. The expertise can be on a regional, a national, or a global (corporate) basis. Smaller organizations may not have these internal experts and therefore must hire consultants on an as-needed basis.

The fields of expertise within organization relevant to risk management are:

a) Occupational Health Specialists
- Occupational Hygienist
- Occupational Medicine (specialized doctors)
- Occupational nurses

All work in the area of industrial environment, chemical and material hazards, ergonomics, stress, noise, job design, etc., as they affect the health of the worker – both short and long term.

b) Safety Specialists
- Safety Supervisors / Managers
- Safety Consultants
- Safety Inspectors – Occupational Health & Safety (OHS) / Alberta Labour

All work in the area of reducing the risks of accidents to people in the workplace by learning from investigations, providing training, coaching and leadership.

c) Design Specialists
- Design Engineers
- Specialized Safety Design Engineers

Ensure that plant and facility designs have built in safety features and meet all government codes and industry practices in this respect.

d) Risk Analysis / Assessment / Management Specialists
- Process Safety Engineers

Perform risk analysis and operability studies on proposed, new and existing facilities to reduce risks to people, environment, assets and production. Develop action items out of the analysis and ensure they get completed (risk management).

e) Professional Engineers / Managers

Consider the impact of all organization operations on land, water and air quality. Provide solutions to protect the environment that are economical and technically feasible. Ensure that all government regulations and industry standards are met.

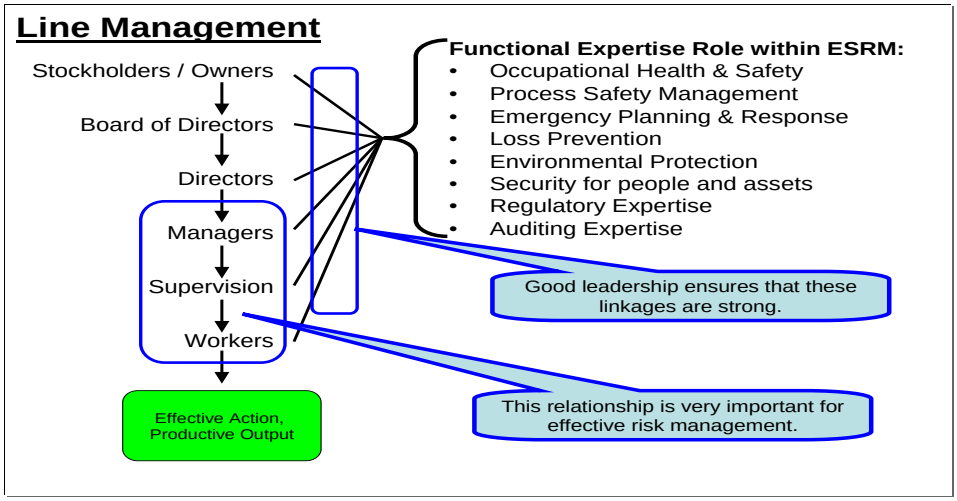


Figure 7.6 The Line Management Model.

For example, imagine the operation of a $6-million 400-tonne Ultraclass truck capable of generating 3,500 HP and being loaded at 100 tonnes per pass by a 1,500-tonne shovel. It is a job that requires continual focus to do safely. For this job to be done safely, the operator must be well trained, follow safe systems of work, use the right tools and equipment, and most importantly, be well led by his/her line manager.

When addressing people-related issues, such as when a worker's practices are substandard, ask yourself these questions:

- Did you set up your employees for success? Did you provide sound values? Are objectives and goals aligned? Have you set clear expectations?
- Have you provided sufficient resources?
- Have you ensured that training and certification were adequate?
- Were the policies and procedures correct, easy to understand and follow?
- Has there been consistent, equitable, and balanced progressive discipline in the workplace?
- Are your behaviours and actions consistent with your expectations of others? Are you "walking the talk"?
- Have you communicated your expectations clearly?

Answers to these questions form the basis for the ABC Model discussed next.

Model 3: The ABC Model – How Antecedents and Consequences Affect or Influence the Behaviours of Team Members

The ABC Model of Human Behaviours is a logical, behaviour-based approach to managing people, consisting of three components: **Antecedents**, **Behaviours** and **Consequences**.

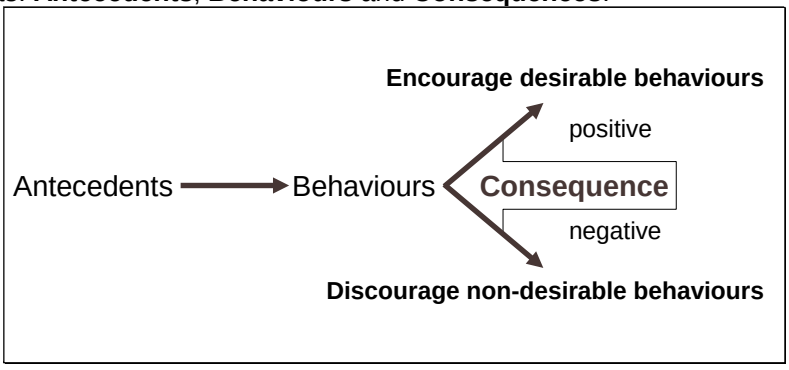


Figure 7.7 The ABC Model.

Antecedents set the stage before any behaviour is exhibited. Antecedents are the expectations that are set by leaders and managers, and can be in many different forms:

- Ground rules, team norms and team values;
- Policies, standards, procedures and posted signs;
- Other workers' behaviours;

- A leader's behaviours (leading by example or not); and
- Verbal instructions and unwritten rules (although good leaders clearly communicate those unwritten rules verbally and through written memos).

By working on antecedents, everyone knows the expectations, setting the stage for everyone to meet those expectations, and thus a positive environment is created versus an adversarial environment. A positive environment will positively affect behaviours, leading to fewer negative results, outcomes and consequences.

Behaviours in this model are the work practices exhibited by or actions taken by people in the workplace. Outcomes are the result of those behaviours/work practices.

Consequences happen after the behaviour is exhibited. Consequences are the feedback on a person's outcomes or, more precisely, the feedback on their behaviour. Consequences can be positive or negative (a paired characteristic) and can influence individual and/or group behaviours. For example:

1) A worker's behaviour produces the right or expected result/outcome. When this happens, providing that the behaviour was acceptable or desirable, then **positive consequences** should follow (commend, pay raise, bonus for safety performance, etc.) not only to recognize and reward the person and their acceptable or desirable behaviour, but also to reinforce the expectation for future acceptable behaviour and to build the desire in the worker and in others to continue to meet the acceptable behaviour.
2) When unacceptable or undesirable behaviours are exhibited, regardless of outcome, **negative consequences** naturally follow (injury due to an incident, progressive discipline, loss of pay raise, loss of job, etc.) not only to correct the person's unacceptable or undesirable behaviour, but also to deter the unacceptable behaviour in them and in others.

There are two other paired characteristics of consequences: immediate or delayed; and certain or uncertain. A brief discussion is provided below.

> *It is a common belief in large organizations that we need to understand why people do things a certain way. By understanding and applying the ABCs model, we can change worker behaviours through application of antecedents and consequences.*
>
> *With the ABC Model, it is believed that by interacting with workers as they do their work with PIC (Positive, Immediate & Certain feedback) or NIC (Negative, Immediate & Certain feedback), we can correct and improve the employee's behaviours into the future, thus achieving the right set of work practices (acceptable behaviours) and better outcomes.*
>
> *However, if we give employees feedback that is uncertain (not clear on the impact to them personally) or delayed (not immediate, rather we say something tomorrow or next week) regardless if it is positive or negative, this will not influence their behaviours in the desired direction and possibly contribute to a degradation in their work practices. If this continues, it could lead to severe disciplinary action and possible dismissal, which no one wants. It takes at least 7 PICs to overcome the impact of any one thing that is uncertain, delayed or negative.*

Current industry practices for progressive discipline are known as Balance of Consequences or Actively Managed Discipline. These policies and processes are applied by Line Management Leaders with guidance from the HR functional expertise to ensure all consequences – both positive and negative – are fair and equitable, balanced and treat people with dignity and respect.

Model 4: The Swiss Cheese Model – Interrelation of Latent Causes and Human Factors

Consider the following points regarding human factors during incidents:

1. A loss incident occurs when humans make errors in the presence of active failures and latent causes.
2. A loss incident is prevented by purposeful and intentional action by a worker.
3. The need to address latent causes becomes apparent.

1. A loss incident occurs when humans make errors in presence of active failures and latent causes.
Imagine that the slices of cheese Figure 7.7 represent a case where an organization's management program is ineffective (i.e. holes in slice 1), its engineering controls have degraded (i.e. holes in slice 2) and its administrative controls have degraded (i.e. holes slice 3). The holes in slice 4 represent substandard work

practices and conditions resulting from unacceptable / at-risk behavior (i.e. workers don't do something they are supposed to do or do something they are not supposed to do).

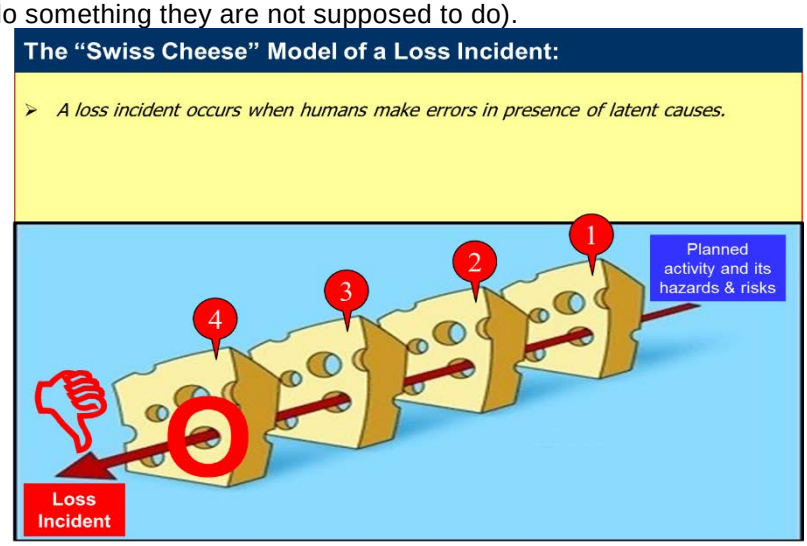


Figure 7.7 The Swiss Cheese Model.

Substandard work practices and conditions can be the result of:

- Workers not knowing what to do (e.g. a gap in training or a gap in learned expertise) even when motivated to do the right thing;
- Simple oversight or mistakes, even when workers know what to do (e.g. other distractions and stresses in the workplace); or
- An intentional decision to not meet expectations: a clear instance of an intentional at-risk behaviour (a rare case), perhaps motivated by misguided priorities and/or values.

The gaps or holes in each slice create a pathway to failure with human error being the trigger. This results in a loss incident or negative outcome.

2. A loss incident could be prevented by purposeful and intentional action by a worker.
Of course, diligent and responsible workers try to avoid loss incidents. Consider the same case (holes in slices 1, 2 and 3) as above. How could a loss incident be prevented through workers' actions (preventing a hole in slice 4)?

A worker takes purposeful, intentional and appropriate action(s) to maintain controls (closes the hole in slice 4). This well-motivated and well-intentioned personnel intervention is the barrier that prevents a loss incident. This action is driven by the desire to meet overarching expectations and to purposely and knowingly account for a deficiency in a management system. The worker knows the systems have failed, but has adjusted or adapted their work practices to overcome the failures.

Leadership should take note of this latter case: these workers are motivated to "do the right thing", and this represents an opportunity to engage workers in addressing weaknesses in the management system. As they take on ownership, commitment is built.

The need to address latent causes is apparent. Now consider a variation on the same case: the intentional work practices (that were performed to prevent a loss incident) are not performed and, in combination with the presence of active failures and latent causes, a loss incident happens. The short-sighted view is that the trigger (cause) to the loss incident is "human error".

However, when the problem is approached by addressing latent causes, the need for human action (or intervention) is reduced as much as possible and perhaps even eliminated. Thus, the possibility of human error is reduced or taken out of the risk equation. In other words, the increased reinforcement of management systems and/or improved designs reduces the frequency and requirement for people to continually take action or to intervene. Thus, incidents can be prevented in two ways:

- By working at reducing the likelihood of human error, the likelihood of an unwanted incident can be significantly reduced.

- By addressing latent causes and working at maintaining management system controls (engineering and administrative controls sustainably managed through the effective implementation of a risk management system), incidents can be prevented even in the presence of human errors.

Example: Logistics – Tanker Railcar Loading Operation

Consider this example to explore how latent causes lead to a loss incident when other causes align.

