Technical Standards and Safety Authority

Guidelines for the Implementation of the Level 2 Risk and Safety Management Plan

December 22, 2010

Table of Contents

INTRODUCTION

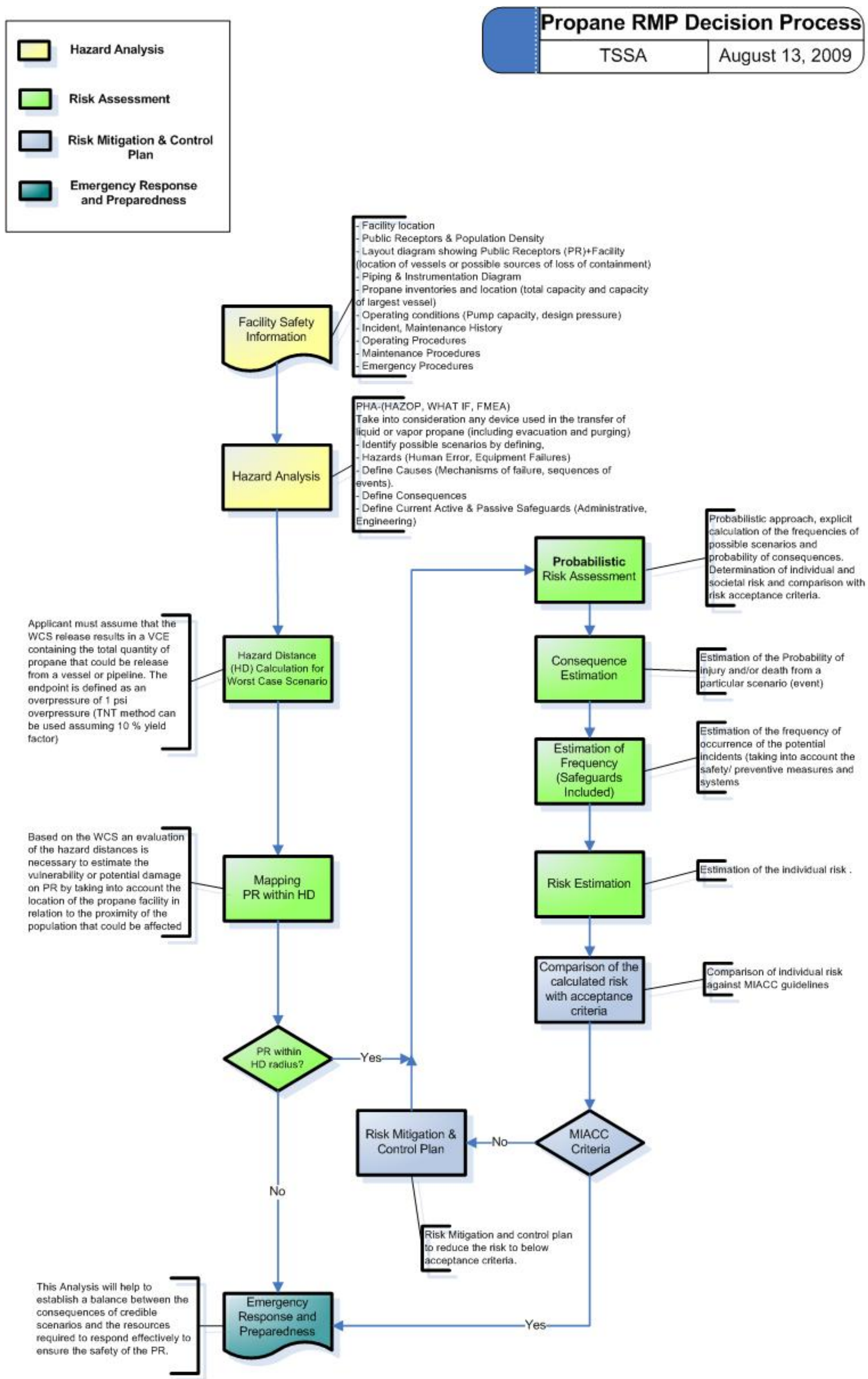
This is the second issue of the guidelines titled Guidelines for the Implementation of Risk and Safety Management Plan originally issued on August 17, 2009. This issue dated December 22, 2010 reflects the changes introduced by the Ontario Regulation 464/10. The changes to the August 17, 2009 document are:

1. The title of the guidelines was changed to "Guidelines for the Implementation of Level 2 Risk and Safety Management Plan". Guidelines for the Implementation of level 1 RSMP are issued as a TSSA advisory FS 183-10 available at: http://www.tssa.org/corplibrary/ArticleFile.asp?Instance=136&ID=CC5B16040D3711E0B7F95D889551D742.

2. Page 9 & 10 – the formula for the Hazard Distance and the distances in Table 2, assume a temperature of 15^0C for propane and 80% fill

A person applying for a new/renewal of licence and subject to requirements laid out in the regulation shall submit a risk and safety management plan with the elements described in the Regulation. The elements of the plan and the decision options available are illustrated in the schematic shown below. The following sections of these Guidelines describe each of the elements in the schematic with reference to the various available and adopted standards applicable to those elements.

Figure 1: Propane risk management plan decision process.



FACILITY SAFETY INFORMATION

The person applying for a license and subject to the requirements of the risk and safety management plan (herewith known as the “Applicant”) should review facility safety information necessary for the facility for the license is sought, and this information should include but not limited to:

1. facility location;

2. public receptors and population density around the facility including distances to the location of each site where Propane stored; definitions for public receptors and methods for obtaining population density are included in the next sections;

3. a facility layout with the following information:

    - the location of each propane storage tank, cylinder storage facility, underground piping or tubing and other propane handling facilities within the container refill centre or filling plant;
    - the location of parking spaces designated by the applicant for tanker truck parking; and
    - the distance from each propane storage tank and cylinder storage facility to the property lines of the centre or plant,

4. propane inventories and location (total maximum capacity and capacity of the largest vessel);

5. facility and transportation system design details. This data is required to analyze the mechanical, electrical, structural, control and other physical characteristics which can lead to a release;

6. piping and instrumentation diagrams (P&IDs) if it is necessary depending on the hazard identification analysis to be conducted by the applicant;

7. operation conditions (pump capacity, design pressure, etc);

8. incident history;

9. emergency procedures;

10. maintenance procedures (for all equipment);

11. operating procedures (for all equipment); and

12. maintenance history.

HAZARD ANALYSIS

Standard/Guideline References

1. Risk Assessment – Recommended Practices for Municipalities and Industry, Canadian Society for Chemical Engineering;

2. CAN/CSA – Q850/97 (Reaffirmed 2002), Risk Management: Guideline for Decision Makers, A National Standard for Canada. Canadian Standards Association; and

3. ISO/IEC Guide 51, Safety Aspects – Guidelines for their inclusion in Standards.

The Q850 guideline defines a "Hazard" as a source of potential harm, or a situation with a potential to causing harm. "Harm", in the context of this regulation refers to physical injury or damage to the health of people (ISO/IEC Guide 51).

Flammability (fires and explosions) is the only recognized hazard associated with the design, installation and operation of propane facilities subject to this regulation.

