



Canadian Society for Chemical Engineering | ***For Our Future***

Process Safety Management Guide

4th Edition

Process Safety Management Guide

4th Edition

Foreword

This document was prepared by the Process Safety Management Division of the Canadian Society for Chemical Engineering (CSCHE). It is based on earlier editions developed through the Major Industrial Accidents Council of Canada (MIACC), a voluntary alliance of interested parties dedicated to reducing the frequency and severity of major industrial accidents. From 1987 until its dissolution in 1999, this partnership included the federal, provincial and municipal governments, industry, labour, emergency response groups, public interest groups and academia. Rights to the document were transferred to the CSCHE on the dissolution of MIACC in 1999. It is sincerely hoped that the information in this document, which provides introductory guidelines for users to consider and not standards or procedures that must be followed, will lead to an even better safety record for the process industries of Canada.

The material in the PSM Guide is based on the approach originally developed by the U.S. Center for Chemical Process Safety (CCPS). The CCPS was established in 1985 as a Directorate of the American Institute of Chemical Engineers to focus on engineering practices that will help prevent or mitigate catastrophic process safety accidents. Its dynamic program of publications, seminars, training courses and research has made CCPS a powerful voice in the international community of those committed to engineering practices that can prevent or mitigate catastrophic accidents in chemical processing.

Although the CCPS has since changed to a risk-based approach that supplements the coverage provided by regulation in the U.S., CSCHE has retained the original twelve-element CCPS structure for use in Canada as it provides a sound basis for site operators in jurisdictions where PSM guidance from competent authorities is not yet established.

For more information on process safety management or on publications available on this and related subjects please visit the process safety management Division website, www.cheminst.ca/PSM, or contact the Division at psm@cheminst.ca.

Canadian Society for Chemical Engineering

550-130 Slater Street

Ottawa, Ontario K1P 6E2

T. 613-232-6252, F. 613-232-5862

E-mail: info@cheminst.ca

www.cheminst.ca

Disclaimer

The proposed application of this publication is stated in the Introduction. While the information presented in this document is intended to assist users in the safe design and operation of facilities handling, using, processing or storing hazardous materials, the user is advised that neither the Canadian Society for Chemical Engineering (CSCHE) nor persons involved in producing this publication warrant to represent, expressly or implicitly, the correctness or accuracy of the information presented herein. This publication is intended to be a general guidance and not advice for specific situations, nor is it to constitute a legal standard of care.

It remains the responsibility of the user of the publication to determine its suitability for the particular application intended, to use the information provided in the publication in a manner appropriate to that application, and to consult with qualified professionals as necessary. Notwithstanding the above, or any other provisions in this publication or any applicable statutory provisions, the Canadian Society for Chemical Engineering, the Chemical Institute of Canada (including without limitation their respective past and present officers, directors, members, employees or volunteers), the organizations, or the persons involved in producing this publication shall not be liable to the user for any damages – whether direct, indirect, general, punitive, consequential, for alleged lost profits, or otherwise – that may result directly or indirectly from the application of this publication.

©Canadian Society for Chemical Engineering 2012

ISBN: 978-0-920804-99-5

PROCESS SAFETY MANAGEMENT GUIDE

Expressions appearing in **boldface** in the text are explained in the Glossary

Introduction

This guide shows the scope of Process Safety Management (PSM) and explains briefly the meaning of its elements and components. The approach is based on that originally developed by the **Center for Chemical Process Safety (CCPS)** of the American Institute of Chemical Engineers (AIChE). This approach was selected after reviewing several currently available alternatives and was chosen because it was comprehensive; well supported by reference materials, tools and an organizational infrastructure; and was based on a benchmark of leading or good industry practice rather than on a minimum standard.

Organizations already practicing PSM but using a different approach (e.g. Occupational Safety and Health Administration 1910.119 or American Petroleum Institute RP750) do not necessarily need to switch to the approach given here; however they should be aware of any items here which may not be addressed under their present PSM scope (e.g. human factors) and should also be able to demonstrate that they have alternative measures in place for proper control of those items.

It is obviously not possible in a document of this length to provide all the necessary information even on the items described. For more information users should consult the accompanying *PSM Standard*, available on the PSM page of the Canadian Society for Chemical Engineering's web site (www.cheminst.ca/PSM), and the additional resources listed in the references at the end of this guide. Many of these are available from the CCPS.

Purpose

The purpose of this document is to provide an overview of PSM and an introduction to the CSCHE's *PSM Standard*. It is aimed mainly at facilities handling hazardous materials, but the approach of PSM is also valid for other branches of engineering, science and technical fields.

PSM was developed after the lessons from several major accidents showed that such events can be difficult to prevent using the **traditional occupational health and safety** approach, which tends to focus on the interface between the individual operator and the equipment or process. Many of the key decisions which lead to serious, unplanned events are beyond the control of the operator or even local site management. Effective control, therefore, calls for a much broader review of the process, including equipment, procedural and organizational factors, together with a **management system** to ensure all hazards thus identified are properly managed throughout the life of the process, regardless of changes in the personnel, organization or operating environment.

PSM provides a guide for this review and control. It does not replace traditional health and safety, but builds on it to give additional insight into how hazards develop and how they can be avoided or controlled.

Scope

PSM is the application of management principles and systems to the identification, understanding and control of **process hazards** to prevent process-related injuries and incidents.

This document describes the application of these PSM principles at facilities that manufacture, store, handle or use hazardous materials. The PSM system originally suggested by the CCPS consists of 12 elements. These elements are shown in Table 1 and are described in this document. The elements are intended to work in conjunction with traditional occupational health and safety programs and applicable federal/provincial/territorial legislation or municipal regulations. A complete framework of PSM elements is recommended for each facility even though some elements or components of PSM may be less applicable to some facilities than to others, depending on the nature and degree of potential hazards

involved. A facility should carefully evaluate the applicability of each item before assuming that it does not apply.

Table 1¹: Elements and Components of PSM

| | |
|---|---|
| <p>1. Accountability: Objectives and Goals Continuity of operations Continuity of systems Continuity of organization Quality process Control of exceptions Alternative methods Management accessibility Communications Company expectations</p> <p>2. Process Knowledge and Documentation Chemical and occupational health hazards Process definition/design criteria Process and equipment design Protective systems Normal and upset conditions Process risk management decisions Company memory</p> <p>3. Capital Project Review and Design Procedures Appropriation request procedures Hazard reviews Siting Plot plan Process design and review procedures Project management procedures and controls</p> <p>4. Process Risk Management Hazard identification Risk analysis of operations Reduction of risk Residual risk management Process management during emergencies Encouraging client and supplier companies to adopt similar risk management practices Selection of businesses with acceptable risk</p> <p>5. Management of Change Change of process technology Change of facility Organizational changes Variance procedures Permanent changes Temporary changes</p> | <p>6. Process and Equipment Integrity Reliability engineering Materials of construction Fabrication and inspection procedures Installation procedures Preventative maintenance Process, hardware and systems inspection and testing Maintenance procedures Alarm and instrument management Decommissioning and demolition procedures</p> <p>7. Human Factors Operator - process/equipment interface Administrative control versus engineering control Human error assessment</p> <p>8. Training and Performance Definition of skills and knowledge Design of operating and maintenance procedures Initial qualifications assessment Selection and development of training programs Measuring performance and effectiveness Instructor program Records management Ongoing performance and refresher training</p> <p>9. Incident Investigation Major incidents Third party participation Follow-up and resolution Communication Incident recording, reporting and analysis Near-miss reporting</p> <p>10. Company Standards, Codes and Regulations External codes/regulations Internal standards</p> <p>11. Audits and Corrective Actions PSM systems audits Process safety audits Compliance reviews Internal/external auditors Corrective actions</p> <p>12. Enhancement of Process Safety Knowledge Quality control programs and process safety Professional and trade association programs Technical association programs Research, development, documentation and implementation Improved predictive system Process safety resource centre and reference library</p> |
|---|---|

¹ The CCPS PSM system described here is taken from References A1 and A2. This material is copyright 1989 by the American Institute of Chemical Engineers and is reproduced by permission of the Center for Chemical Process Safety of AIChE. In 2007 the CCPS moved from the twelve-element system to a risk-based approach using a different set of categories from those shown in this framework, as facilities in the U.S. were generally familiar with PSM due to regulation by OSHA and various state authorities. However, the CScHE's PSM Division decided to retain the original CCPS system for use in Canada, where PSM is not regulated, as it is more self-explanatory for site operators who may be unfamiliar with what PSM comprises.

The Site Self-assessment Tool

Under the Major Industrial Accidents Council of Canada (MIACC), tools were developed for hazardous installations and surrounding communities to conduct a self-assessment of their level of prevention and preparedness for major incidents. The revised *Site Self-assessment Tool* is now featured in the boxes in this guide.

