Technical Standards and Safety Authority

Operating Engineers Safety Program

Path 2 Risk & Safety Management Plan (RSMP)

Implementation Guide

Operating Engineers Safety Program Path 2 Risk & Safety Management Plan Implementation Guide

Table of Contents

1. INTRODUCTION

1.1 Background

In 2019, the Government of Ontario amended the *Technical Standards and Safety Act, 2000*, to provide the Minister of Government and Consumer Services (The Minister) authority to approve alternate rules for the Operating Engineers' regulation. On October 2, 2020, the Minister, through her authority under the Act, approved TSSA's proposed alternate rules for the Operating Engineers regulation.

These alternate rules exist in parallel to the current regulation. Part 1 of the alternate rules adopt a risk-based regulatory framework recommended by a panel of industry experts.

Under the alternate rules, a registered plant may consider one of two alternate regulatory paths:

- **Path 1 category-based approach**, where plant's staffing requirements are determined based on a system that considers various factors that contribute to the plant's safety risk

- **Path 2 performance-based approach**, where plants develop and implement their own site-specific Risk and Safety Management Plan (RSMP). In this approach, the operating engineer staffing would be addressed in a manner specific to an industrial facility and the corresponding hazard scenario. The RSMP would not only reflect the count and category of staffing, but also requirements such as specialized training and expertise in order to ensure the risk to both workers and the public is kept within the prescribed individual risk tolerances and is brought to as low as reasonably practicable.

The alternate rules provide businesses with flexibility and choice to either utilize the alternate rules or to continue adhering to requirements in the current regulation.

1.2 What is Path 2?

The regulatory framework for Path 2 Risk and Safety Management Plans (RSMPs) focuses on the adoption and use of the recently issued Canadian process safety management (PSM) standard, CSA Z767-17 or a successor standard (hereinafter referred as the Standard). The Standard has been written to be broadly applicable across industry sectors and organization sizes. Companies or organizations using these principles are found in the chemical, food, mining, nuclear, petroleum, pulp and paper, transportation, and utilities sectors. This Standard is applicable to large, integrated manufacturing sites, as well as to small businesses or retail sites. This Standard may also be applied to municipalities that can have hazardous scenarios, such as loss of containment in water treatment, arenas, or swimming pool facilities.

If a plant develops and implements an RSMP that satisfies the process safety management standard's (i.e. CSA Z767) requirements, it may qualify for Path 2 and certain sections of the current Operating Engineer regulation that are covered by the RSMP would no longer apply to the facility.

1.3 Purpose of the Implementation Guide

This guide is intended to assist facilities with developing and implementing an RSMP that is in satisfactory compliance with CSA Standard Z767 Process Safety Management.

The overall purpose of the RSMP is to cover all aspects of process safety management on an integrated "total quality management" basis, such that all the recognized components of effective safety management are recognized, developed and implemented.

1.4 How Much is Involved?

Preparing and implementing a RSMP is a significant undertaking. The amount of effort required to assemble an RSMP will vary depending upon the size and nature of the industrial facility.

The review and approval by TSSA will take additional time and will include an on-site visit.

1.5 What Does the Path 2 RSMP Project Look Like?

A typical Path 2 RSMP project is shown graphically in Figure 1-1.

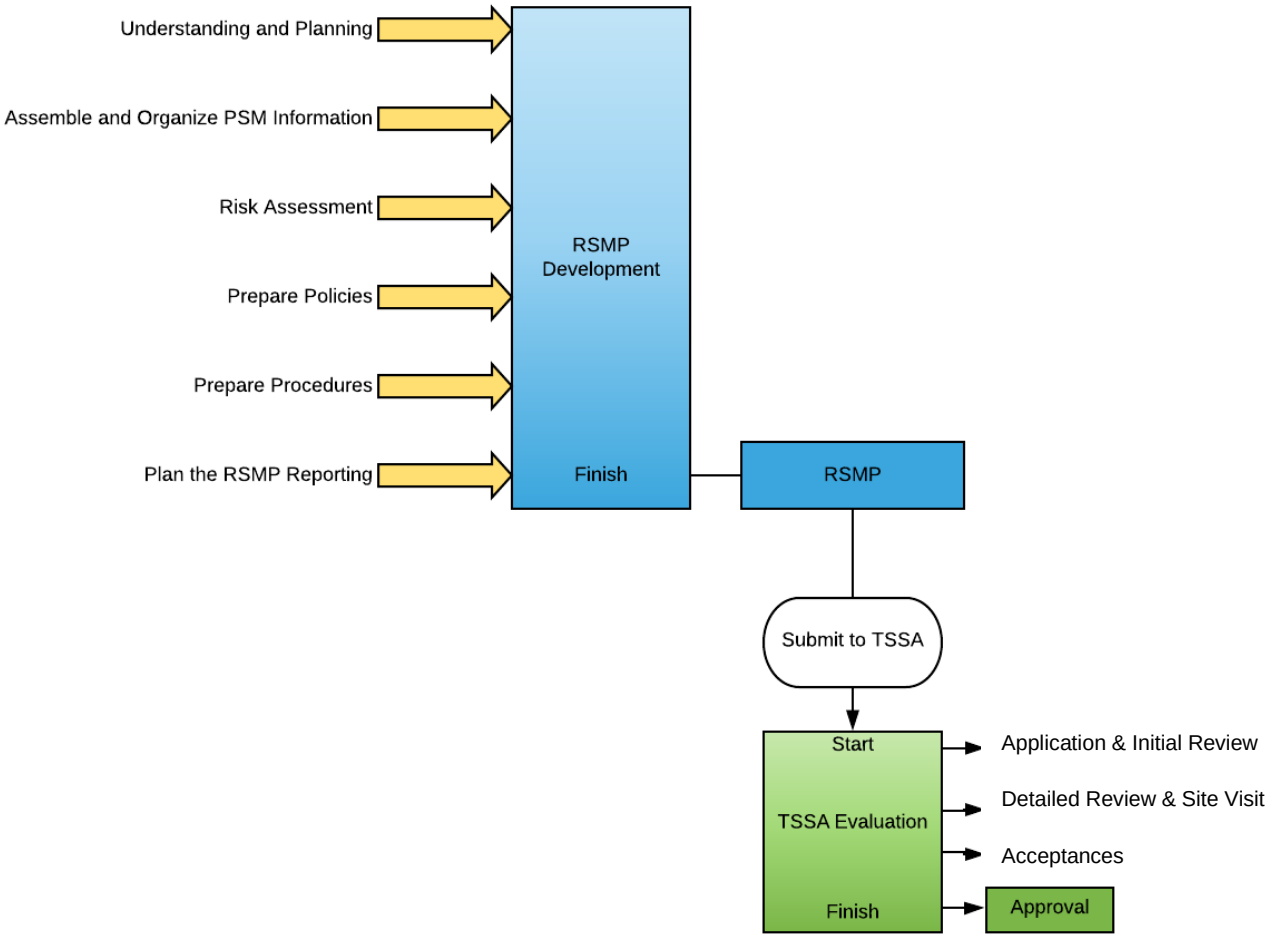


Figure 1-1: Simplified Path 2 RSMP Project

1.6 Referencing the Alternate Rules

Before drafting the RSMP, it is imperative for the plant user (and others involved in the creation of the document) to familiarize themselves with the alternate rules. The RSMP submission must meet the requirements in the alternate rules including the following:

1. is prepared in accordance with CSA standard Z767-17 (Process Safety Management) or a successor standard specified by the chief officer;

2. is in the form established by TSSA and in accordance with any applicable guidance materials;
3. describes the safety hazards associated with the plant
4. sets out the plant user's plan for managing those safety hazards;
5. describes the qualifications of operating engineers, operators and other plant personnel proposed to staff the plant;
6. shall be prepared and approved by a professional engineer lawfully entitled to practice in Ontario and shall bear the signature and seal, or the electronic equivalent, of the professional engineer; and
7. shall be approved by a member of senior management of the plant user who is responsible for plant safety.

1.7 Structure of the Guideline

This Guideline is structured as a chronological approach for the creation and implementation of a RSMP. Below are descriptions of subsequent sections of the guideline.

Section 2 - Understanding the Process Safety Management (PSM) Elements – familiarizes the reader with the Standard and its components, plus provides an overview of the necessary information, policies, procedures and reporting aspects of the Standard.

Section 3 – Assembling PSM Information – outlines the industrial facility information required to develop an RSMP.

Section 4 – Assessing Your Industrial Facility's Safety Risk – provides guidance on how to conduct the **risk assessment**.

Section 5 – Preparing Your RSMP – provides guidance on incorporating the various CSA Z767 elements into your written plan.

Section 6 – Implementing Your RSMP – provides guidance for putting the RSMP into action.

Section 7 – TSSA Oversight and Assistance – discusses the RSMP submission and acceptance processes, as well as how TSSA will work with an industrial facility to assist and support the Path 2 regulatory approach.

1.8 Definitions

The CSA Z767 Standard contains all the process safety terminology required.

Some of the more important terms you will encounter are defined below.

Alternate rules – the rules made by a director and approved by an order of the Minister made under section 36.1 of *Technical Standards and Safety Act, 2000.*

As low as reasonably practicable (ALARP) – the concept that risk is tolerable only if it can be demonstrated that all reasonable and practicable measures have been taken, commensurate with the level of assessed risk. Assuming risk is within the prescribed individual risk tolerances, this is usually accomplished by showing the benefits of further risk measures are less than the cost of the measures. If the risk is not within the prescribed individual risk tolerance, the risk must be brought within it, irrespective of benefit cost.

Conduct of operations – the execution of operational and management tasks, in a deliberate and structured manner, that attempts to institutionalize the pursuit of excellence in the performance of every task and minimize variations in performance.

Consequence – the outcome of an event or a chain of events.
Note: the outcome usually involves the release of hazardous material or energy, which can create health or safety impacts, economic losses, and environmental impacts. There can be more than one consequence from a single event.

Hazardous material – a substance (gas, liquid, solid, combustible dust or mist) capable of creating harm to people, property, or the environment.
Note: this includes materials which are flammable, toxic, corrosive or explosive.

Individual risk – the annual likelihood of death or serious injury to which an individual is exposed from a hazard.

Inherent safety – the concept that incorporates safety as part of the fundamental design of a process rather than through employing additional safeguards.
Note: the four main principles associated with inherent safety are:

a) minimization – can the amount of hazardous material or energy present within a process or facility be reduced?
b) substitution – can material be replaced with a different less hazardous material?
c) moderation – can a hazardous material be used in a safer manner? For example, at a lower pressure?
d) simplification – can the systems be made less complicated to operate to reduce the likelihood of error?

