ENERGY
SAFETY
CANADA

Safety Critical Equipment Guideline

National Safety Association
for Canada's Energy Industry

Edition: #1
Release Date: MONTH YEAR



Disclaimer

This document is intended to be flexible in application and provide guidance to users rather than act as a prescriptive solution. Recognizing that one solution is not appropriate for all users and situations, it presents generally accepted guidelines that apply to industry situations, as well as recommended practices that may suit a company's needs. While we believe that the information contained herein is reliable under the conditions and subject to the limitations set out, Energy Safety Canada does not guarantee its accuracy. The use of this document or any information contained will be at the user's sole risk, regardless of any fault or negligence of Energy Safety Canada and the participating industry associations.

Copyright/Right to Produce

Copyright for this document is held by Energy Safety Canada, 2026. All rights reserved.

Energy Safety Canada encourages the copying, reproduction and distribution of this document to promote health and safety in the workplace, provided that Energy Safety Canada is acknowledged. However, no part of this publication may be copied, reproduced or distributed for profit or other commercial enterprise, nor may any part be incorporated into any other publication, without the written permission of Energy Safety Canada.

ENERGY INDUSTRY'S SAFETY ALLY

For over 75 years, Energy Safety Canada has been the national safety association for Canada's energy industry. Created by industry, for industry, we are dedicated to keeping energy workers safe and driving safety performance.

What We Do:

- Deliver industry-recognized training to meet industry needs.
- Collaborate with industry to drive continuous safety improvements.
- Provide safety and labour market data, insights and tools.
- Serve as the industry certifying partner for the Certificate of Recognition program.

Proudly Serving Our Industry

We are proud to work on behalf of Canada's energy industry associations.

TABLE OF CONTENTS

1.0 Introduction 5

2.0 Purpose / Scope 7

3.0 Identification of Safety Critical Equipment 7

3.1 Approach 1: Prescriptive - Generic 8

3.2 Approach 2: Risk Based – Qualitative - Generic 8

3.3 Approach 3: Risk Based – Semi-Quantitative – Generic of Facility-Specific 9

3.4 Approach 4: Risk Based – Quantitative – Facility-Specific 9

3.5 Summary 9

4.0 Glossary 10

Appendix A – Published Referenced Resources 12

1.0 INTRODUCTION

Process Safety Management (PSM) aims to stop unintentional releases of hazardous materials or energy that could lead to fires, explosions, or serious injuries. Using the Swiss Cheese Model, PSM is built on multiple layers of protection—with each layer represented as a slice of cheese with holes (weaknesses). If the holes in the barriers align, there is potential for the release of hazardous materials.

Safety Critical Elements are defined layers of protection intended to prevent the release of hazardous material or energy, or to mitigate the consequence of a release. The safety critical element layer of protection includes systems and devices that must operate reliably when required and may include sensing elements or logic solvers (e.g., Programmable Logic Controllers (PLC), Basic Process Control System (BPCS) and Safety Instrumented System (SIS), and final elements (e.g., trip valves, and equipment shutdown).

Throughout this document, "SCE" refers to Safety Critical Equipment, not Safety Critical Element. By definition, a Safety Critical Element is made up of Safety Critical Equipment. Examples are presented in Table 1:

Safety Critical Element	Safety Critical Equipment (SCE)
High Pressure Trip	Pressure Indicator / Transmitter Logic Solver (BPCS, PLC) Trip Valve
High Temperature Trip	Temperature Indicator / Transmitter Logic Solver (BPCS, PLC) Trip Valve
Pressure Safety Valve	PSV

Table 1: Safety Critical Element vs Safety Critical Equipment

SCE forms the functional core of each defensive layer in process safety. Failure of SCE can create holes in the Safety Critical Elements (defensive layers), and if these holes align, an incident can occur. Figure 1 illustrates how these SCE failures can make processes susceptible to an incident.

The hazard arrow (left > right) illustrates how multiple failures across these pieces of equipment can align, allowing a major accident to occur.