- A worker diligently and intentionally pays particular attention to a rail-car loading operation – never leaves the post while filling and does tasks contrary to written procedure – because the filling totalizer, the high-level switch and the high quantity / high level alarms have failed. In other words, the worker has a "work-around".
- These engineering controls have failed because: previous reports have been ignored; there is no process to report / prioritize / repair instrument failures; there are no resources to repair; it is low priority to repair; obsolete technology / no commitment to update; and so on.
- Suppose the attentive worker can't come in today or is re-assigned to or departs the organization for another job.

Questions:

- Does the replacement worker (whether temporary or permanent) know this critical "work-around" knowledge?
- What is the likelihood of a loss incident?
- Will the manager "blame" the replacement worker should a loss incident occur?
- What might you determine in your root cause analysis?

Model 5: The Training and Learning Cycle Model

The Learning Cycle describes how workers can become complacent in their job and the actions management must take to prevent this situation from happening. When complacency sets in, the workers do not abide by the required controls to manage the residual risk of their activities; thus, risks increase to an unacceptable level. "Normalization of deviation", also referred to as "organizational complacency", is the state of the organization when the acceptance of substandard work practices and substandard work conditions is wide-spread. The Four Quadrants of the Learning Cycle are depicted in Figure 7.9. It begins with a worker being new to a job or task, then going through training, then gaining competency, but ultimately becoming complacent.

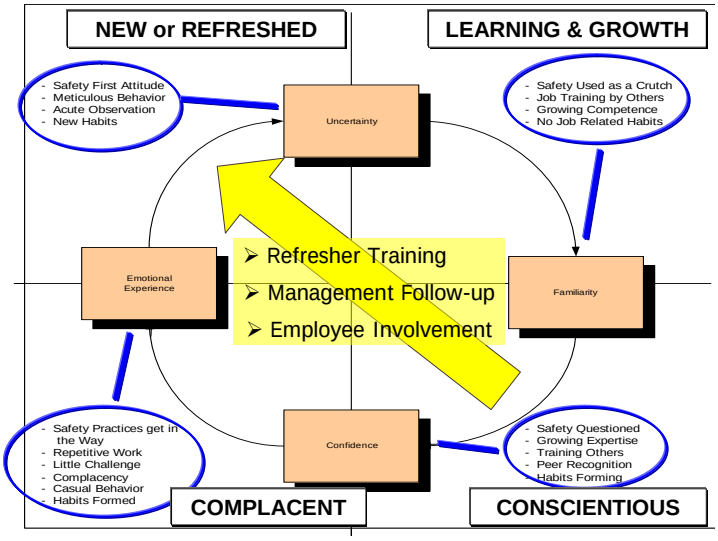


Figure 7.9 The Learning Cycle.

To reset the Learning Cycle to avoid the complacent stage and prevent incidents, consider undertaking these activities:

1. Management Follow-up or MBWA (management by walking about): lead by example.
    - Actively and visibly addressing substandard work practices is most effective in preventing complacency. In order to address substandard work practices, several techniques have been developed such as the Behaviour Observation / Interaction / Intervention Program. Based on

basic safety principles, managers, supervisors and workers can be trained to systematically observe, recognize, interact, intervene, correct, report and take action to eliminate substandard work practices and conditions.

2. Employee Involvement: If they are part of the solution, they own it and won't let it lapse.
    - New employees in an industrial situation, even with initial safety training, find it difficult to distinguish substandard work practices and substandard conditions because it is an unfamiliar environment; it takes experience. This experience, to observe and distinguish, can take some time, and not all employees become workplace smart at the same rate. By teaching awareness and systematic observation / intervention skills in the particular plant or place of work and encouraging employee involvement, the entire workforce is set on a pathway for continuous improvement in safety and job performance.
3. Refresher Training
    - Figure 7.9 explains why refresher training is necessary. Figure 7.10 demonstrates the effectiveness of training and refresher training. The retention of skills and knowledge builds with each repeated training session or practice session; thus, the worker remains "sharp" in their knowledge and skills set, preventing complacency.

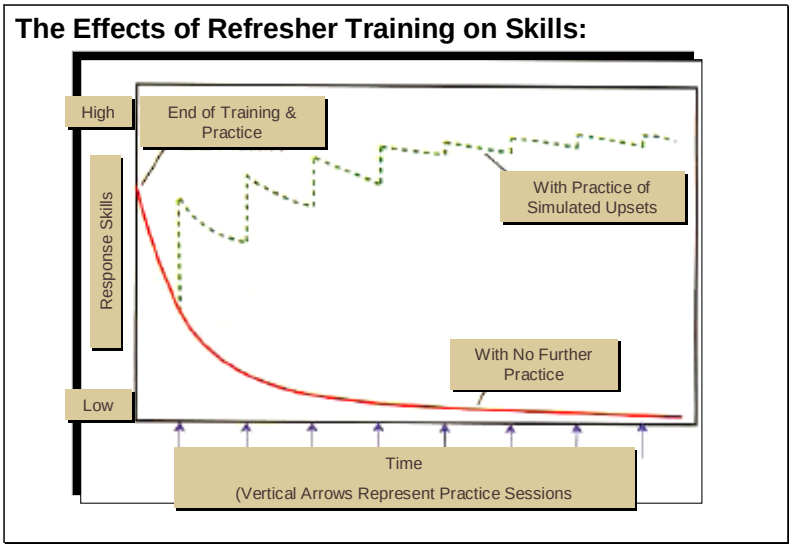


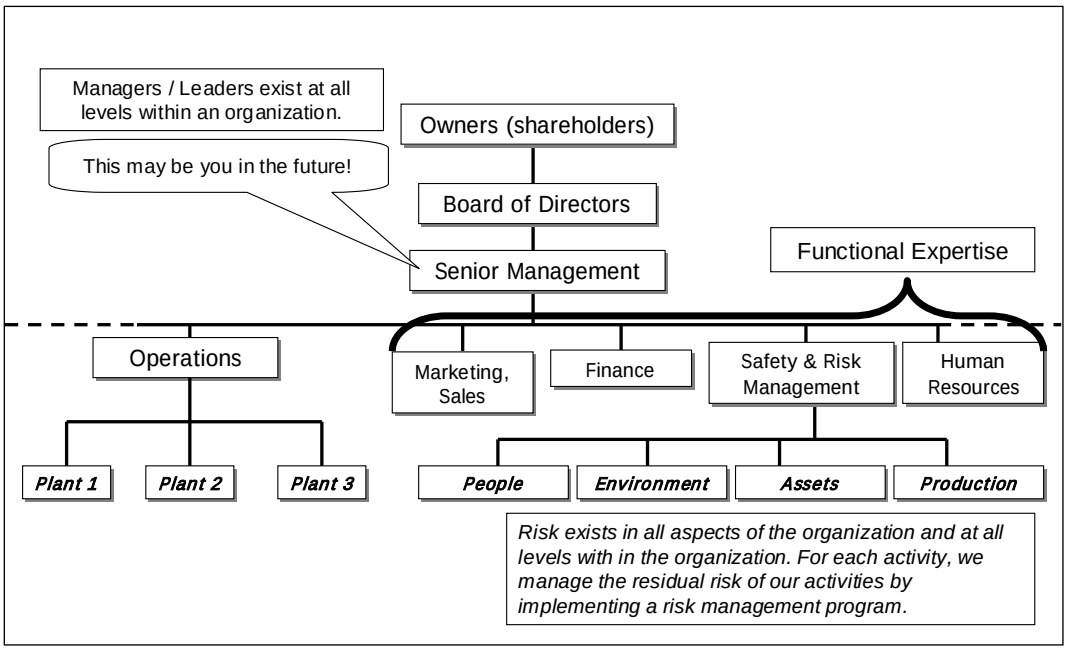
Figure 7.10 The effects of refresher training on worker skills.

Section 7.5: Organizational Design – How Organizations Work

Put together any number of people and all you have is a crowd. If those people are assembled with a set of common goals, values and/or beliefs, then you have the beginnings of an organization. In this section, we will learn about how organizations exist and function to see how risk management is applied within and executed by the employees in the organization.

The Organization Chart, a Typical Model of an Organization

For almost any organization, regardless of size or type (for-profit businesses, not-for-profit organizations, governments, etc.), its structure can be described using an organization chart. For small entities, one chart may describe all positions within the organization. For very large entities, divisions, departments or sections are described using additional charts that can be seen as parts within the larger organization chart. Typically, an organization chart is used to show the lines of responsibility by position within the organization, as well as the names of those persons in those positions. The former is used for public communication and the latter for internal communication. When you join an organization, you need to identify your place within the organization.



Exercise 1: Review APEGA's website and locate the components of an organization as discussed in this section.

Exercise 2: Thinking about an organization that you've worked or volunteered for, draw a simple organization chart and identify your place within the organization.

Corporate Mechanisms and Supporting Documents

An organization becomes an entity when it:

- describes itself with a vision statement and/or a mission statement;
- defines the scope and boundaries of its corporate behaviours with a set of core values and ethics, and/or a set of policies or policy statements;
- defines where it wants to go or evolve by defining a set of goals, objectives and strategicaused byusiness plans;
- describes how it functions or how it performs work using a management system, work processes, standards and/or procedures; and
- executes its vision and mission statement by implementing its strategicaused byusiness plan.

An organization does not need every one of the above documents; however, as it becomes larger or more complex, these documents enable leaders to steer the organization in the right direction in order to complete its plans, meet its goals and fulfill the vision of the organization. Ideally, these activities will be conducted within the boundaries of ethics and the law, and with a minimum of losses.

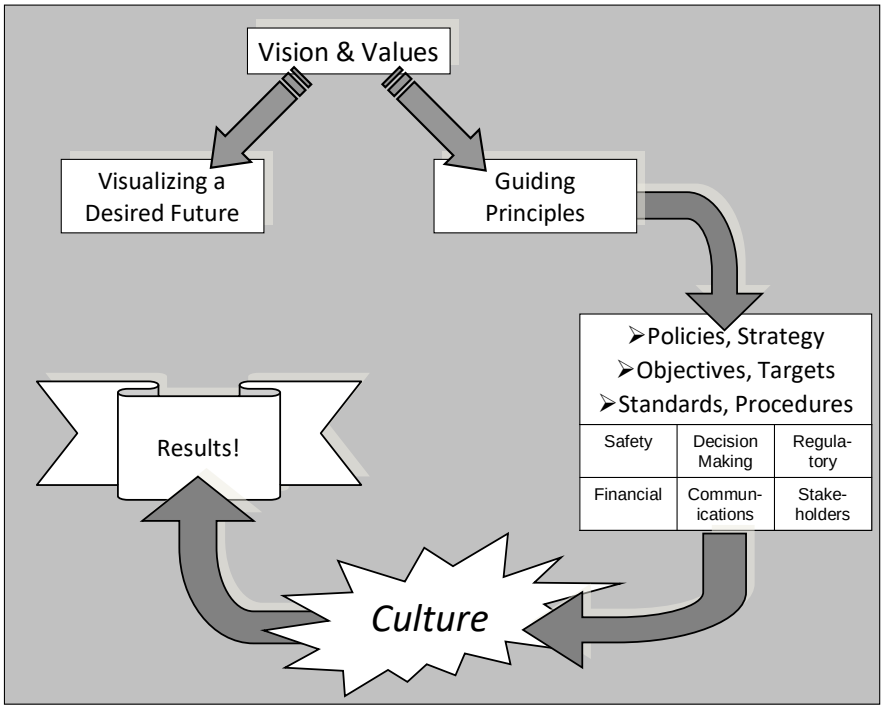


Figure 7.11 Schematic flow of the corporate mechanisms and supporting documents in an organization.

Referring to Figure 7.11, corporations set a vision that communicates a desired future for the organization. It is supported by a stated set of values in the form of guiding principles that are the basis for decision-making. These visions and values ignite motivation and commitment among employees when properly translated to influence policies and resulting strategies, which in turn set objectives and measurable targets. These are supported by standards and procedures that all act to influence how core work processes are carried out.

The culture of the organization is defined by *how* work is conducted and determines the results for the organization. Corporate documents in the form of visions, values, guiding principles, core values and policies directly influence safety and risk management within the organization.

Discussion on Policy Statements

Policy statements are important because they define the rules and sometimes the manner/means by which all persons within the organization are bound to work and behave. They are especially important to the worker: if a worker follows and works within the policy and something goes wrong, then the worker is insulated from personal liability because they were executing their work in accordance with policy. Thus, the organization becomes liable and not the person. Obviously, if a worker strays outside of policy, then the worker could be held personally liable.

A well-written policy statement consists of a number of terms:

- Management's responsibilities must be defined.
- Management's commitment must be stated.
- It must state what the organization or organization will do to uphold its policy.
- It must state the expectations and obligations for its employees, its contractors and its visitors. It gives direction or guidance especially in absence of specific policies or procedures (i.e. when the situation requires a decision or action and there is nothing specific on that situation or course of action, then employees can look to the corporate policy for guidance and base their decision or actions on that policy).
- It must show management's commitment to the policy. To demonstrate commitment, senior management must date and sign the policy statement, keep it current and prominently display the current policy in corporate offices and prominent areas within the organization (key communications points or gathering areas, reception areas, etc.), as well as on the corporate website. This gives a *living sense* to the document and to the organization.