Layer of Protection Analysis (LOPA) – a semi-quantitative assessment of process risk at various independent protection layers with a view to identifying what, if any, additional layers of protection are required for compliance or ALARP.

Management of change - a management system to identify, review and approve all modifications to equipment, procedures, programs, raw materials, and processing conditions, as well as organizational and staffing changes other than replacement in kind. The management of change system is applied prior to implementation of the change to help ensure that changes are properly analyzed for potential adverse impacts and unintended consequences.

Management system- a system intended to achieve specific objectives that includes the following components:

a) clearly stated objectives;
b) clearly defined responsibilities for achieving the objectives;
c) tools, resources, procedures, programs, and schedules necessary to achieve the objectives;
d) a means of measuring performance; and
e) a feedback and control mechanism to correct deviations.

Plant user - a person or persons in control of a plant as owner, lessee or otherwise, but does not include the operating engineers or operators who operate, control or maintain the plant; plant user has the responsibility for a hazardous material or hazardous energy in a facility.

Process hazard – a physical or process situation that can cause human injury, damage to property, or damage to the environment through the release of a hazardous material or hazardous energy.

Process safety – a discipline that focuses on the prevention of releases of hazardous material or energy, with an emphasis on high consequence events.

Process safety culture – the attitudes, values, norms, beliefs, and behaviours that a particular group of people share with respect to risk and safety.
Note: the essence of a positive culture is to bring continuous, positive improvement to process safety through a disciplined and well understood PSM program.

Risk – a measure of the human injury, environmental damage, or economic loss, in terms of the incident's likelihood and its magnitude of injury, damage, or loss.

Safeguard – a device, system or action that would likely interrupt the chain of events or minimize consequences following an initiating event.

SIF – **Safety Instrumented Function** – a set of equipment or instrumentation designed to reduce risk (e.g. sensors, controls, actuators, monitors, shutdowns, interlocks, etc.)

SRS – **Safety Requirements Specification** – contains the function and integrity requirements for each Safety Instrumented Function.

Worst credible scenario – a reasonably plausible event scenario which has the largest public safety consequence.

1.9 How to Use This Guide

To complete your RSMP, you will need to:

1) **Familiarize yourself with the CSA Z767 Standard**

   Section 2 will provide this orientation, although you should read it and other sections with a copy of the Standard in hand. Appendix A is a brief gap questionnaire for those wishing to self-assess how close they currently come to meeting the Standard.

2) **Assemble and organize the relevant information**

   Section 3 provides guidance on what information is involved and how to organize and store it.

3) **Conduct a risk assessment**

   Section 4 (supplemented by Appendix B) will provide an overview of the scope, techniques and output of the required risk assessment.

4) **Prepare the necessary policies, procedures and reporting protocols**

   Section 5 summarizes the required policies, procedures and periodic reports; Appendix C provides further detail and some templates to use.

5) **Assemble the RSMP into a written document**

   Section 5 provides guidance on documenting the RSMP.

6) **Develop the RSMP**

Section 6 outlines some guidance, governance, training and cultural aspects for rolling out the RSMP to the facility and corporate staff.

7) **Submit the RSMP to TSSA**

Section 7 demonstrates how submit the RSMP and explains TSSA's approval and support processes.

2. UNDERSTANDING THE PSM ELEMENTS

2.1 CSA Z767: Process Safety Management

In August 2017, the Canadian Standards Association published the first edition of the Standard.

In the Standard, *process safety management* is defined as follows:

> *Process safety management (PSM) is the application of management principles and systems for the identification, understanding, avoidance, and control of process hazards to prevent, mitigate, prepare for, respond to, and recover from process-related incidents. These principles and techniques may be applied across industry sectors.*

The expressed purpose and scope of the Standard are as follows:

> *The purpose of this Standard is to identify the performance requirements for organizations that plan to implement or have implemented a PSM system.*
>
> *This Standard identifies the various policies, practices, and procedures that may be used to implement a PSM system.*

There are four foundational pillars in the Standard, with four elements under each pillar as shown in Table 2-1. Review Table 2-1 and become familiar with the nature of each of the sixteen elements.

Table 2-1: The Standards PSM Elements

Process Safety Management Elements			
Process Safety Leadership	**Understanding Hazards and Risks**	**Risk Management**	**Review and Improvement**
1. Accountability	5. Process knowledge and documentation	9. Training and competency	13. Investigation
2. Regulations, codes and standards	6. Project review and design procedures	10. Management of Change	14. Audit process
3. Process safety culture	7. Process risk assessment and risk reduction	11. Process and equipment integrity	15. Enhancement of process safety knowledge
4. Conduct of operations – senior management responsibility	8. Human factors	12. Emergency management planning	16. Key performance indicators

2.2 Practical Overview of the Elements

As a practical matter, each element requires a facility to produce either a policy or a procedure, or both. Table 2-2 below summarizes the five types of requirements – information (data assembly), analysis, policy, procedure and data reporting framework– that will be found in an RSMP.

For example, two elements out of sixteen require assembling and organizing relevant information. They are: *2. Regulations, codes and standards and 5. Process knowledge.*

Table 2-2: CSA Z767 Requirements by Element

CSA Z767 Standard Requirements

		Type of Requirements				
Pillar	**Element**	**Data Assembly**	**Analysis Required**	**Policy**	**Procedure**	**Regular Reporting**
Process Safety Leadership	accountability			✓		
	regulations, codes and standards	✓		✓		
	process safety culture			✓		
	conduct of operations - senior management responsibility			✓	✓	✓
Understanding Hazards and Risks	process knowledge and documentation	✓		✓	✓	
	project review and design procedures		✓	✓	✓	contingent
	process risk assessment and reduction		✓	✓	✓	✓
	human factors		✓		✓	
Risk Management	training and competency			✓	✓	✓
	management of change		✓	✓	✓	contingent
	process and equipment integrity			✓	✓	✓
	emergency management planning				✓	✓
Review and Improvement	investigation		✓		✓	contingent
	audit process		✓		✓	✓
	enchancements of process safety knowledge			✓		
	key performance indicators					✓

Some considerations for RSMP development:

- Some of the various policies, procedures and ongoing report templates may already exist or can be introduced into existing documents.
- The remainder of the new policies could easily be combined in a single policy statement.
- Two of four required risk analyses are for future events that may not occur. In preparing the RSMP two analyses are required: *risk assessment* and *human factors*.

In Appendix A, there is a simple, easy-to-understand questionnaire to assess the gap between an industrial facility's current risk and safety practices, and those prescribed by the Standard.

2.3 Chronological Approach

The first task should be assembling the information as laid out in *Element 2 – Regulations, Codes and Standards and Element* 5 – *Process knowledge and documentation*. These two elements are simply designed to collect all necessary information to support the other elements. Guidance on these tasks is provided in the next section.

Element 7 – *Process risk assessment and risk reduction* – should be performed early in RSMP development. The risk assessment is an important task for both the facility and for TSSA. A well-considered modelling of the worst-case scenario and its effects on public safety is critical to inform the type, and the level of risk management planning is appropriate.

For instance, an industrial facility with only a low temperature, low pressure boiler would often have a low safety risk and its RSMP plan would be less detailed than, for instance, a refrigeration facility with significant amounts of ammonia, or an industrial facility with compressed flammable material.

2.4 TSSA Expectations

TSSA expects that all Path 2 RSMP will address all the PSM elements outlined in the Standard.

TSSA also expects that the amount of analysis and planning in the RSMP will be commensurate with the industrial facility's public safety risk as determined by the risk assessment.

3. ASSEMBLING AND ORGANIZING PSM INFORMATION

3.1 General

CSA Z767 Elements 2 and 5 specify the documentation required to be maintained by the facility under the Standard.

This base load is listed in the Standard and shown below in Table 3-1 for reference.

Table 3-1: Examples of Required Process Safety Information (as per CSA Z767-17, p.34-35)

Drawings	• Piping and instrumentation diagrams (P&IDs) • Area electrical classification • Safety plot plan with fire protection equipment • Flame and flammable gas detection layout • Toxic gas detection • Cause and effects diagrams and logic narratives • Ventilation systems design
Data Sheets	• Instrument data sheets • Mechanical safety systems: PSV, hardwired trips and guards • WHMIS information
Lists	• Line designation table • Equipment lists and valve labels • Valve locking lists • Designation of process safety-critical equipment • Process interlocks (non-SIS systems)
Standards and Codes	• Design codes and standards employed • SIS and SIF (safety requirement specifications) • Overpressure protection by system design information
Reports	• Materials of construction and suitability in handling process materials • Corrosion hazard review reports • Materials selection diagram • Incidents and near misses
Other	• Emergency shutdown device design basis, valve list and test records • SIF (part of SIS) test records • Instrument grounding arrangement diagrams • Corrosion allowance • Data regarding ventilation system design • Process control systems • Critical alarms, systems, etc.

3.2 TSSA Expectations

TSSA expects that all supporting documents will be included in the RSMP application package. As well, TSSA will be looking for the applicant to demonstrate how the specified information will be organized, accessibly stored, and readily available to all operators, operating engineers, consultants and stakeholders, including TSSA staffs. These documents are to be updated throughout the plant's life cycle.

4. ASSESSING YOUR INDUSTRIAL FACILITY'S PROCESS SAFETY RISK

For most industrial facilities, the risk assessment requirement is the most plant-specific and technical part of compliance with the Standard.

4.1 The Risk Assessment

The PSM element of risk assessment is both important and technical. As laid out in the Standard, it consists of the following chronological tasks:

1. Ensure competence of those doing the risk assessment
2. Establish public receptors (those adjacent who may be exposed to adverse events)
3. Identify hazard scenarios and select one (or more) worst credible scenarios, if there are hazard scenarios which post negligible risks to the risk receptor, the duty owners need to provide justification for why these hazard scenarios should be excluded. These would be included as part of the application
4. Model the consequences of the identified scenario(s) to ascertain whether it impacts staff on site or public receptors (death, injury or damage)

If it does,

5. Model the likelihood and consequences of all credible scenarios that impact staff on site or public receptors
6. Mitigate any risk that is above the prescribed individual risk tolerance to within that tolerance
7. Mitigate all risks to *As Low as Reasonably Practicable* (ALARP)

Each task is outlined below.