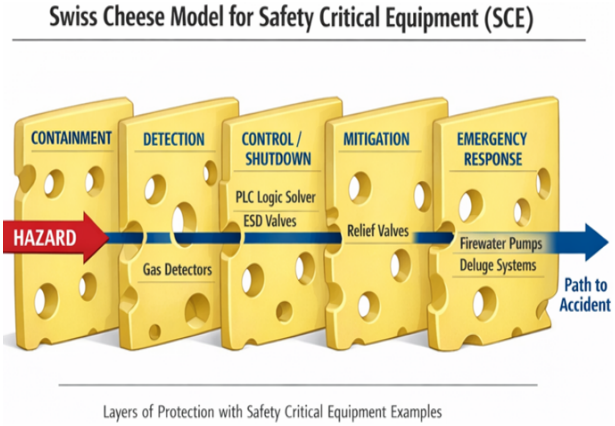


Figure 1: SCE Cheese Model, CAPP

By managing SCE, organizations help ensure that proper identification, design, change management, inspection, testing and maintenance activities are performed to keep the holes in each layer small and misaligned. Examples of SCE are shown below. Note: The two SCE groups Detection and Control / Shutdown form a Safety Critical Element and are therefore combined.

Examples of SCE

Containment

- Pressure vessels
- Piping
- Seals / gaskets
- Storage tanks

Detection

- Gas detectors
- Flame detectors
- Pressure transmitters

- Temperature alarms

Control / Shutdown

- PLC logic solver
- High-pressure trip system
- Emergency shutdown valves or interlocks

Mitigation

- Relief valves (PSVs)
- Blowdown systems
- Inerting systems

Emergency Response

- Firewater pumps
- Deluge systems
- Sprinklers
- Emergency ventilation

Process Safety Management			
Process Safety Leadership	Understanding Hazards and Risks	Risk Management	Review and Improvement
Accountability and Management Review	Process Safety Information and Documentation	Training and Competency	Investigation
Regulations, Codes and Standards	Project Review and Design Procedures	Management of Change (including Pre-Startup Safety Review – Operational Readiness)	Audit Program
Process Safety Culture	Risk Management Framework	Integrity Management	Enhancement of Process Safety Knowledge
Conduct of Operations and Operational Discipline	Human Factors	Emergency Management	Performance Indicators for Process Safety

Table 2: Process Safety Management

Table sourced from CSA Z767:24

The highlighted process safety management systems in Table 2 directly manage the identified SCEs and help ensure they are functional.

This guidance document outlines four approaches to identify SCE:

1. Prescriptive – Generic (refer to API RP 14C)
2. Risk-Based – Qualitative – Generic
3. Risk-Based – Semi-Quantitative – Generic or Facility-Specific
4. Risk-Based – Quantitative – Facility-Specific

The process for identifying Safety Critical Equipment will vary by company, depending on factors such as asset complexity, risk tolerance, regulatory requirements, the maturity of their PSM system, and other organization-specific considerations.

Within Section 3, several subsections include notes for consideration. These are listed in the endnote section, with the roman numeral from the subsection corresponding to the applicable endnote.

2.0 PURPOSE / SCOPE

The purpose of this document is to provide an overview of how to identify SCE, ranging from simplified, prescriptive methods to a fully risk-based approach. The method used to determine the SCE may depend on the maturity of the company's process safety management system and understanding, as well as the complexity or exposure level of the asset / facility.

This document provides guidance only on the identification of SCE and does not apply to any other aspects of equipment integrity programs.

The target audience for this document includes those responsible for ensuring asset integrity and reliability of SCE, such as maintenance and reliability engineers, process safety specialists and maintenance and operations personnel. It also includes those whose work may impact SCE through projects and management of change, such as facilities / project engineers and operations engineers.

The goal of identifying and managing SCE is to reduce the risk of process safety-related incidents.

3.0 IDENTIFICATION OF SAFETY CRITICAL EQUIPMENT

The identification of SCE is critical to effective management in preventing, controlling and mitigating Major Accidents (MA). Companies may establish criteria, including a risk matrix, to determine the threshold for major accident hazards, in addition to regulatory requirements.