The process of Hazard Analysis answers the fundamental question, "What can go wrong?" Its prime purpose is to identify hazard scenarios (situations or events) which can lead to undesirable consequences that can cause harm. The output of the hazard analysis phase should be a list of unique hazardous scenarios for which both scenario frequency and scenario consequences can be estimated.

Hazard Analysis involves, at a minimum:

- establishing the undesirable consequences of interest;
- the identification of hazard scenarios associated with material, system, process and facility characteristics that can produce these undesirable consequences;
- analysis of possible causes for the hazard scenarios; and
- identification of current safeguards the safeguards needed to prevent and/or control the hazards as well as the safeguards to mitigate the possible consequences.

With respect to the hazard for propane facilities, the undesirable consequences of interest are:

- vapour cloud explosions (VCE);
- boiling liquid expanding vapour explosion (BLEVE); and
- thermal radiation flux for fires (jet fire, flash fire or fireball).

It is assumed that there is a possibility of harm when public receptors are exposed to any one of these undesirable consequences.
Hazard analysis focuses on failures associated with equipment, instrumentation, utilities, human actions (routine and non-routine), and external factors that may impact the safety of a propane facility. Hazard Analysis should not only focus exclusively on random failures of hardware, but should also consider all types of operator error that can result in the undesirable consequences.

Selection and Application criteria for Hazard Analysis

Hazard Analysis employing HAZID (Hazard Identification) techniques are widely used in the industry and can be carried out at various stages during the lifecycle of the facility. HAZID techniques seek to identify hazards in an absolute or relative way. Relative way use checklists or hazard indices based on experience and lesson from incidents. Absolute methods are based from design intent e.g. HAZOP.

Methods will be influenced by many factors including the amount of existing knowledge about the process, old or new facilities, operating conditions, resources etc.
There are several well established techniques that can be applied to systems, processes, and facilities in order to identify specific events which could lead to the release of propane. Some of the most frequently applied techniques include:

- What-If Analysis;
- Hazard and Operability Analysis (HAZOP); and
- Failure Mode and Effect Analysis (FMEA).

The following sections provide brief description of the above mentioned techniques to carrying out the Hazard Analysis process. The suggested standards/guidelines for the using these techniques is provided. It is highly recommended that the applicants follow these guidelines or other best practice guidelines as a minimum standard while conducting the hazard analysis process.

What-If Analysis

Standard/Guideline References

1. Centre Guidelines for Hazard Evaluation Procedures with Worked Examples; for Chemical Process Safety, American Institute of Chemical Engineers.

This technique is a systematic, team based study to identify risks. The facilitator and team use standard 'what-if' type questions to investigate how a system, plant item, organization or procedure will be affected by deviations from normal operations and behaviour. This technique is widely applied to systems, plant items, procedures and organizations generally. In particular it is used to examine the consequences of changes and the associated risks thereby altered or created.

The system, procedure, plant item and/or change has to be carefully defined before the study can commence. Both the external and internal contexts are established through interviews and through the study of documents, plans and drawings by the facilitator.

Another key input is the expertise and experience present in the study team which should be carefully selected. All stakeholders should be represented if possible together with those with experience of similar items, systems, changes or situations.

The general process followed is that:

1. Before the study commences, the facilitator prepares a suitable prompt list of words or phrases that may be based on a standard set or be created to enable a comprehensive review of hazards or risks;

2. At the workshop the external and internal context to the item, system, change or situation and the scope of the study are discussed and agreed;

3. The facilitator asks the participants to raise and discuss:

    - known risks and hazards;
    - previous experience and incidents;
    - known and existing controls and safeguards; and
    - regulatory requirements and constraints.

4. Discussion is facilitated by creating a question using a 'what-if' phrase and a prompt word or subject. The 'what-if' phrases to be used are "what if…", "what would happen if…", "could someone or something…", "has anyone or anything ever…." The intent is to stimulate the study team into exploring potential scenarios, their causes and consequences and impacts;

5. Hazard scenarios are summarized and the team considers controls in place; and

6. The description of the scenarios, its causes, consequences and expected controls are confirmed with the team and recorded.

Hazard and Operability Studies

Standard/Guideline References

1. IEC 61882, Hazard and Operability Studies: Application Guide, International Electrotechnical Commission.

HAZOP is a structured and systematic technique for examining a defined system, with the objective of:

- identifying potential hazards in the system. The hazards involved may include both those essentially relevant only to the immediate area of the system and those with a much wider sphere of influence, e.g. some environmental hazards; and
- identifying potential operability problems with the system and in particular identifying causes of operational disturbances and production deviations likely to lead to nonconforming products.

A characteristic feature of a HAZOP study is the "examination session" during which a multidisciplinary team under the guidance of a study leader systematically examines all relevant parts of a design or system. It identifies deviations from the system design intent utilizing a core set of guide words. The technique aims to stimulate the imagination of participants in a systematic way to identify hazards and operability problems. HAZOP should be seen as an enhancement to sound design using experience-based approaches such as codes of practice rather than a substitute for such approaches.

The basis of HAZOP is a "guide word examination" which is a deliberate search for deviations from the design intent. To facilitate the examination, a system is divided into parts in such a way that the design intent for each part can be adequately defined. The size of the part chosen is likely to depend on the complexity of the system and the severity of the hazard. In complex systems or those which present a high hazard the parts are likely to be small. In simple systems or those which present low hazards, the use of larger parts will expedite the study. The design intent for a given part of a system is expressed in terms of elements which convey the essential features of the part and which represent natural divisions of the part.

The selection of elements to be examined is to some extent a subjective decision in that there may be several combinations which will achieve the required purpose and the choice may also depend upon the particular application. Elements may be discrete steps or stages in a procedure, individual signals and equipment items in a control system, equipment or components in a process or electronic system, etc.

In some cases it may be helpful to express the function of a part in terms of:

- the input material taken from a source;
- an activity which is performed on that material; and
- a product which is taken to a destination.

Thus the design intent will contain the following elements: materials, activities, sources and destinations which can be viewed as elements of the part.

The HAZOP team examines each element (and characteristic, where relevant) for deviation from the design intent which can lead to undesirable consequences. The identification of deviations from the design intent is achieved by a questioning process using predetermined “guide words”. The role of the guide word is to stimulate imaginative thinking, to focus the study and elicit ideas and discussion, thereby maximizing the chances of study completeness. Basic guide words and their meanings are given in Table 1.

Table 1: Basic guide words and their generic meanings.

Guide word	Meaning
NO OR NOT	Complete negation of the design intent
MORE	Quantitative increase
LESS	Quantitative decrease
AS WELL AS	Qualitative modification/increase
PART OF	Qualitative modification/decrease
REVERSE	Logical opposite of the design intent
OTHER THAN	Complete substitution

HAZOP is particularly useful for identifying weaknesses in systems (existing or proposed) involving the flow of materials, people or data, or a number of events or activities in a planned sequence or the procedures controlling such a sequence. As well as being a valuable tool in the design and development of new systems, HAZOP may also be profitably employed to examine hazards and potential problems associated with different operating states of a given system, e.g. start-up, standby, normal operation, normal shutdown and emergency shutdown. It can also be employed for batch and unsteady-state processes and sequences as well as for continuous ones. HAZOP may be viewed as an integral part of the overall process of value engineering and risk management.