4.2 Competence

The Standard (CSA Z767) requires "competence" in risk assessment. To this end, the risk assessment should be performed by a team with expertise in engineering, operation and maintenance of the equipment and process being evaluated. An industrial facility may not have access to qualified staff who have competence in the use of generally accepted process risk assessment methods. If so, the industrial facility may choose to employ outside competence, for instance a professional engineering firm with skill in risk assessment or another qualified consultancy.

Appendix B addresses the PSM risk assessment methods and techniques in more detail.

4.3 Public Receptors

Public receptor generally means any place where people live, work, or gather, with the exception of roads. Buildings, such as houses, shops, office buildings, industrial facilities, the areas surrounding buildings where people are likely to be present, such as yards and parking lots, and recreational areas, such as parks, sports arenas, rivers, lakes, beaches, are considered public receptors[1]. The risk assessment

[1] As per the general guidance provided by the United States Environmental Protection Agency (EPA) for risk management plans.

will need to establish (geographically and numerically) the public receptors in the vicinity of the industrial facility.

4.4 Hazard Scenarios

The hazard scenarios selected will depend upon the industrial facility equipment, hazardous materials (if any) and conditions.

As an example, for facilities with boilers, one hazard scenario is a water/steam side explosion; another might be a fuel side explosion. For facilities with ammonia, a toxic ammonia release would be a credible scenario. For facilities with flammable material held under pressure, a release and ignition of a release are to be selected for modelling of thermal radiation, overpressure effects, or the generation of missiles.

4.5 Consequence Modelling

Consequences might involve toxicity, explosion, or fire scenarios.

When predicting the extent of toxic, thermal, overpressure or shrapnel effects, competent risk engineers use generally accepted predictive models that compute hazardous material or energy release. These models are based on volume, temperature, pressure and containment characteristics. They use generally accepted assumptions about release flow and timing, ignition, combustion efficiency, and the toxic, radiation or overpressure impacts at different distances.

More detail and references on these generally accepted risk assessments and assumptions are provided in Appendix B.

Having identified credible hazard consequence events, a worst-case event (or events) should be selected based upon its potential impact on on-site staff and public receptors. Should the considered event(s) show exposure to toxic materials, overpressure, thermal radiation, etc., above thresholds, the consequences of all hazard events should be determined, and their frequency of occurrence predicted.

4.6 Frequency Estimation

As noted above, should a hazard scenario result in above-threshold impacts, the frequency of the event should be predicted. The risk to an individual exposed is then the product of the frequency of the hazard occurrence and the probability of death or injury that results. More detail and references on how this might be done are provided in Appendix B.

4.7 Risk Reduction

Once the risk assessment is complete, you will need to consider whether any public safety risk exists above the prescribed individual risk tolerances.

If so, you need to further consider what (if any) measures could cost effectively reduce the risk to the exposed public receptors.

This is a relatively technical question involving an analysis of what additional physical or operational risk reduction measures are available to reduce either the risk likelihood or severity, the cost of these measures and their risk reduction benefit.

Further guidance is provided in Appendix B.

4.8 TSSA Expectations

TSSA expects a considered, credible, quantitative and competent risk assessment.

The basis of the risk acceptability criteria is intended to account for aggregated risks towards a risk receptor (i.e. general public, on-site workers). The estimated risks for a facility need to be aggregated to have a meaningful comparison. If there are scenarios which pose negligible risks to the risk receptor, the application needs to provide justification on why these risk scenarios should be excluded. These have to be included as part of the application.

The risk assessment should assess the risk to workers and public receptors and then determine and act upon two items:

1. whether any risk is outside the prescribed individual risk tolerance; if so, add additional risk mitigation (e.g. a Layer(s) of Protection) until the risk is reduced.

2. whether any public safety risk could be further mitigated to *As Low as Reasonably Practicable* (ALARP); if so, add the beneficial Layers of Protection.

ALARP is one of the fundamental objectives of process safety management and is discussed further in Appendix B.

5. PREPARING YOUR RSMP

At this point, you should be ready to draft the written plan. The plan will need to consist of:

1. policies
2. procedures
3. ongoing report forms
4. the risk assessment results and risk reduction analysis

There are a number of ways of incorporating these into the RSMP. A detailed template is shown in Table 5-1 below.

Table 5-1: Sample RSMP Table of Contents

RISK & SAFETY MANAGEMENT PLAN

Table of Contents

Appendices

A. Process Safety Information

This appendix should contain all the relevant process safety information. See TSSA RSMP Implementation Guideline Section 3, Table 3-1.

B. Risk Assessment and Risk Reduction Analysis

This appendix should attach the Risk Assessment and Reduction Report (required by both CSA Z767 Section 6.3 and TSSA RSMP Implementation Guideline Section 4).

C. Detailed Procedures

This appendix could be in a separate volume and should contain all the relevant procedures (see Section 4).

D. Reporting Forms

This appendix should contain all the relevant reporting forms (see Section 6). The Management will ensure compliance with all applicable regulations, codes and standards.

5.1 Policies

As noted earlier in this Guideline many of the Standard's PSM elements require a policy as shown in Table 5-2 below.

Table 5-2: CSA Z767 Policy Requirements, By Element

Pillar	Element	Policy Required
Process Safety Leadership	Accountability	Senior management will be responsible and accountable for the RSMP, including goals, performance, approvals and controls
	Regulations, codes and standards	Senior management will ensure compliance with all applicable regulations, codes and standards
	Process safety culture	A process safety culture will be imbedded at all levels, including a policy statement establishing process safety as a measure of successful operation
	Conduct of operations – senior management responsibility	Similar to above policy requirement
Understanding Hazards and Risks	Process knowledge and documentation	All necessary documentation on process and process safety is complete, accurate and accessible
	Project review and design procedures	Approval of projects[1] shall require a process safety risk assessment of the project

	Process risk assessment and reduction	A process risk assessment will be conducted at least every five years and all process risks will be both tolerable and *as low as reasonably practicable*
	Human factors	In mitigating risk, human factors will be considered as a layer of protection and as a risk exposure
Risk Management	Training and competency	All personnel (including contractors) will have the necessary qualifications, competencies, experience and training for their jobs, including a training plan
	Management of change	A management of change system will be in place including a risk assessment and an approval procedure
	Process and equipment integrity	An overall policy on process and equipment integrity, stipulating that procedures and schedules are in place for inspection testing, maintenance and safe work permits
	Emergency management planning	A policy on emergency response management and an emergency response plan (ERP) that is tailored to the appropriate level of risk
Review and Improvement	Investigation	A policy requiring a system to record and report all incidents, including an investigation and lessons learned protocol on significant incidents
	Audit process	A policy requiring a system to periodically audit the PSM program, including a procedure, schedule and follow up on corrective action
	Enhancements of process safety knowledge	A policy on continual improvement to the PSM program
	Key performance indicators	A policy on performance indicators for the PSM program

The term "project" is undefined in the CSA Z767 but can be understood to mean new project (green field), expansions and retrofits.

5.1.1 Helpful Hints on Policies

Some or all of the above policy requirements can be combined into a single PSM policy statement, or some could be inserted into existing operating, maintenance, personnel or organizational policies.

Appendix C contains further discussion, templates and reference links on the various PSM policy elements.

5.1.2 TSSA's Expectations on PSM Policy

TSSA does not require a predetermined format or structure for the PSM policies. That said, once the plant user selects a policy format or template, TSSA expects that policies will follow a consistent format. In addition, TSSA expects that all policy elements would be incorporated.

TSSA expects a clear commitment from the plant's senior management to the PSM policies, which include dated signatures or other means that demonstrate senior management's endorsement.

5.2 Procedures

Table 5.3 below summarizes the CSA Z767 elements that require a procedure. Where no procedure is shown, no formal procedure is mandated. However, developing robust procedures for every element of the RSMP is generally recommended.

Table 5-3: CSA Z767 Procedure Requirements, By Element

Pillar	Element	Procedure Required
Process Safety Leadership	Accountability	Approval procedures
	Regulations, codes and standards	
	Process safety culture	
	Conduct of operations – senior management responsibility	Operating procedures
Understanding Hazards and Risks	Process knowledge and documentation	
	Project review and design procedures	A risk assessments and approval procedure for new projects
	Process risk assessment and reduction	A risk assessment and risk reduction procedure similar to that set forth in CSA Z767
	Human factors	Human factors in mitigation and exposure are to be considered in the above procedure
	Training and competency	A training plan and schedule

Risk Management	Management of change	A risk assessment and approval procedures for managing significant change to process or operations
	Process and equipment integrity	Testing, inspection and maintenance procedures, including record-keeping
	Emergency management planning	An emergency response plan and procedures, including testing the of the plan
Review and Improvement	Investigation	An incident reporting procedure and record plan, and an investigation procedure for serious incidents
	Audit process	A PSM program audit procedure
	Enhancements of process safety knowledge	A plan for continuous improvement
	Key performance indicators	A procedure for recording and reporting key performance indicators

5.2.1 Helpful Hints on Procedures

Some of the required procedures may already exist for industrial facilities. Examples could include the operating, testing, inspection and maintenance procedures or the training program.

The length and detail of a procedure for any given industrial facility will depend upon the safety risk as revealed in the risk assessment.

5.2.2 TSSA's Expectations on Procedures

TSSA expects that the procedural elements of the Standard are clearly captured in the RSMP, communicated clearly to all plant staff affected by the respective procedures, and followed in practice. TSSA will review the implementation of the procedures during audits.

6. IMPLEMENTING YOUR RSMP

6.1 Implementation Logistics

Once all of your RSMP documentation had been stamped by a professional engineer, reviewed by TSSA, and authorized by TSSA with any applicable terms and conditions, the next step is to implement the policies, procedures and reporting in accordance with the plan.

CSA Z767 is relatively silent on implementation. Accordingly, the implementation process has some flexibility with the structure, style and schedule. TSSA expects a formal implementation plan at the time of the RSMP submission. TSSA's RSMP reviewers (including inspectors) will review the implementation plan and ask questions on the implementation of the RSMP during the site visit phase (i.e. prior to TSSA's acceptance).

It is imperative that your RSMP include your near-future plans (i.e. within 3 months of your acceptance) and your longer-term plans that involve periodic reviews and improvements to the RSMP.

6.2 Implementation Indicators

Key indicators of successful RSMP implementation would include:

- clear senior leadership knowledge of and commitment to the RSMP
- clear operating staff knowledge of and commitment to the RSMP and its procedures
- training log for staff
- incident reporting log with follow up and, as required, investigation
- an accessible information system
- testing, inspection and maintenance records
- a log of key performance indicators
- audit reports
- plan for implementing any recommendations or risk mitigation from the risk assessment
- updating the plan based on material changes to the plant, and notifying TSSA

And, as appropriate,

- risk assessment and approval logs on new projects and substantive process changes (Management of Change)

6.3 TSSA's Expectations for RSMP Implementation

TSSA expects that the RSMP would be understood and embedded at all levels of the organization. After Path 2 registrations are issued, TSSA will periodically inspect and audit the facility to make sure that the RSMP was implemented as outlined in the plan.

