CANADA'S OIL & NATURAL GAS PRODUCERS

Guide

Identification of Safety Critical Equipment (SCE)

March 2019

2019-0009

The Canadian Association of Petroleum Producers (CAPP) represents companies, large and small, that explore for, develop and produce natural gas and oil throughout Canada. CAPP's member companies produce about 80 per cent of Canada's natural gas and oil. CAPP's associate members provide a wide range of services that support the upstream oil and natural gas industry. Together CAPP's members and associate members are an important part of a national industry with revenues from oil and natural gas production of about $101 billion a year. CAPP's mission, on behalf of the Canadian upstream oil and natural gas industry, is to advocate for and enable economic competitiveness and safe, environmentally and socially responsible performance.

2100, 350 – 7 Avenue S.W.
Calgary, Alberta
Canada T2P 3N9
Tel 403-267-1100
Fax 403-261-4622

1000, 275 Slater Street
Ottawa, Ontario
Canada K1P 5H9
Tel 613-288-2126
Fax 613- 236-4280

1004, 235 Water Street
St. John's, Newfoundland and Labrador
Canada A1C 1B6
Tel 709-724-4200
Fax 709-724-4225

360B Harbour Road
Victoria, British Columbia
Canada V9A 3S1
Tel 778-410-5000
Fax 778-410-5001

Overview

The ultimate goal of all Safety Critical Equipment is to reduce the risk of a Process Safety related major incident/accident. This guide provides an overview of considerations used to identify Safety Critical Equipment (SCE) with the objective to ensure the industry has effective safeguards in place to manage major accident hazards.

This document provides an overview of the methodologies that can be used to identify SCE, ranging from simplified, prescriptive methods to a fully risk-based approach. The methodology selected may depend on the maturity of a company's process safety management system, the presence of Major Accident Hazards, or on the complexity or exposure level of the asset/facility. It applies to such assets as wells, facilities and pipelines as well as truck and rail when connected to the mentioned assets.

The target audience for this document includes those responsible for ensuring asset integrity and reliability of SCEs, such as maintenance and reliability engineers, process safety engineers, maintenance and operations personnel, along with those who impact SCEs through projects and management of change, such as facilities/project engineers and operations engineers.

Contents

1 Introduction

Process Safety management is the identification, prevention, control and mitigation of unintentional releases of hazardous materials or energy from primary containment that have the potential to become serious incidents (fires, explosions, severe to fatal injuries, etc.).

One of the Key components to achieve effective Process Safety Management is the creation and maintenance of safeguards to prevent the release of hazardous materials and to mitigate the effects of hazardous materials that may be released to the environment. This approach is often represented in the Bow Tie (see Figure 1-1). The Bow Tie Method is typically used to identify the Safety Critical Elements used to prevent and mitigate the impact of Major Accident Hazards (see glossary for a definition).