Two key points to consider in judging the credibility of and importance of a policy statement are:

a) Its date of posting. Is it recent enough to be part of the current people within the organization?
b) The person who committed to the policy statement(s) with their signature. Is it the person currently in charge of the organization responsible for issuing and upholding those policy statements?

Section 7.6: Leadership in Risk Management - Putting Theory into Practice

The premise of shaping culture and affecting the safety performance of the organization is to proactively address the base of the incident pyramid – inspect and correct substandard conditions and substandard work practices. This proactive action will prevent "near miss" or "close call" incidents and prevent incidents with real consequences. Organizational culture can also be shaped by the manner in which managers address actual loss incidents (i.e. events with consequences).

The mark of proactive management is for a manager to check and act on substandard conditions and work practices. By setting the example, and by setting the expectation that all workers in the organization to routinely identify, report and correct substandard practices and conditions, the manager can and will positively influence the workplace culture. It is through these means that performance will improve.

These management actions and behaviours are synergistic: by encouraging and setting the example with good conditions and work practices, safety culture is improved, and thus more and more workers increase their personal commitment to safety, and improvements are seen throughout the incident pyramid. The opposite is no less true: by letting things slide, performance degrades beginning with conditions and practices, inevitability resulting in events with serious consequences.

It is possible for leaders to shape their culture and affect their organization's performance (and the incident pyramid ratios), provided that they are collecting comprehensive data and acting on their findings. In other words, the leadership effort and focus on practices and conditions in the workplace ensures the desired outcomes will follow, as will the results.

Leadership and its Impact on Culture in the Workplace

Leading corporations would assert that:

- Safety is an essential part of doing business, a value.
- Management must be visibly committed and accountable.
- Double standards must not exist, and must not even be perceived to exist.
- Management must provide the necessary climate, leadership, and resources for continuous improvement.
- Every employee must be personally committed and accountable to safety and risk management. This commitment is necessary for the survival of your organization and essential to your career.

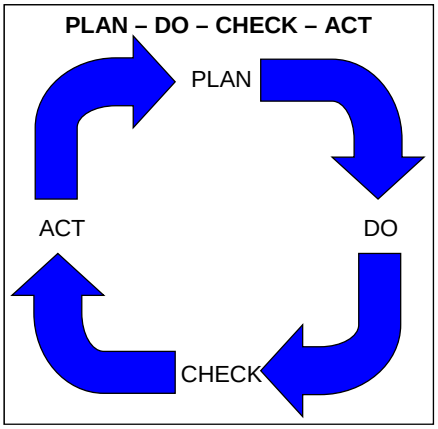
Further, managers in these leading corporations have a common base on which all operate:

- Do not expect rewards for performing an essential job requirement. Safety is a moral imperative. Besides, you are expected and required to work safely (the law).
- Do not use the narrow or "piece-meal" approach to safety and risk management. The only key to success is a holistic, long-term approach.
- Exercise care and look for latent (root) causes for problems, even or especially in times of crisis.
- Emphasize the proactive approach, rather than the reactive.

The Fundamental Process of Management – The Plan-Do-Check-Act Cycle

The fundamental process of management consists of four steps: **Plan-Do-Check-Act** (PDCA, originally conceived by Walter A. Shewart, and widely proposed by W. Edwards Deming). This fundamental process is based on two tenets of management: 1) managers must be proactive; and 2) the organization must be a place of continuous improvement.

The Plan-Do-Check-Act Cycle can be applied within the Risk Management Process to test the effectiveness of an organization's management system, as well as to test the effectiveness of the associated processes and practices at the team level. It is particularly effective for managing residual risks.



PLAN: Design or revise business process components to improve results

DO: Implement the plan and measure its performance

CHECK: Assess the measurements and report the results to decision makers

ACT: Decide on changes needed to improve the process

This fundamental management process – and its steps – relates to **any manager's work** regardless of level or title. As the models suggest, a manager's job is never complete. Management must continually cycle through this process so as to sustain and improve the performance of the organization. That is, they must have a ***bias for action*** for all steps of the PDCA Cycle. Managers can proactively learn from loss incidents at other organizations (learn from others) and from "third-party audits" where latent causes may be discovered before a loss incident occurs.

Management must be vigilant, must pay attention to and must never let down their guard of the organizations they lead. Otherwise, the effectiveness of how they manage residual risk can degrade over time, controls become ineffective and, ultimately, an unwanted incident will happen. Conversely, the desired outcome is a risk management system where residual risks are continuously and properly managed, where controls are effective, where the risk of unwanted incidents is low (i.e. acceptable) and should an incident happen, the organization is well-prepared to respond to and mitigate the consequences of that incident.

What can be done to improve performance?

The following management activities can positively impact the ratios of the incident pyramid:

- Thoroughly investigate and analyze major incidents, and implement actions to prevent recurrence. Share the lessons learned from the incident to ensure organizational learning in order to prevent similar types of incidents elsewhere within the organization.
- Consistently work to reduce the more numerous minor injuries and near misses. Investigate and analyze these as well. They provide a much larger basis for investigation and taking action to improve control.
- Thoroughly investigate near miss incidents. In many cases, it was simply a matter of luck that there was no impact on PEAP. All the lessons can be learned and corrective action taken without having suffered any negative consequences.
- Create a self-reporting and self-resolution process. To do this, management must show the leadership and create the climate so that everyone is empowered to:
    - Be actively aware for substandard work practices and conditions.
    - Promptly resolve substandard work practices and conditions.
    - Promptly report those substandard work practices and conditions and action taken, or prompting management that more action is needed.

The most enlightened and empowered organizations work very hard at the self-reporting and self-resolution process for addressing substandard work practices and conditions in the workplace. Here are some ideas to encourage self-reporting and self-resolution processes:

- Management must place a continuous and strong emphasis on reporting and self-resolution by communicating the value of these reports with friendly encouragement at safety meetings.
- Encourage reporting by recognizing those who have submitted reports.

- Set the example by getting out to the plant or shop floor and addressing substandard conditions. Workers will appreciate the interest that leaders have in the workplace conditions. *When substandard practices are observed, be careful to fully understand the situation before intervening! This is a difficult task and must be done right. A leader must correct substandard work practices but cannot react in such a manner so as to kill the goodwill built by a self-reporting and self-resolution process. Aim for a "no fault" response.*
- Provision for anonymity (i.e. it is optional to list name on the report or a hotline phone number).
- Emphasis placed on the positive and progressive aspects of the action taken.

Bias for Action, The Planned Inspection and Managing the Residual Risk

The way to manage the residual risk is to ensure that:

- The management system and its elements are functioning effectively.
- There are no management system weaknesses, no loss of control, no inadequacies and no latent causes.
- Actions are taken to eliminate latent causes if they are found or discovered.

Latent causes (management system weaknesses) were discussed in the **Root Cause Analysis of an Incident** and **Linking Latent Causes to Recommendations for Actions** (see Chapter 4). These chapters stated that by addressing latent causes (i.e. addressing the management system weaknesses), loss incidents can be prevented. Further, latent causes arise in the engineering controls and in the administrative controls. Latent causes are revealed in three basic ways:

- Proactively through planned inspections;
- Proactively by learning from others; and
- Reactively after incident investigations within the manager's facility.

Corrective and preventative actions must be taken regardless of origin in order to address the latent causes.

Leaders and manager are responsible and accountable for managing residual risks. It is not just about managing a budget, ensuring productivity schedules are met and keeping workers and supervisors happy. Leaders must manage the risks so that nothing unexpected happens. In short, management must have a bias for action in planned inspections, in the effective analysis of incidents, the identification of corrective and preventative actions, and the effective implementation of those actions.

The Planned Inspection

The one best practice to detect deficiencies in the engineering and administrative controls before an incident happens (the latent causes) is the formal planned inspection at the organizational level. The planned inspection of the organization can go by several different names (formal inspection, formal audit, integrated audit, corporate audit, system audit, program audit, third-party audit, third-party certification audit, gap assessment and closure plan, internal assessment, etc.). However, the purpose and desired outcome are the same: to find deficiencies in the management system and correct them before an incident happens.

The planned inspection at the organizational level can be driven by government regulations, industry association policies and standards (whether imposed or adopted), and corporate policies and standards, especially where there is a need to test the implementation of the risk management system / program at the organizational (system) level.

The process and technique for conducting a planned inspection at the organizational level was fully discussed in **Job Observations and Planned Inspections** (see Chapter 5).

Bias for Action and Managing the Residual Risk

Put yourself in the place of the manager in these two examples that illustrate the connection between having a bias for action and managing the residual risk: 1) Proactive Response to Bad News Elsewhere; and 2) Proactive Response to a Third-party Audit at Your Plant. Successful managers model themselves on these examples as discussed here.

i) Proactive Response to Bad News Elsewhere

You read in the news media that a refinery (just like the one you are managing here in Alberta) in another part of the continent has had a large release, explosion and fire, and has resulted in a number of fatalities and widespread damage. You surmise a couple of possible causes, based on your knowledge of the technology and

the few facts presented in the news media, and you don't wait for an official report or for direction from your boss or corporate risk management office.

Instead, you call your team together the next morning, present the news item and your findings, and you generate discussion on any weaknesses in your management system for your refinery. You and your team members agree on a number of things – preventative actions – to inspect (i.e. check to ensure no weaknesses, or where found, action is taken). By the way, mid-morning, your boss calls to ask if you had heard about the refinery explosion, and you reply with a brief update on what proactive action you and your team are taking to ensure the residual risks in your refinery are being managed.

Over the next few weeks, more information is learned through the media, through industry associations and through information shared between organizations and colleagues. You update your actions to reflect the new information. One month later, you reconvene your team members to review progress on the checks. Most items are satisfactory; however, a couple of weaknesses were found. To your pleasure, your team members have already acted on the weaknesses and have already checked to ensure the effectiveness of those actions. On that same day, you are able to provide a brief update to your boss, who is herself having to respond to senior management about their concerns over this incident at the other refinery.

ii) Proactive Response to a Third-party Audit at Your Plant

On a three-year cycle, your plant is subject to an intensive, integrated safety audit (a highly specialized planned inspection), where all aspects of your risk management system / program are rigorously audited by expert auditors. Over the previous two years, in preparation for this audit, you have conducted and your team have conducted several planned inspections of your own system / program, looking for weaknesses and addressing those weaknesses, so you are confident your operation will pass with flying colours.

Despite this work, at the closing meeting of the audit (this is where the auditors present their final report to you with their findings and their recommendations), a list of recommendations is presented. This list addresses management system weaknesses (latent causes) that they found in your management system. They did praise you on the fact that your management system is sound and robust, with few weaknesses, and that they had to work very hard to find the ones they did find. This is, in fact, a great compliment from the expert auditors. After discussion and agreement with the auditors and including your team members, you accept the list of recommendations.

Subsequently, you and your team members finalize the list and create an action plan – preventative actions – based on those recommendations. Your list of actions includes priorities, owners and resources, and due dates. Your action item owners have bought into the actions and have readily taken ownership of those actions because they were actively involved in developing the actions to address the weaknesses. (NOTE: This culture is in good part due to your leadership – for committing yourself to improve your management system and for actively taking ownership of issues that are your issues.)

On a monthly frequency, you and your team reconvene to check the progress on those actions. You are pleased that most actions are being completed and checked for effectiveness, per the plan. Some actions haven't been completed because of unforeseen complexities, yet you have been kept in the loop on those ones and are not surprised. You update your boss three months after the closing meeting, and quarterly thereafter, until all actions have been completed, and checked that the actions are effective. You move on to a higher position within the organization, and are pleased of two achievements: 1) your facility never had a serious incident, and 2) you were and remain able to sleep well at night knowing you have applied your best effort to ensure people are working safely in a safe workplace.

Managers and the Follow-up from Planned Inspections and Investigations

Typically, the manager for the operation is responsible for any actions or action plans that were generated from a planned inspection or an incident investigation / root cause analysis.

For incident investigations and root cause analysis, the manager is accountable and responsible for ensuring that:

- The root cause analysis has been conducted to a level sufficient for the seriousness or potential seriousness of the event.
- The analysis has drilled down to the latent causes.
- The corrective and preventative actions have been identified.

For planned inspections, the manager is accountable and responsible for ensuring that:

- The planned inspection was sufficiently thorough (breadth and depth) and that it represented a good sample of the population of activities in the facility such that weaknesses in the management system / program have been identified.
- The corrective and preventative actions have been identified.

For the identified corrective and preventative actions, the manager is accountable and responsible for:

- Driving the organization (people) to complete the actions in a timely manner.
- Checking the effectiveness of those actions after completion.