If TSSA finds that the plant user was not successful at implementing the plan during this first audit, TSSA will take follow-up actions, which could include the revocation of the plant's Path 2 approval status.

TSSA also expects that this knowledge and compliance would be evidenced by the RSMP reporting elements. All aspects of the RSMP may be verified and/or audited by TSSA at any point in time.

7. SUBMISSION AND ASSESSMENT OF THE RSMP

7.1 Submission of the RSMP

When the RSMP is completed and stamped by a professional engineer (P. Eng) and signed off by a member of the senior management in charge of plant safety, it can be submitted to TSSA for approval of the industrial facility to operate under the Path 2 rules.

The application package for a new plant registration under Path 2 needs to include the following elements:

- Application for a Registration of a Plant (ARP) form
- Full plant equipment list (PEL) form containing all the technical specifications of the plant equipment
- Completed RSMP containing:
    - a stamp from a professional engineer
    - a signature from a senior management member who will be responsible for the plant's safety
- Applicable pre-payment fee to process the application

It is imperative that the information contained in the application package is accurate and as comprehensive as possible to avoid delays to the application processing.

7.2 TSSA's Response, Evaluation and Acceptance

TSSA's framework for review and approval will follow the following process:

Table 7-1: TSSA Approval Process

	Approval Process Steps	Stage
1.	Receipt of the application package by TSSA	Initial Review
2.	Acknowledgement and initial response to applicant	
3.	Initial Review by TSSA intake agent for application completion	
4.	TSSA's BPV/OE Engineering Review TSSA risk department review	Technical Reviews
5.	Site inspections by TSSA OE inspector	Inspector's Review
6.	TSSA OE chief's review	Chief's Review + Acceptance
7.	Acceptance letter sent to applicant (with possible conditions)	
8.	Acceptance or rejection by the applicant	Applicant's Acceptance
9.	New plant registration issued under Path 2	Path 2 Authorized

Acceptance and approval of the RSMP depends upon the due diligence, completion, and the adequacy of risk mitigation strategies outlined in the plan.

TSSA's detailed technical reviews by engineering staff and risk advisors will examine whether the RSMP being submitted has considered and followed all of the requirements in line with the Standard (as summarized in the template RSMP provided in Table 5-1). During this time, TSSA's reviewers may contact the professional engineer or the responsible senior management member (who have both signed off on the RSMP) for additional details, supporting materials or clarifications on the RSMP contents.

TSSA will conduct an in-person inspection (based on the outcomes of the engineering review) to verify details in the application package, and to assess whether the plant is ready to implement various policies and procedures listed in the RSMP. During this time TSSA will look for a concrete plan of action from the plant user (including longer-term plans to update the RSMP over time). This includes identifying how and when each element of the RSMP will be implemented on site.

Once the Chief Officer is satisfied that the policies, procedures and risk mitigation measures will be implemented, TSSA will "accept" the plant user's proposal to be governed by the Path 2 rules. The plant user will receive an acceptance letter with any applicable terms and conditions. A decision form will be enclosed with the acceptance letter that will require the user to review any changes, terms and conditions to the RSMP. The user will be asked to accept TSSA's final decision with a signature from the senior management member who is responsible for plant safety.

Alternatively, the plant user has the option to decline TSSA's acceptance and continue to follow the requirements of the regulation.

Simplified diagram of review process:

7.3 TSSA Fees

TSSA fees can be found on our website under the "Applications, Forms & Fees" section

7.4 Keep the RSMP updated

One of the key components of alternate rules is the constant self-improvement through measuring and tracking the plant's safety performance over time. In fact, one of the 16 elements of the CSA-Z767 requires plant users to periodically audit the PSM program and clearly outline the audit procedure and schedule as a part of the RSMP. The plant is also expected to address the corrective actions identified in the audit in a timely manner.

In addition, such changes resulting from corrective actions will also require TSSA to review your RSMP to make sure policies, procedures and processes in your RSMP are adequate in managing the safety risks at your plant.

For example, if a plant user makes major changes to the RSMP as a result of a new secondary school being built in the plant's vicinity (identified during the plant's periodic revalidation of risk assessment of

the plant), the changes will need to be re-evaluated by TSSA staff through "re-registration" process (i.e. an application package with a revised RSMP needs to be re-submitted to TSSA). To expedite and assist TSSA in this re-registration and review process, TSSA encourages users to submit a change log to pinpoint which policies, procedures and processes in the RSMP have been updated.

7.5 Oversight of Alternate Rules Plants

TSSA maintains a policy of risk-based scheduling of inspections for all plants in Ontario (regardless of their alternate rules status). Plants that may pose a higher risk are inspected more frequently. Inspections for Path 2 plants may closely resemble management "audits" more so than a traditional TSSA inspection.

7.6 Have a Question about the Process?

If you require more information from TSSA regarding the application process, please visit the OE Alternate Rules Frequently Asked Questions (FAQs) section of TSSA.org.

If your question is not answered in the FAQs, please send an email to: alternate_rules@tssa.org.

APPENDIX A: CSA Z-767 Gap Analysis Questionnaire

CSA Z767 STANDARD
GAP ANALYSIS QUESTIONS

These questions help assess gaps between what your industrial facility does presently and what the CSA's Process Safety Management (PSM) standard requires. The questions are provided for information purposes only. They are neither required nor reviewed by TSSA.

You answer 'yes' or 'no.' Count your 'yes' answers and divide the sum by 70. The percentage provides a high-level indication of the alignment between your facility's process safety management and CSA's standard Z767 standard.

Name: _____
Position: _____
Industrial facility _____
Location: _____

CSA Z767 STANDARD
GAP ANALYSIS QUESTIONS

1. Process Safety Leadership

1.1 Accountability

Yes/No

_____ Is your senior management quite involved in process safety? Do they attend safety meetings?
_____ Does senior management set safety goals?
_____ Does senior management look at safety issues when giving approvals, making decisions or allowing exceptions?
_____ Is this senior management commitment to safety documented?

1.2 Regulations, Codes and Standards

_____ Do you maintain a list of all applicable regulations, standards and codes applying to the industrial facility?
_____ Is there a system for ensuring compliance with these regulations, standards and codes?
_____ Does the system flag new regulations?

1.3 Process Safety Culture

_____ Is there a policy on safety? Does it cover process safety?
_____ Is there an open and healthy safety culture?
_____ Is everyone involved: senior management, supervisors and workers?
_____ Are there any safety meetings? Is equipment and process safety discussed?
_____ Is there safety training?

1.4 Conduct of Operations, Senior Management Responsibility

_____ Does the senior management meet regularly with facility managers and operators on safety?
_____ Is there a code of conduct?
_____ Is there clear support and no repercussions for operators who stop operations that appear to be unsafe?
_____ Are all of the above well documented?

2. Understanding Hazards and Risks

2.1 Process Knowledge and Documentation

Is there a file document and control system for:

_____ a. information on all hazardous materials (Materials Safety Data Sheets, etc.)?

_____ b. all design, drawings, process flow, P&IDs, control and shutdown key documents?

_____ Are there accessible procedures for start-up, normal operations, shutdown and maintenance? Are operators trained in these procedures?

_____ Are these documents regularly reviewed and updated?

2.2 Project Review and Design Procedures

_____ Is there an approval process and design procedure for new projects, upgrades or expansions?

_____ Does the process entail an assessment of the risks, hazards and risk controls?

_____ Is there a plot plan review that looks at layout, exposures and the adjacent public?

_____ Is the above documented?

2.3 Process Risk Assessment and Risk Reduction

_____ Are the plant users (and their agents) knowledgeable in risk assessment?

_____ Have the worst case process safety hazard events been identified?

_____ Have their causes, likelihood and consequences been assessed in a risk assessment?

_____ Do you have criteria for determining whether a risk event is tolerable or not?

_____ Have any risk reduction measures ever been implemented and monitored?

_____ Do you think your process safety risks has been reduced to as low as practicable?

2.4 Human Factors

_____ Has your industrial facility done any analysis of engineering and automated process controls versus administrative/manual process controls?

_____ Does your management believe that industrial facility staffing is optimal?

3. Risk Management

3.1 Training and Competency

_____ Do all personnel possess the necessary qualification and competencies for their job?
_____ Is there a formal training and examination program?
_____ Is there a training log?

3.2 MOC

_____ Is there a Management of Change policy and procedure that is used when necessary?
_____ Is there a clear definition of what constitutes a Change?
_____ Does the MOC procedure incorporate risk analysis of the change?

3.2 Process and Equipment Integrity

Are there written procedures and schedules for:
_____ a. maintenance?
_____ b. inspections?
_____ c. testing?

Do the procedures address:
_____ a. pressure vessels and piping?
_____ b. instrumentation and control systems?
_____ c. relief systems?
_____ d. emergency shutdown systems?
_____ e. electrical and HVAC?
_____ f. solids handling?
_____ Are there quality control procedures for incoming equipment and material?
_____ Is there a safe work procedure?
_____ Is there a safety meeting before each start-up?

3.4 Emergency Management Planning

_____ Is there an emergency response plan and procedures?

Does it include:
_____ a. worst case scenario(s)?
_____ b. a map of the emergency planning zone?
_____ c. roles and responsibilities in incident response?
_____ d. emergency contacts, including first responders, neighbours and regulators?
_____ e. emergency response procedures?
_____ Is the emergency response plan tested through simulation?
_____ Is there a post-incident lessons learned session afterwards?

4. Review and Improvement

4.1 Investigation

_____ Is there an incident form and reporting system?
_____ Is there an incident investigation procedure for serious incidents?
_____ Are incident reports regularly reviewed by senior management?

4.2 Audit Process

_____ Do you have process safety audits or inspections?
_____ Are these conducted by objective and competent personnel?
_____ Are these documented and reviewed by senior management?

4.3 Enhancement of Process Safety Knowledge

_____ Are there policies and procedures for continuous improvement in process safety?
_____ Do you belong to an industry association?
_____ Do you follow industry discussion about safety?

4.4 Key Performance Indicators

_____ Are there key performance indicators used for process safety? (e.g. incidents, equipment failures, number of audits or inspections recoveries; number of mechanical or instrumentation failures, etc.)
_____ Are these KPIs regularly recorded?
_____ Are they communicated throughout the organization?