The questions assess the current level of awareness and use of the techniques outlined in the guide. The techniques are important for proper control of major hazards in any facility that manufactures, uses, stores, makes ready for transport or disposes of hazardous substances. This obviously applies to sites meeting the criteria under Section 200 of the Canadian Environmental Protection Act, but other sites have also tested the tool and reported that it was a positive experience that helped site managers identify vulnerabilities in their existing systems for control of process-related incidents.

Although the questions are arranged in the original CCPS 12-element structure used in this guide, they are just as applicable and easy to follow for any company using an alternative approach to PSM.

The questions are in three levels to help in setting priorities for future work. The questions at the essential level each cover a topic that could be a last line of defence, where a gap in protection would not necessarily be detected by other means. All facilities with the potential for major hazards should therefore meet at least the essential level. However, each item from the higher levels should also be considered before assuming that it is not applicable. This applies especially to element 4 (process risk management): For any site with the potential for a major incident, the organization having control should be aware of the main techniques, and decisions pertaining to their use at that location should be made by a competent person.

How to Use the Self-assessment Tool

Experience with the *Site Self-assessment Tool* shows that it can generally be completed in two to four hours.

Important: Results can vary greatly between sites or business divisions within the same company management system, depending on local culture. Use a separate questionnaire for each location being assessed and encourage discussion among those familiar with actual practice at that location rather than basing answers on assumptions about how the system is supposed to work. .

Review all the questions shown in the boxes in this guide, and answer A, B, C, or D to each question depending on the awareness and use of that item at the site, based on the following:

- A** Widespread and comprehensive use wherever significant hazard potential exists.
- B** Moderate use, but coverage is uneven from unit to unit or not comprehensive in view of potential hazards.
- C** Appropriate personnel are aware of this item and its application, but little or no actual use.
- D** Little awareness or use of this item.

To achieve a given level (e.g. essential) a site must score A on all questions for that level. A spreadsheet version of the self-assessment tool for easy scoring of results is available on the PSM page of the Canadian Society for Chemical Engineering's website (www.cheminst.ca/PSM) .

The PSM division of CSE may also offer some free telephone assistance to the process industries in Canada to help in understanding or interpreting this guide and the accompanying self-assessment questions and *PSM Standard*. Contact the CSE at psm@cheminst.ca to find how to obtain this assistance.

1 ACCOUNTABILITY: OBJECTIVES AND GOALS

Management commitment at all levels is necessary for PSM to be effective. The objectives for establishing accountability are to demonstrate the status of process safety compared to other business objectives (e.g. production and cost), to set objectives for safe process operation and to set specific process safety goals. These objectives should be internally consistent (i.e. supported by appropriate resources). Key components of accountability are:

1.1 Continuity of operations

Management is responsible for resolving the conflicts between meeting production/cost targets and shutting down or reducing output for planned or unplanned maintenance or modifications. To avoid compromising process safety, continuity of operations is best addressed at the planning stage by features such as spare and redundant equipment, multi-train rather than single stream operations, independent capability to shut down small sections of the plant, etc.

1.2 Continuity of systems

Accountability for process systems extends beyond the process units in question, to include adequate resourcing of supporting job functions or units for each phase of the life cycle of the process. It also extends beyond the organization itself to include relationships with external providers of goods and services where these could significantly impact process safety. Assignment of resources should be driven by the process hazards rather than by the economic viability of the process.

1.3 Continuity of organization

Changes in organizational structure can have a severe impact on process safety. Accountability should be flexible enough to accommodate such changes while ensuring that process safety tasks are properly assigned and performed throughout the change.

1.4 Quality process

Accountability for process safety has much in common with accountability for quality. Process safety problems can be seen as non-conformance with specifications, and many of the techniques used to establish systems for quality can be applied to control process safety performance.

1.5 Control of exceptions

Flexibility is important in management systems since it is often not practical to attempt to specify in advance exactly how each situation should be handled. Variance procedures should allow exceptions to be managed with appropriate controls by assigning accountability to qualified personnel.

1.6 Alternative methods

Accountability is more difficult with performance standards, which identify only desired results, than with specification standards, which also identify the means to be used. Where guideline methods are suggested, (e.g. for process hazard reviews), persons using alternatives should be accountable for ensuring that the method selected is at least as effective as the guideline method for the intended purpose.

1.7 Management accessibility

Successful PSM makes senior managers accountable for being accessible to their staff for support and guidance on process safety decisions, and for resolving conflicting views among safety, engineering, maintenance, production and business managers.

1.8 Communications

Senior managers should communicate their understanding of process safety accountability for their unit and individuals within it. This accountability should also include communication and coordination of overlapping responsibilities between individuals/units to ensure no gaps occur.

1.9 Company expectations

Broad process safety goals should be established by management and should include philosophical issues as well as detailed targets. The decision-making process should be driven by the safety culture of the organization rather than by *ad hoc* solutions. Metrics should be established to monitor performance and compare results with design intent, and targets must be consistent with other aspects of the organizational vision or master plan, i.e. they must match any other constraints and the availability of resources.

Expectations and performance should be periodically reviewed to control the tendency for substandard behaviour or conditions to be treated as normal (normalization of deviance) where they could lead to a serious incident. Good performance in personnel safety should not be taken as an indicator of the effectiveness of control of major hazards.

Questions on Element 1 ACCOUNTABILITY: OBJECTIVES AND GOALS

Essential

- (a) Are responsibilities clearly defined and communicated, with those responsible held accountable?
- (b) Is there a system which designates the accountability for safe work at the site, including contract personnel?

Enhanced

- (a) Is there a policy statement expressing management's commitment to process safety/loss prevention?
- (b) Is the system for accountability designed to handle possible exceptions by specifying how decisions default?
- (c) Does the system feature performance metrics and goals for process safety, and monitor and manage performance regarding those goals?
- (d) Does the system attempt to benchmark and encourage a safety culture?

Comprehensive

- (a) Are employees recognized for their personal efforts in the continual improvement of process safety?
- (b) Is there clear accountability for maintaining the integrity of the facility's assets?
- (c) Is accountability continuous (i.e. regardless of changes in personnel, production schedules, organizational structure, etc.)?
- (d) Does the system ensure effective implementation of all items covered by the questions under *PSM Guide* element 1 (Accountability: Objectives and Goals)?
- (e) Does the system ensure any systemic deviation from approved safe work practices and normal operation within prescribed limits is periodically reviewed, acknowledged and addressed?
- (f) Is there active involvement and exchange of PSM knowledge with industry PSM groups?
- (g) Is there active involvement, relative to site and company capability, in promoting and supporting adoption of PSM by other process industry sites in Canada?

2 PROCESS KNOWLEDGE AND DOCUMENTATION

Information necessary for the safe design, operation and maintenance of any facility should be written, reliable, current and easily accessible by people who need to use it. Process safety information is needed in the following areas:

2.1 Chemical and occupational health hazards

This normally takes the form of Material Safety Data Sheets (MSDS) for every potentially hazardous material used, stored or produced at a site, plus information on reactivity, chemical and physical properties for use by those involved in process development and design.

2.2 Process definition/design criteria

This is information needed to operate a facility within its design range and to enable potential changes to be properly reviewed for their impact on the facility's safety and reliability. Minimum information required is:

- Process flow diagram;
- Safe upper and lower limits for levels, temperatures, pressures, flows, time, cycles and compositions;
- Evaluation of the effects, including those on health, safety and the environment, of operating outside of these safe limits;
- Process chemistry, including process stability and chemistry of side reactions, by-products and contaminants, and potential reactivity hazards;
- Maximum intended inventory;
- Material and energy balances.

2.3 Process and equipment design

This covers the data needed to ensure and maintain the mechanical and process integrity of the equipment at a facility. Minimum information requirements are:

- Piping and instrumentation diagrams (P and IDs);
- Materials of construction;
- Process control systems, including software integrity;
- Ventilation system design;
- Relief system design and design basis;
- Design codes and standards employed;
- Electrical classification drawings;
- Plot plan.

2.4 Protective systems

These are data on systems which either prevent or mitigate incidents.

Examples include:

- **Critical** alarms;
- **Critical** interlocks;
- Pressure relief and venting systems;
- Fire detection and protection equipment;
- Emergency isolation valves;
- Effluent treatment systems (scrubber, quench tank, etc.).

2.5 Normal and upset conditions (operating procedures)

Operating procedures should be readily accessible to those who work with or maintain the process. There should be a system for updating procedures to ensure they reflect current operating practice (including changes of process chemistry, technology, equipment, facilities or organization) and regular certification that procedures are current and accurate. Procedures should address:

- Steps for each operating phase, including:
 - Initial start up of a new facility;
 - Normal and temporary operations;
 - Emergency shutdown, including identification of conditions which require shutdown;
 - Normal shutdown;
 - Start-up following an emergency or normal shutdown.
- Plant operating limits:
 - Consequences of deviating from established operating limits;
 - Steps required to correct or avoid a deviation from operating limits.
- Safety systems and their functions.