For any planned inspection or investigation that the manager has not deemed to be sufficient, the manager should re-engage the inspection team or the incident investigation / root cause analysis team.

Discussion: The Effective Management of Action Plans

In **Tools and Process for How to Prioritize Recommendations** (see Chapter 4), a method is provided for turning recommendations into actions. Any and all recommendations must be validated, prioritized and appropriately assigned as actions in order to make things happen. Successful managers effectively manage the corrective and preventive actions within their organization because major studies may have many actions, and there may be many studies in progress. Successful managers:

- Identify action items from the planned inspection or root cause analysis, and list actions by priority and category.
- Appropriately assigns to owners and sets expectations for the timely completion of action items to all Action Owners (i.e. reasonable due dates).
- Ensures the Action Owner(s) understands their action items and seeks a commitment from them to complete their assigned action by a realistic, target due date.
- Reviews requests for scope and date changes from the action owner and grants extensions.
- Monitors progress on actions to ensure timely completion. Intervenes when progress is not being made. Progress may be reviewed / stewarded by senior management.
- Checks the effectiveness of the action and takes any appropriate follow-up action.
- Ensures action list has a wide circulation to appropriate stakeholders within the organization.
- Assigns a project manager for complex studies. The action plan should be assembled into an overall completion plan, including bar chart, arrow diagram, project planning system, etc.
- Assesses all sets of action plans. The priorities of the action items must fit into the priorities of the operation (including any other action plans) as this is the most effective way to reduce overall risk.
- Monitors changes in plans. Often plans of action can change. Communication of the changes to all involved is important. As well, each "change" should be reviewed for risks before implementation ("Management of Change").

The Connection to the Fundamental Management Process

Each of the steps of the fundamental management process Plan – Do – Check – Act (PDCA) is evident in the examples and discussions above. Specific to the examples, consider what might have happened had the manager not taken an active interest in the news reports and/or had not made the effort to conduct a self-inspection in the operation. Specific to the discussions, consider what might have happened had actions not been completed and/or had not been checked for effectiveness.

The PDCA cycle must be applied by the manager on a micro scale as well as on the macro scale. By applying this process effectively – to check for weaknesses and act on those weaknesses – on any and all elements of the management system, the manager will have worked towards eliminating any latent causes and thus significantly reduced the risks within their operation. In other words, the manager is proactively managing the residual risks. Through effective application, management system weaknesses can be discovered; thus, the overall system and its performance are on a cycle of continuous improvement.

Section 7.7: Safety Metrics – Use of Lagging and Leading Indicators

Incident occurrence is usually measured in the form of Injury Frequency Rates and Injury Severity Rates. It is important for organizations to track safety performance, however, these are ‘lagging indicators’ because they are

tracking incidents which have already happened (a reactive measure). There are a number of problems with this approach, including the potential for suppression of reporting and making hasty decisions when measures are disappointing, as well as taking no action when good measures (decreased numbers) are a result of luck. Additional lagging indicators can consist of the following:

- # of first aid cases
- Total recordable incident rate
- Lost time incident rate
- # of fatalities
- # of incident investigations performed

A more proactive approach is the use of leading indicators, which are measures or activities taken to prevent incidents from occurring. If used correctly, leading indicators focus resources on incident prevention, as well as allow management to actively demonstrate leadership and empower workers to engage in discussions about how to prevent future incidents. Leading indicators must be measurable, positive, simple, and result in incident prevention. In other words, personnel resources and time focused on tracking leading indicators should result in a positive focus on safety and incident prevention (i.e. what you want to achieve, not the negative results). The choice of leading indicators are specific to the organization and its activities, but some common ones consist of the following:

- # of Job Safety Analysis/Standard Operating Procedures reviewed
- # of job observations and planned inspections carried out
- # near miss incident reports received and reviewed
- # substandard condition and practices reports received and reviewed
- # of daily/weekly/monthly safety meetings held
- # of management safety tours completed
- # of FLRAs, SQRAs completed
- # of tailgate safety meetings completed
- # of site inspections undertaken
- # of orientations (general and site specific) completed
- # of near miss report followed up on
- # of substandard condition and practice report followed up on
- # safe behavior awards presented to employees

Superior organizations use leading indicators to improve safety culture, promote communication, prevent incidents, and ultimately improve the overall safety performance of the organization.

Incident-Focused Managers – An Inefficient Approach

Any effective loss management program requires a long-term commitment. This commitment must start at management level. However, great care must be taken when a manager assesses any program. Beware of the short-term pitfalls.

Managers who focus on short-term results may also be known as "incident-focused". An incident-focused organization believes that the absence or presence of incidents determines the success or failure of a program. Therefore, a reactive climate is emphasized and ingrained. The incident-focused manager commands employee acceptance or responsibility for safety and a sincere commitment to achieving zero incidents. The approaches used to ensure this commitment are often in the form of: 1) employee pledges to work safely; 2) awareness campaigns; 3) and incentive programs. These approaches are based on three assumptions:

- Employee commitment and voluntary compliance are achievable through pledges, awareness and incentive programs, without management commitment and responsibility.
- Individual awareness results in safer behaviour and fewer incidents.
- Incident frequency rates are valid indicators of short-term safety performance.

It has been demonstrated, though, that these approaches do not work over the long-term (i.e. they are not sustainable). Although pledges, awareness programs, and incentive programs are intended to improve safety performance, they lack substance in making real change. Each of these approaches, their pitfalls, and alternative approaches are discussed below.

The Pitfalls of Incentive Programs and an Alternative Approach:
Incentive programs usually have small prizes or gifts if an acceptable level of incidents occur during a specified time. According to Dial "incentive programs are a consequence of two management assumptions:

1) That the work environment is completely supportive to working safely. An incentive program sends the message that management has done all it can and that it is employee's lack of awareness and desire that is causing incidents to occur; [and]
2) That working safely is not part of the organization's culture. In fact, working safely is so far outside the culture that management is willing to tender rewards in an attempt to coax employees to work safely."

Incentive programs often address the specific incident problems, but ignore the more important systemic weakness in the safety process. Symptomatic solutions only relieve the symptoms, leaving the underlying problems unaltered. Incentive programs are attractive because of their apparent ease of clearing up problems. Usually however, all they do is reduce the number of reported incidents. *"Tell me how I'm measured … and I'll tell you what you want to hear."* Incentive programs also become self-perpetuating. Soon, a safety program will become dependent on these "prizes". Therefore, the need for better and better prizes will eventually consume the program.

Recommended Alternative: Reinforcement in terms of recognition for good performance is all that is needed. These have been found to be effective: hard hat stickers, safety dinners, wall of fame, etc. While these seem trivial, these do have an impact and can support the desired culture. One particular organization had a "hard hat sticker program". The sticker had the employee's "number of safe years" printed on it, and each year the employee received the next incremental "safe year" sticker. When the organization announced it was going to phase out the hard hat sticker program (perhaps because they thought it trivial?), the employees clearly voiced their opinion as to how they valued it. Not only did the organization retain the program, but it also re-emphasized the stature of the "safe work years" with celebratory dinners every 5 years, spouses included!

Organizations can implement other well thought out recognition and reinforcement programs which are meaningful to employees and meet the long-term goals and culture of the organization. This is another opportunity to engage employees: form a team to decide which performance indicators to recognize for the organization.

The Pitfalls of Pledges and an Alternative Approach
Managers sometimes attempt to obtain more acceptance of responsibility by their employees by asking them to take an individual safety pledge, without giving them any further "tools" for improvement. It is impossible for an employee to respond safely unless (s)he possesses the ability to respond safely. The mere endorsement of a pledge neither promotes safety nor provides the capabilities to work safely.

Recommended Alternative: Beyond saying improvement is required, management shows commitment through providing the resources (tools, lighting, equipment, etc.) to meaningfully improve the work environment and support employee efforts to work safely.

The Pitfalls of Awareness Programs and an Alternative Approach
Awareness, as the name implies, simply makes someone aware of something. Without a motivational factor, change does not happen; or if it does, it is not sustainable. Factors other than awareness influence behaviour. For example, most smokers are aware of the health hazards associated with this activity; however, this awareness often does not change their behaviour. Incident-focused managers are not cognizant of less obvious factors and have not acquired the necessary knowledge and skill needed to create a pro-safety and loss management environment.

Recommended Alternative: Management must create and carry-out a long-term plan with a proactive approach. This will require resources, but will also engage and build commitment with employees.

- Start by educating Management.
- Leadership by example (i.e. Walk the Talk).
- Implement near miss investigations, risk analysis and risk assessment.
- Institute a "management of change" mind-set.
- Work towards engagement (i.e. full employee involvement and ownership of their jobs, their equipment and their results).

While pledges, awareness programs and incentive programs have some merit for recognition, they lack substance in their ability to make real sustainable change. The informed manager, who can implement meaningful programs that effectively engage and motivate employees, will build commitment in his/her employees.

Section 7.8: Effectiveness, Engagement, and Collaboration for High-Performance Teams

Take a moment to think about your past experiences on teams. A few word pairs may inspire you on your thoughts, not only about your experiences (negative and positive), but also about your preferences in the future:

- Friction versus support
- Resistance versus guidance
- Discord versus harmony
- Animosity versus collaborative work
- Reluctance versus being on-board

It is obvious as to which are the preferred and positive characteristics, so it would seem common sense that everyone would work towards these. But more often than not, teams and people evolve towards the non-preferred set because it is easier to cope with less-than-optimum settings to get the team project completed and behind one's self. To be supportive, to offer guidance, to find harmony, and to find the pathway to being onboard, people must exert sufficient effort to get the work done, must bring adequate knowledge and skill to bear on the work including competencies in individual and team work, and must employ effective task performance strategies. The theories, principles, and tools presented in this and in other chapters are intended to develop competencies in the attributes of individual and team work.

Effective and skilled team members beget effective teams that attain high performance and success. Effective team leaders know how to engage team members, their employees, and coach their team members to collaborate with their teammates. The characteristics of high-performance teams are intertwined with the characteristics of effective team members and effective team leaders.

Team Effectiveness in Theory and in Practice (Hackman et al., 2000)

Teams are:

1) A real group of two or more people; an intact social system, complete with a purpose or common objective, boundaries, interdependence among members and differentiated member roles.
2) They have one or more group tasks – or main objectives – to perform.
3) They operate in an organizational context.

Team Effectiveness is:

1) The productive output of the team, which meets or exceeds the standards of quantity, quality, and timeliness.
2) The social processes the team uses in carrying out the work enhance the member's capability to work together interdependently in the future.
3) The team experience, on balance, contributes positively to the learning and personal well-being of individual team members

Why Teamwork?

Organizations have an increasingly educated workforce who can be effective in their jobs without a top-down management style. That said, no one person can have all the knowledge (i.e., technology has made such a shift that one person can no longer understand all the knowledge available).

Teamwork can be beneficial when organizational structures are not able to respond quickly to market demand (i.e., effective teams can provide quicker decision making). Those working in a specific area should be empowered to make the decisions that affect their roles (i.e., the people doing the job have the best skillset / knowledge to implement that role). This way, it is the best decision for that area.

Through teamwork and shared responsibility, employees feel more committed to the organization vision and goals. Team synergy creates something beyond what any one person can do. They have better results and success. To ensure effective teamwork, take away forms of competitiveness that is unhealthy (e.g., withholding knowledge from other employees, sabotaging others, taking credit for success others contributed to, etc.).

Conditions that Foster Team Effectiveness

To foster team effectiveness, a team must overcome three hurdles (process criteria):

1) Must exert sufficient effort to get the work done.
2) Bring adequate knowledge and skill to bear on the work.
3) Employ effective task performance strategies.

To overcome these three hurdles, four conditions must be met: Direction, Structure, Context, and Coaching, as further described below:

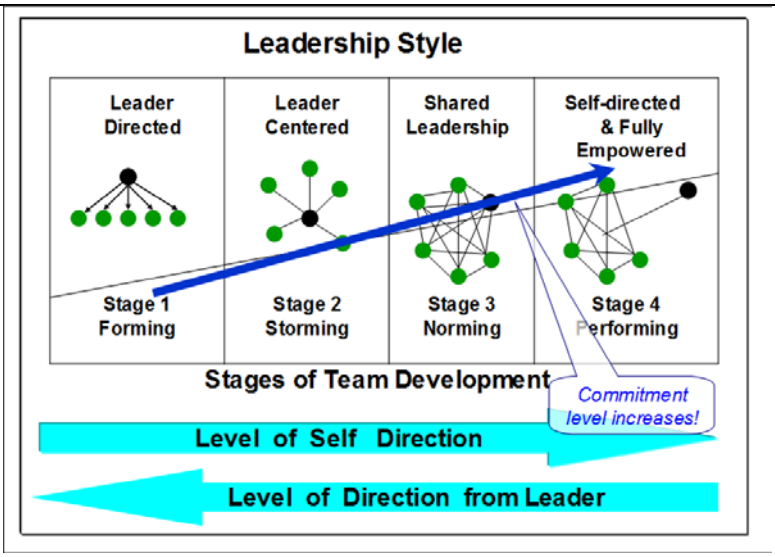
1) DIRECTION: Clear, engaging direction
- Challenging
- Consequential
- Clear
- Avoid giving too much direction or the message may be lost in transmission; you need to constantly check that intended messages are received; you need to be flexible

2) STRUCTURE: An enabling team structure
- Task design
- Team composition
- Core norms of conduct
- A group size of 8-10 people is the maximum; it is easy to overemphasize the performance benefits of large teams and ignore their coordination costs; need a balance of technical skills, a high level of interdependence, and cooperation

3) CONTEXT: A supportive organizational context
- Reward system (team based)
- Educational system
- Information system
- Think about how team-based rewards will actually work; train intact teams over time; team-level information is critical; ensure teams use information systems

4) COACHING: Available, expert coaching
- For effort (help team minimize coordination, communication, and motivation problems)
- For knowledge and skill (help team use and develop member skills / talents)
- For performance strategies (help team avoid failures)
- Enabling Performance Conditions
- Team Effectiveness in Practice
- Managers / leaders should have some experience working in the team; minimize the number of teams/groups an individual has to manage.