Score (yes / 70)

APPENDIX B: Detailed Guidance & References on Process Safety Risk Assessment

This Appendix will set forth further guidance, references and templates for the process risk assessment as stipulated in Section 6.3 of the CSA Z767 Standard.

For ease of reference to the CSA Z767 Standard, this Appendix is laid out with the Section numbers corresponding to the Section numbers in the Standard.

6.3 Process Risk Assessment and Risk Reduction

6.3.1 Framework

The Standard specifies that plant user ("facility operator") shall identify the hazards associated with their processes, assess the risks associated with those processes, consider whether further risk reduction measures are cost effective, and then document these analyses.

6.3.2 Staff Competence

Plant users will ensure that those involved in the hazard identification, consequence modelling, likelihood analysis, risk estimation, and risk mitigation analysis are, as a group, knowledgeable and competent in all relevant aspects of risk assessment.

If one or more of these skills is missing, consideration could be given to adding an outside consultant to the risk assessment team. The associated costs to do so will need to be weighed with the benefits of increased competence and credibility, particularly in consequence modelling of releases, explosions and fires.

6.3.3 Establish the Context

The risk assessment process is shown graphically in Figure B-1.

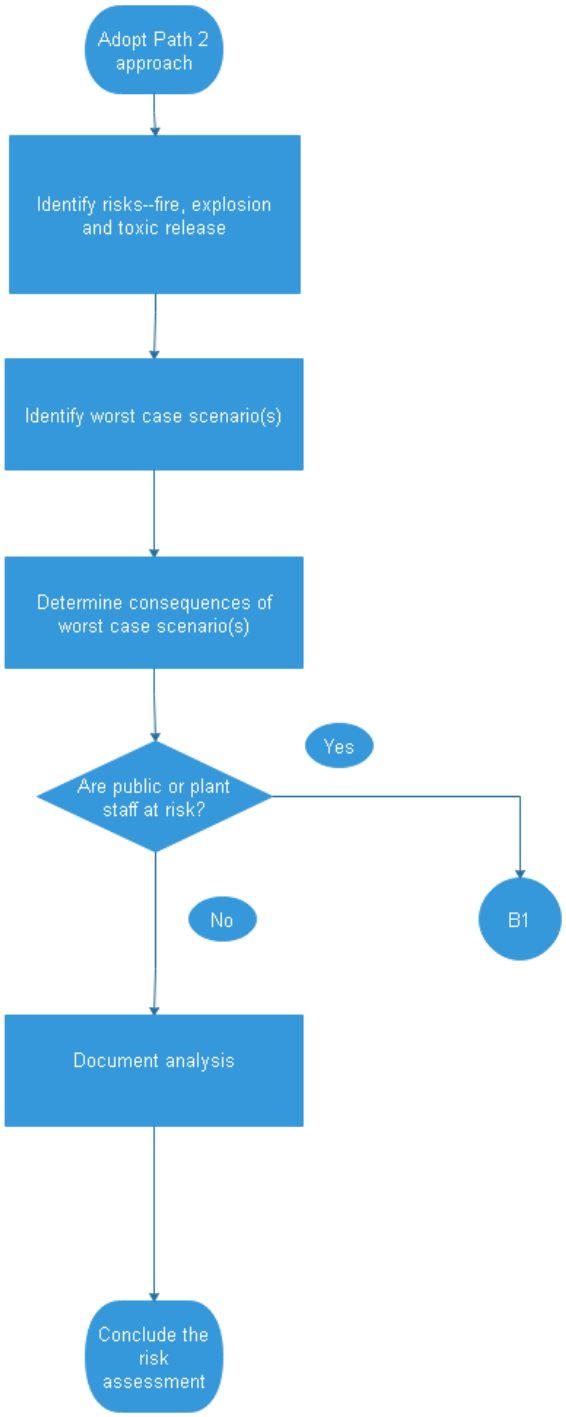


Figure B-1: Flowchart for Risk Assessment (*Continues on the next page)

The risk assessment needs to quantify the likelihood and consequence of scenarios that can result in health, safety, or environmental consequences. If the consequence analysis demonstrates that the toxic, overpressure, thermal radiation or other endpoints following a release or other incident might affect industrial facility staff or public receptors, the risk assessment will need to be iterative in determining whether the risk can be reduced through additional safeguards or measures. From the likelihood (event frequency) and consequences, an individual risk of death or injury can be calculated for all individuals exposed to the consequences of hazard occurrence.

The context for the risk assessment will emerge from the nature, size, risk and local environment of the facility.

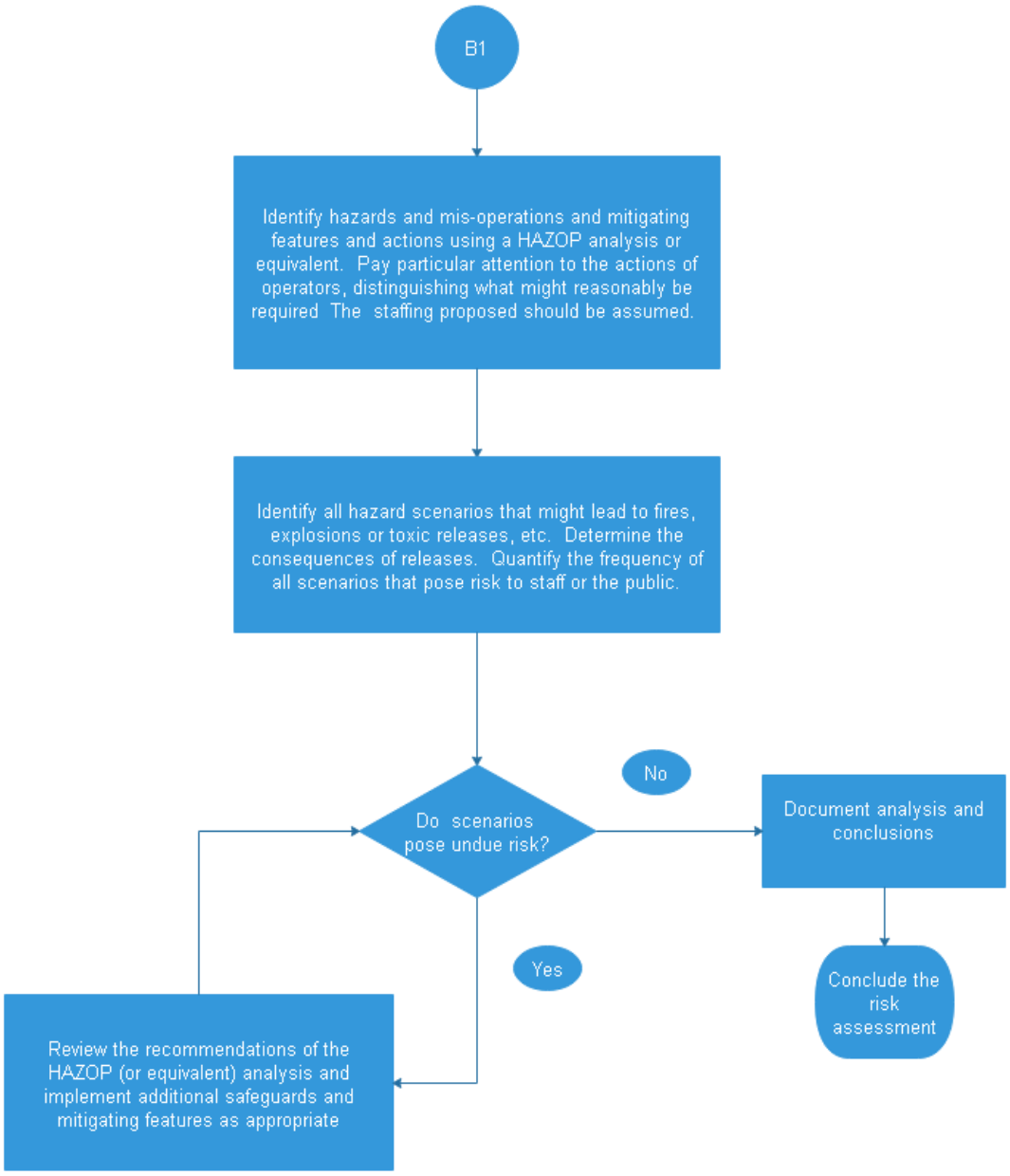


Figure B-1 Continued: Flowchart for Risk Assessment

6.3.4 Hazard Identification

CSA Z767 stipulates that the hazards and hazard scenarios associated with the facility shall be identified and documented.

These hazards may include exposure to toxic gases (including those arising from the evaporation of toxic liquids), asphyxiation in enclosed spaces, fire and thermal radiation (from pool fires, jet fires, flash fires or fireballs), and explosion (vapour cloud explosions and boiling liquid expanding vapour explosions—BLEVEs—including steam-side boiler explosions).

Hazard Identification involves, at a minimum:

- establishing the undesirable consequences of interest.
- incident enumeration - identifying hazard scenarios associated with material, system, process and facility characteristics that can produce these undesirable consequences.
- determining release rates - where the hazard scenario involves a release of flammable or toxic material, there will be a wide range of release rates. Normally, a finite number of releases are selected for analysis. For instance, for any given process line, one release might involve flow through a hole with a diameter 10% of the pipe diameter and a second a full-bore rupture of the line.
- identifying possible causes for the hazard scenarios - e.g., a steam side boiler explosion or BLEVE might result from overpressure, overheating or corrosion.
- identifying existing safeguards that might prevent or control the hazards and mitigate the possible consequences.
- identifying new safeguards and controls for risk reduction.
- identifying who is responsible for implementing these new safeguards and controls and when and how they will be implemented.

A single incident may have multiple serious outcomes (e.g., a propane release might result in a vapour cloud explosion, a BLEVE or a flash fire), and domino effects are also possible. In these cases, more than one worst credible scenario should be carried forward into consequence analysis.

Hazard analysis focuses on failures associated with equipment, instrumentation, utilities, human actions (routine and non-routine), and external factors that may impact safety. As noted in Section 6.4, below, the possibility of human error needs be considered in the Hazard Analysis, particularly if the analysis is performed to help establish staffing levels (i.e., requirements for Operating Engineers). Particular attention should also be paid to the possibility of common-cause failures.