Failure Modes and Effects Analysis (FMEA)

Standard/Guideline References

1. IEC 60812, Analysis techniques for system reliability – Procedure for failure mode and effects analysis (FMEA), International Electrotechnical Commission.

Failure Modes and Effect Analysis (FMEA) is a systematic procedure for the analysis of a system to identify the potential failure modes, their causes and effects that could lead to undesirable consequences. Here, the term system is used as a representation of hardware, software (with their interaction) or a process.

FMEA is applicable at various levels of system decomposition from the highest level of block diagram down to the functions of discrete components or software commands. The FMEA is also an iterative process that is updated as the design develops. Design changes will require that relevant parts of the FMEA be reviewed and updated.

FMEA is considered to be a method to identify the severity of potential failure modes and to provide an input to mitigating measures to reduce risk. Application of FMEA is preceded by a hierarchical decomposition of the system (hardware with software, or a process) into its more basic elements. It is useful to employ simple block diagrams to illustrate this decomposition (IEC 61078). The analysis then starts with lowest level elements. A failure mode effect at a lower level may then become a failure cause of a failure mode of an item in the next higher level. The analysis proceeds in a bottom-up fashion until the end effect on the system is identified.

FMEA generally deals with individual failure modes and the effect of these failure modes on the system. Each failure mode is treated as independent. The procedure is therefore unsuitable for consideration of dependent failures or failures resulting from a sequence of events. In determining the impact of a failure, one must consider higher level induced – resultant failures and possibly the same level of induced failures. The analysis should indicate, wherever possible the combination of failure modes or their sequence that was a cause of a higher level effect.

The following steps should be followed in order to complete the analysis:

1. FMEA planning and scheduling to ensure that the time and expertise is available to do the analysis;

2. define the system, by breaking down into subsystems, devices, and parts;

3. define part functions;

4. identify potential failure modes & potential causes of failure for each part function;

5. define current controls and safeguards;

6. evaluate the potential effects of failure; and

7. define current controls for mitigating the effects of failure.

The FMEA process also provides a mechanism to prioritize and screen hazards for further risk assessment by using the calculation of a Risk Priority Number (RPN). The RPN may be used to determine those hazard scenarios that need to be evaluated further as part of the risk assessment.

Another key input is the expertise and experience present in the study team which should be carefully selected. All stakeholders should be represented if possible together with those with experience in similar items, systems, changes or situations.

HAZARD DISTANCE CALCULATION FOR WORST CASE RELEASE SCENARIO AND COMPLIANCE WITH OPTION 1

Standard/Guideline Reference

1. Risk Management Program Guidance for Propane Storage Facilities (40 CFR 68), United States Environmental Protection Agency.

It is required under the regulation that the applicant determines the hazard distance applicability to facility seeking a license. Hazard Distance is defined using the EPA's "Risk Management Program Guidance for Propane Storage Facilities (40 CFR PART 68)".

Hazard distance is the distance at which 1 psi overpressure is felt resulting from a vapor cloud explosion (worst case scenario) involving the contents of a single largest vessel on a site.

The Worst Case Release Scenario is defined by the release of the contents of the total capacity at the facility or the single largest vessel (or piping) containing Propane which will result in a vapor cloud explosion (VCE).

In general, if two or more vessels that contain a regulated substance and are connected through piping or hoses for transfer of the regulated substance, the applicant must consider the total quantity of the regulated substance in all the connected vessels and piping when determining the threshold quantity in a process. If the vessels are connected for transfer of the substance using hoses that are sometimes disconnected, the applicant shall still have to consider the contents of the vessels as one process, because if one vessel were to rupture while a hose was attached or a hose were to break during the transfer, both tanks could be affected. Therefore, the applicant must count the quantities in both tanks and in any connecting piping or hoses. The applicant cannot consider the presence of automatic shutoff valves or other devices that can limit flow, because these are assumed to fail for the purpose of determining the total quantity in a process.

This requirement specifies the hazard distance for consequence analysis of a vapor cloud explosion (VCE) of Propane as an overpressure of 1 pound per square inch (psi). This endpoint was chosen as the threshold for potential serious injuries to people as a result of property damage cause by an explosion (e.g. injuries from flying glass from shattered windows or falling debris from damages houses).

For the worst-case consequence analysis, you must also assume the entire contents of the cloud to be within the flammability limits and the vapor cloud detonates.

As a conservative assumption, if you use the method presented here, you must assume that 10 percent of the flammable vapor in the cloud participates in the explosion.

Consequence distances to an overpressure level of 1 pound per square inch (psi) may be determined using the following equation, which is based on the TNT-equivalency method:

$$D = 17 \times \left(0.1 \times W_f \times \frac{HC_f}{HC_{TNT}}\right)^{1/3}$$

where: **D** = Distance to overpressure of 1 psi (meters)
W_f = Weight of flammable substance (kilograms or pounds/2.2) f (for conversion purposes, density of propane assumed to be at 15 deg. C)
HC_f = Heat of combustion of flammable substance (kilojoules per kilogram) (Propane: 46,333 kjoule/kg)

HC_{TNT} = Heat of explosion of trinitrotoluene (TNT) (4,680 kilojoules per kilogram)
The factor 17 is a constant for damages associated with 1.0 psi overpressures. The factor 0.1 represents an explosion efficiency of 10 percent. To convert distances from meters to miles, multiply by 0.00062.

Table 2 provides the worst-case distance to a 1 psi overpressure for propane tanks.

Table 2: Distance to a 1 PSI overpressure

Nominal Water Capacity (USWG)	Distance to Endpoint (m)
5,000	333
10,000	420
25,000	570
30,000	606
60,000	763
90,000	874

Mapping Public Receptors within Hazard Distance

Based on the calculated hazard distances for the worst case scenario an evaluation of the distances is necessary to estimate the vulnerability or potential damage on the public receptors by taking into account the location of the propane facility in relation to the proximity of the population that could be affected.

This diagram should show whether any public receptors are within a circle whose radius is equal to the hazard distance calculated from the worst case and alternative scenarios. Public receptors include 'offsite residences, institutions (e.g. schools and hospitals), industrial, commercial, and office buildings, parks, or recreational areas inhabited or occupied by the public at any time without restriction by the stationary source where members of the public could be exposed to overpressure, radiant heat, as a result of an accidental release of propane. Offsite means areas beyond your property boundary and areas within the property boundary to which the public has routine and unrestricted access during or outside business hours. Public roads are not public receptors.

Compliance with Option 1

If there are no public receptors within the radius area of the hazard distance then the applicant is in compliance with Option 1 and could proceed to the development of an Emergency Response and Preparedness Plan described later in this guideline.

Compliance with Option 2

If the applicant is unable to demonstrate compliance with Option 1, then they should conduct a Probabilistic Risk Assessment which requires the quantitative estimate of risk using methods described in the next chapter of this guideline and comparing the estimated risk with the risk acceptance criteria described later.