Identifying SCEs enables proper maintenance, testing and control of the SCEs to ensure that major hazard risks are managed appropriately. If SCEs are not identified, there is a risk that the equipment may not perform its intended safety function.

Various degrees of rigour can be applied to identify SCE. A company may select the degree of rigour based on the maturity of its process safety management system, the types of risk assessments available, or the relative risk of its facilities.

There is no requirement for companies to adopt a single, common approach to identifying SCE. However, companies are encouraged to select and adapt their toolbox of techniques to their requirements, choosing greater depth and rigour for facilities with greater complexity and higher risk.

Regardless of the approach used to identify SCE, SCE must be identified at the device or 'tag' level at each facility to ensure that the required assurance activities, such as function testing and maintenance, are completed.

Companies should also establish a holistic approach to identification as the first step in

the lifecycle of SCE, supported by their regular inspection and performance assurance system.

It is also beneficial to have a bowtie overview of the SCE identification process to help ensure complete identification not only of the preventative (left-hand side of the bowtie, LHS) barriers to major hazard scenarios, but also of the mitigation barriers (right-hand side, RHS). It is important to note that common risk identification techniques, such as HAZOP, often focus on LHS barriers and are not intended for RHS barriers.

In addition, one may use the list of generic barrier functions or a checklist after the identification process is complete to help ensure that all relevant functions have been considered.

Four methods are outlined in Sections 3.1 to 3.4 for consideration.

3.1 Approach 1: Prescriptive - Generic

- Develop a prescriptive list of process components that should be considered safety-critical for a specific application and/or a service.
- The prescriptive list can be developed using industry guidance, such as API RP 14C, or by a multidisciplinary group based on an understanding of the key risks that need to be managed at the facilities. [i]

The API RP 14C safety analysis is based on the following premises:

- Process components function in the same manner regardless of specific facility design.
- Each process component is analyzed for "worst-case" input and output conditions.
- If fully protected when analyzed on its own, the analysis will be valid for that component in any configuration.
- If every component is protected, the system will be protected.
- When components are assembled into a system, some devices can be eliminated. [ii]

3.2 Approach 2: Risk Based – Qualitative - Generic

- Use qualitative risk assessments, such as What-If, Hazard and Operability (HAZOP) or Failure Mode and Effects Analysis (FMEA). [iii]
- Identify the scenarios that could result in a Major Incident. [iv]
- Select the Independent Protection Layers (IPLs) against Major Incidents. [v]
- Validate the list of safeguards from the risk assessment against API RP 14C for process components to generate tables of SCE. [vi]
- Validate the list of credited safeguards or IPLs against API RP 14C or bow-tie studies to capture any mitigative safeguards that may not have been identified in studies such as What-If, HAZOP or FMEA.
- Apply the generated table(s) from the generated tables of SCE across all similar process components at all facilities.

3.3 Approach 3: Risk Based – Semi-Quantitative – Generic of Facility-Specific

- Use semi-quantitative risk assessments, such as a semi-quantitative HAZOP or FMEA, followed by Layer of Protection Analysis (LOPA) or a bow-tie analysis. Coupling the HAZOP/FMEA with LOPA moves the risk assessment method to a semi-quantitative approach. [vii]
- Review the risk assessment for scenarios that could result in a Major Accident. [viii]
- Select all “credited” safeguards or independent protection layers (IPLs) as SCEs. For an IPL to be considered SCE, three requirements must be met:
  - » The safeguard must demonstrate a reliability of 90 per cent or greater (or a risk reduction

factor of at least 10) in its contribution to achieving the required risk reduction for the Major Incident.

  - » The safeguard must be independent of the associated threat and other safeguards mitigating the risk of the Major Incident.
  - » The safeguard must be auditable.