There are several well-established techniques that can be applied to risk identification, including:

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

Additional details on these techniques can be found in the text “Guidelines for Hazard Evaluation Procedures with Worked Examples, Center for Chemical Process Safety, American Institute of Chemical

Engineers"[2]. The process hazard analysis is best performed by a team with expertise in engineering and process operations. The team should include at least one employee who has experience with, and knowledge of the process being evaluated; one member of the team must be knowledgeable in the controls and specific analysis methods being used. Software is available to help manage and document the hazard identification (e.g. PHA-Pro).

The output of the hazard identification analysis is a list of scenarios (a "risk register"), including importantly worst credible scenarios. The risk register could also include less severe scenarios and any action items to potentially mitigate them.

6.3.5 Consequence Analysis

CSA Z767 stipulates that the potential consequences of the one (or more) worst credible hazard scenarios shall be characterized and documented.

Modeling tools of varying levels of sophistication can be used. In general, the simpler tools will be more conservative in their predictions, meaning they will predict larger consequences than more sophisticated models.

Consequence can be expressed in terms of exposure to a hazard level (the end points described above) or characterized using a probit function. The latter is described in the CSA Z-767-17 standard and in UK HSE documentation on "Methods of approximation and determination of human vulnerability for offshore major accident hazard assessment"[3].

In determining consequences, the surrounding population and its demographics need to be considered. Mitigation factors, such as escape or an ability to shelter in place, can also be considered.

For each hazardous material, at least one worst-case release scenario needs to be modeled, this scenario being defined by the release of the contents of the total capacity at the facility or the single largest vessel (or piping) containing the hazardous material of concern, using an appropriate discharge rate. Typically, the discharge duration to consider will be 10 minutes; this might be curtailed if leak detection and isolation is possible.

For toxic releases, the "end point" is a toxic concentration that poses a danger to those exposed. The concentration provided for the US EPA Risk Management Program[4] can be followed. Chronic exposure to toxic chemicals need not be considered. To determine the extent of dispersion of a toxic material, the tables and methods presented in guidance provided for the US EPA Risk Management Program can be followed; alternatively, RMP*COMP or other appropriate software can be used to identify the toxic endpoint, neutral/buoyant or dense gas dispersion models can be used with site-specific (urban or rural) terrain and meteorology (atmospheric stability, wind speed and direction) data to ascertain the possible consequences of a toxic release.

---

[2] "Guidelines for Hazard Evaluation Procedures with Worked Examples"; Center for Chemical Process Safety, American Institute of Chemical Engineers; https://www.scribd.com/doc/240424869/Guidelines-for-Hazard-Evaluation-Procedures-2nd-Edition-With-Worked-Examples

[3] "Methods of approximation and determination of human vulnerability for offshore major accident hazard assessment"; Health and Safety Executive; November 2011; http://www.hse.gov.uk/foi/internalops/hid_circs/technical_osd/spc_tech_osd_30/spctecosd30.pdf

[4] "Risk Management Plan (RMP) Rule"; United States Environmental Protection Agency; https://www.epa.gov/rmp

Jet fires are modeled by assuming the jet fire occurs on rupture with immediate ignition. The GRI jet flame model embedded in most modelling software can be used to determine the heat flux. Alternatively, for jet fire involving natural gas, the models described by Stephens[5] can also be used.

Thermal radiation from confined and unconfined pool fires can also be modeled. The offsite threshold for concern (endpoint) for thermal radiation is typically set at 2 kW/m^2, a level that will cause pain within 60 seconds. The onsite threshold will be 5 kW/m^2, a level deemed acceptable for escaping personnel.

Flash fires require delayed ignition. 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 consequence consists of primarily an exercise in dispersion modeling, the hazard zone being essentially the extent of the flammable zone of the cloud. To account for non-uniform dispersion (i.e., pockets of gas), the flammable cloud could be assumed to extend to the distance at which a concentration of ½ the lower flammable limit is predicted.

A vapour cloud explosion also requires delayed ignition. For a detonation and significant overpressure, there needs to be sufficient confinement of the flammable gas or turbulent mixing. The endpoint for vapour cloud and other explosions is typically set at a 1 psi overpressure—an overpressure that will shatter windows and partially demolish houses. TNT-equivalency methods can be used to model the effect of vapour cloud explosions, BLEVEs and other explosions and determine the distance to this endpoint. TSSA guidelines for the Implementation of the Level 2 Risk and Safety Management plan can be used for a vapour cloud explosion involving propane. As these last two models assume the involvement of the full contents of the tank in the explosion, predictions of damage will be conservative given that the mass of flammable gas in the cloud will be less than the mass in the tank. Conversely, however, we need to recognize that ignition can occur anywhere in the cloud. Equations and the source of data for vapour cloud explosions involving other materials are provided in the US NRC Regulatory Guide 1.91[6]. Other models (e.g., multi-energy models). and software might also be used.

For BLEVEs (and steam side boiler explosions), the available models for overpressures are based on the similarity of the blast waves to those generated by high-explosive detonation. Boiler explosions will not, in general, result in a 1 psi shock being seen much beyond 60 m from the explosion. There may, however, be substantial damage both to the structure housing the boiler and possibly to adjoining structures. Vessels of pressurized gas do not have sufficient stored energy to create a major shock wave.

For BLEVEs involving flammable materials, thermal radiation from a fireball may also need be considered.

In addition, BLEVEs (including steam side boiler explosions) and other explosions might result in tank fragments, pipes and other debris being propelled 1000 m or more from the explosion[7]. While missile damage from BLEVEs is more difficult to model, it needs be recognized when considering emergency

[5] "A Model for Sizing High Consequence Areas Associated with Natural Gas Pipelines, Report GRI-00/0189, Prepared for the Gas Research"; Mark J, Stephens; October 2000; https://pstrust.org/docs/C-FerCircle.pdf

[6] "Evaluations of Explosions Postulated to Occur at Nearby Facilities and on Transportation Routes Near Nuclear Power Plants", Regulatory Guide–1.91 DC-1270, July 2011; https://www.nrc.gov/docs/ML1217/ML12170A989.pdf

[7] "BLEVE—Response and Prevention, TP13649E-3"; Transport Canada; https://www.tc.gc.ca/eng/tdg/publications-menu-1240.html

response and possible evacuation. Equations are presented in the CCPS[8] text to predict how far debris might travel. While in the event of BLEVE or vessel rupture, fragments are most likely to be propelled in an axial direction, they will also be thrown to the side.

Should the occurrence of the worst credible hazard event result in above-threshold impacts to on-site staff or public receptors, all scenarios that might result in such impacts shall be identified and their consequences determined.

6.3.6 Likelihood Analysis

CSA Z767 stipulates that the likelihood of the consequences of the identified hazardous scenarios that pose a risk to industrial facility staff and the public shall be assessed and documented. The likelihood analysis shall consider:

a. both internal and external events; and
b. equipment and process control failures, and human error.

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

- historical data analysis
- fault tree analysis
- event tree analysis
- human reliability analysis
- Safety Integrity Level (SIL) assignment
- Layer of Protection Analysis (LOPA)

[8] "Compressed Air Basics"; Michael L. Stowe, P.E.; May 2017; https://www.aiche.org/resources/publications/cep/2017/may/compressed-air-basics

Additional details on these techniques can be found in the text "Guidelines for Hazard Evaluation Procedures with Worked Examples, Center for Chemical Process Safety, American Institute of Chemical Engineers"[9]. Software is available to help perform likelihood analysis (e.g. CAFTA). Failure frequency and probability data for use in the likelihood analysis can be obtained from an analysis of industrial facility failure and maintenance data or from other acceptable sources, including:

- FRED (Frequency Rate Event Data) database from the UK Health and Safety Executive[10]
- NPRD-2011 database from Reliasoft/Quaternion Software[11]
- National Board of Boiler and Pressure Vessel Inspectors (NBBI) database[12]
- Military Standard MIL-STD-1629 and Australian Association of Chemical Engineers[13]

If nuclear failure rate data[14] are used, care should be taken not to apply data obtained for equipment designed and manufactured to higher standards than might be anticipated in the non-nuclear industry. In general, there will be little to be gained by modeling at a level of detail for which no data are available.

Human reliability data - estimates of the probabilities of errors of omission and commission - are provided by THERP[15]. An increased probability of error when operators are under stress should be noted. With human error, it should be assumed conservatively that the same operator will make the same mistake on multiple systems.

As noted above, particular attention shall also be paid to common-cause failures; such failures might originate in mis-calibration error on multiple instruments, a loss of industrial facility instrument air or other utilities or a fire under a cable tray.

6.3.7 Risk Estimation

CSA Z767 stipulates that the risk for the identified hazardous scenarios shall be estimated as a function of consequence and likelihood. In practice, the individual risk for an exposed individual is the sum, for all

[9] "Guidelines for Hazard Evaluation Procedures with Worked Examples"; Center for Chemical Process Safety, American Institute of Chemical Engineers; https://www.scribd.com/doc/240424869/Guidelines-for-Hazard-Evaluation-Procedures-2nd-Edition-With-Worked-Examples

[10] "Failure Rate and Event Data for use within Risk Assessments"; UK Health and Safety Executive; February 2019; http://www.hse.gov.uk/landuseplanning/failure-rates.pdf

[11] "Nonelectric Parts Reliability Data"; Quanterion Solutions Inc.; 2011; https://www.quanterion.com/product/publications/nonelectronic-parts-reliability-data-nprd-2011/

[12] "National Boiler Inspectors Association (NBIA) database"; https://www.nationalboard.org/default.aspx

[13] "Military Standard Procedures for Performing a Failure Mode, Effects and Criticality Analysis"; Unites States of America Department of Defence; November 1980; http://www.barringer1.com/mil_files/MIL-STD-1629RevA.pdf

[14] "Industry-Average Performance for Components and Initiating Events at U.S. Commercial Nuclear Power Plant", S. A. Eide, et al, NUREG/CR-6928, February 2007.; https://www.nrc.gov/docs/ML0706/ML070650650.pdf

[15] "Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications, Final Report", A. D. Swain, H. E. Guttmann, NUREG/CR- 1278, August 1983.; https://www.nrc.gov/docs/ML0712/ML071210299.pdf

hazard scenarios, of the products of the hazard scenario frequencies and the likelihood of death or injury to that individual given the occurrence of that hazard.

This means that both the consequence of each credible scenario (in terms of deaths) and its likelihood (annual probability) are to be estimated.

6.3.8 Risk Criteria

CSA Z767 implies that the consequence and likelihood of the worst credible scenario(s) should be compared with "risk criteria" to determine whether the "individual risk" is tolerable or not.