PROBABILISTIC RISK ASSESSMENT AND COMPLIANCE WITH OPTION 2

Standards/Guidelines References

1. Risk Assessment – Recommended Practices for Municipalities and Industry, CSChE, 2004 ;
2. CAN/CSA – Q850/97 (Reaffirmed 2002), Risk Management: Guideline for Decision Makers, A National Standard for Canada. Canadian Standards Association;
3. Guidelines for Evaluating the Characteristics of Vapor Cloud Explosions, Flash Fires, and BLEVEs", CCPS, AICHE, 1994;
4. Guidelines for Process Quantitative Risk Analysis, second edition, CCPS, AICHE, 2000;
5. IEC 61025, Fault Tree Analysis, International Electrotechnical Commission;
6. NUREG-0492, Fault Tree Handbook, US Nuclear Regulatory Commission;
7. ARAMIS - Accidental Risk Assessment Methodology for Industries in the Context of the Seveso II Directive;
8. Guidelines on Quantitative Risk Assessment, Purple Book, Ministry of Housing, Spatial Planning and the Environment, The Netherlands;
9. Methods for calculating Physical Effects, Orange Book, Ministry of Housing, Spatial Planning and the Environment, The Netherlands; and
10. Methods for calculating and processing probabilities, Red Book, Ministry of Housing, Spatial Planning and the Environment, The Netherlands.

Applicants unable to comply with Option 1 should undertake a probabilistic risk assessment to estimate the cumulative level of risk posed by their facility and compare this risk estimate with acceptance criteria described later in this chapter.

The applicant should estimate the risk associated with those hazard scenarios identified in the Hazard Analysis stage that could lead the undesirable consequences of interest (VCE, BLEVE, and/or thermal radiation flux from fires). Risk should be estimated in terms of harm to public receptors as a function of the identified hazard scenarios and the undesirable consequences of interest.

The risk assessment to be carried out to demonstrate compliance with Option 2 has the following steps:

Step 1 – Frequency Analysis;
Step 2 – Consequence Analysis;
Step 3 – Risk Estimation (Individual Risk); and
Step 4 – Comparison with Risk Acceptance Criteria

Step 1 – Frequency Analysis

The risk of harm presented by a facility is dependent on the frequency at which the hazard scenarios can be expected to occur and the undesired consequences which could result from the event. The hazard scenarios which were identified using the techniques outlined in the Hazard Analysis section must be analyzed to determine their expected frequency.

A number of different techniques are available to estimate the frequency of hazard scenarios occurring at a specific facility. The techniques may include:

- historical data analysis;
- fault tree analysis;
- event tree analysis; and
- human reliability analysis,

All of these techniques rely on past experience to a certain extent. Fault and event trees are the most common frequency modeling techniques for complex situations that require tracking of chains of events. Human reliability analysis and external events analysis can be considered essentially as components of fault and event tree analysis, the information generated from their application to be fed into the fault and event trees. Frequency represents the number of events in a given time duration and is expressed in units such as events per year.

Historical Data Analysis

Use of historical data in the estimation of hazardous event frequencies is a suitable approach if the operating experience of the equipment is sufficient to produce a statistically meaningful database. Historical data can be used in two different ways:

- to estimate directly the frequency of the hazardous event of interest ("top event") identified in the Hazard Analysis step; and
- to estimate frequency of events or causes that contribute to the occurrence of the top event.

The latter is generally used in conjunction with fault trees.

There are common types of equipment that are used in the various industries (e.g., pumps, valves, pipelines). Industry average failure frequency rates are available for these pieces of equipment. However, not all facilities experience failures at the same rate. These rates can vary considerably depending on site or company conditions such as:

- management practices;
- operating practices;
- appropriateness of design, plant layout, and construction materials;
- level of testing, inspection and maintenance;
- equipment age;
- severity of operating conditions; and
- nature of the materials handled.

Therefore, it is best to use site- or company-specific release data if it is available. However, any given site or company will not generally experience a significant number of major events to form a statistically significant database. In this case, it will be necessary to use general industry data for overall failure rates as a first approximation. When using general industry data, it is common practice to adjust the data up or down by up to an order of magnitude based on engineering judgement, depending on the specific site or company conditions.

Fault Tree Analysis

When failure rate data is not available for the undesired event or the top event, or its accuracy is not judged to be sufficient, it is possible to estimate the event frequency using analytical methods, specifically Fault Tree Analysis. Fault Tree Analysis uses a "backward logic" which begins with the undesired consequence of interest (e.g., flash fire from containment), analyzes the system to determine the basic cause(s) of the undesired event, and enables the user to quantify the likelihood of the top event. This is done through a "top down" tree whose branches identify the main causes and influencing factors contributing to the top event. The tree-like or branching investigation of each scenario gives rise to the name ‘fault trees’. Since the method is deductive, it focuses attention on the particular event in question, thereby eliminating time spent following trains of thought which do not lead to hazardous situations.

Construction of Fault Trees

Fault Tree Analysis is used to estimate the likelihood of a hazard scenario. This technique starts with a particular undesired top event, such as a flammable material release and fire or explosion from a particular system. It then breaks down the causes of an accident into all the identifiable contributing sequences, and each sequence is separated into all necessary components or events. The presentation of all this information is facilitated by the use of a logic diagram, or ‘fault tree’. The fault trees are generally developed only as far as necessary down to a level where failure or event frequencies are known with a reasonable degree of accuracy from past experience or historical data. The elemental parts of a fault tree at the bottom level are known as "basic events".

To quantify a fault tree, failure rates are assigned to the basic events at the bottom levels of the tree. The occurrence rates for human error and equipment failure used in the fault trees are based either on information reported in the literature, specific facility or company history, or on analyst estimates which combine information supplied by the company (operating procedures, personnel organization and experience, and design information) with information from other sources in the literature. If available, it is best to use site-specific failure data when quantifying the tree. This data is often available from preventive maintenance records or from a review of incident reports. The sequence of events forms pathways, along which are found ‘AND’ or ‘OR’ gates. These gates connect the basic initiating event and contributing events to the higher-order events. When the occurrence of all of a set of lower-order events is necessary for the next higher order event to occur, they are joined by an ‘AND’ gate.

By multiplying together the probabilities of each event in the set, the probability of the next higher event is obtained. When the occurrence of any one of the set of lower order events is sufficient for the next higher order event to take place, the events in the set are joined by an ‘OR’ gate, and their probabilities are added. Probabilities of the top events are expressed as a yearly rate, e.g., 10^{-4} chance of occurrence per year (once in every 10,000 operating years on average). Since the probability of each top event (accident scenario) is to be expressed as a yearly rate, no more than one event leading into an ‘AND’ gate can be a frequency. Otherwise, the overall rates will be in terms of something similar to ‘occurrence rate per year squared’ - a meaningless concept. Thus, at most one event leading into an ‘AND’ gate can be expressed as a frequency; the remaining events are expressed as conditional probabilities, or failures per demand. At ‘OR’ gates it is essential that all the events entering the gate be quantified in the same units, i.e., as either frequencies or probabilities, since they are to be added. The next higher-order event will be in the same units as the events preceding it. One of the most common mistakes is to multiply two or more frequencies together, yielding meaningless results.