- Validate the list of credited safeguards or IPLs against API RP 14C or bow-tie studies to capture any mitigative safeguards that may not have been identified in studies such as HAZOP, LOPA or FMEA.
- Generate a facility-specific list of SCE. It is understood that these approaches will typically identify Safety Critical Elements. To determine the Safety Critical Equipment, the Initiator, Logic Solver and Final Element must be identified for each Safety Critical Element. This information is typically found on a Shutdown Key.
- This approach can also be done generically using typical risk assessments for similar facilities. [ix]

3.4 Approach 4: Risk Based – Quantitative – Facility-Specific

- Utilize semi-quantitative risk assessments (such as a semi-quantitative HAZOP followed by LOPA) and full Quantitative Risk Assessment (QRA) from each facility, if available. [x]
- Review the risk assessment for scenarios that could result in a Major Incident. [xi]
- Select all independent protection layers (IPLs) as SCE. These are, by definition, safeguards that can demonstrate reliability of 90 per cent or greater (or a risk reduction factor of at least 10) in their contribution to achieving the required risk reduction for the Major Incident.
- Validate the list of credited safeguards or IPLs against API RP 14C or bow-tie studies to capture any mitigative safeguards that may not have been identified previously.
- From the QRA, if available, create a list of all mitigative safeguards that were considered to provide risk reduction.
- Generate a facility-specific list of SCE components from both sources.

3.5 Summary

SCE is critical to the prevention and mitigation of major incidents, and the systematic identification of SCE is necessary to ensure that adequate inspection, testing, and maintenance programs are in place. The four approaches in this document provide operators with options for identifying SCE based on their own needs and conditions.

Regardless of the approach used, companies are encouraged to develop an internal flowchart for identifying SCE and to maintain a database to assist in managing SCE performance. This helps ensure that SCE is identified and managed systematically and consistently.

4.0 GLOSSARY

Term	Description
API RP 14C	An American Petroleum Institute Recommended Practice providing guidance on safety analysis and safety devices for offshore production facilities.
Basic Process Control System (BPCS)	A control system used for normal process operation that may also form part of a safety function if it meets required reliability and independence criteria.
Bow-Tie Analysis	A visual risk assessment tool that links causes of hazardous events (left-hand side) to consequences (right-hand side) and identifies preventive and mitigative barriers.
Control / Shutdown	Safety functions that act to stop or control a hazardous process, typically using logic solvers, interlocks, and shutdown valves.
Detection	A safety function that identifies abnormal or hazardous conditions using equipment such as gas detectors, flame detectors, pressure transmitters, or temperature alarms.
Emergency Response	Systems and equipment used to protect people and assets during an emergency, including firewater pumps, deluge systems, sprinklers, and emergency ventilation.
Failure Modes and Effects Analysis (FMEA)	A systematic method to identify failure modes of equipment and assess their effects on system performance and safety.
Final Element	The physical device that carries out the safety action, such as a trip valve, shutdown valve, or motor shutdown.
Hazard and Operability Study (HAZOP)	A structured, systematic qualitative risk assessment method used to identify hazards and operability problems in a process.
Hazard Identification (HAZID)	A high-level risk identification technique used to identify potential hazards early in the lifecycle.
Independent Protection Layer (IPL)	A safeguard that reduces risk by preventing or mitigating hazardous events and meets criteria for independence, effectiveness, and auditability.
Layer of Protection	A physical, engineered, or administrative measure that reduces the likelihood or severity of a hazardous event.
Layer of Protection Analysis (LOPA)	A semi-quantitative risk assessment method that evaluates whether existing protection layers sufficiently reduce risk to acceptable levels.
Logic Solver	A device or system (such as a PLC, BPCS, or SIS) that processes input signals and initiates appropriate outputs as part of a safety function.
Major Accident (MA)	A hazardous situation with the potential to result in significant consequences such as fatalities, serious injuries, major asset damage, or significant environmental impact.
Major Incident	An event resulting from the realization of a Major Accident, usually involving loss of containment of hazardous material or energy.
Management of Change (MOC)	A formal process to review and control modifications to equipment, processes, or procedures that may impact safety.
Mitigation	Safety functions that reduce the consequences of a hazardous event after it has occurred, such as pressure relief devices or blowdown systems.