2.6 Process risk management decisions

Risk management decisions should be documented, showing the decisions made and the basis on which they were made. This is a sensitive area because of implications for liability and due diligence, and should be carefully coordinated with the company's legal department.

2.7 Company memory (management of information)

Knowledge and information gained from plant experience which is likely to be important for future safety of the facility should be documented in a system so that it is not overlooked or forgotten as personnel or the organization change.

Questions on Element 2 PROCESS KNOWLEDGE AND DOCUMENTATION

Essential

- (a) Are the safety, health and environmental hazards of materials on site clearly defined (e.g. MSDS)?
- (b) Is there current comprehensive documentation covering safe operating procedures and all process safety-critical operating parameter limits together with consequences of operation outside those limits?
- (c) Does the documentation cover start-up, shutdown, normal, emergency and temporary operations?

Enhanced

- (a) Is there documentation outlining the protective systems installed to prevent process safety related incidents?
- (b) Is process safety-critical equipment clearly identified to operational staff and managed as such?

Comprehensive

- (a) Is all the information about: hazards of materials on site; operating basis; process and equipment design basis; and protective systems design basis (including consequences of deviations), documented, kept up-to-date and accessible to those who need it?
- (b) Is there documentation on the reliability of process safety critical equipment throughout its life cycle?
- (c) Is all information needed to sustain safe operations — including operating, inspection, maintenance, skills, capabilities, and training requirements — documented, kept up-to-date and accessible to those who need it?
- (d) Is the core knowledge base centralized (with appropriate read-only access) and managed by those with expertise in database design and management?
- (e) Is the knowledge base periodically assessed to ensure the information is adequate to meet the process safety needs of relevant elements at each point in the unit's life-cycle, including:
 - (i) Minimum knowledge requirements;
 - (ii) Management review audit to examine the process knowledge for all modes of operation and life cycle stages; and
 - (iii) System review to ensure identified gaps (e.g. usability, adequacy) are identified and addressed?

3 CAPITAL PROJECT REVIEW AND DESIGN PROCEDURES

3.1 Appropriation request procedures

The approval process for new capital projects should ensure the request has identified potential risks, together with capital and other resources necessary to manage those risks. Process safety reviews must be satisfactorily completed at appropriate stages for the project to proceed.

3.2 Hazard reviews

Hazard reviews ensure potential **risks** associated with hazardous materials and energy have been identified and that adequate capital and other resources are made available to minimize exposures to those on site, the public and the environment.

The scale of review required will depend upon the hazards of the proposed process and also the stage of the project, since the more intensive review techniques require information which becomes available only as the design proceeds.

3.3 Siting

Siting of a proposed expansion or new plant should consider the following factors:

- **Buffer zones** between the plant and the public;
- **Worst credible scenarios** for release of a toxic chemical, explosion or fire, and effect(s) on exposed groups;
- Exposure hazard to and from adjacent plants or facilities;
- Possible exposures due to natural events such as earthquake, flood, tornado, etc.;
- Effects of transportation of hazardous material feedstocks or products through local communities.

3.4 Plot plan

Here the proximity of equipment and storage of hazardous materials are evaluated. A plot plan review should include:

- Congestion (e.g. overlapping hazard zones, difficult access, possible confinement of vapour release, etc.);
- Location of control rooms, offices and other permanent and temporary buildings;
- Storage areas;
- Loading and unloading areas;
- Drainage and containment;
- Other process areas;
- Potential for offsite impact;
- Insurance requirements;
- Federal, provincial and local regulations;
- Company/industry spacing guidelines.

3.5 Process design and review procedures

The design process should include a system for review and approval, with appropriate sign off, at each stage of the design process. Normal stages are: conceptual design, process design, detailed engineering design, construction and commissioning. The depth of each review will depend upon the complexity and degree of hazard of the process.

3.6 Project management procedures and controls

These controls ensure fabrication and installation of equipment corresponds to design intentions. A key control is the pre-startup safety review required before new or modified facilities are put into service. Minimum requirements for this review are:

- Confirm that construction meets design specifications;

- Ensure safety, operating, maintenance and emergency procedures are in place and adequate;
- Confirm that a **process hazard analysis** has been done and that recommendations have been resolved or implemented prior to start up;
- Confirm that modified facilities meet the management of change requirements;
- Ensure necessary training has been completed;
- Ensure critical equipment has been identified and incorporated into a preventative maintenance program.

Project management controls should be documented and form part of the project file.

Questions on Element 3 CAPITAL PROJECT REVIEW AND DESIGN PROCEDURES

Essential

- Are all project proposals for new or modified facilities subjected to documented hazard review before approval to proceed?
- Does the system for hazard review of capital projects meet the criteria for the corresponding level (essential/enhanced/comprehensive) of PSM element 4 (Process Risk Management)?
- Do the design reviews assess the hazards of normal, intermittent and also abnormal aspects of operating the process?
- Are (pre-startup) hazard reviews completed prior to startup for all new facilities or modifications to existing facilities?
- Are the following completed on all new facilities or modifications to existing facilities:
 - Construction inspections, as part of the construction process, to ensure the facility is built as designed;
 - Turnover inspections, when the facility is mechanically complete and prior to commissioning;
 - Commissioning checks, prior to the introduction of process fluids?

Enhanced

- Is the design philosophy based on the principle of inherent safety?
- Does the hazard review consider plant siting and layout?
- Are fail-safe features/redundancy considered?

Comprehensive

- Does the company follow engineering standards which are current and maintained?
- Is there a system to manage deviations from standards?
- Are hazard reviews completed on the conceptual design and during subsequent design phases for all new facilities or modifications to existing facilities?
- Prior to decommissioning or abandoning equipment, is the equipment subjected to the same reviews as those required for all new facilities or modifications to existing facilities?

4 PROCESS RISK MANAGEMENT

4.1 Hazard identification

The most important step in process risk management is hazard identification. *If hazards are not identified, they cannot be considered in implementing a risk reduction program, nor addressed by emergency response plans.*

For a quick guide to the hazardous rating of a site and assessment techniques that can be used, see Reference 4a. There are several methods for hazard identification such as **What If, Checklist, HAZOP, FMEA, Bow-tie Analysis, LOPA, Fault Tree Analysis**, etc. (see Reference 4d, which explains the techniques with examples of how to use them and also provides a detailed checklist in the appendices). The **Dow Fire and Explosion Index** and **Dow Chemical Exposure Index** (References 4b, 4c) are recommended as useful tools for assessing the degree of hazard.

4.2 Risk analysis of operations

Once hazards have been identified, the **risks** are estimated from the potential consequences and the likelihood of occurrence, using qualitative and/or quantitative methods such as Fault Tree, Event Tree, Risk Indices, etc. The total risk is then evaluated by comparing against criteria for acceptability (See Reference 4i).

4.3 Reduction of risk

Following risk evaluation, steps must be taken to reduce those risks which are deemed unacceptable. Such steps might include: inventory reduction, alternative processes, alternative materials, improved training and procedures, protective equipment, ensuring that items identified from hazard and risk analysis are closed off, etc.

Inherent safety is an approach that eliminates or greatly reduces hazards by design of the process. Strategic decisions typically must be implemented early in the process design, but are inherent, passive and thus less prone to failure. Tactical decisions can be implemented late in process design, but are characterized by repetition and high costs. Being active and procedural in nature, they need continuous supervision to remain effective. Inherent safety is therefore best applied in a hierarchy:

- *Minimize*: Use smaller quantities of hazardous substances.
- *Substitute*: Replace a material with a less hazardous substance.
- *Moderate*: Use less hazardous conditions, a less hazardous form of a substance, or facilities which minimize the impact of the release of hazardous material or energy.
- *Simplify*: Design processes and facilities which eliminate unnecessary complexity and are forgiving of operating errors.

4.4 Residual risk management

Since risk cannot be completely eliminated, plans are needed to control the residual risk of incident occurrence within acceptable limits and mitigate effects should an incident occur. It is vital to document the rationale and resolution of all recommendations.

There should be a written emergency response plan containing, as a minimum:

- Emergency escape routes and evacuation procedures;
- Procedures for those required to operate critical systems;
- Procedures to account for people following an evacuation (headcount);
- Rescue and medical duties;
- Emergency reporting procedures;
- Emergency response procedures (fire suppression, spill control, etc.);
- Organizational responsibilities during an emergency.

Each site should have a site wide alarm and/or communication system which:

- Has distinctive alarms to indicate alert, evacuate and "all clear";

- Has an easily remembered means of activation (e.g. a special telephone number);
- Is regularly tested and maintained.

Employees should be trained in the use of the emergency plan and regular drills carried out to test its effectiveness. Copies of the plan should be easily available to all employees.

In addition to the minimum requirements, a good plan will contain:

- Coordination with local community fire department and/or other response personnel;
- Provisions for visitors, contractors and the handicapped;
- Designated assembly areas with alternatives if needed;
- Establishment of an emergency control centre sited in a safe area;
- Internal and external communications.