Since the basis of the risk acceptability criteria is intended to account for aggregated risks towards a risk receptor, (i.e. general public, on site workers), in order to have a meaningful comparison, the estimated risks for a facility need to be aggregated. If there are risk scenarios which post negligible risks to the risk receptor, the duty owners need to provide justification on why these risk scenarios should be excluded. These would be included as part of the application.

The risk criteria framework described in Figure B-2 shall be used for Path 2. Equivalent safety to demonstrate ALARP (As Low as Reasonably Practicable) means that risk is tolerable only if it can be demonstrated that all reasonable and practicable measures have been taken commensurate with the level of assessed risk.

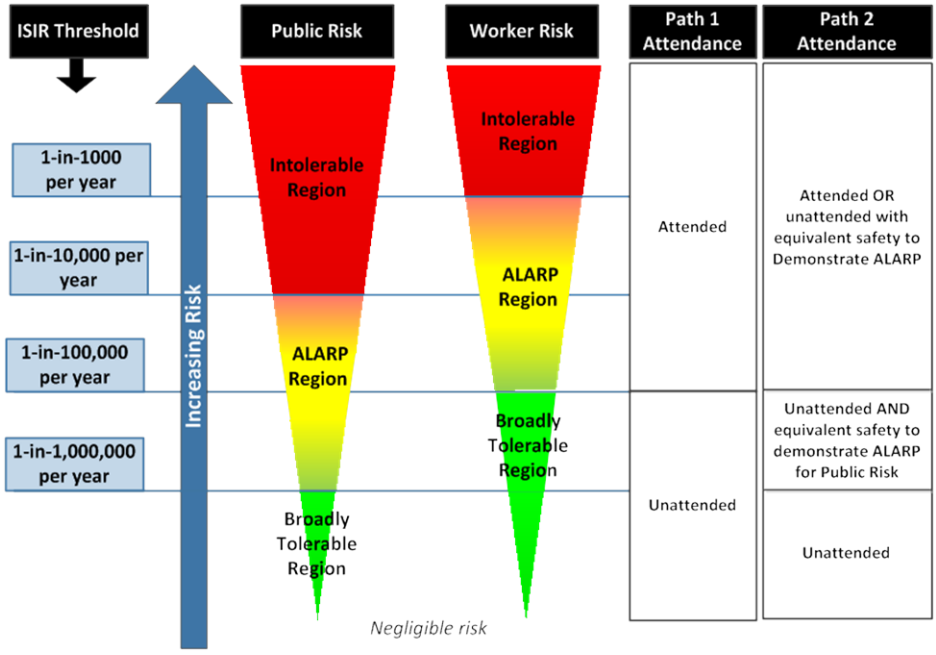


Figure B-2: Path 2 ALARP Principle (adapted from CSA Z767-17)

If the risk exceeds that which is deemed tolerable, a more detailed risk assessment might reduce uncertainty and unnecessary conservatism.

TSSA has determined that individual worker risk from process safety risk hazards shall not exceed 10^{-3} per year, and 10^{-4} per year for individual public risk

6.3.9 Risk Management

CSA Z767 stipulates that a risk mitigation and control plan shall be developed for the facilities which the risk is greater than that specified by risk criteria.

As part of this mitigation plan, the facility will need to identify necessary actions that can be carried out to reduce the risk to within the risk acceptance criteria and then provide a schedule for implementation.

- **Risk Reduction and Control Measures**

After risks have been identified, analyzed and evaluated, if analyzed risks are deemed to be intolerable or in the ALARP region, risk control measures are required to be introduced by the plant user.

Plant users should identify risk reduction options, evaluate them, and implement those options that provide sufficient risk reduction to ensure that the risk is either broadly tolerable or ALARP. Residual risk in the ALARP region "is tolerable only if it can be demonstrated that all reasonable and practicable measures have been taken" (CSA Z767-17, p.37).

Hierarchy of Risk Controls

Risk control measures could be categorized according to a "Hierarchy of Controls" in Table 1. To reduce the risk of harm, various approaches can be employed ranging from eliminating hazards to reducing likelihood and severity of hazardous events and preference should be given to those higher in the hierarchy.

Hierarchy	Explanation
Elimination	Something that removes a hazard completely. While this is clearly the most effective type of control measure, it is often not practicable to eliminate hazards. For example, if a toxic material is an essential raw material, then removal is most likely not possible
Substitution	Using a less hazardous material to meet the same need as a highly hazardous material
Intensification	Reducing the total inventory of a hazardous material
Prevention	Something that prevents accident scenario from occurring or significantly reduces the likelihood
Reduction	Control measures that reduce the magnitude of the consequences from the LoC – for example a scrubbing system or a dyke, usually by detecting unwanted conditions and acting to stop a scenario

Table 1. Example Hierarchy of Control Measures (HSE)

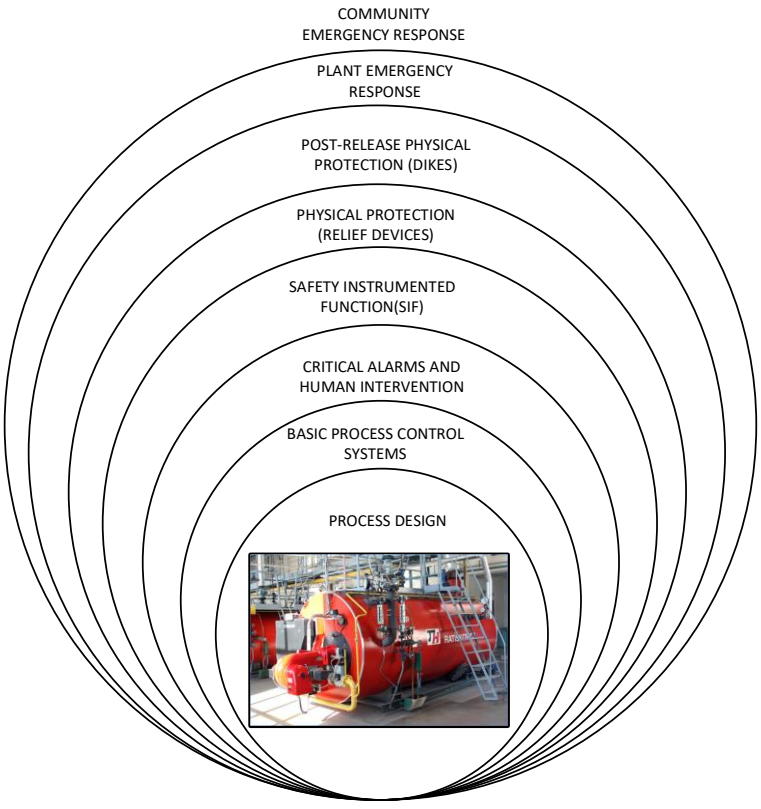
Identification of Control Measures

The Hazard Identification process will assist with the identification of control measures. Controls may also be identified during risk estimation and assessment processes and is particularly relevant for individual "high risk" or scenarios that are major contributors to cumulative risk. Plant users should also review control measures following the completion of the Risk Assessment to determine if further potential control measures need to be identified. It is important that persons responsible for designing or implementing control measures also look at behavioural response issues via administrative controls and human factors (e.g. emergency, operating and maintenance procedures) and strive towards work environments prone to less errors.

Where the control measures involve people, the human capacity and limitations must be carefully and demonstratively considered. For example, if an employee is required to perform a task that constitutes a control measure (such as isolating a piece of equipment within a specific time during an emergency), it must be clear that the employee would be able and willing to do this under the conditions that may prevail.

Criticality of Controls

While multiple layers of defence are the preferred approach to managing hazards, see B- 3, it is important that plant users and operators recognize that some layers are more important than others. A key output from the Risk Assessment process should be the identification of those control measures that are critical to safe operation. These critical control measures should receive the highest level of ongoing management attention to ensure that they are not degraded.



B-3 Layers of Defense Against a Possible Accident

When specifically considering boiler operations, reasonable outcomes from risk management and the intersection with the various Layers of Protection are presented in the UK Guidance on the Safe Operation of Boilers for a limited number of boiler types[16].

An example of a methodology that can be used is Layers of Protection Analysis (LOPA) which represents a semi-quantitative tool used to evaluate single scenarios. It addresses the frequency of initiating events and the subsequent likelihood that independent protection layers fail. LOPA delivers a simple, order of magnitude risk assessment that lies between hazard evaluation and quantitative risk assessment described herein. LOPA is an acceptable technique subject to the caveat that quantitative estimates should err on the conservative side and that no unwarranted assumption be made about the independence of layers of protection (i.e., possibility of component failures and plant users' and/or operators' errors—which may persist across multiple layers—should be recognized and addressed).

The CCPS-AIChE outline of the concept of layers of protection as follows:

- Layer 1: Process design (e.g. inherent safer designs);
- Layer 2: Basic controls, process alarms, and operator supervision;
- Layer 3: Critical alarms, operator supervision, and manual intervention;
- Layer 4: Automatic action (e.g. SIS or ESD);
- Layer 5: Physical protection (e.g. relief devices);
- Layer 6: Physical protection (e.g. dikes);
- Layer 7: Industrial facility emergency response;
- Layer 8: Community emergency response.

LOPA can be represented mathematically as an equation which multiplies the frequency of an initiating event by the probabilities that each independent protection layer will fail to perform its intended function.

Note that Layer 3 (manual ESD) requires an operator who is trained in activating emergency shutdown when critical alarms go off. Such an operator need not be an Operating Engineer.

6.3.10 Revalidation of the Risk Assessment

As required by the Management of Change Policy, a risk assessment is to be completed or updated whenever there is a change to the facility, operation, or operating environment that is outside of the context of the previous risk assessment.

In any event, the risk assessment is to be revalidated at least every 5 years as part of the overall revalidation of the RSMP.

[16] "Guidance on Safe Operation of Boilers Ref: BG01"; A joint document by the Safety Assessment Federation and The Combustion Engineering Association produced in consultation with the Health & Safety Executive; February 2013; http://www.safed.ie/wp-content/uploads/2017/11/BG01_update_1___21st_Feb_2013.pdf

6.4 Human Factors

As described in Section 6.3, CSA Z767 stipulates that human factors are to be considered in both risk identification and quantification.

In doing so, the design of operator process/equipment interfaces, written guidelines and procedures, staffing levels, and the working environment (noise, vibration, lighting, temperature) should all be considered from the perspective of their effect on both the levels of protection (line of defence) against hazard occurrence provided by operators and the possibility that their actions might initiate hazard occurrence. Errors of both commission and omission need be considered. The operator will contribute to one or more lines of defence (one or more *layers* of protection).