Tuckman's Model for Leadership Style and Team Development:

Tuckman's Model suggests that the leadership style, as depicted in the upper segment of the graphic, will vary at each stage of team development as depicted in the lower segment. It should be noted that the leadership style and stage of team development are not necessarily in lock-step with each other (i.e., the original leader in the "leader-directed" stage will need to adopt the "leader-centered" leadership style or foster development of the "leader-centered" leadership style in other team members before the team can advance to the storming stage).	

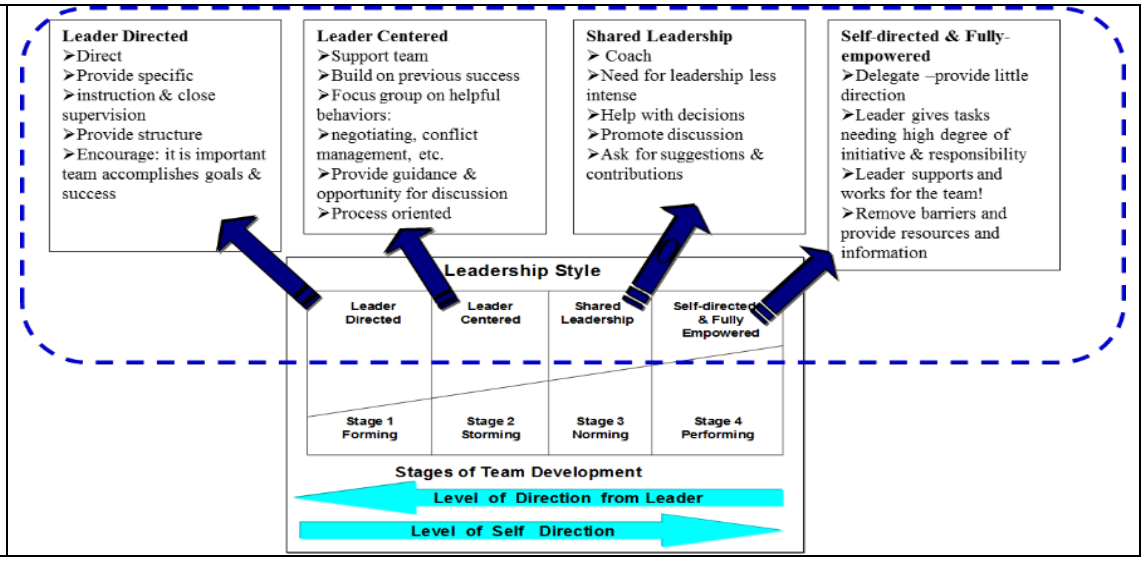
With team evolution, the commitment level rises, a characteristic of an improving team culture, and the performance level and output of the team increases.

Exploring the Four Leadership Styles in Tuckman's Model

Tuckman defined the four leadership styles as:

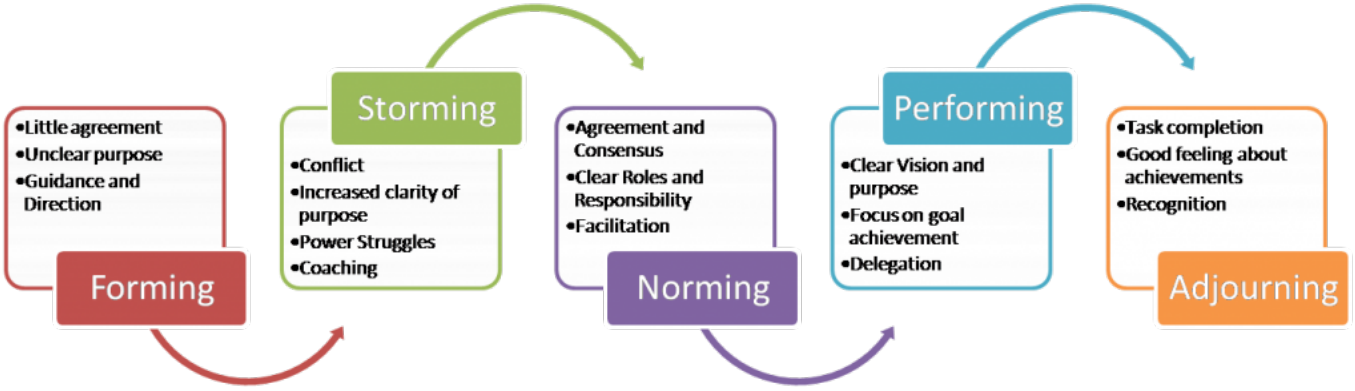
- Leader Directed;
- Leader Centered;
- Shared Leadership; and
- Self-directed and Fully-empowered.

Each of the four leadership styles is characterized.



The Five Stages of Team Development

Improvements in this model by Tuckman & Jensen (1977) defined the five stages of team development as being: **Forming, Storming, Norming, Performing, Adjourning**. Each stage is uniquely characterised, as depicted in this diagram:



Team-Member Effectiveness, Engagement, and Collaboration

Effective team members are highly capable in these seven skills:

1) Cooperation:

- A situation in which people work together to do something.
- The actions of someone who is being helpful by doing what is wanted or asked for.

How does this look on my team? You cooperate when you volunteer or agree to take on some action that works toward completion of your team project and when you complete that action to the satisfaction of all team members. You are not cooperating if you do not take on any actions or complete those actions unsatisfactorily.

2) Coordination

- The process of organizing people or groups so that they work together properly and well.
- The process of causing things to be the same or to go together well.

How does this look on my team? You coordinate your actions, whether it is in the execution of your action or in response to a request from someone else, in a timely manner with all other actions being undertaken by other team members. These series of coordinated actions are dependent on the sequence of execution and completion. You are not coordinating when you do not complete your actions in a timely manner or when you cause the delay of others in completing their actions.

3) Communication:

- The act or process of using words, sounds, signs, or behaviours to express or exchange information or to express your ideas, thoughts, feelings, etc. to someone else.

How does this look on my team? You communicate information relevant to the functioning of the team and attainment towards the team project (your contributions to the team include your work product, your completed actions, updates on tasks, your status for attending meetings) in a timely manner. You communicate information through various different media: a text message, an email (with attachments), an upload to a shared virtual drive, a letter, a document, a telephone call, etc. You are not communicating when you do not share information or when you share it late. Communication is not only about formulating and delivering a message, it is also about receiving a message.

4) Comforting (psychological / emotional support)

- Done through some action taken by you to cause someone to feel less worried, upset, frustrated, confused, over-whelmed, depressed, over-worked, frightened, etc.

How does this look on my team? When a teammate is expressing some emotional discomfort or turmoil (whether caused by circumstances in the team environment or external to the team) that impacts the performance of the team, then you provide comfort and support by offering a helping hand in any manner to alleviate the turmoil. You are not providing comfort when you brush it off or make ill-willed statements such as “suck it up”.

5) Conflict Resolution

- The act of finding an answer or solution to a conflict, problem, etc.
- The act of resolving something.

How does this look on my team?

Team Deliverables: It is inevitable that a team will experience some kind of conflict concerning the deliverables of the team project, whether it is about what to do, how to do it, or when to do it. The application of the appropriate work processes and methodologies taught in this course are the means to resolve these kinds of conflicts. It is part of the team project experience to enjoy these kinds of conflicts because it is an opportunity for you to learn to effectively apply these work processes.

Individual Participation and Fair Contributions: The other kind of conflict a team experiences is the lack of participation and fair contribution to the team through a failure to cooperate, coordinate, communicate, etc. The reasons for a team member’s lack of fair contribution are many. The path forward can be very complex, but as a start, the other team members must agree upon the lack of fair contribution and analyze the reasons. This team self-analysis may reveal the appropriate steps to take.

6) Cohesion

- A condition in which people or things are closely united.

How does this look on my team? You will know that your team is cohesive when you feel good about the team. There is a genuine and sincere appreciation expressed and felt by all team members for their contributions. A cohesive team is effectively applying the previous skills listed above (i.e., cohesion is a result of the execution of these). A team that lacks cohesion typically has problems in these previous 5 skills, and this may be expressed through in-fighting, resentment, and put-downs. Look at where there are breakdowns in the first 5 skills.

7) Collaboration

- To work with another person or group to achieve or do something.
- To work jointly with others in an intellectual endeavour.

How does this look on my team? What Does It Mean to Collaborate on a Team Project? It seems obvious to “share the workload”: some members work on one part of the project, others work on another part of the project. The benefit is obvious: less workload for individuals on a team versus having to undertake the project as an individual. But it is more than sharing the workload.

All members must be given an opportunity to contribute to all parts of the project – not the first in isolation from the second – and all members must be engaged in the review of the contributions of other team members. The benefits here include: the sharing of ideas, the avoidance of duplication of effort, and the attainment a superior work product.

Team collaboration yields the pinnacle of team performance. The previous 6 skills must be effectively practiced by all team members before a team is able or capable of collaborating. Team collaboration is more than just the sum of the previous 6 skills. Team collaboration means that all team members are given an opportunity, and follow

through on that opportunity, to contribute to all parts of the team project, and not simply to complete their individual part.

For example, the team is collaborating when all team members are in the same room, and one person is leading the team through the process to create the key set of recommendations (per **Chapter 4.6: Tools and Process for How to Prioritize Recommendations**), and all members are contributing towards the application and completion of that process. A team is not collaborating when one (or two) persons work on this process and then share their work with the others for comment. It captures the first 5 skills, but it is not collaboration. All team members do not necessarily have to contribute 100% to all parts of a team project for a team to collaborate. There are certain activities in the team project where it makes sense to simply coordinate, communicate, and cooperate, (i.e., divvy up the work) and other activities where collaboration has high value added.

The most important objective in collaboration is to ensure the teamwork product is consistent across the content of the project. Consider the inconsistency when one member creates the list of process hazards for a gasoline refinery, and another member creates the root cause analysis and does not include gasoline (fuel) as one of the immediate causes. Consistent teamwork product is reached through engagement of all team members in all parts of the project.

Active Listening – A Special Skill for Communicating

Verbal communication between two people consists of two activities: speaking and listening. This brief discussion focuses on "active listening". As the phrase implies, listening is more than just hearing the words: it includes striving to understand the speaker's message. Active listening is fundamentally important for teams. Active listening requires patience and common courtesy:

- Do not interrupt the other person when they are speaking.
- Do not distract the other person by doing some other activity.
- Do not distract yourself: thinking of a rebuttal, reply, objection, counter-argument, or something else while the person is speaking prevents us from really understanding what the person is conveying.
- All of these are mistakes that can lead to miscommunication and misunderstandings.

Active listening requires the listener to ask open-ended questions to learn, clarify, and explore the thoughts of the speaker.

- The same words can have different meanings to the speaker and the listener, and different words can have the same meanings.
- Skilled active listeners formulate and ask open-ended questions to search and reveal the true meaning of the message.

Misunderstandings arise in the literal language, spoken and written, because the meanings of words may be different (as we have so many times illustrated within the expert field of risk management) depending on the person's educational, cultural, and ethnic backgrounds. This is an issue even where the first language for all persons is English. To illustrate the need to actively listen, consider the meaning of the word "priority" in this discussion:

New Person to the organization: "Safety should be a priority"
Experienced Person (the mentor / coach / supervisor): "No, safety is a value, not a priority."

Are these two people really at odds? Are they both trying to get across the same message? It is only through the desire to understand by probing with questions that a common understanding (or perhaps an opposing understanding) clearly emerge between the two.