Where emergencies could result in serious offsite impacts, vigilance should be maintained on land use developments in the surrounding area to ensure buffer zones are sufficient for present and potential future site activities.

Also see Reference 4h for more information on emergency preparedness and Reference 4j on land-use planning.

4.5 Process management during emergencies

Plans should cover management of both the process where the emergency occurs and also other processes which interact with or are near to that process.

4.6 Encouraging client and supplier companies to adopt similar risk management practices

The purpose of this step is to minimize the risks of incidents at upstream/downstream facilities and while materials are being transported between sites. This will help reduce incidents, ensure continuity of production and avoid litigation.

4.7 Selection of businesses with acceptable risk

Sometimes risks cannot easily be reduced to an acceptable level, or the cost of doing so is prohibitive, in which case it may be necessary to exit a business. For new businesses or acquisitions, this situation can be avoided through the Capital Project Review process (see Section 3).

Questions on Element 4 PROCESS RISK MANAGEMENT

Note: The questions on preparedness under this element cover those aspects of the former MIACC Community Self-assessment Tool that are typically a site responsibility. Aspects for which the community is responsible are not shown here; for more information contact the relevant provincial emergency measures organization.

Essential - Prevention

- (a) Is there a system in place, conducted by competent personnel, to identify and assess the process hazards from materials and situations present at this site?
- (b) Does the system ensure review and mitigation or acceptance of risks at the appropriate worker and management level?
- (c) Is there either: guidance in place to identify the type of risk assessment methodology that should be used to assess the risk; or does the facility use at least the What If and/or Checklist method for assessing risks?
- (d) Has the facility completed at least one comprehensive documented facility process hazard review?
- (e) Are corrective actions from risk assessment and process hazard review documented and followed up?

Essential - Preparedness

- (f) Is there a documented site emergency response plan that includes the following:
 - (i) A list of the plant hazards and associated risks;
 - (ii) A response plan covering each potential major incident scenario;
 - (iii) A list of resources to support the plan (personnel, equipment, supplies)?
- (g) Is there a system that ensures the plan is kept current and periodically tested?
- (h) Has the site designated a representative to act as a spokesperson during an emergency?
- (i) Has the site communicated its emergency response capability and resources to the community?
- (j) Has the site undertaken a program to inform the community about site-related hazards and what to do in case of an emergency?

Enhanced - Prevention

- (a) Does the facility use the following techniques to form part of the site risk management system when there is potential for a major process risk (must use at least two to achieve “enhanced” status):
 - (i) What If and/or Checklists;
 - (ii) Failure modes and effects analysis (FMEA);
 - (iii) Dow Fire and Explosion Index (FEI) or Chemical Exposure Index (CEI);
 - (iv) Hazard and operability studies (HAZOP);
 - (v) Bow-Tie analysis;
 - (vi) Safety Integrity Levels (SILs);
 - (vii) Layer Of Protection Analysis (LOPA);
 - (viii) Fault Tree Analysis (FTA)?
- (b) Does the system indicate how human factors are integrated in the development of process hazard scenarios?
- (c) Does the system specify periodic process hazard reviews at defined intervals?

Enhanced - Preparedness

- (d) Has the site communicated potential emergency requirements to the local authorities for inclusion in the community emergency plan?
- (e) Has the site spokesperson been adequately trained on the strategy and process for disseminating information during an emergency?
- (f) Does the site participate in a joint emergency training program with its community?
- (g) Is the plan regularly audited for compliance and effectiveness?

Comprehensive - Prevention

- (a) Does the facility use the following techniques to form part of the site risk management system when there is potential for a major process risk (must use at least four to achieve “comprehensive” status):
 - (i) What If and/or Checklists;
 - (ii) Failure Modes and Effects Analysis (FMEA);
 - (iii) Dow Fire and Explosion Index (FEI) or Chemical Exposure Index (CEI);
 - (iv) Hazard and operability studies (HAZOP);
 - (v) Bow-tie Analysis;
 - (vi) Safety Integrity Levels (SILs);
 - (vii) Layer Of Protection Analysis (LOPA);
 - (viii) Fault Tree Analysis (FTA)?
- (b) Is there a process in place to categorize the risk of potential scenarios for control and mitigation?
- (c) Does the site monitor land use developments in the vicinity and intervene where these are incompatible with present and permitted potential site activities?

Comprehensive - Preparedness

- (d) Has the site established and documented mutual aid agreements with neighbouring industry?
- (e) Has the site developed and documented an emergency recovery plan to minimize disruption of the community by a site emergency?

5 MANAGEMENT OF CHANGE

A system to manage change is critical to the operation of any facility. A written procedure should be required for all changes except replacement in kind. The system should address:

- A clear definition of change (scope of application);
- A description and technical basis for the proposed change;
- Potential impact of the proposed change on health, safety and environment;
- Authorization requirements to make the change;
- Training requirements for employees or contractors due to the change;
- Updating of documentation including: drawings, process safety information, operating procedures, maintenance procedures, alarm and interlock settings, fire protection systems, etc.;
- Contingencies for "emergency" changes.

5.1 Change of process technology

While process changes occur for several reasons, it is essential that these changes do not compromise process safety. Changes must always be under proper control. Variance procedures should ensure proposed operation outside current operating limits is subject to prior review and approval by qualified personnel, who must be available if authority is needed at short notice.

5.2 Change of facility

Equipment changes may introduce additional hazards or increase risk. A management of change system should therefore include an assessment of hazards and risks associated with the change. Major equipment changes should be covered by the Capital Project Review (see Section 3). Procedures should also be used for smaller changes, since major hazards can be introduced by minor changes, e.g. a cross connection or instrumentation change. The procedure should be simple, but require approval by qualified personnel.

5.3 Organizational changes that may have an impact on process safety

Changes in organization must address the transition period as well as the way the new organization is to work. Even where no staff losses occur the change in reporting relationships can lead to problems. Departure of staff, and especially elimination of organizational units (e.g. through downsizing) pose special challenges since accountability and safe control of operations must continue despite the often sudden loss of key knowledge and skills.

5.4 Variance procedures

Exceptions can be expected for all procedures, and there should be systems to allow exceptions to be promptly managed and under control. Though variance procedures call for review and approval by qualified personnel, they should be easy to use. The system should ensure all involved understand the basis for the approval and the new limits established for the variance.

5.5 Permanent changes

Permanent changes should be subject to the usual steps of planning, organizing, implementation and control, and should be handled in conjunction with other plant programs such as the systems for work order, purchase order, Capital Project Design and Review, etc. Appropriate risk management should be a part of this process.

5.6 Temporary changes

Temporary changes should be subject to conditions similar to those applied to permanent changes, and the time limit for the change should be clearly defined. Steps must also be taken to ensure all equipment, etc. is returned safely to normal conditions at the end of the change.

Questions on Element 5 MANAGEMENT OF CHANGE

Essential

- (a) Is there a system to manage any modifications to:
 - (i) Technology/materials/products;
 - (ii) Equipment/controls/software/process operations?
- (b) Does the system cover temporary, experimental and emergency work?
- (c) Does the system ensure all changes including operating procedures are reviewed for hazards prior to commissioning, startup, shutdown or implementation of the change?
- (d) Are personnel informed of the change and given any necessary training before they are expected to operate the facility?

Enhanced

- a) Does the site's Management of Change (MOC) system include the following characteristics:
 - (i) Definition of change;
 - (ii) Rationale for change with associated risks of (not) doing the change;
 - (iii) Approval requirements;
 - (iv) Time sensitive change limitations (e.g. temporary, emergency, weather);
 - (v) Verification and closure of identified hazards?

Comprehensive

- a) Is there a system to manage any modifications to individual/organizational responsibilities?
- b) Is there a system to provide refresher training on how to conduct process hazards analysis during the MOC process?
- c) Is the MOC system integrated into the facility's ongoing process risk management system?

6 PROCESS AND EQUIPMENT INTEGRITY

Procedures for fabricating, inspecting and maintaining equipment are vital to process safety. Written procedures should be used to maintain ongoing integrity of process equipment such as:

- Pressure vessels and storage tanks;
- Piping, instrumentation and electrical systems;
- Process control software;
- Relief and vent systems and devices;
- Emergency and fire protection systems;
- Controls including monitoring devices and sensors, alarms and interlocks;
- Power transformers, elevating devices, cranes; and
- Rotating and hydraulic equipment.

A documented file should be maintained for each piece of equipment.

6.1 Reliability engineering

Equipment critical for process safety should be identified so that schedules can be established for monitoring and inspection to enable cost effective correction of problems before they develop to the critical stage.

6.2 Materials of construction

Systems should be established where necessary to supplement industry standards such as piping and pressure vessel codes. Critical items may need special tracking to verify materials used are as specified.