Event Tree Analysis

Event tree analysis is a “forward looking” method that takes an initiating event, identifies post initiating-event influencing factors, and combines the information into a logic tree in which the occurrence of each influencing factor is either “true” or “false.”

Two types of event trees are commonly used in risk assessments. These are referred to as pre- and post-incident event trees. Pre-incident event trees are generally used to develop and track the responses of a control system after failure of that control system, this failure being the initiating event. Each possible outcome following the initiating event is tracked with a series of positive or negative branches, examining what would happen if the next line of defense functions as designed or fails to function, each with its associated probability of failure. In this way, probabilities of undesirable consequences of interest can be estimated. Post-incident event trees are used to track possible outcomes following hazardous material release on other “top events” examined by a fault tree, and to estimate the frequencies of these outcomes.

Human Reliability Analysis

This component of frequency analysis refers to quantitative examination of human responses to given routine and emergency situations which require human intervention. The information is generally in the form of conditional probability of "failure to respond in the appropriate manner to a given signal" or "failure to perform a certain task correctly." Failure rates will be higher for high-stress situations, and also depend on environmental conditions, timing of events, experience, availability of written procedures and training levels. In risk analyses, this information is used in fault and event trees. Human reliability analysis is an important component of risk analysis. Reviews of past accidents show that human error accounts for the vast majority of these events. The technique most widely used for estimating human error probabilities is called THERP. The method uses event trees drawn in a different format to arrive at a human error probability. In these event trees failure paths branch right and success paths branch left.

Uncertainties in Frequency Estimation

The greatest influence on uncertainty in risk results can be attributed for uncertainties in frequency estimates. They arise from:

- uncertainties in modeling;
- errors in modeling;
- omissions in modeling of safety features; and
- uncertainties in failure data.

Each of these can cause the estimated frequency to deviate from the "true mean" frequency. Uncertainties in modeling occur due to a variety of reasons. The analyst may not have sufficient design, layout, or operating information to enable the development of accurate logic tree models. Another type of uncertainty may arise from taking short cuts in the modeling in order to simplify the effort required. Usually conservative assumptions can be made for the above factors.

Errors in modeling may arise if due care is not taken in developing fault/event tree models or in the identification of appropriate failure data.

Omission in taking credit of safety features can cause a hazardous event frequency to be overestimated significantly (by up to two orders of magnitude or more). The magnitude of this uncertainty alone may be greater than the cumulative uncertainties in all other assessments. If the results are acceptable, then there is no need for a second iteration and the analyst would have confidence that frequency and risk have not been underestimated.

In the above factors, the analyst has control over the uncertainties. However, when it comes to failure data based on historical observations, the analyst has little control over the uncertainties. This data tends to be generic (i.e., "average") and limited. The unique conditions at a specific plant (e.g., component service, age, or environmental conditions) may not be captured in the data. In addition, not all components or component failure modes may have data available. Inevitably, approximations are made; these should be made conservatively. Failure rates that are available will also have significant uncertainties—divisors (i.e., component years of service) may not be well known or the number of component failures in the database may be under-reported. This is particularly important if using generic hazardous event frequencies (i.e., BLEVEs per tank-year) in that they are unlikely to capture the design, layout, operational and mitigation features of a particular plant. Here, the uncertainty in the frequency estimates may be so significant to render the risk results meaningless.

Step 2 – Consequence Analysis

For the undesirable consequences of interest associated with the identified hazard scenarios, the consequence analysis step involves the estimate of the magnitude of physical harm and damage to the public receptors within the hazard distance should those hazardous scenarios occur.

Consequence estimation can be accomplished by a combination of:

- comparison to past incidents;
- expert judgement; and
- using mathematical models (consequence modeling), which can be at various levels of detail; and sophistication.

Consequence Modeling is an analytical approach used to determine the possible physical effects resulting from the release of propane. The inputs to this analysis include the physical and chemical characteristics of propane and the characteristics of the system in which it is contained.

This section of the guide describes the important underlying physical mechanisms for the three undesirable consequences of interest, and gives guidance on the type of models that should be used to provide an acceptable level of accuracy in estimates of event consequences (and hence individual risk, which is the desired end point for comparison against the Risk Acceptability guidelines).

The focus is on estimation of thermal radiation (heat intensity) levels from fires, and explosion overpressures. Each of these effects is capable of causing serious injuries or fatalities. Results are normally expressed at selected receptor locations and, for time-varying hazards, as a function of time.

Consequence modeling generally involves three distinct steps:

1. estimation of the source term (source term modeling), i.e., how much material in what form (gas/ liquid/two-phase) is being released from containment as a function of time, and development of the release scenarios or possible outcomes (fire, explosion, etc.) following the release;

2. estimation of the hazard level (hazard modeling) as a function of time and at selected receptor locations, i.e., estimation of:

   - thermal radiation flux for fires (for a jet fire, pool fire, or fireball); and
   - overpressure for explosions (for a confined explosion, boiling liquid expanding vapour explosion [BLEVE], or vapour cloud explosion [VCE]); and

3. estimation of damage level on the selected receptor, based on the hazard level at the receptor location (vulnerability modeling).

<u>Physical Mechanisms And Parameters Important For Determining Source Terms And Outcomes Of Releases</u>

The total mass of the release and its rate of release are probably the most important parameters that influences the hazard zone associated with a release. A release rate will normally vary with time and as a function of hole size and location, containment conditions, system inventory, and external conditions. In the case of an instantaneous release, the source strength is specified in terms of the total mass released. For a “continuous” release, the source strength is a function of outflow expressed in terms of mass per unit of time. In order to determine the strength of the source, the physical state of the contained propane must be defined and described. The physical properties of propane, together with containment pressure and ambient temperature, determine the physical state.

<u>Thermal Radiation Effects</u>

Thermal radiation effects arise from flash fires, pool fires, jet fires, or fireballs. These involve the combustion of flammable mixtures. Intensity of thermal radiation (measured in terms of thermal radiation flux or energy per unit area and time) at a receptor outside a fire depends on its distance from the fire, the flame height, flame emissive power, and atmospheric transmissivity.

Flash Fires

For flash fires, the controlling factor for the amount of damage that a receptor will suffer is whether the receptor is physically within the burning cloud or not. This is because most flash fires do not burn very hot and the thermal radiation generated outside of the burning cloud will generally not cause significant damage due to the short duration. Thus, modeling of flash fire consequences consists of primarily an exercise in dispersion modeling, the hazard zone being essentially the extent of the flammable zone of the cloud.

Other Types of Fires

For the other types of fires, available models are broadly classified as either point source models (simple or with multiple sources), or view factor models based on either an equivalent radiator or a solid flame approach. They differ in their required input parameters according to the type of fire and to the level of detail and complexity inherent in the inputs and submodels needed to describe the physical event. Point source models are generally less complex than the view factor models. They are appropriate when the receptor is sufficiently separated from the fire that the specific shape and size of the fire is no longer important. In contrast, view factor models allow the geometry of the flame, as well as the receptor configuration, to be taken into account in the estimation of thermal flux. These are therefore more applicable to cases where the receptor is close to the fire and/or when the geometric details of the fire are important (e.g., wind effects, receptor orientation).