Misunderstandings also arise when the stated words do not express the emotions or feelings behind those words. Consider also this exchange where the words stated are clearly different than the intent:

Newly hired Design Engineer in the firm: "This engineering design manual is totally confusing. It jumps between topics and makes no sense."
Experienced and Lead Design Engineer for the firm (who is now on the defensive) immediately and without hesitation responds: "I think not. It isn't to those with experience. Experts with over 100 years of total engineering experience have collaborated on creating this manual, and it has stood the test of time with experts in this field."

In this exchange, the new hire is clearly confused and frustrated with the manual, but has stated their confusion in terms that seem to diminish the value of the manual (i.e., "the manual is confusing"). The Lead Design Engineer is obviously put on the defensive and responds with a curt retort. A better response would have been for the Lead to pause, listen to those words and the expression or emotion behind those words, and ask an open-ended question

(e.g., “How is this manual confusing to you?”). This would open dialogue and tame the potential animosity between the two, result in the Lead coaching the new hire on how to navigate through the manual, and open opportunities for potential improvements to the manual to ensure better communication.

A newly graduated engineer cannot be expected to understand and fit into the culture of his / her new organization right away, but every new hire should learn to ask for help in a non-threatening manner which can lead to healthy professional relationships.

As one should expect, the onus is on the second person – the leader – to ensure the meaning of the communication is clearly understood through active listening skills. This onus does not relieve the first person from doing all they can to ensure a clear message has been sent.

As demonstrated in the second exchange, our emotions and attitudes play a significant role in how we express ourselves and how we interpret the messages sent by others. Thus, not only is it essential to actively listen, it is essential that we state our message in clear terms consistent with our emotions. A simple and plainly expressed statement (e.g., “I am confused with how this design manual is organized” or “I am frustrated with not knowing whom to contact about the issue”) is far more productive than stating “Doesn’t anybody know what they do here?”.

Lastly, non-verbal communication is over 90% of how we send (speak or write) and how we receive (listen or read) a message. Cues in non-verbal communication in the North American context include:

- Body posture: An open body posture lets the speaker know you are receptive and paying attention.
- Body position: A position at eye level helps the speaker feel comfortable. A forward lean gives the message we are attentive.
- Facial expressions: Calm and relaxed
- Tone: Calm and even
- Eye contact: Eye contact 100% of the time
- Space: A distance that is comfortable for the speaker and yourself
- Gestures: Open and relaxed gestures

Understanding body language can be applied with some degree of success within a homogeneous culture. But in diverse workplaces, it could be easily misinterpreted (i.e., what is highly normal and comfortable in one ethnic culture (e.g., eye contact 100% of the time) is highly uncomfortable in another). Therefore, it is important for you to pay attention to cultural differences and cultural norms, and take these differences and norms into account during communications.

ENGG404

Glossary:
Important Definitions and Terms

Definitions of Terms and Phrases

TERM	**DEFINITION**
Acceptable Level of Risk	Defines the level of risk the organization is willing to accept. It is informed by public opinion and corporate policy. Regulations may define basic levels of acceptable risk and in general, leading organizations will set standards that exceed regulations. Acceptable risk is different for different organizations. Risk management tools may be employed to determine the level of risk.
Accident	Many people understand the term accident. However, the connotative meaning of accident refers to an undesired event that is believed to be beyond the control of people; an undesired event that results in harm to people, damage to property, damage to environment or loss to process - or a combination of all. Accidents are then deemed an inevitable consequence of doing business. Contrast this with the position taken by leading organizations and loss prevention specialists: they believe all accidents are preventable. It is arguable that the term accident is not only wrong, but the very use of the term accident is counterproductive to loss management initiatives. See **Incident** or **Event**.
Accident Ratio Study	See the **Incident Pyramid.**
Activity	An activity describes a condition where things are being done. It can describe: ➢ A task or job being performed by a person, or ➢ A complex set of unit process operations in an industrial facility that an organization utilizes. Sometimes, the phrase “an activity or operation” is stated; this means the same as **activity**. The use of this word relates to risk, as in “the risk of the activity” or “the risk of the operation”. Examples of tasks performed by a person: walking; walking in winter conditions; climbing stairs; ascending or descending a ladder; using a hammer; using a power drill; operating a crane; driving a truck; working on a crane; overhauling a pump; entering a confined space; issuing a work permit; welding. Examples of unit operations that an organization utilizes: a pump and piping system for transferring fluids from one vessel to another; a tank used for storing, filling, and emptying materials; a mine; a drilling rig; a rail-car loading or off-loading facility; a reactor system; a fired furnace.
Administrative Controls	An administrative control specifies a safe plan for the safe execution of work. It may be in the form of policies, procedures, and the best practices. Policies and procedures are well-defined, and establish actions to safely and efficiently execute work. Best practices are based on the skills and knowledge of trained and competent workers in their field of expertise. Administrative Controls are put in place to prevent an incident from happening, or to mitigate the incident to a safe level should it happen. Some examples of administrative controls are: operating procedures, maintenance procedures, training requirements, procedures that control life-critical jobs (e.g. work permits, confined space entry, work at elevation, work in atmospheres immediately dangerous to life or health), and emergency response plans and tactics. These, in part, can effectively implement the intent of the risk management system.

TERM	**DEFINITION**
Adverse Impact	Adverse impact on the environment: ➢ If a loss incident results in an emission of a contaminant or pollutant or a substance, either as a single one-time spill / release or continual or continuous spill / release over a period of time, and ➢ If such emission is toxic or noxious or harmful in any way to anything in the surrounding environment of the spill / release, ➢ Then it is highly likely to cause harm to or has negatively affected something in the environment such as a person or persons, or business other than the owner of the emission source, or a waterway or ground water, or plants or vegetation, or one or more animals). The extent of the adverse impact is based on the consequences (Impact on PEAP), is qualitative in nature, and can be subjective i.e. subject to interpretation in a court of law. Note that in some jurisdictions, an organization may be guilty of an offence if the spill / release causes, or is likely to cause, or may have caused an adverse impact. See also **regulatory exceedance**.
ALARP Procedure	In risk assessments, risk can fall within a region where control measures shall be implemented in order to reduce the risk to a level that is as low as reasonably practicable **(ALARP).** This may or may not mean that the level of risk is acceptable. For further explanation see **What is an Acceptable Level of Risk?**
Analysis, Hazard Analysis	Analysis is the detailed examination of something to identify its constituent elements or structure. For example, hazard analysis is a process that evaluates activities, facilities, or systems to identify elements that have the capability to cause harm or loss, otherwise known as hazards. A hazard analysis may not consider the probabilities of those hazards. A hazard analysis may or may not derive the necessary actions (safeguards or control measures) to mitigate or eliminate the hazards. Analysis is sometimes synonymous with assessment, as in hazard assessment or hazard analysis, or safety assessment or safety analysis. In the field of risk management, assessment and analysis have been used interchangeably. It is important to know the intent and desired outcomes of the assessment or analysis. See **Assessment**.
Assessment	A process that evaluates activities, facilities, or systems against requirements or expectations. For example, a gap assessment and closure plan identifies gaps in requirements or expectations (non-compliances or non-conformances), and also identifies the necessary actions to address or close the gaps i.e. come into compliance. Sometimes synonymous with analysis, as in hazard assessment or hazard analysis, or safety assessment or safety analysis. As can be seen, assessment and analysis have been used interchangeably. It is important to know the intent and desired outcomes of the assessment or analysis. See **Analysis**.
Basic Causes	For incidents, basic causes are related to human factors, and can be further divided into personal factors, job factors, and design factors. These are the underlying human factors that allowed, perhaps even invited, the **immediate causes** to develop (substandard practices or substandard conditions). They are difficult to identify; and are often not evident until after an incident has been researched and investigated. Refer to the **Cause and Effect Models** for insight to see this relationship as it pertains to an incident.

TERM	**DEFINITION**
Competent Person	In the Alberta Occupational Health and Safety Code 2009, competent, in relation to a worker, means adequately qualified, suitably trained and with sufficient experience, to safely perform work; without, or with only a minimal degree of, supervision.
Complacency	The attitude of workers and the culture of an organization: ➢ As a result of the incremental, gradual decline (deviations, degradation, deterioration) in workplace conditions and/or workplace practices to the point that those conditions and practices are not meeting requirements (sub-standard), and are not effectively managing risks at an acceptable level or are creating new hazards in the workplace, ➢ AND the acceptance of those sub-standard conditions and sub-standard practices. Some examples that demonstrate complacency include: "taking short-cuts" or breaking rules; "check the box" or "pencil whipping" on a check-list; not rigourously following procedures; not keeping the work area neat and organized, not storing tools and equipment neatly and in the appropriate shelf / container / box, not maintaining the house-keeping in the work area.
Controls or Control Measures	Controls or measures effectively implement the intent of the risk management systems that limit exposure to harm and loss. See **Engineering Controls** and **Administrative Controls.**
Corporate Values	Corporate Values express management commitment, and is the explicit statement by senior management of the ethos (characteristic spirit and beliefs) of the organization.
Critical Few	A basic management principle stating that a small percentage of specific items account for the majority of all incidents and costs. (The 80/20 Rule, Vilfredo Pareto, 1843–1923.)
Direct Supervision	In the Alberta Occupational Health and Safety Code 2009, direct supervision, in relation to a worker, means a competent worker that: (a) is personally and visually supervising the worker who is not competent, and (b) is able to communicate readily and clearly with the worker who is not competent;
Engineering Controls	Process equipment and process hardware (e.g. pressure vessels and pressure relief valves; automated process control systems, their sensors, and their control devices; fire suppression systems, etc.) and process software (logic that automatically activates control devices) that are put in place to prevent an incident from happening or to mitigate the incident to a safe level should it happen. These, in part, can effectively implement the intent of the risk management system.

TERM	**DEFINITION**
Engineering Safety and Risk Management	ESRM is the integrated system / program for, or the approach to, the management of the continuous reduction of risk to people, environment, assets, and production / productivity. Within the industrial setting, it may be referred to as Industrial Safety and Risk Management, Industrial Safety and Loss Management, or Process Safety Management. Those who immediately benefit from risk management are organization personnel, associated contractors, and the public at large. It is also beneficial to the organization's business success and sustainability. Risk management may also protect the environment from undesirable release exposures due to emissions or spills. A Risk Management Program defines techniques and requirements to effectively identify and manage risk exposures to acceptable levels. Specific to Engineering Safety and Risk Management, it is the whole process of recognition, assessment and management direction to identify, and control / mitigate (eliminate or reduce), to an acceptable level, the risk to people, environment, assets, and production / productivity. The Risk Management Process specifically describes the initiation of a review to identify hazards, their risks, and establish controls to keep risk exposures to acceptable levels, particularly in large industrial facilities, but is being adopted by other service industries and commercial activities. Each step requires different activities to be concluded to carry out effective risk management. The result is a process that has evolved globally for over 25 years and is considered to be a direct enabler for sustainable industrial development.
Event Tree Analysis (ETA)	Event Tree Analysis is a process for determining the potential outcomes of an initiating event. It describes how a sub-standard practice or condition may escalate to a much larger incident.
Fault Tree Analysis (FTA)	Fault Tree Analysis is a proactive causal analysis. It is a systematic and deductive process used in reliability analysis of complex systems to determine the technical causes or component failures leading to a system failure. Further, the probabilities of the failures of individual components and the resulting chains of cause-effect consequences can be estimated, and the probability of a system failure (major incident) can be estimated. It can also be used as a means for methodically trouble-shooting the system failure. An automobile is a large complex machine or system, and is made of sub-systems such as the fuel system, the ignition system, the transmission, and so on. Each of these sub-systems is made of assemblies and components; any of which can malfunction to prevent safe and efficient automobile operation.
F.A.I. (First Aid Injury) or ***First Aid Case (F.A.C.)***	An injury that is limited to first aid only. A first aid injury may be attended to at the job site or at a first aid station by a first aid responder, emergency responder, paramedic, health care worker, or physician i.e. it is not who treated the injury, but the nature of the injury that defines the level of severity. This injury classification is less severe than a **medical aid or medical treatment case.**
Flashpoint	The lowest temperature at which vapours emanating from a volatile inflammable (flammable) substance ignite in air when exposed to flame.
Frequency Rate	This typically refers to a measure of injury frequency. See **Injury Frequency Rate**. Frequency Rate can also be applied to incidents involving environment, reliability, asset utilization, organization assets, productivity, and lost business. Different metrics apply in these applications.
Hazard	A potential source of serious harm to people, environment, assets, or production / productivity.