6.3 Fabrication and inspection procedures

Quality assurance should include a materials control system which ensures installed equipment:

- Meets the requirements of the design specification;
- Is traceable to its manufacturer;
- Has met all required testing, with test results available on site; and
- Is labelled to be clearly identifiable to those doing installation.

6.4 Installation procedures

Critical steps in installation should be identified during planning, and field inspection used to verify that installation corresponds to design.

6.5 Preventative maintenance

The preventative maintenance (PM) system should include:

- A method of identifying critical equipment;
- A method to establish PM frequencies for critical equipment;
- A mechanism to ensure PM is done at the specified frequency; and
- A record of the above.

Risk-based inspection may also be used to assist in managing inspection and maintenance resources while ensuring that critical equipment is fit for service.

6.6 Process, hardware and systems inspection and testing (pre-startup safety review)

Pre-startup safety reviews should be conducted before commissioning a new or modified process, replacing equipment or recommissioning mothballed equipment. The review should cover both equipment and operating procedures to ensure that all elements are in place and functional.

Subsequent inspection and testing of process equipment should then be:

- According to **good engineering practices**;
- At a frequency determined by applicable codes and standards, or more frequently if operating experience suggests this is necessary;
- With a system to ensure corrective action is taken when results fall outside of acceptable limits; and
- With documentation that includes:
 - Date of inspection;
 - Name of inspector;
 - Serial number or other equipment identifier;
 - Description of the tests done;
 - Results of the inspection or test, and
 - Recommended action.

6.7 Maintenance procedures

Proper control of maintenance should include safe work practices which apply to both employees and contractors, such as:

- Permits to work and their application (hot work, confined space entry, lock out/tag out, excavation, **master tag**, etc.);
- Opening of process equipment; and
- Control of access to the facility by maintenance, contractor, laboratory and other personnel and vehicles.

6.8 Alarm and instrument management

Proper alarm and instrument management includes not only equipment hardware but also computer components and software instructions for process control. These may be addressed via **functional safety** (e.g. under IEC 61511/61508) or **safety instrumented systems**, and should include:

- Identification and prioritization of critical alarms and interlocks;
- A procedure to control changes to alarm set points and interlock systems; and
- A system of regular testing of interlock systems and pressure safety valves (PSVs).

6.9 Decommissioning and demolition procedures

Procedures should address safe removal from service, dismantling, decontamination and related disposal of waste.

Questions on Element 6 PROCESS AND EQUIPMENT INTEGRITY

Essential

- (a) Is there a system to ensure critical equipment:
 - (i) Is adequately specified;
 - (ii) Is designed and fabricated to specifications;
 - (iii) Is correctly installed and commissioned;
 - (iv) Is operated within design limits; and
 - (v) Is correctly maintained?
- (b) Does the system cover:
 - (i) Raw material suitability;
 - (ii) Materials of construction compatibility;
 - (iii) Fabrication/installation and inspection procedures;
 - (iv) Preventative/predictive maintenance procedures; and
 - (v) Critical instrument programs.
- (c) Are written operating procedures in place and accessible, covering startup, shutdown, normal and emergency conditions?
- (d) Are systems established and enforced for:
 - (i) Confined space entry;
 - (ii) Safe control of maintenance/project work, including by contractors;
 - (iii) Lock/tag out to prevent unplanned release of materials;
 - (iv) Opening potentially hazardous lines or equipment;
 - (v) Control of hot work; and
 - (vi) Master tag?

Enhanced

- (a) Are operating procedures reviewed on a defined frequency and updated as necessary?
- (b) Are written procedures in place for the inspection and testing of critical equipment?
- (c) Are facility inspections conducted on a routine basis to identify substandard conditions?

Comprehensive

- (a) Are facilities designed and built to engineering standards and recognized and generally accepted good engineering practice?
- (b) Are risk-based inspection programs in place?
- (c) Are there systems to ensure asset integrity via:
 - i) Design integrity;
 - ii) Technical integrity; and
 - iii) Operating integrity?

7 HUMAN FACTORS

Human factors are a significant contributor to many process incidents. Three key areas are operator–process/equipment interface, administrative controls and human error assessment.

7.1 Operator–process/equipment interface

Design of equipment may increase the potential for error. Examples are: confusing equipment, positioning of dials, colour coding, different directions for on/off etc. Computerized control systems can confront operators with unmanageable amounts of information during an upset condition. Interfaces which should be examined for potential problems are:

- Alarm display;
- Information display; and
- Ergonomics.

A task analysis (a step-by-step approach to examine how a job will be done) can be used to determine what can go wrong during the task and how these potential problem areas can be controlled.

7.2 Administrative control versus engineering control

Hazards may be controlled by the use of procedures or by the addition of protective equipment. This balance is often a matter of company culture and economics.

If procedures are well understood, kept current and are used, then they are likely to be effective. Similarly, protective systems need regular testing and maintenance to be effective. The problem of administrative versus engineering controls should be considered and a balance selected by conscious choice rather than allowing it to happen by default.

7.3 Human error assessment

Human error is a fact of life. Individuals and organizations do not perform reproducibly until failure like machines, but behave in ways which are strongly influenced by intention or choice and thus by such factors as understanding, judgment and motivation. Actions may vary depending upon the individual or the situation.

Effective PSM calls for an understanding of human error so that systems can be devised to prevent its occurrence or mitigate its effects. This applies to all aspects of PSM including design, construction, maintenance and operation.

Human error should therefore be treated as normal when designing equipment, procedures, etc. By anticipating likely human failure modes, the system can be designed to facilitate both recognition of when an error has occurred and recovery to a safe state.

Common human failure modes include:

- Slips and lapses, where instructions are followed but a step is missed or performed at the wrong time;
- Mistakes, where the instruction being followed is not appropriate for the situation; and
- Violations, where an instruction is willfully disregarded.

It is useful, apart from looking at the ways in which people can fail, to consider also how they function normally. There are three main behaviour modes:

- Knowledge-based, which is used when no rules apply but some appropriate action must be found. It is the slowest, but most flexible approach;
- Rule-based, where decisions have been codified into a series of “If..., Then...” situations; the rules do not necessarily need to make sense — they only need to work, and users need to know the conditions under which a particular rule applies; and

- Skill-based, which consists of rapid responses to internal states with only occasional attention to external information to check that events are going according to plan; this often starts out as rule-based behaviour.

Typically, process design and initial start-up is largely knowledge-based, and important aspects of this knowledge are then codified into rule-based policies and procedures for ongoing operation. As operation by the rules becomes more familiar, behaviour then becomes more skill-based. The implications of this should be taken into account when assessing human error, because the nature of error differs by mode. Common examples are failing to spot hazards or underestimating their significance in knowledge-based mode, and following the wrong rule or applying it in the wrong way in rule-based mode. In skill-based mode, actions involve far less conscious thought about the task at hand, which often takes place in the background while most of the attention is on something else. This is why relying on careful behaviour is not an effective defence at the skill-based level — it is far better to design for easy error detection and recovery, as noted above.

Human error assessment should include understanding of both **active** and **latent failures**. Active failures are those that cause an immediate adverse effect, such as opening the wrong valve. Latent failures are those where the effect may not be noticeable for some time, if at all, but have allowed a gap to form or exist so that, in certain conditions, an incident could occur. Latent failures are often due to management or design error in failing to foresee or allow for effects of decisions.

See Reference 7b for an explanation of this subject.

Questions on Element 7 HUMAN FACTORS

Essential

- (a) Is there a system in the design of equipment, work stations or operating procedures to consider the potential for human error?
- (b) Is there a system that will identify, communicate and address potential human errors associated with routine and non-routine tasks?

Enhanced

- (a) Does the system consider the following in the control of human factor-related issues:
 - (i) Compatibility of interface between operator and process/equipment;
 - (ii) The balance between administrative controls (e.g. systems and procedures) and engineering controls; and
 - (iii) The use of aids such as checklists, pictures, diagrams, etc. in (operating) procedures to help reduce the potential for human error?
- b) Does the system include guidance on use of at least two of the following techniques to identify human factors issues:
 - i) Checklist;
 - ii) Interviews;
 - iii) Questionnaires;
 - iv) Hazard and operability studies (HAZOP);
 - v) Failure modes and effects analysis (FMEA)?

Comprehensive

- (a) Does the site have a system to consider the following in the control of human factor-related issues:
 - i) Understanding of the different characteristics of skill, rule and knowledge-based behaviour modes; and
 - ii) The potential effects of latent (as well as active) errors?
- b) Is formal assessment of human error potential taken into account in the design and operation of the facility?

8 TRAINING AND PERFORMANCE

Personnel need to be trained in the right skills and to have ongoing retraining to maintain these skills. The following sections describe the steps in achieving this.

8.1 Definition of skills and knowledge

Key functions should be identified and their required skills, knowledge and abilities documented. Training is then given to ensure people doing these jobs are capable of doing them properly.