Explosion Effects

Explosion overpressure effects that are of interest here result either from the rapid combustion of a fuel/air mixture (confined explosion or VCE), or a sudden release of pressure energy (BLEVE).

BLEVE

For BLEVEs, the available models are based on the similarity of the blast waves in the far-field to those generated by high-explosive detonation. The compressed gas' stored energy is first calculated based on pressure at the time of burst. The energy of explosion is obtained as the difference between the initial and final states, assuming isentropic expansion. This energy contributes primarily to the production of a blast wave and of missiles. The fraction of pressure energy that contributes to the blast wave can be taken to be about 40%. Overpressure and impulse are then read from charts which relate detonation-blast parameters to charges of high explosive with the same energy. In the near field, this similarity to high explosives is not valid, and correction factors based on numerical simulations should be used. Missile damage from BLEVEs is more difficult to model and of relatively little importance in risk assessments.

Confined Explosions

Confined explosions occur when a flammable mixture in a confined space is ignited. The modeling of confined explosion effects is analogous to the modeling of BLEVEs. Here the explosion energy released is obtained from the enthalpy of combustion.

VCE

For a fuel/air mixture outside containment, conditions favouring a VCE as opposed to a flash fire include:

- the mass of the cloud (e.g., 5 tonnes appears to be a lower limit for propane vapour cloud explosions outside containment);
- flame speed;
- degree of confinement; and
- degree of turbulence in the cloud.

A rapid violent release, if not ignited immediately, may result in sufficient mixing through self-generated turbulence for explosive conditions to occur. The portion of the vapour cloud within the explosive range at the time of ignition will contribute directly to the explosion. The resulting overpressure at a given point is a function of:

- the distance from source;
- fuel properties;
- mass of the cloud; and
- degree of confinement (affected by the presence of obstacles).

Two different types of models are generally used in practice for estimating VCE overpressures at a distance from a source.

1. The TNT equivalency method relates the explosive potential of a release to the total quantity of fuel in the vapour cloud, whether or not it is within flammable limits. The explosive power of the vapour cloud is expressed as an energy equivalent amount of TNT located at the centre of the cloud. The value of the proportionality factor is determined from damage patterns observed in a large number of similar vapour cloud explosion incidents. Calculated blast overpressures tend to be high near the cloud centre (regardless of physical surroundings) and a gradual decay is observed as distance from the cloud centre increases. This translates into a localized high damage zone with low to moderate damage in outlying areas.

   It is important to apply conservative values to the proportionality constants used for the TNT method. An explosion efficiency of 0.06 to 0.10 should be used even in areas which are not tightly confined. Scaling factors should be averaged among several literature sources and used to calculate overpressure profiles. These data are often material specific and, if not averaged, could introduce additional errors.

2. The multi-energy method reflects current consensus that one of the controlling factors of severe explosions is turbulence. One source of such turbulence is the high velocity flow of fuel being ejected from a pressurized system. Explosive combustion rates may develop in such a turbulent fuel air mixture. Another source of turbulence is combustion within a partially confined/physically obstructed environment. The expansion of combustion gases against a confining structure can cause exponential increases in the combustion rate and an overall increase in overpressure. The explosive power of a vapour cloud is determined primarily by the energy of fuel present in the confined areas of a vapour cloud. It should be noted that, in cases where VCEs may be possible, the footprint of the flash fire zone (the zone within the lower flammability limit [LFL] of the material) should also be estimated and used in the overall risk estimation with its corresponding frequency.

The next and final step in consequence modeling is estimation of the level of damage on the receptor. For all hazards except flash fires, there are two commonly used methods for this:

- fixed-limit methods; and
- the PROBIT method.

The fixed-limit method consists of comparing the estimated average (or maximum) hazard level to which a receptor is exposed, against fixed limits which are available from the literature. The advantage of the fixed-limit method is its simplicity. Its disadvantage is that it can be very misleading for time-varying hazards, which is generally the case under major accident conditions.

A more appropriate and the recommended method are to use the PROBIT method, which can readily handle time-varying situations.

To apply this method, a “hazard load” L is estimated at each receptor point,

L = F I^dt for thermal radiation hazards (I is the time varying thermal radiation flux resulting from the fire);

L = P_o for explosion hazards (P_o is the overpressure resulting from the explosion).

Here, the integration essentially represents the total amount of contaminant or thermal energy received by the receptor (weighted by the power n), and n is an empirical PROBIT parameter appropriate for the chemical and type of hazard. The integration is performed over the time of exposure during the hazardous event. (Effect of evacuation or sheltering in a building can thus be incorporated into the results if desired).

The PROBIT (probability unit) Y is estimated as:

Y = k1 + k2 Ln(L)

where k1 and k2 are additional empirical PROBIT parameters.

Flash Fires

For flash fires, the maximum extent of the hazard zone is generally based on the lower flammable limit (LFL) of the material. Sometimes, LFL/2 is also used to take into account the possibility of having high-concentration pockets of gas which might result from concentration fluctuations in the atmosphere. However, this is not the whole story. Ignition of a gas cloud can occur as the leading edge of the cloud reaches an ignition source and the cloud will burn towards the source. Hence, the flash fire will only affect the area between the ignition point and the release location. By estimating the probability of ignition as the cloud reaches each ignition source, one can estimate the probability of affecting any receptor as a function of distance from the release point.

A common assumption for probability of fatality for people caught in a flash fire is 10% for those having protective (fire-retardant) clothing (such as NOMEX suits), and 90% for those without such protection. Both are somewhat on the conservative side and include major injury, which will lead to overestimates of risk of fatality.

Uncertainties in Consequence Modeling

Uncertainties in consequence estimation arise due to uncertainties in modeling the sources term, the migration of a hazard away form the hazard source (hazard modeling), the effects of a level of hazard on receptors (vulnerability modeling), and due to assumptions made with respect to the degree of protection afforded to receptors. As discussed below, these uncertainties are for the most part treated conservatively.

In the estimation of consequences, a major source of uncertainty is the modeling of the source term. The source term describes the rate of release of material from containment and into the carrying medium (e.g., atmosphere). In effect, the source term determines the amount of the material released. There are a number of uncertainties related to source term. These include:

- hole characteristics – size, location, shape;
- orientation of the release – vertical, horizontal;
- degree of pooling of flashing two-phase discharges; and
- degree and size of confinement – release outdoors/indoors, into a dike area; and
- amount of material involved.

With the above, conservative assumptions can usually be made to avoid underestimation of consequences.

Step 3 - Risk Estimation

Following estimation of frequencies and consequences of representative hazard scenarios, the next step is to fully quantify the risk. Risk can be quantified as location/individual Risk

Estimation of Location/Individual Risk

Location risk assumes a receptor at a certain location relative to the risk source to be outdoors and present all the time. Individual risk takes into account the fraction of time a receptor could be indoors/outdoors, and may also take into account the fraction of time the receptor may not be at that location. The appropriate parameter must be used to be consistent with the intended meaning in the risk acceptability criteria (described later).