TERM	**DEFINITION**
Hazard Identification	The process to identify or recognize factors or conditions which may potentially promote failure or loss. This step is often experience-driven but must also adapt to new inputs. Checklists and other risk management tools may also be used to identify hazards. The motivation to identify hazards is the trigger for the risk management process to begin, and hazard identification is the first step in this process.
Housekeeping	It is cleanliness and orderliness in the workplace or at the job-site. It is a way of controlling hazards along the route between the job-site and the worker, or controlling hazards in the area of the job-site or work-site itself. Good housekeeping means having no unnecessary items in the work place and keeping all necessary items in their proper places. It includes: proper cleaning of materials and equipment and tools; wiping up spills; collecting trash and properly discarding it; maintaining clear aisles, exits, and work areas; orderly and properly storing materials, tools, and equipment, etc. when not in use.
Human Factors	1) **Human factors** are related to **basic causes** within the root cause analysis process and associated cause and effect models. Refer to the **Cause and Effect Model** for insight to see the relationship as it pertains to an incident. 2) **Human factors** relates to the discipline that considers the optimization of the interface between the human and technology for the purpose of minimizing human error. There are two sub-sets of the human-technology interface: the human-machine interface and the human – information systems interface. 3) **Human factors** relates to the "soft-side" of risk management i.e. understanding and managing behaviours in the workplace, and engaging people in the workplace.
Immediate Cause	The circumstances that immediately precede an incident or develop during it. **Immediate causes**, which generally include substandard practices and/or substandard conditions, are usually easy to identify. Immediate causes are sometimes referred to as the **technical causes** of an incident. Refer to the **Cause and Effect Model** for insight to see this relationship as it pertains to an incident.
Incident or Event; Incident Description	An incident is an undesired and specific event, or sequence of events that could result in or has resulted in harm to people, harm or damage to the environment, loss or damage to property or assets, loss to a process or loss of production / productivity — or a combination thereof. Although incident and event can be used interchangeably, consider an **incident** as a collection of events that sequentially result in harm i.e. a loss incident. Compare these examples: ➢ The **incident**, for example, is: "The worker was sprayed in the eyes with a corrosive liquid, and suffered an eye injury". This form of **Incident Description** is the term used to identify the starting point of a **root cause analysis**. ➢ The **sequence of events** leading up to the incident: "The worker picked up a transfer hose for an acid solution. The worker connected it to the off-loading connection on the tanker truck. While connecting, the worker removed his splash-proof protective eye-wear because the eye-wear was fogged up in the humidity and the worker couldn't see the valve in the dim light under the truck. The worker opened the valve to start off-loading. The liquid sprayed from the incomplete connection and into the eyes of the worker." **Incident description** is the term used to identify the starting point of a root cause analysis. The discipline in the use of these terms is especially critical for the incident investigation method and the associated root cause analysis process. See **Incident Investigation, Analysis, Causation, and Action**.

TERM	**DEFINITION**
Incident Investigation	In the narrow sense, it is the process to systematically gather information about an incident in order to establish the details of the **incident**, and the **sequence of events** in the incident. In a broader sense, it also includes the process to identify the causes of the incident, and to recommend ways of preventing the incident from happening again.
Incident Pyramid	The Incident Pyramid is based on the **Accident Ratio Study** conducted in the U.S.A. in 1969. Even though the data is 30 years old, it still applies today. See **Building A Safety Culture and The Incident Pyramid**.
Incident Recall	A team process to encourage employees to consider all incidents, including near-miss or close-call incidents, in a no-fault / no-blame working environment, and to develop mitigating actions on the strength of the information.
Individual Risk	Where one voluntarily carries out an activity e.g. working at a construction site or driving a car, and knowingly accepts the risks associated with that activity. Associated risk frequencies are calculated on a basis of one year of exposure to the activity or the environment. Contrast this with **Societal Risk**.
Industrial Safety and Risk Management	The integrated approach to the management of the continuous reduction of risk to people, environment, assets and production in the industrial setting. Those who benefit from this risk reduction are organization personnel, associated contractors and the public at large. Basically synonymous with **Engineering Safety and Risk Management**.
Initial Cause	See **Immediate Causes**.
Initiating Event	This is the first unplanned or uncontrolled release of energy that has a potential for escalation depending on other circumstances and / or conditions.
Injury Classification	Workplace injuries have varying degrees of severity. Injury classification ranks injury incidents from least severe to most severe. Typical ranking is: **first aid case**, **medical aid** or **medical treatment case, restricted work case** or **modified work case, lost-time injury** or **days away from work case**, and **fatality**. Lost time injuries include the last five. Some reports may state “Lost time Claims”, meaning that a “lost time injury” has been verified as work-related AND resulted in lost time from work. *Formal regulations and standards exist for defining and differentiating these classifications, and these can vary by jurisdiction and corporation; thus, it is important to note that organizations and organizations in Canada may not uniformly report the nature of their injuries because of the jurisdiction in which they operate, the agency / authority to which they report, and their internal performance reporting metrics as described in their corporate policies. Be certain of the definition and criteria for the measurement when comparing statistics.* *Further, the classification of an event as to “work related” or “not work related” is not as simple as “the injury happened at work”. When considering the classification of an injury, it will be necessary to refer to the regulations, standards, and corporate policies for classifying injuries and reporting in the corporate metrics. The detailed discussion on this is beyond the scope if this program.*

TERM	**DEFINITION**
Injury Frequency Rate (IFR)	IFR is an expression of the measure of injury frequency. Frequency rate = (number of injuries x 200,000 hours) / (Total exposure hours) Where total exposure hours = the number of persons x the number of hours worked. 200,000 hours represents the total approximate time that 100 persons would work in one year. Other expressions: IFR = Number of injuries per 200,000 worker-hours worked IFR = Number of injuries per 100 worker-years worked Note: The progressive reduction in injury frequencies by leading organizations has caused some to adopt a more sensitive metric where: IFR = the number of injuries per 1,000,000 hours worked (500 years). Depending on the metrics, may be stated as Total Recordable Injury Rate or Lost Time Injury Rate. Not always the same so check on the metrics.
Injury Severity Rate (ISR)	ISR is an expression of the frequency of lost-time injuries. Severity rate = (number of lost work days x 200,000 hours) / (Total exposure hours) Where total exposure hours = the number of persons x the number of hours worked. 200,000 hours represents the total approximate time that 100 persons would work in one year. Other expressions: ISR = Number of lost workdays per 200,000 worker-hours worked ISR = Number of lost workdays per 100 person-years worked Note: some organizations use a weighted severity rate that includes all injury classifications. The ISR then infers that injuries that are serious result in more days away from work for treatment and healing.
Latent Causes; Loss of Control; Inadequate Control; Root Causes	Latent causes describe the deficiencies in the management system. These are sometimes referred to as: root causes, systemic causes, or point to loss of control, or inadequate / non-existent controls in the management system. Other descriptions include: weaknesses, failures, or gaps in the management system, or the euphemistic “management system improvement opportunity”. Leaders / Managers should drive the incident investigation and associated root cause analysis processes down to a level that identifies latent causes. Refer to **Incident Investigation, Analysis, Causation, and Action**
Loss Management, or Loss Control or Loss Prevention	A systematic approach to prevent and reduce losses due to unwanted incidents with adverse impacts on **People, Environment, Assets, and Production**.
Loss Control Reporting	A system to report all losses to people, environment, assets and production equipment, and production or productivity.
L.T.I. (Lost Time Injury) or D.A.W.C. (Days Away From Work Case)	An injury incident where **medical treatment** was given and recovery requires time away from work on the next scheduled shift. Typically expressed as “more than the initial day of injury lost due to the injury incident”. This injury classification is more severe than a **medical aid or medical treatment case**, but less severe than a **fatality** classification.
Management System Failure, Weakness, Gap	See **Latent Causes; Loss of Control; Inadequate Control; Root Causes.**

TERM	**DEFINITION**
M.A.C. (Medical Aid Case) or MTC (Medical Treatment Case)	An injury incident requiring **medical aid** or **medical treatment** by a licensed physician. After receiving the medical aid or treatment, the worker resumes working with minimal or no restrictions, and typically on the same day, or next day of scheduled work. This injury classification is more severe than a **first aid case**, but less severe than a **restricted work case, a lost-time injury** or **days away from work case**.
Medical Aid or Medical Treatment	Medical treatment or medical aid is some form of medical attention more substantial than **first aid**, in that it can only be administered by a licensed physician. The definition can be extraordinarily complex. Refer to US-OSHA regulations for a complete definition.
Monitoring and Response	Any activity that is intended to detect deviations and variances in conditions and the potential risks associated with those deviations. The activity can range from visual checks to advanced technology sensing systems, including automatic process control systems. Monitoring and planned response to deviations and variances should be the responsibility of staff at all levels, every day.
Near-Miss Incident, Close Call	An undesired incident that did not result in harm to people, or damage to assets i.e. no physical consequences. Under slightly different circumstances, a near-miss could have resulted in harm to people, environment, assets or production – or a combination thereof. The near miss phrase is widely used, and its origin is enigmatic. One might more readily identify with the phrase “that was a close call”.
Parts Per Million (ppm)	Parts per million. A means for expressing low concentrations of pollutants in air, water, soil, human tissue, food or other materials, according to the fraction of mass or volume occupied by the pollutant; e.g. one part salt in one million parts water. Other measures may include ppb or ppt (billion or trillion).
Permit to Work (PTW)	Is a site-specific, task-specific hazard assessment form. All hazards relevant to the task being performed and hazards relevant to the work area in which the work is being performed, must be identified on the work permit. Because all potential hazards can rarely be anticipated when the work permit is printed, the work permit should include a blank area where a worker can include “other” hazards that need to be eliminated or controlled.
Personal Protective Equipment (PPE)	Any device worn by a worker to protect against hazards; for example, dust masks, gloves, ear plugs, hard hats, protective eye-wear, and steel-toed safety boots. PPE is considered the “last line of defense” in organizations with superior risk management systems and programs.
Practice or Work Practice	The execution, doing or carrying-out of an administrative control. The work may be done by following a policy, a procedure, or by best practice. See **Administrative Controls**. From an audit perspective, work practices can meet standards, or be sub-standard. ➢ Standard (acceptable) practice: when the work is done in accordance with policy, procedure, or best practice. ➢ Sub-standard (unacceptable) practice: when the work does not meet requirements of policy, procedure, or best practice. The area of work practice needs meticulous attention. Note: within the workplace, “work practices” and “behaviours” are synonymous.
Preventative Maintenance	A system for preventing the unplanned and unwanted failure of machinery and equipment by: knowing the expected service life of components of the machinery or equipment; conducting routine inspections; planning and scheduling repairs based on those inspections; maintaining, servicing, and adjusting the machinery and equipment in accordance with the manufacturer’s specifications. These activities support preventative maintenance: updating reliability records and service records; planning routine inspections and maintenance; scheduling parts replacement; maintaining inventories of parts and parts scheduled for replacement; conducting reliability studies. Also referred to as Asset Management.

TERM	**DEFINITION**
Procedures	Step-by-step description of the safe and efficient actions to complete tasks, jobs, work, or **activities**.
Process or Production Process	More definitively, it is a process unit operation that involves chemical production, or component or assembly manufacturing, or material handling processes. It is any **activity** involving the production, manufacture, use, storage, or movement (transportation, shipping, and handling) of a material, including potentially hazardous material. Process is sometimes used to describe a **work process**.
Process Change	Any modification involving substitute materials, other than in-kind equipment replacements, or the operation of facilities at conditions outside the established process, mechanical, or technical design envelope. It can also refer to a change to a **work process**.
Production Interruptions	Sporadic or chronic unplanned interruptions of the **production process**, productivity, or business activity.
Program or System:	Relative to Engineering Safety and Risk Management, it is a series of steps taken to ensure that stated objectives are achieved. A typical system includes consideration of these key elements: • agreed upon objectives and documented procedures; • resources responsible and *accountable* for implementation and execution; • a measurement process to determine if desired results are being achieved; and • a feedback mechanism to provide a basis for further improvement.
Regulatory Exceedance	In most jurisdictions, emission sources (i.e. a smokestack, a scrubber vent, a waste water effluent stream to a water body) are disclosed by the organization / operator of the facility to a government agency as may be required by law. The emission source and its properties (i.e. flow-rate; composition or concentration of a trace contaminant(s); other physical or chemical property; cumulative quantity over a period of time) are being measured either on a continuous, continual, or periodic basis. The government agency may issue an “environmental license to operate” the emission source e.g. an “air permit” or a “water permit”. Generally, the license to operate will define specifications or specify limits pertaining to the emission source and its properties e.g. “flow-rate not to exceed x kg/hr”, “SO2 concentration not to exceed y ppm for any duration”, etc. A regulatory exceedance occurs if and when some property about that emission source exceeds a specification defined in the “license to operate” the emission source and/or in the regulations. This is an objective and quantitative measurement. See also **adverse impact**.
Residual Risk	The risk level associated with a risk exposure that is managed with safeguards and control measures in place. The safeguards and control measures are intended: a) to prevent or mitigate the exposure to an unwanted or uncontrolled release of energy, or prevent inadvertent exposure to a controlled release of energy, and b) to mitigate the incident to a safe level using emergency response plans should loss of control happen. The remaining or residual risk level of a risk exposure must be evaluated to determine acceptability. See **Acceptable Level of Risk**. Once determined to be acceptable, residual risk requires continual management to maintain it at acceptable levels. Acceptability may be defined by corporate policy, stakeholder sentiment, legal requirements, or a combination thereof.