8.2 Design of operating and maintenance procedures

The job procedures, together with job descriptions and job safety analysis, provide the building blocks for development of training programs.

8.3 Initial qualifications assessment

Specification, testing and evaluation can be used to ensure prospective employees have the aptitude and base knowledge/skills which, with appropriate training, will enable them to do the job.

8.4 Selection and development of training programs

Both employees and contractors must be trained to understand and use site safety systems. Particular areas which should be covered include:

- General safety rules;
- Permit to work procedures;
- Use of personal protective equipment;
- Emergency procedures;
- Specific hazards of the area in which they will be working; and
- Specific hazards of the materials which they may encounter.

A competency test should be administered to employees and contractors to ensure the information given has been understood. It is especially important that people supervising contractors understand the training given.

8.5 Measuring performance and effectiveness

A method of testing or verification should be used to ensure the training is understood to a level consistent with doing a job safely.

8.6 Instructor program

Specific criteria should be used for instructor selection and training to ensure instructors have sufficient teaching/communications skills as well as the necessary technical knowledge.

8.7 Records management

Records of training received by each person in each task are needed. These should include: the name of the trainer, the date of the training and the results of the competency verification. This document is then used to track training received and to schedule retraining.

8.8 Ongoing performance and refresher training

Refresher training is needed to ensure skills/personnel remain at a level consistent with the safe operation of facilities. This is especially true where procedures are changed and/or new equipment is added.

Questions on Element 8 TRAINING AND PERFORMANCE

Essential

- (a) Is there an evergreen documented inventory of job positions and associated minimum and desired knowledge, skills and capabilities needed to sustain safe operation of the facility?
- (b) Does the above cover both normal and a defined range of non-normal situations?
- (c) Is training — if needed — provided in time to ensure the above requirements are met and maintained?
- (d) Is competence tested after training is completed?

Enhanced

- (a) Is there a system of establishing initial qualifications to ensure prospective employees have the aptitude and base knowledge/skills which, with appropriate training, will enable them to fulfill the requirements of their function?
- (b) Is formal and periodic training conducted in:
 - (i) Operating and maintenance procedures;
 - (ii) Process hazards and designated substances;
 - (iii) Emergency preparedness/release mitigation;
 - (iv) Work permit systems;
 - (iv) Personal protective equipment; and
 - (v) Relevant regulations, codes, standards, industry practices and company policy?
- (c) Does the training program include periodic or 'just-in-time' refresher training?

Comprehensive

- (a) Are instructor qualifications defined and competence tested?
- (b) For each of the Essential, Enhanced and Comprehensive levels, are all items covered under element 8: Training and Performance formally documented?
- (c) Is there a career progression plan with associated training for each employee?
- (d) Is the training program designed to support the back-up, short-term and long-term succession plan for the organization?

9 INCIDENT INVESTIGATION

9.1 Major incidents

Investigation of **incidents**, including **near misses**/abnormal events, is a vital part of PSM.

Minimum requirements for incident investigation include:

- A clear definition of what is meant by “major incident” and any other categories used for classification;
- Investigation of every actual or potential **process-related incident**;
- Investigation done promptly by a team with at least one person knowledgeable in the process (see Reference 9a);and
- A report to management following the investigation stating:
 - Incident date;
 - Incident description;
 - Factors which contributed to the incident; and
 - Recommendations to prevent recurrence.

In addition to these minimum requirements, a good system should include:

- Procedures for doing an investigation; and
- Training of people involved in investigation, with emphasis on **root cause analysis**.

9.2 Third party participation

The presence of external team members encourages objectivity, fresh perspectives, specialist skills and freedom from bias, and adds to the credibility of the investigation.

9.3 Follow-up and resolution

Investigating incidents is of little use unless accompanied by follow-up. The follow-up system should address the recommendations made in the report and ensure timely implementation of corrective actions.

9.4 Communication

Key results of the investigation should be shared, as appropriate, with other parts of the plant, the organization, and the process industry and other industries where the lessons learned could usefully be applied.

9.5 Incident recording, reporting and analysis

Recording of incidents enables a system of analysis of incident reports to identify opportunities for elimination of commonly recurring causes.

9.6 Near-miss reporting

Lessons from near-misses are often as important as from actual incidents. Significant near-misses and abnormal events should be recorded and analyzed as part of the incident investigation system.

Questions on Element 9 INCIDENT INVESTIGATION

Essential

- (a) Is there a documented program to report and investigate all significant incidents (spills, leaks, fires, explosions, injuries, etc.)?
- (b) Are basic causes and corrective action determined?
- (c) Does the system document actions required, responsibilities and follow-up?
- (d) Is there a list of incident investigation methodologies that are used with qualified personnel to lead the investigation?

Enhanced

- (a) Does the documented program to report and investigate all significant incidents also cover near-misses?
- (b) Are investigation reports communicated to all appropriate personnel throughout the organization?

Comprehensive

- (a) Does the feedback include lessons learned, both from within the company and elsewhere, and actions taken to eliminate future incidents, and are these formally incorporated into corporate standards?
- (b) Is incident data analyzed for adverse trends and are corrective actions implemented to address these adverse trends?
- (c) Are lessons learned from incident investigations shared with industry peers and other organizations?

10 COMPANY STANDARDS, CODES AND REGULATIONS

A **management system** is needed to ensure the various internal and external published guidelines, standards and regulations are current, disseminated to appropriate people and departments, and applied throughout the organization.

10.1 External codes/regulations

Legislated items include, for example:

- Environmental regulations;
- Occupational health and safety regulations;
- Planning and zoning regulations;
- Boiler and pressure vessel codes;
- Electrical and building codes; and
- Fire codes.

External standards include such items as:

- Industry-wide standards such as those published by the American Petroleum Institute (API), American Society of Mechanical Engineers (ASME), American Society for Testing and Materials (ASTM) and American National Standards Institute (ANSI).;
- Professional technical bodies such as CCPS, AIChE design groups (e.g. the Design Institute for Emergency Relief Systems (DIERS)), CSE, Chlorine Institute; and
- National/international codes, such as those published by the Canadian Standards Association (CSA), National Fire Protection Association (NFPA), International Labour Office (ILO), etc.

10.2 Internal standards

These take many forms depending upon the nature of the operation. Typical examples include:

- General standards (e.g. maintenance practices (hot work, inspection, etc));
- Reporting procedures (incident reporting, equipment data etc.) and behaviour in plant areas (smoking, driving, etc.);
- Specific process standards (e.g. chemistry, process design principles, metallurgy, etc.); and
- Mechanical, electrical, civil, and instrument design standards.

Questions on Element 10 COMPANY STANDARDS, CODES AND REGULATIONS

Essential

- (a) Is there a documented system that is kept current on the laws, regulations, standards, codes, etc. applicable to site operations?
- (b) Is there a system to implement and ensure compliance with current laws, regulations, standards, codes, etc.?

Enhanced

- (a) Is there a system for monitoring emerging developments in laws and regulations likely to be applicable to site operations?
- (b) Is there a system to monitor non-regulated industry good practice (e.g. codes, standards)?

Comprehensive

- (a) Is there a system for monitoring emerging developments in standards, codes, etc. likely to be applicable to site operations?
- (b) Does the organization participate in providing reviews and comments invited by regulators and industry committees?



11 AUDITS AND CORRECTIVE ACTIONS

The purpose of safety audits is to determine the status and effectiveness of safety management efforts versus goals and also the progress toward those goals. Some types of audits are listed below.

11.1 PSM systems audits

Management systems audits verify that the systems are effective in ensuring company/plant policies and procedures are being implemented. They also identify opportunities where systems may be strengthened.

11.2 Process safety audits

Process safety audits provide increased assurance that facilities are being operated and maintained in a way which properly protects the safety and health of those on site, the environment, the surrounding community, plant assets and continuity of operations.

11.3 Compliance reviews

Compliance reviews verify adherence to regulations and to company/plant standards and procedures.

11.4 Internal/external auditors

Audits should be conducted by trained personnel and partially staffed with expertise from outside the plant to provide objectivity and fresh ideas.

11.5 Corrective actions

The most important result of an audit is corrective action to reduce risks. An action plan to resolve recommendations with assigned responsibilities is needed. There must be a follow-up system to verify completion and track/report outstanding recommendations. This should include a high-level review to ensure the balance between company expectations and actual performance is reasonably consistent and that **normalization of deviance** is within acceptable limits.

Questions on Element 11 AUDITS AND CORRECTIVE ACTIONS

Essential

- a) Is there a basic audit/inspection system to regularly assess whether the PSM systems covered at this level are indeed being applied?
- b) Does the system include a mechanism to report the findings from the audit and communicate them to the stakeholders?
- c) Is there a process to track completion of plans to address the reported findings?