Mitigative Barrier	A safeguard that can acts to reduce the consequences of a hazardous event after it has occurred.
Performance Assurance	Activities undertaken to confirm that safety critical equipment continues to meet its performance standards.
Prescriptive Approach	An SCE identification method based on predefined lists or standards rather than explicit risk assessment.
Preventive Barrier	A safeguard that acts to prevent the occurrence of a hazardous event.
Process Component	A single functional piece of production equipment and associated piping (e.g., separator, pump, heater, or tank), as defined in API RP 14C.
Process Safety Management (PSM)	A structured management system aimed at preventing unintentional releases of hazardous materials or energy that could result in fires, explosions, or serious injuries.
Programmable Logic Controller (PLC)	A programmable device used as a logic solver in control or shutdown systems.
Quantitative Risk Assessment (QRA)	A detailed risk analysis method that numerically estimates the likelihood and consequences of hazardous events.
Risk-Based Approach	An SCE identification method that uses qualitative, semi-quantitative, or quantitative risk assessments to select SCEs.
Risk Matrix	A qualitative or semi-quantitative tool used to categorize risk based on likelihood and consequence.
Safety Critical Element	A defensive layer in process safety composed of one or more items of Safety Critical Equipment. A Safety Critical Element performs a defined safety function, such as detection, shutdown, or mitigation.
Safety Critical Equipment (SCE)	Individual items of equipment whose failure could prevent, control, or mitigate a Major Accident Hazard (MAH) or could directly contribute to a major incident. SCEs include sensing elements, logic solvers, and final elements that must operate reliably when required.
Safety Instrumented System (SIS)	An independent system designed to achieve or maintain a safe state of the process when specified conditions are violated.
Swiss Cheese Model	A conceptual model used in process safety to illustrate how multiple layers of protection reduce risk. Each layer has weaknesses (“holes”), and a major incident occurs when the holes align across layers.

APPENDIX A – PUBLISHED REFERENCED RESOURCES

Published Standards and Guidance Documents

Ref. ID	Published Resource	Publishing Organization / Author	Resource Type	Application Within SCE Guide
A 1	API RP 14C – Recommended Practice for Analysis, Design, Installation, and Testing of Basic Surface Safety Systems	American Petroleum Institute (API)	Internationally recognized industry recommended practice	Primary prescriptive reference for identification of safety devices and surface safety systems; basis of the Prescriptive (Generic) SCE identification approach. Referenced in Introduction, Section 3.1, validation activities, and Glossary.
A 2	CSA Z767:24 – Process Safety Management	Canadian Standards Association (CSA Group)	National standard	Source of the Process Safety Management (PSM) framework used to align management systems with SCE lifecycle requirements. Referenced in Table 1 1.

Published Risk Assessment Methodologies and Techniques

Ref. ID	Published Methodology	Publishing Organization / Primary Origin	Resource Type	Application Within SCE Guide
A 3	Hazard and Operability Study (HAZOP)	Institution of Chemical Engineers (IChemE); IEC 61882	Structured hazard identification methodology	Used to identify hazardous scenarios, causes, and safeguards supporting qualitative and semi quantitative SCE identification (Sections 3.2–3.4; Glossary).
A 4	Failure Modes and Effects Analysis (FMEA)	IEC / ISO (e.g., IEC 60812)	Systematic failure analysis methodology	Applied to identify equipment and system failure modes and consequences relevant to SCE identification (Sections 3.2–3.4; Glossary).
A 5	Layer of Protection Analysis (LOPA)	CCPS (AIChE)	Semi quantitative risk assessment methodology	Used to assess risk reduction and confirm the adequacy of credited Independent Protection Layers acting as SCEs (Sections 3.3–3.4; Glossary).
A 6	Quantitative Risk Assessment (QRA)	Various recognized technical publications and standards bodies	Quantitative risk assessment methodology	Applied in the highest-rigour SCE identification approach to quantify risk and identify Preventive and mitigative safeguards (Section 3.4; Glossary).
A 7	Bow Tie Risk Analysis	Published by multiple safety organizations (e.g., CIEHF, Shell, ISO 17776 guidance context)	Barrier based risk analysis methodology	Used to demonstrate linkage between threats, preventive barriers, mitigative barriers, and SCEs (Sections 3.2–3.4; Glossary).