TERM	**DEFINITION**
Restricted Work Case or Modified Work Case	An injury incident where **medical treatment** may have or may not have been given, however the nature of the injury requires, as directed by a physician, that the worker restrict their work to certain activities within their normal job (i.e. restricted work), or is assigned different duties or different job (i.e. modified work). This injury classification is more severe than a **medical aid or medical treatment case**, and has less or the same severity as a **lost-time injury.**

Risk	The possibility of injury, loss or environmental incident created by a hazard. The level of risk is a function of the probability of an unwanted incident and the severity of the consequence(s) of the incident. Hazards are a source of risk. Risk is expressed, quantitatively, semi-quantitatively, or qualitatively as the "Level of Risk i.e. the magnitude of a risk", per ANSI/ASSE/ISO Guide Z690.1-2011. APEGA Guideline for Management of Risk in Professional Practice, V1.0, September 2006, defines "Risk: Combination of the probability of an event and its consequences. The term "risk" is generally used only when there is at least a possibility of negative consequences. In some situations, risk arises from the possibility of deviation from the expected outcome or event. This guideline focuses on negative consequences and minimizing the possibility of loss."
Risk Identification	Risk identification is the "process of finding, recognizing, and describing risks, and involves the identification of risk sources, events, and their potential consequences" per ANSI/ASSE/ISO Guide Z690.1-2011. It encompasses more than hazard identification: it moves beyond to consider adverse outcomes of the risk exposure.
Risk Analysis	Risk analysis is the "process to comprehend the nature of risk and to determine the level of risk" per ANSI/ASSE/ISO Guide Z690.1-2011. It is the use of available information to estimate risks of a hazard to individuals or populations, property or the environment. Risk analyses, which are used when the potential losses are critical and need to be identified in absolute terms generally contain the following steps: scope definition, hazard identification and risk estimation.
Risk Estimation	Risk estimation is the process of combining the probabilities and consequences to quantitatively or semi-quantitatively describe risk; this is a term used in the APEGA Guideline for Management of Risk. This process is embedded in the ANSI term for risk analysis.
Risk Evaluation	The process of "comparing the results of the risk analysis with risk criteria to determine whether the risk is acceptable or tolerable" per ANSI/ASSE/ISO Guide Z690.1-2011. The stage at which values and judgments enter the decision-making process to determine whether the risk is acceptable (tolerable) or needs to be acted upon (intolerable).
Risk Criteria	Risk criteria are the "terms of reference against which the significance of a risk is evaluated" and are "based on organizational objectives with internal and external context" per ANSI/ASSE/ISO Guide Z690.1-2011. In practice, risk criteria are described in organization / corporate policies and translated to the axes of a risk matrix or risk table acorganizationing the risk matrix.
Risk Assessment	Risk assessment is the "overall process of risk identification, risk analysis, and risk evaluation" per ANSI/ASSE/ISO Guide Z690.1-2011. Risk assessment ranks the risk levels, to enable informed decisions that concern the mitigation or control of a risk. Otherwise, all risks would be treated equally. APEGA Guideline for Management of Risk in Professional Practice, V1.0, September 2006, defines "Risk assessment: The overall process of risk analysis (process of identifying hazards and estimating their probability and consequences), risk estimation (process of combining the probabilities and consequences), and risk evaluation (process of evaluating the risk to determine if it can be tolerated or accepted)."

Risk Control	The process of implementing actions to manage risk. The results of risk assessment are used in this process. Risk controls reduce or mitigate but never totally eliminate a risk. Other terms for risk controls: safeguards, control measures, risk reduction solutions.
Risk Acceptance	Risk acceptance is the “informed decision to take a particular risk” per ANSI/ASSE/ISO Guide Z690.1-2011. In practice, risk acceptance is an informed decision to proceed with a particular activity with its associated level of risk.
Risk Communication	A process to facilitate public or private communication of risks to enable understanding of those risks. The communication is between the owner of the risk, and those potentially affected by the risk.
Risk Management Work Process	Risk management work process is the systematic application of management policies, procedures, and practices to the activities of identifying, analyzing, evaluating, and managing the residual risk of activities that have been accepted by the organization.
Risk Management System	Risk Management System is defined as the integrated approach to the management of the continuous or ongoing reduction of residual risk to PEAP in the industrial setting. It is the documented set of management policies, procedures, and practices that enable the implementation of the risk management work process. It can consist of a number of elements, and sections within those elements. A risk management system can be a standardized approach based on a standard such as APEGA Guideline for Management of Risk in Professional Practice, V1.0, September 2006.
Risk Management	The complete process of identifying the hazards, assessing risk, making decisions about implementing effective risk controls and then managing the accepted residual risk. After those controls and their associated actions are in place, continuous management attention is needed for successfully limiting risk exposures and mitigating risks. This includes: auditing (checking the effectiveness of the safety program), ensuring accountability for actions, and re-evaluating the effectiveness of those actions from time to time. APEGA / ISO defines “Risk management: Coordinated activities to direct and control an organization with regard to risk.” APEGA further adds “Risk management generally includes hazard identification, risk assessment, risk control or treatment, risk acceptance and risk communication.”

Root Cause Analysis (RCA)	A systematic investigative approach used to analyse and incident in order to determine the chain of causes, from **incident description** through to **immediate causes** and **basic causes,** and down to **latent causes** (loss of controls or management system failures). After the latent causes are identified, it then becomes possible for management to identify actions to address the latent causes (to address the management system failures), all with the intent to prevent re-occurrence of the incident. Correction of latent causes not only prevents a recurrence of the incident under investigation, but also arrests other potential incidents from occurring in that many incidents frequently share the same latent cause
Root Causes	See **Loss of Control or Inadequate Control**.
Severity Rate	This typically refers to a measure of injury severity. See **Injury Severity Rate**. Severity Rate can also be applied to incidents involving environment, reliability, asset utilization, organization assets, productivity, and lost business. Different metrics apply in these applications.
Sequence of Events	See **Incident** or **Event**
Societal Risk	Societal risk is the risk associated with the impact of an incident or several incidents on more than one individual. The individuals are involuntarily exposed to the risk, and are subject to the impact of the event. Examples: the encroachment of residential development on a legacy industrial site, or the installation of an industrial operation with new risks within an existing development, increases the exposure of individuals in event of an incident. Societal risk is not as clearly defined as individual risk is in terms of acceptability. Societal risk is the sum of all risks imposed, and is typically represented by the F-N (Frequency vs Number of Fatalities) Curve. Societal risk is a function of F and N: $R = \sum_{k} F_k N_k$ *Where:* *F_k = frequency of the k^{th} incident scenarios* *N_k = number of fatalities resulting from the k^{th} scenario, and* *R = the societal risk or total risk to society.* The FN Curve demonstrates the rigour and additional effort required to protect larger groups. For example: For N escalating from 10^1 to 10^2 (a change of 1 order of magnitude), requires 2 orders of magnitude of effort to reduce risk (frequency) e.g. from 10^{-7} to 10^{-9}.
Stewardship	Stewardship is the process to report on the implementation, supervision, or management of the **controls** put in place to reduce risk. The stewardship process needs to ensure that prescribed actions used are always done to comply with or meet management standards. Expressed another way: Stewardship acts to convey that we are operating in accordance with agreed-upon actions and requirements (corporate policy, legal requirements, etc.) to control risk. Compare the stewardship process with the audit process where actions are taken to confirm that we are operating in accordance with agreed-upon actions and requirements, and where not confirmed, actions are defined to bring into compliance.
Sustainability	To be sustainable, an organization must focus on the so-called “Triple Bottom Line”: ➢ Economic Responsibility: return on investment, investing for the future, and growth opportunities ➢ Social Responsibility: meeting the needs of societies, building community capacity . ➢ Environmental Responsibility: protecting and enhancing the environment, the life-cycle of products, and resource consumption

Sustainable Development	As defined by The UN World Commission on Environment and Development: “Development that meets the needs of the present without compromising the ability of future generations to meet their own needs.”
System	A typical system includes consideration of these key elements: agreed objectives and documented procedures, resources responsible and accountable for implementation and execution, a measurement process to determine if desired results are being achieved and a feedback mechanism to provide a basis for further improvement.
Task	A set of related steps that make up a discrete part of a job. Every job is made up of a collection of tasks. Example: • Answering a phone or entering data into a computer are tasks associated with an administrator's job. • Assembling the forms and pouring concrete are tasks for the job of building a foundation. • Dismantling, machining, and re-assembling an engine block are the tasks for the job of rebuilding an engine.
Task Analysis, Job Analysis, Job Safety / Hazard Analysis	A technique used to identify, evaluate and control health and safety hazards linked to particular tasks. A task analysis systematically breaks tasks down into their basic components so that each step of the process can be evaluated thoroughly. Some versions also aim to improve the efficiency of the tasks or job. Also known as **job hazard analysis** or **job safety analysis**.
Total Exposure Hours	The metric **Total Exposure Hours** is a product of the number of persons and the number of hours worked. A typical person works a nominal 2,000 hours per year (a nominal 40 hours per week, 50 weeks per year). The value of 200,000 hours thus represents the total approximate time that 100 persons would work in one year, and is one basis for an injury frequency calculation.
Uncertainty Range	In risk assessment, there is a degree of uncertainty when calculating risk. The span between the lower and upper limits of risk determination define the uncertainty range. See **Societal Risk**.
Work Process	A disciplined approach to how an organization performs work on an on-going or periodic (daily, weekly, etc.) basis. Among many things, a work process should define: a scope, range of application, and boundaries; purpose or objective; roles and responsibilities; a set of procedures or instructions; supporting software tools and databases; and interlocking or connecting work processes.

Some Terms are Best Explained: "Observation, Conclusion, Recommendation, and Opinion" …

In a case study or when facing a real problem of issues and concerns in the work place, a decision must be made i.e. what do you do?

Consider the simple case of the weather and the decision about outdoor activities:

- Observation: The person reads an outdoor thermometer; the reading is "-20 degC".
- Conclusion: The same person concludes that it is cold outside.
- Recommendation: The same person decides to wear a winter coat, gloves, and toque to go outside.
- Opinion: One person looks through the window, sees a snowy landscape, and thinks it is cold outside.
- Opinion: One person may think the weather is perfect for playing hockey on the outdoor rink, whereas another person may think it is too cold for any outdoor activity.

Some Terms are Best Explained by Discussion: "Practical" versus "Practicable"

Several regulations, standards, and codes will make specific use of the term "practicable" as will some of our guest speakers, whereas one might think that the intended word is "practical".

Merriam-Webster defines "practical" as:

1a: of, relating to, or manifested in practice or action: not theoretical or ideal
<a practical question> <for all practical purposes>
1b: being such in practice or effect: virtual <a practical failure>
3: capable of being put to use or account: useful <he had a practical knowledge of French>

Merriam-Webster defines "practicable" as:

1: capable of being put into practice or of being done or accomplished: feasible <a practicable plan>
2: capable of being used: usable <a practicable weapon>

A lay distinction can be stated by way of example: something that is practicable is both useful and feasible, whereas a practical thing may be useful but not feasible.

Consider the Transporter on the USS Enterprise of Star Trek fame. It is a highly practical device in that it can transport inanimate and living objects over vast distances, from one remote point to another, through harsh environments, in a matter of moments, at an apparently low energy cost, and all without harm to the objects. The futuristic Transporter is highly practical as compared to current modes of transport. However, it is not practicable because it is not feasible - the technology doesn't exist. *(Narration based on an idea borrowed from The University of Victoria, English Department.)*

Now consider a technology with which we are much more familiar, and its history: the (pressurized) steam engine invented by Thomas Newcomen, and improved and patented by Sir James Watt. In its infancy, it was a highly practical engine having mobility, adaptability to many different operations, and high power to weight ratio versus other mechanical forms of power supplies such as the water mill, the windmill, or the Savery / Newcomen (atmospheric) steam engine. However it was not immediately practicable given that new technologies needed to be developed such as: methods and processes for smelting and forging of specialized metals; specialized metals for pressure containment, corrosion and heat resistance, and high mechanical static and dynamic loadings; machine tools and techniques to craft the mechanical components to tight dimensional tolerances and balances; fabrication methods (riveting, cutting, and fitting) to assemble the components; precise machine synchronization for operation at high speeds. All of these technologies were needed in order to overcome inefficiencies and prevent catastrophic failures, and were developed and applied so that steam engines became reliable and efficient; thus steam engines became practicable for local power sources and for all surface modes of mass transportation.

Of course, the steam engine became obsolete with the development of the internal combustion engine and the diesel-electric locomotive engine. These technologies themselves were not practicable in their early days but have become highly practicable with advances in materials engineering and manufacturing technologies.