Enhanced

- a) Does the audit process formally assess:
 - (i) Compliance with laws and regulations;
 - (ii) PSM systems (to ensure company policies, procedures, etc. are being followed and are also effective in achieving the design intent);
 - (iii) Safety and health of employees and contractors; and
 - (iv) Effects of the facility on the environment and the community?
- b) Does the audit system include internal self-assurance audits?

Comprehensive

- a) Is there a system for benchmarking audit processes and techniques against best industry practice?
- b) Are audits completed by competent personnel using generally recognized procedures for sampling and verification?
- c) Does the audit system include independent management assurance audits?

12 ENHANCEMENT OF PROCESS SAFETY KNOWLEDGE

A management system for process safety should be designed for continuous improvement. Safety requirements are becoming more stringent, while knowledge of systems and technology is growing (e.g. consequence modeling techniques). Safe operation of a process plant calls for personnel to stay abreast of current developments, so that policy decisions on their application can be made on the basis of informed knowledge.

12.1 Quality control programs and process safety

Programs for quality control of production, services, environment, etc. share many common features with PSM, and there are benefits in an integrated approach that applies the concepts of quality management programs, such as establishing goals, monitoring and reporting of progress (e.g. Plan, Do, Check, Act) to PSM. This can help defend against normalization of deviance.

12.2 Professional and trade association programs

Many of the programs and resources developed by professional and trade associations can be useful for enhancing process safety knowledge, as tools and support may have been adapted for the specific needs of an industry or sector. Companies should therefore encourage participation in such bodies, so that they can monitor developments, communicate relevant information to those within the company who could benefit from it, and also provide input to those external bodies.

12.3 Technical association programs

Participation in bodies with a focus on PSM enables access to tools and resources but also to networks of organizations and individuals with specialized knowledge on every aspect of PSM. These bodies include the CCPS and its parent AIChE, API and, in Canada, the CSE PSM division.

12.4 Research, development, documentation and implementation

Research and development programs should include process safety inputs from departments such as safety, environment, operations, engineering, and maintenance. Data supplied from research projects should be documented, available to those who need to know, and communicated to plant operations to ensure that new knowledge is incorporated into the enhancement of process safety.

12.5 Improved predictive systems

Information contained in incident reports, equipment failures, and maintenance records should be catalogued and analyzed for opportunities for continuous improvement in process safety.

12.6 Process safety resource centre and reference library

Safety information should be readily accessible, and thus there is a minimum requirement for a process safety resource system. This may be quite simple for a small organization but should nevertheless contain:

- Material relevant to the design technology and operation of the process; and
- A search facility available locally or through arrangement with another organization (e.g. a large reference library accessible locally or via the Internet).

Examples of material contained in such a system might include:

- Incident reports;
- Plant equipment design data;
- Design practices and specifications;
- Appropriate laws and regulations;
- Trade association information;
- Physical and chemical properties, including reaction kinetics and safe handling information;
- Technical papers;
- Case histories concerning incidents which illustrate PSM principles; and
- Appropriate reference books.

Questions on Element 12 ENHANCEMENT OF PROCESS SAFETY KNOWLEDGE

Essential

- a) Is there a search facility for finding information on process safety, either in the company or via external means such as a reference library, the Internet, etc.?
- b) Is there a system to ensure growth in process safety knowledge through (any one of the following for Essential):
 - i) On the job;
 - ii) Self-directed study;
 - iii) Service on technical committees;
 - iv) Formal instruction;
 - v) Presentations;
 - vi) Reviews, publications;
 - vii) Learning from internal or external incidents?

Enhanced

- a) Is there a system to ensure growth in process safety knowledge through (any two of the following for Enhanced):
 - i) On the job;
 - ii) Self-directed study;
 - iii) Service on technical committees;
 - iv) Formal instruction;
 - v) Presentations;
 - vi) Reviews, publications;
 - vii) Learning from internal or external incidents?

Comprehensive

- (a) Is there a system for staying abreast of changes in safety requirements, developments in safety systems and technology, etc. regarding:
 - (i) Materials and processes used on site; and
 - (ii) Process industries, etc. in general?

GLOSSARY AND DEFINITIONS

Active and Latent Failures: Active failures are acts or conditions directly precipitating the incident situation. They usually involve the front-line staff, the consequences are immediate and can often be prevented by design, training or operating systems. Latent conditions are the managerial influences and social pressures that make up the culture, influence the design of equipment or systems, and define supervisory inadequacies. They tend to be hidden until triggered by an event. Latent conditions can lead to latent failures arising from human error or violations. Latent failures may occur when several latent conditions combine in an unforeseen way.

API, ASME, etc: These acronyms refer to industry standards setting, testing and certifying bodies. Examples include:

- American National Standards Institute (ANSI)
- American Petroleum Institute (API)
- American Society of Mechanical Engineers (ASME)
- American Society for Testing and Materials (ASTM)
- Canadian Standards Association (CSA)
- Chlorine Institute
- Design Institute for Emergency Relief Systems (DIERS)
- International Electrotechnical Commission (IEC)
- International Labour Organization (ILO)
- National Fire Protection Association (NFPA)

Bow-Tie Analysis: A simple and effective tool for communicating risk assessment results, combining simplified Fault and Event Trees in one diagram to show clearly the links between the potential causes, preventative and mitigative controls and consequences of a major incident. Bow-tie diagrams may be used to display the results of various types of risk assessments and are useful training aids. They may also be integrated with semi-quantitative analysis techniques such as LOPA depending on the level of complexity required.

Buffer Zone: Refers to a controlled area separating the public and other facilities from the consequences of a **process-related incident**.
(Contact CSChE for more information on buffer zones.)

Critical: An adjective describing actions, conditions, systems, procedures, or equipment which are indispensable to the safe and environmentally responsible operation of a facility.

DOW Chemical Exposure Index: A method of rating the relative potential of acute health hazard to people from possible chemical release incidents. See Reference 4c.

DOW Fire and Explosion Index: A step-by-step quantitative evaluation of the realistic fire, explosion and reactivity potential of process equipment and its contents. See Reference 4b.

Fault Tree Analysis: A deductive technique that focuses on one particular incident scenario or main system failure, and provides a method for determining causes of that event. See Reference 4d.

Failure Modes and Effects Analysis (FMEA): A systematic, tabular method for evaluating and documenting the causes and effects of known types of component failures. See Reference 4d.

Good Engineering Practices: Those practices generally accepted in the industry as necessary to ensure the safe operation of a facility.

Hazardous Material: A substance (gas, liquid or solid) capable of creating harm to people, property or the environment (e.g. materials which are flammable, toxic, etc.).

Hazard and Operability Study (HAZOP): A systematic method in which process hazards and potential operating problems are identified using a series of guidewords to investigate process deviations. See References 4d, 4g.

Incident: Any unplanned event that did, or easily could have, resulted in undesirable consequences.

Layer of Protection Analysis (LOPA): A semi-quantitative method of risk assessment which lies between qualitative techniques such as **HAZOP** or **PHA** and full quantitative risk analysis. Used to determine safety integrity levels under standards such as IEC 61511.

Management System: A system intended to achieve (a) specific objective(s). Components of a management system include:

- Clearly stated objective(s);
- Clearly defined responsibilities for achieving this (these) objective(s);
- Tools, resources, procedures and schedules necessary to achieve this (these) objective(s);
- A means of measuring progress, and
- A feedback and control mechanism to correct deviations.

Master Tag: A permit which lists all tags, lockouts, etc. placed on equipment for a given job as part of a temporary change, maintenance work order, etc. The master tag enables subsequent return of all equipment settings (such as valve positions) to the original status even if done by a different team from those who took the equipment out of service.

Near Miss: An event that generates no actual adverse consequences, but could easily have done so with a slight change in circumstances.

Normalization of Deviance: A long-term phenomenon in which individuals or teams repeatedly accept a lower standard of performance until that lower standard becomes the normal.

Process Hazard Analysis (PHA): The action of identifying undesired events which could lead to the materialization of a hazard and the estimation of the magnitude and likelihood of any harmful effects resulting from this materialization.

Process Flow Diagram: A drawing showing the major equipment and design flows of a process in diagrammatic form. The drawing is intended to show the process design basis in the form of temperatures, pressures, heat balance and mass balance.

Process Hazard: A physical situation with a potential for human injury, damage to property or damage to the environment through the release of energy in the form of fire, explosion, toxicity or corrosivity.

Process-Related Incident: Unintended, episodic event of the following type which results from the failure of process equipment or its operation:

- Explosion or implosion;
- Fire;
- Exposure to hazardous material(s); and/or
- Release of hazardous materials or energy.

Risk: A measure of the likelihood and consequence of a specified undesired event occurring within a specified period or in specified circumstances.

Risk-Based Inspection (RBI): A method that uses risk as the basis for prioritizing and managing inspection whereby inspection and maintenance resources are allocated to provide a higher level of coverage on equipment, etc. having a higher risk than on that where the risk is lower. See Reference 6a.

Root Cause Analysis: A method of examining incidents which looks beyond the immediate causes to identify the systemic underlying factors which allow a hazardous situation to occur. See Reference 9a.