APPENDIX C: Background & References on RSMP Policy and Procedures

This Appendix provides further detail, references and templates for preparing the facility's RSMP and the various policies and procedures stipulated by the CSA Z767 Standard.

There are a number of source templates available, including the following:

1. HNI Risk Advisors' Process Safety Management Plan[17]
2. Energy Resources Australia's Process Safety Policy[18]
3. Canadian Centre for Occupational Health and Safety's Guide to Writing an OHS Policy Statement[19]
4. CCPS, "Guidelines for Process Safety Documentation"[20]

C.1 Accountability

This element requires a simple, straightforward policy statement that senior management will be responsible and accountable for the RSMP including goals, performance, approvals and controls.

C.2 Regulations, Codes and Standards

This element simply requires a policy of compliance with all applicable regulations, codes and standards.

C.3 Process Safety Culture

This element requires a policy statement within the PSM policy that process safety culture will be imbedded at all levels, including a statement establishing process safety as a measure of successful operation.

C.4 Conduct of Operations

This policy requirement is effectively equivalent to the one above (C.3) for process safety culture.

C.5 Process Knowledge and Documentation

This element requires a policy statement that all necessary documentation will be up to date and accessible to all that need it.

[17] "Process Safety Management Plan"; HNI Risk Advisors; http://www.hni.com/hs-fs/hub/38664/file-13959618-docx/docs/process_safety_management_program.docx

[18] "Process Safety Policy"; Energy Resources Australia; November 2014; https://www.energyres.com.au/uploads/general/ERA_Process_Safety_Policy.pdf

[19] "Guide to Writing an OHS Policy Statement"; Canadian Centre for Occupational Health and Safety; https://www.ccohs.ca/oshanswers/hsprograms/osh_policy.html

[20] Center for Chemical Process Safety, "Guidelines for Process Safety Documentation", New York, 1995

C.6 Project Review and Design Procedures

This policy statement requirement is simple and straightforward, namely that approval of projects[21] shall require a process safety risk assessment of the project.

The procedure for doing so would be equivalent to the procedure for the risk assessment laid out in sections 4.1-4.5 of this Guide.

C.7 Process Risk Assessment and Reduction

The policy should require a risk assessment at least every five years or whenever a material change is made, and that all process risks will be both tolerable and as low as reasonably practicable.

C.8 Human Factors

The risk assessment policy above should include consideration of human factors.

C.9 Training and Competence

There needs to be a policy that all personnel (employees and contractors) shall possess the necessary qualifications and competencies to perform their functions and tasks safely and effectively.

Procedurally, both initial and refresher training is be provided to all personnel. Initial training should provide an overview of the process and its operating procedures with an emphasis on the specific safety and health hazards of the process, emergency operations including shutdown, and other applicable safe work procedures. Refresher training in operating procedures should be provided at least every 3 years and more often if necessary. The plant user is responsible for ensuring that each worker trained has understood the training and is competent to operate the process safely as evidenced by observation by senior operators and/or testing if classroom training is provided.

Licensed staff (e.g., Operating Engineers and Professional Engineers) should undertake such continuing professional education as is required to maintain their licenses and skills.

A record of process safety training received by each person should be maintained, including:

1. the name of the course and provider;
2. the date of the training;
3. the results of any competency verification; and
4. the date required for refresher training, if necessary.

C.10 Management of Change

The PSM policy shall include a policy statement outlining a Management of Change (MOC) process. The primary focus of the MOC system is to manage risks related to design changes and modifications to chemicals, technology, equipment (other than replacement “in kind”), operating, test, maintenance and inspection procedures, and staffing and organization to ensure that changes made do not create new hazards and that employees and contractors are informed of the changes and trained in any new

[21] Note 1: the term "project" is undefined by CSA Z767 but can be understood to mean new projects (greenfield), expansions, major renovations, etc.

procedures prior to start up. The management of change (MOC) process will develop and/or update safe work procedures and associated training for non-routine hazardous tasks. The guidance presented in Exhibit 7-7 of the General RMP Guidance of the EPA's RMP[22] rule will suffice to ensure changes do not detract from industrial facility safety.

Temporary changes are subject to the same review as permanent changes. In addition, management of temporary change requires:

1. a time limit for a temporary change be clearly defined;
2. a system for further review and approval if an extension of the time limit is required
3. a plan to ensure that all equipment is returned safely to the previous approved design conditions at the end of the temporary change, including removal of any temporary equipment that was installed as part of the changes.

C.11 Process and Equipment Integrity

The responsible organization shall have written policies and procedures to inspect, test, and maintain the ongoing integrity of process equipment, establish a test and maintenance schedule, perform equipment inspection, implement a quality inspection program for incoming materials and establish safe work practices.

This expectation transcends CSA Z767 and is covered by both sound maintenance practice and current regulations.

The guidance for a maintenance program presented in Section 7.6 of the General RMP Guidance of the EPA's RMP[23] rule will suffice to ensure process equipment integrity. Documentation is also required demonstrating that process safety critical equipment has been identified and that a system of regular testing of its process safety critical equipment has been stablished and maintained. For documentation on equipment inspection, the requirements of Section 7.3.3 b) of the CSA Z767-17 Standard can be followed. For documentation on quality inspection, the requirements of Section 7.3.4 of the CSA Z767-17 Standard should also be followed.

[22] "General Guidance on Risk Management Program for Chemical Accident Prevention" United States Environmental Protection Agency; https://www.epa.gov/sites/production/files/2013-11/documents/chap-07-final.pdf

[23] "General Guidance on Risk Management Program for Chemical Accident Prevention" United States Environmental Protection Agency; https://www.epa.gov/sites/production/files/2013-11/documents/chap-07-final.pdf

C.11.1 Establishing Safe Work Practices for Alarm and Management Systems

The responsible organization shall have safe work practices for alarm and instrument management that includes:

a. equipment hardware
b. computer components
c. software functions for process control

The alarm and instrument management program would cover:

1. identification and prioritization of critical alarms and interlocks
2. a procedure to control changes to alarm set points and interlock systems a system of regular testing of alarms, interlock systems, pressure safety valves (PSV), and other equipment identified as critical safeguards

C.11.2 Pre-Startup Safety Review

A pre-startup safety review (PSSR) should be conducted before starting up a new or modified process or process equipment. The guidance presented in Section 7.8 of the General RMP Guidance of the EPA's RMP rule[24] will suffice for this purpose.

C.11.3 Safe Work Practices: Personnel Safety and Access Control

The AIChE/CCPS Safe Work Practices tool[25] can be used to help. In addition, access control by personnel and vehicles could be addressed.

C.11.4 Temporary Suspensions or Removal from Service

Policy and procedure for this are already addressed under the Management of Change policy and procedure (Section 7.2 above).

C.11.5 End of Service Requirements

The facility should include a general policy to safely and properly dismantle, decommission, and dispose of equipment and waste related to its operations.

[24] "General Guidance on Risk Management Program for Chemical Accident Prevention" United States Environmental Protection Agency; https://www.epa.gov/sites/production/files/2013-11/documents/chap-07-final.pdf

[25] "Safe Work Practices (SWP)"; Centre for Chemical Process Safety; https://www.aiche.org/ccps/resources/tools/safe-work-practices

C.12 Emergency Management Planning

An emergency response and preparedness plan is required to manage the consequences of hazardous scenarios. An E2 plan required under Canada's Environmental Emergency Regulations[26], a plan that conforms to CAN/CSA Z767-17, CAN/C5A-Z246.2 or CSA Z1600 or the TSSA Guidelines for the "Implementation of the Level 2 Risk and Safety Management Plan" will meet the requirements.

The policy should include the updating and testing at least once every calendar year, and a full-scale exercise made at least once every 5 years (or after significant changes to the facility are made). Records are required of these updates and tests as specified in the E2 regulations.

C.13 Investigation

There is need for a system to identify, report, investigate (as necessary), and record all incidents, including near misses and abnormal events.

An incident investigation should be conducted by a team consisting of at least one person knowledgeable in the process involved, including a contract employee if the incident involved the work of a contractor, and other persons with appropriate knowledge and experience to investigate and analyze the incident thoroughly. Guidance for this investigation procedure as presented in Exhibit 7-9 of the General RMP Guidance of the EPA's RMP rule[27] will suffice for this purpose.

C.14 Audit Process

This element requires a policy to periodically audit the PSM program, including a procedure, schedule and follow up on corrective action. TSSA may request evidence of audits during TSSA inspections.

C.15 Enhancement of Process Safety Knowledge

The PSM policy requires a statement on continual improvement to the PSM program.

[26] "Implementation guidelines for Environmental Emergency Regulations: chapter 5" (https://www.canada.ca/en/environment-climate-change/services/canadian-environmental-protection-act-registry/publications/implementation-guidelines-emergency-regulations/chapter-5.html#to5_1).

[27] "General Guidance on Risk Management Program for Chemical Accident Prevention" United States Environmental Protection Agency; https://www.epa.gov/sites/production/files/2013-11/documents/chap-07-final.pdf

C.16 Key Performance Indicators

The final PSM element stipulates a policy and reporting procedure on performance indicators (KPIs) for the PSM program.

There is latitude in the number and nature of KPIs selected. Typically, KPIs for process safety performance are incident-based, for instance:

Typical KPIs

Safety Systems

- safe operating limit excursions
- primary containment inspection or testing results outside acceptable limits
- safety systems that failed on demand
- activation of a safety instrumented system
- activation of mechanical shutdown system
- activation of pressure relief device (PRD)
- loss of primary containment (LOPC) events

Maintenance, Inspection and Testing

- delay in completion of inspections
- number of non-conformances identified through inspection/maintenance

Action Items Follow-Up

- overdue incident investigation action items
- overdue actions related to regulatory/compliance issues

Training, Competency, and Capability

- overdue training
- non-conformances related to procedures and safe working practices.

Guidance on selection and reporting of Key Performance Indicators is available from a number of industry sources including International Association of Oil & Gas Producers "Process Safety – Leading key performance indicators"[28] and Centre for Chemical Process Safety's "Process Safety Leading and Lagging Metrics"[29].

[28] "Process Safety – Leading key performance indicators"; International Association of Oil & Gas Producers; July 2016; http://www.energysafetycanada.com/files/pdf/process_safety/PSM_Supplement_to_Report_456.pdf

[29] "Process Safety Leading and Lagging Metrics"; Centre for Chemical Process Safety; January 2011; https://www.aiche.org/sites/default/files/docs/pages/CCPS_ProcessSafety_Lagging_2011_2-24.pdf