Published Safety and Management Concepts

Ref. ID	Published Resource	Publishing Organization / Author	Resource Type	Application Within SCE Guide
A 8	Swiss Cheese Model of Accident Causation	James Reason	Safety and accident causation model	Used to illustrate layered defenses and the role of SCEs in preventing and mitigating major incidents (Introduction).

NOTE: For regulatory requirements on SCE, see the Acts, Regulations and Codes of various jurisdictions.

END NOTES

[i] **NOTE 1:** According to API RP 14C, a Process Component is a “single functional piece of production equipment and associated piping used in a process station, such as a separator, heater, pump, or tank.” API RP 14C does not mention SCEs; rather, it identifies "Safety Devices" associated with "Process Components," including instrumented systems and mechanical devices including PSVs.

NOTE 2: Application of a generic prescriptive list should include validation against facility-specific conditions, hazards and operating conditions to avoid misapplication.

NOTE 3: Some mitigative barriers (RHS barriers) are not included in API RP 14C and should be added by the user, such as fire protection.

[ii] **NOTE 4:** The basis for the API RP 14C prescriptive approach is not an integrated analysis like HAZOP, and process components are analyzed in isolation. It is incumbent on the user to apply appropriate additional hazardous analysis methodologies to ensure that hazards are identified and mitigated.

NOTE 5: Not all safety devices identified or specified in API RP 14C are commonly classified as SCE. Users should screen SCEs using the qualification criteria (see Section 3).

NOTE 6: For companies with multiple, very similar assets, extending the generic list of SCE across similar assets can be a cost-effective approach. However, validation against facility-specific conditions, hazards, operating conditions, etc. is highly recommended.

[iii] **NOTE 7:** In a typical qualitative risk assessment, safeguards are either not credited or, if credited, only a ‘barrier count’ process is followed to ensure adequate risk reduction. Calculation of the final mitigated likelihood is rarely considered.

[iv] **NOTE 8:** For screening Major Incidents, a risk matrix and threshold levels of risk or risk severity can be used.

[v] **NOTE 9:** User should select the relevant independent protection layers (IPLs) as SCE, considering qualification criteria.

[vi] **NOTE 10:** Review the notes under Approach 1 when referring to API RP 14C for validation.

[vii] **NOTE 11:** In a typical semi-quantitative risk assessment, safeguards are credited, if they are an IPL, at PHA stage. Later, a LOPA process or equivalent is employed for calculation of final mitigated likelihood.

NOTE 12: There are hybrid approaches to PHA in which semi-quantitative assumptions, such as frequency bands or IPL crediting consistent with LOPA concepts, are incorporated directly into HAZOP worksheets.

[viii] **NOTE 13:** For screening Major Incidents, a risk matrix and threshold levels of risk or risk severity can be used.

[ix] **NOTE 14:** For companies with multiple, very similar assets, extending the generic list of SCEs to all of them is a cost-effective approach. However, validation against facility-specific conditions, hazards, and operating conditions is highly recommended.

[x] **NOTE 15:** In a typical semi-quantitative risk assessment, safeguards are credited at the PHA stage. Later, a LOPA process or equivalent is employed to calculate the final mitigated likelihood.

NOTE 16: There are hybrid approaches to PHA where semi-quantitative assumptions, e.g., frequency bands or IPL crediting consistent with LOPA concepts, are incorporated directly into HAZOP worksheets.

[xi] **NOTE 17:** For screening Major Incidents, a risk matrix and risk or severity thresholds can be used.

Phone:
1 800 667 5557

Email:
Safety@EnergySafetyCanada.com

Web:
EnergySafetyCanada.com