Traditional Occupational Health and Safety: The protection of people from hazards not caused by process-related incidents.

Worst Credible Scenario: While it is not possible to define this precisely, the following suggestions may help:

- Incidents which have already happened somewhere in the industry;
- A scenario with a predicted frequency of 1 in 10,000 years or less;
- Incidents involving less than three simultaneous and independent failures;
- Release of 100% of hazardous material in the system over a period of 30 minutes; or
- Complete failure of equipment as a result of known causes such as metal embrittlement.

REFERENCES

This guide is an introduction to the accompanying *PSM Standard* (ISBN: 978-0-920804-97-1) which is available on the CScHE's website on the PSM Subject Division page (www.cheminst.ca/PSM). The Standard identifies the requirements of a management system for implementing PSM at facilities handling or storing potentially hazardous materials.

The Internet now provides information and references on many elements of PSM, but the short list below covers some of the most useful references. A list of suggested search strings is also available on the CScHE's PSM Subject Division website to help when searching the web for information on specific PSM elements or components. Operators of hazardous installations in Canada may also be able to get over-the-phone help from a member of the Division in navigating and using the reference material. Contact the division through the website for more information.

1. Accountability and General References

- a) CCPS, *Guidelines for Technical Management of Chemical Process Safety*, 1989, ISBN 0-8169-0423-5.
- b) CCPS, *Plant Guidelines for Technical Management of Chemical Process Safety*, 1992, ISBN 0-8169-0499-5.
- c) CCPS, *Guidelines for Risk Based Process Safety*, 2007, ISBN 978-0-470-16569-0.
- d) Hopkins, A., *Safety, Culture and Risk: The Organisational Causes of Disasters*, 2005, ISBN 1-921022-25-6.
- e) U.S. Occupational Safety and Health Administration, 29-CFR-1910.119, *Process Safety Management of Highly Hazardous Chemicals*.
- f) Crowl, D.A. and Louvar, J.F., *Chemical Process Safety: Fundamentals with Applications* (3rd Edition) Prentice Hall, 2011, ISBN-10: 0131382268, ISBN-13: 978-0131382268
- g) *Lees' Loss Prevention in the Process Industries: Hazard Identification, Assessment and Control* (3rd Edition); Sam Mannan (Editor); ISBN 10: 0-7506-7555-1, ISBN 13: 978-0-7506-7555-0
- h) CCPS, *Guidelines for Process Safety Metrics*, 2009, ISBN 978-470-57212-2.

2. Process Knowledge and Documentation

- a) CCPS, *Guidelines for Process Safety Documentation*, 1995, ISBN 978-0-8169-0625-3.
- b) American Petroleum Institute, *Risk Based Decision Making*, API publication 1628B, 1996.

3. Capital Projects Review and Design

- a) Kletz, T.A., *Process Plants: A Handbook for Inherently Safer Design*, CRC, 1998, ISBN 1560326190.
- b) CCPS, *Guidelines for Facility Siting and Layout*. 2003 ISBN 978-0-816-90899-8
- c) CCPS, *Guidelines for Equipment Design for Process Safety*. 1993, ISBN 0-8169-0565-7
- d) CCPS, *Guidelines for Performing Effective Pre-Start-up Safety Reviews*, 2007, ISBN: 978-0-4370-13403-0
- e) Cheremisinoff, N., *Pressure Safety Design Practices for Refinery and Chemical Operations*. William Andrew, 1998, ISBN 0-8155-1414-X.

4. Process Risk Management

- a) CScHE, *A Quick Guide to Identifying Process Hazards and Flowchart*, available on the PSM division website.
- b) AIChE, *Dow's Fire and Explosion Index Hazard Classification Guide*, latest edition, ISBN No. 0-8169-0623-8.
- c) AIChE, *Dow's Chemical Exposure Index*, latest edition, ISBN 0-8169-0647-5.
- d) CCPS, *Guidelines for Hazard Evaluation Procedures. Third Edition with Worked Examples*, 2008. ISBN-10: 0471978159, ISBN-13: 978-0471978152.
- e) Conseil pour la réduction des accidents industriels majeurs (CRAIM), *Risk Management Guide for Major Industrial Accidents*, 2007 edition, available from www.craim.ca.
- f) Environmental Protection Agency (US) Risk Management Program guidance, www.epa.gov/oem/content/rmp/rmp_guidance.htm#General.

- g) Kletz, T. A., *Hazop and Hazan: Identifying and Assessing Process Industry Hazards* (3rd Edition), CRC, 2008, ISBN-10: 1560322764, ISBN13: 9781560322764.
- h) Canadian Standards Association, *Emergency Preparedness and Response*, CAN/CSA-Z731-03.
- i) CScHE, *Risk Assessment Recommended Practices for Municipalities and Industry*, 2004, ISBN No. 0-920804-92-6, available on the PSM division website.
- j) Major Industrial Accidents Council of Canada, *Risk-based Land Use Planning Guidelines*, 1995, available on the PSM division website.
- k) Greenberg, H.R., and Cramer, J. J., *Risk Assessment and Risk Management for the Chemical Process Industry*, John Wiley and Sons, 1991, ISBN 0-4712-8882-9.
- l) Knowlton, R. Ellis, *A Manual of Hazard and Operability Studies - the Creative Identification of Deviations and Disturbances*, 1992, ISBN 0-9684016-3-5.
- m) Canadian Standards Association, *Risk Management: Guideline for Decision Makers*, CAN/CSA-Q850-97 (R2009).
- n) CAN/CSA-ISO 31000-10, *Risk Management - Principles and guidelines*, 2009.
- o) CAN/CSA-IEC/ ISO 31010-10, *Risk Management- Risk assessment techniques*, 2010.

5. Management of Change

- a) Sanders, R. E. *Management of Change in Chemical Plants: Learning from Case Histories*, Butterworth-Heinemann Ltd. 1993, ISBN 0-7506-1135-9.
- b) CScHE PSM Division, *Management of Organizational Change*, 2004, available on the PSM division website: http://psm.chemeng.ca/Products/OCM_Guidelines.pdf
- c) CCPS, *Guidelines for the Management of Change for Process Safety*, 2008, ISBN 978-0-470-04309-7.

6. Process and Equipment Integrity

- a) Health and Safety Executive (UK), *Best Practice for Risk Based Inspection as a part of Plant Integrity Management*, RR363/2001, www.hse.gov.uk/research/crr_pdf/2001/crr01363.pdf

7. Human Factors

- a) Kletz, T. A., *An Engineer's View of Human Error*, London: The Institution of Chemical Engineers, third edition 2001, ISBN No. 1-5603-2910-6.
- b) CCPS, *Guidelines for Preventing Human Error in Process Safety*, 1994, ISBN 978-0-816-90461-7
- c) Health and Safety Executive (UK), *Reducing error and influencing behaviour*, HSG48, London HMSO, 1999. ISBN 978-0-717-62452-2.
- d) CCPS, *Human Factors Methods for Improving Performance in the Process Industries*, 2007. ISBN 13-978-0-470-11754-5.
- e) Grandjean, E., *Fitting the Task to the Man*, London, Taylor and Francis, 4th Edition, 1988. ISBN: 0-85066-380-6.
- f) Health and Safety Executive (UK), *Repositioning Human Factors - Identifying barriers to understanding human factors in prevention of major accidents among key decision makers and managers in the industries concerned*, 2009, HSE Research Report RR758.

8. Training and Performance

- a) CCPS, *Conduct of Operations and Operational Discipline: For Improving Process Safety in Industry*, 2011. ISBN: 978-0-470-76771-9.
- b) CCPS, *Guidelines for Safe Process Operations and Maintenance*, 1995, ISBN 978- 0-816-90627-7
- c) CCPS, *Guidelines for Technical Planning for Onsite Emergencies*, 1995, ISBN 978-0-816-90653.

9. Incident Investigation

- a) CCPS, *Guidelines for Investigating Chemical Process Incidents*, 2nd edition. 2003, ISBN 978-0-816-90897-4
- b) CCPS, *Incidents that Define Process Safety*, 2008, ISBN 078-0-470-12204-4.

- c) American National Standards Institute/American Petroleum Institute RP 754, *Process Safety Performance Indicators for Refining and Petrochemical Industries*, 2010.
- d) CCPS, *Process Safety Leading and Lagging Metrics - You Don't Improve What You Don't Measure*, 2011,
http://www.aiche.org/uploadedFiles/CCPS/Metrics/CCPS_metrics%205.16.08.pdf.

10. Company Standards, Codes and Regulations

There are no references for this element.

11. Audits and Corrective Actions

- a) CCPS, *Guidelines for Auditing Process Safety Management Systems*, 2nd Edition, 2011
ISBN No. 978-0-470-28235-9.

12. Enhancement of Process Safety Knowledge

- a) CCPS website.
- b) CShE website.