> *Location/Individual Risk at a receptor point = Event Frequency x Event Location/Individual Consequence at that receptor point*

The total facility risk is then the sum of the risks of all the evaluated hazard scenarios at a receptor point. Repeating the process at different receptor points will generate a risk curve where generally risk decreases with increasing separation distance from the risk source (see Figure 2). The units of individual risk measure can be expressed as "the annual chance that a person living at a given location near the propane facility might die due to potential incidents in that facility." (Risk acceptability guidelines are for a specific receptor location and not for a receptor who may spend some of his or her time away from that receptor location. Hence, the risk calculation should also assume continuous exposure of the receptor).

In the calculation of the total facility location/individual risk, it is important that all significant representative hazard scenarios are identified. Due to the large number of potential scenarios in complex installations, scenarios with similar consequences are normally grouped together to reduce the amount of effort required to quantify their consequences. Then a representative scenario is selected for each event category and is assigned the total frequency of all events falling into that category of events. With respect to this regulation, the representative scenario selected for each scenario category is generally the worst credible case in that category of scenarios. This is done to ensure that the risk estimates are conservative (i.e., risks are over-estimated) so that public safety is not compromised.

For events with little or no dependence on meteorology and wind direction (such as explosions and fireballs) in facilities that can be considered as point sources (such as chemical plants and storage facilities), the mathematical expression for the total individual risk is relatively straightforward:

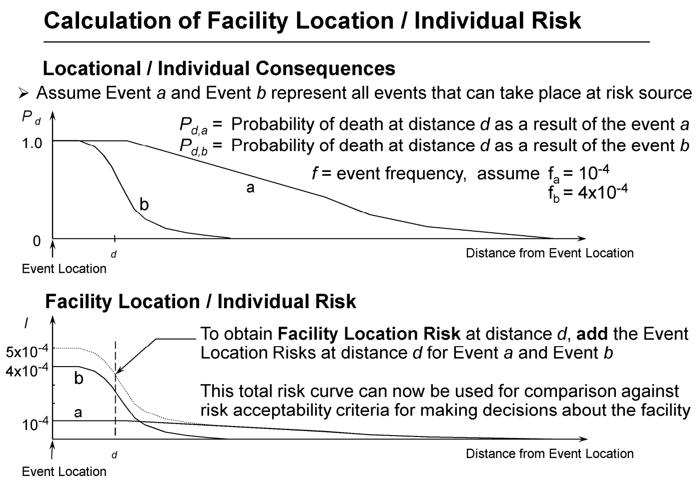
$$I(P;P') = \sum f_h \, P_{e,h}(P;P').$$

Here $P_{e,h}(P;P')$ denotes the probability of harm (e.g., fatality) at receptor location P due to the risk source at P´ and hazard scenario ***h***, f_h denotes the annual frequency of the hazard scenario ***h***, the multiplication of the two gives the event location/individual risk at receptor point P, and the sum is over all the scenario categories.

For meteorology- and wind direction-dependent events (such as flammable gas clouds), the treatment is more complex, requiring consideration of joint frequency of occurrence of different weather conditions with wind direction.

For the purposes of this regulation, calculation of location risk for fires should assume unprotected outdoor receptors, and for overpressure events (VCE, BLEVE) calculation of location risk shall assume an indoor receptor in a typical dwelling structure (more discussion is needed for specific assumption about conditional probability of death for individuals caught in a damaged building due to structural damage or glass breakage).

Figure 2: Calculation of facility location / individual risk.



Step 4 - Comparison with Risk Acceptance Criteria

The estimated location risk should be compared with the acceptance criteria defined by the Major Industrial Accidents Council of Canada (MIACC) risk acceptance criteria guidelines, modified by the CSChE Process Safety Management Division to address the weaknesses identified in applications across Canada since the first publication of the MIACC guidelines.

MIACC Guidelines for Individual Risk Acceptance Criteria

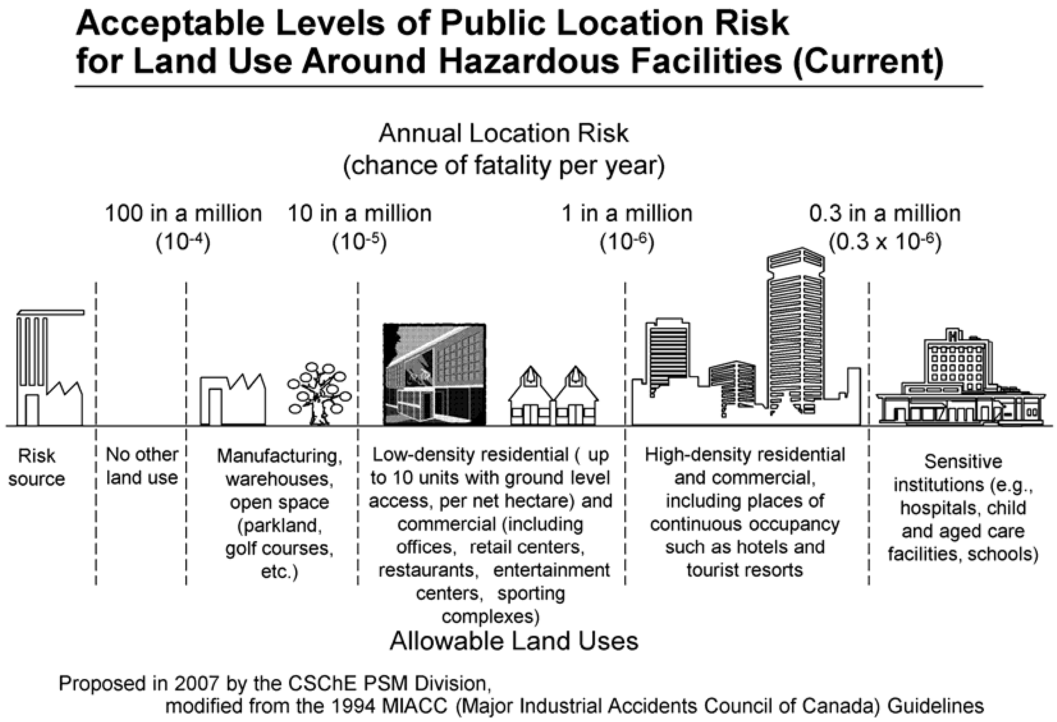
The development of this guideline took place under the auspices of the former Major Industrial Accidents Council of Canada (MIACC) before MIACC's dissolution in November 1999. The project was then transferred to the newly-formed Process Safety Management division of the Canadian Society for Chemical Engineering (CSChE). Details regarding this guideline and associated documents are now available through the CSChE.

During 1988-1992, the MIACC Working Group 1 (then Risk Assessment Expert Committee) developed a simplified risk analysis methodology (referred to as Version 1 below), which formed the basis of the 1994 MiniGuide for Hazardous Materials Risk Assessment for Municipalities and Industry (MIACC, 1994)1. The full supporting documentation for the Version 1 methodology explaining its scientific basis, and also providing basic information on the risk management process, was then published as Risk Assessment Guide for Municipalities and Industry (MIACC, 1997).
Parallel to this work, MIACC's Land Use Planning Working Group proposed a set of guidelines for acceptable levels of risk for given types of land use, on the basis of European standards and discussions with experts in both Canada and abroad (MIACC, 1995).

In 2004, the CSChE PSM Division published an updated set of risk assessment guidelines which superseded the MIACC risk assessment guides. This is reference 1 of this section.

In 2007, the CSChE PSM Division proposed a revised set of risk acceptability guidelines for land use, to take into account the experience gained across Canada with the 1995 MIACC guidelines. The MIACC publication is still valid in its generalities, except the figure that defines the numerical risk criteria for different types of land use around a hazardous facility. This figure is given below.

Figure 3: Acceptable levels of public risk for land use around hazardous facilities (current).



The guidelines for-acceptable levels of risk indicated in the figure above are as follows:

From risk source to 1 in 10,000 (10^{-3} risk contour): no other land uses except the source facility, pipeline or corridor

1 in 10,000 to 1 in 100,000 (10^{-4} to 10^{-5}) risk contours: uses involving continuous access and the presence of limited numbers of people but easy evacuation, e.g. open space (parks, golf courses, conservation areas, trails, excluding recreation facilities such as arenas), warehouses, manufacturing plants

1 in 100,000 to 1 in 1,000,000 (10^{-5} to 10^{-6}) risk contours:: uses involving continuous access but easy evacuation, e.g., commercial uses, low-density residential areas, offices

1 in 1,000,000 to 0.3 in 1,000,000 (10^{-6} to 0.3×10^{-6}) risk contours: all other land uses including institutional uses, high-density residential areas, etc., except for sensitive receptors, such as schools, hospitals, elderly and child care facilities.

Beyond the 0.3 in 1,000,000 (0.3×10^{-6}) risk contour: all land uses without restriction.

In the absence of clear guidance in the MIACC guidelines, TSSA has additionally issued an advisory that provides an interpretation on the various land use patterns referenced in the MIACC criteria using other best practices including the United Kingdom's Planning and Development around Hazardous Installation (PADHI) guidelines.

It is important to emphasize that these guidelines do not prohibit all activities or structures within the various risk contours, but rather restrict land use within each zone to control the risk exposure. As is the case for many other land use questions (e.g. flood plains), the contours are used to define special restrictions on land uses.

RISK MITIGATION AND CONTROL PLAN

A risk mitigation and control should be developed for the facilities which have public receptors within the hazard distance. As part of this plan, the applicant should identify the necessary actions that can be carried out to reduce the risk to within the risk acceptance criteria defined in the previous section.
The applicant should demonstrate that the identified treatment or control options will avoid, reduce, and/or mitigate the risk to acceptable limits. Typical risk mitigation and control options may include:

- reducing the frequency of the hazards identified by applying administrative and/or engineering that go beyond the requirements of the applicable codes and standards and proving their effectiveness; (e.g. logging and tagging procedures, QA/QC and inspection, well-documented plant logs, work permitting procedures, pressure relief device, equipment supports fireproofed, equipment grounding to prevent static electricity, environmental monitors to detect leaks, area fire detectors and alarms, additional corrosion allowance, reducing inventory); and

- mitigating the consequences by implementing mitigation controls that go above and beyond the requirements of applicable codes and standards and proving their effectiveness.(e.g. propane tank burying or mounding earth around it to create a physical barrier against fire and explosion, water systems, thermal isolation, dikes, fire walls, blast walls, increased spacing of equipment, etc.).

- avoiding the risk including considering the option of closing or relocating the facility;

EMERGENCY RESPONSE AND PREPAREDNESS PLAN

The applicant must prepare an Emergency Response and Preparedness Plan as part of the requirements for the propane risk management plan.

The purpose of an emergency and preparedness plan is to:

- contain and control incidents so as to minimize the consequences to the public receptors;
- implement the necessary measures to protect the public from the effects of major incidents; and
- communicate the necessary information to the public and to the services or authorities concerned in the area.

The Emergency Response and Preparedness Plan constitute an important document that will help the industry and municipalities to respond immediately in case of an accidental event or emergency such as fires and explosions. In an emergency situation, there is a period of confusion and disorder proper emergency planning and preparedness reduce the risk.

The applicant should prepare two types of emergency plans, internal for the measures to be taken inside the facility and external for measures to be taken outside the facility. In the elaboration of both plans the applicant shall make sure these are elaborated in consultation with personnel employed, inside the facility and the public is consulted on external emergency plans.

Standards/Guidelines for Reference

1. Seveso II, Article 11 (Recommended by the Propane Expert Panel);
2. APELL; and
3. NFPA.

Data and Information to be Included in the Emergency Plans

1. Internal Emergency Plans

a. names or positions of persons authorized to set emergency procedures in motion and the person in charge of and coordinating the on-site mitigatory action.

b. name or position of the person with responsibility for liaising with the authority responsible for the external emergency plan.

c. for foreseeable conditions or events which could be significant in bringing about a major accident, a description of the action which should be taken to control the conditions or events and to limit their consequences, including a description of the safety equipment and the resources available.

d. arrangements for limiting the risks to persons on site including how warnings are to be given and the actions persons are expected to take on receipt of a warning.

e. arrangements for providing early warning of the incident to the authority responsible for setting the external emergency plan in motion, the type of information which should be contained in an initial warning and the arrangements for the provision of more detailed information as it becomes available;

f. arrangements for training staff in the duties they will be expected to perform, and where necessary coordinating this with off-site emergency services; and

g. arrangements for providing assistance with off-site mitigatory action.

2. External Emergency Plans

a. names or positions of persons authorized to set emergency procedures in motion and of persons authorized to take charge of and coordinate off-site action;

b. arrangements for receiving early warning of incidents, and alert and call-out procedures;

c. arrangements for coordinating resources necessary to implement the external emergency plan;

d. arrangements for providing assistance with on-site mitigatory action;

e. arrangements for off-site mitigatory action;

f. arrangements for providing the public with specific information relating to the accident and the behavior which it should adopt; and

g. arrangements for the provision of information to the emergency services of other Member States in the event of a major accident with possible transboundary consequences

APELL PROCESS STEPS

Step 1 Identify the emergency response participants and establish their roles, resources and concerns.

Step 2 Evaluate the risks and hazards that may result in emergency situations in the community and define options for risk reduction.

Step 3 Have participants review their own emergency plan for adequacy relative to a coordinated response, including the adequacy of communication plans.

Step 4 Identify the required response tasks not covered by the existing plans.

Step 5 Match these tasks to the resources available from the identified participants.

Step 6 Make the changes necessary to improve existing plans, integrate them into an overall emergency response and communication plan and gain agreement.

Step 7 Commit the integrated plan to writing and obtain approvals from local governments.

Step 8 Communicate the integrated plan to participating groups and ensure that all emergency responders are trained.

Step 9 Establish procedures for periodic testing, review and updating of the plan.

Step 10 Communicate the integrated plan to the general community.