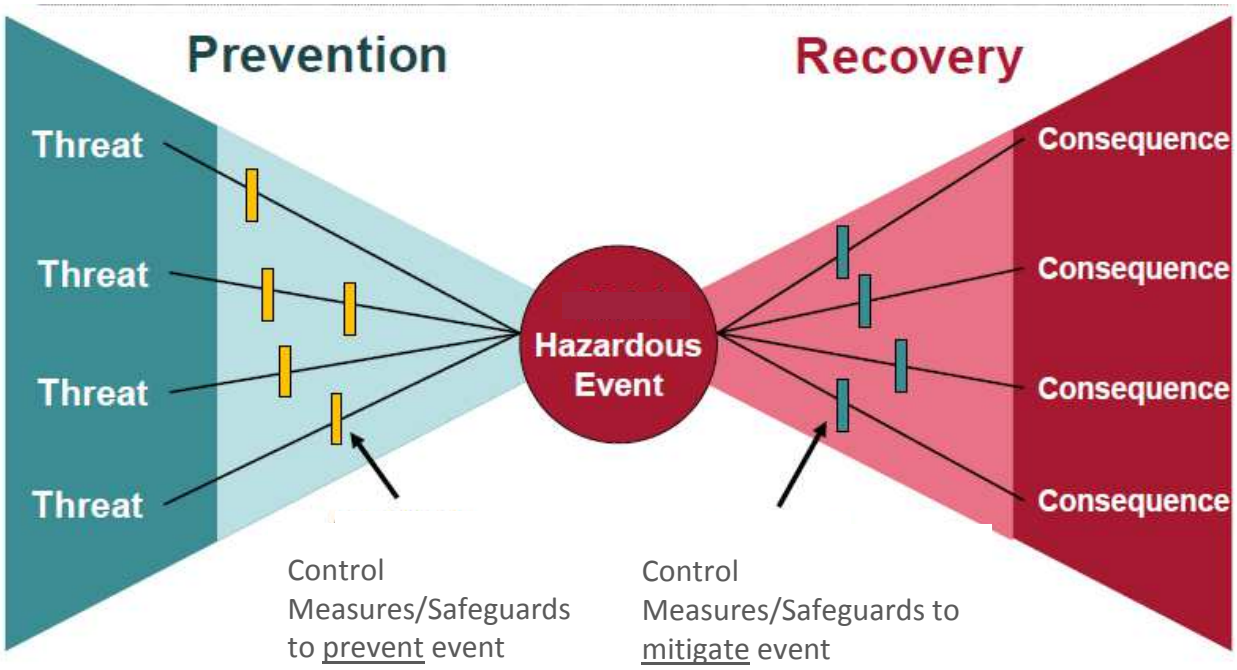

Figure 1-1 Bow Tie Method

Safety Critical Equipment (SCE) is any equipment within a Safety Critical Element that is relied upon in order for the Element to function as required. To illustrate, a high-pressure trip would be Safety Critical Element. Associated with the element are the Pressure transmitter or switch, the PLC (logic solver), and the final valves that are actuated in the plant. Therefore, this one element has 3 (or more) pieces of equipment.

Notably, a single piece of Safety Critical Equipment could belong to multiple Safety Critical Elements. For instance, a gas compressor may be related to a number of Safety Critical Elements such as hydrocarbon containment and overpressure protection.

Safety Critical Equipment plays an important role on both sides of the bow tie. The identification of SCE's ensures adequate inspecting, testing and maintenance programs are in place, and appropriately prioritized. The identification of Safety Critical Equipment is typically part of the equipment integrity element of an overarching process safety management system (see Table 1-1).

NOTE: Throughout this document "SCE" refers to "Safety Critical Equipment" and not to "Safety Critical Element."

Table A-1 Identification of SCE within Process Safety Management

Process Safety Management			
Process Safety Leadership	**Understanding Hazards and Risks**	**Risk Management**	**Review and Improvement**
Accountability (and Management Review)	Process Knowledge and Documentation	Training and Competency	Incident Investigation
Regulations and Standard	Capital project review and design procedures	Management of Change (including Pre Startup Safety Review – operational readiness)	Audits and Corrective action
Safety culture	Process Risk Assessment and Risk Reduction	Equipment Integrity	Enhancement of process safety knowledge
Conduct of Operations	Human Factors	Emergency Response Planning	Performance Indicators

This document outlines four approaches to identify SCE:

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

The choice of what approach to utilize will be up to each company to determine based on the complexity of their asset, their risk tolerance, state of their process safety management system and other company specific factors.

1.1 Purpose

The purpose of this document is to provide an overview of the methodologies that can be used to identify SCE, ranging from simplified, prescriptive methods to a fully risk-based approach. The methodology selected may depend on the maturity of a company's process safety management system, or on the complexity or exposure level of the asset/facility. For example, an operator may use a fully risk-based approach for larger facilities, such as natural gas plants, and use a more simplified, prescriptive approach at unmanned wellsite facilities.

The ultimate goal of Safety Critical Equipment is to reduce the risk of a Process Safety related major incident/accident.

1.2 Scope

This document is intended for personnel tasked with the responsibility to identify "Safety Critical Equipment" in the upstream petroleum industry. It applies to such assets as wells, facilities and pipelines as well as truck and rail when connected to the mentioned assets.

Although the scope is not intended to apply to the drilling, completion, workover, mining and transportation operations, the approach and similar principles may have application in these as well as other industries.

The scope of this document includes guidance on only the identification of Safety Critical Equipment (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 SCEs, such as maintenance and reliability engineers, process safety engineers, maintenance and operations personnel, along with those who impact SCEs through projects and management of change, such as facilities/project engineers and operations engineers.

2 Identification of Safety Critical Equipment

Various degrees of rigour can be applied to identify SCE at the device level. A company may select the degree of rigour based on the maturity of their process safety management systems, based on the type of risk assessments they have available, or based on the relative risk of their facilities.

SCE must be identified at the device or 'tag' level at each facility to ensure required function testing and maintenance is completed.

Four methods are outlined below for consideration as described in 2.1.

2.1 Approach 1: Prescriptive – Generic

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

The 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 standing alone, 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.

2.2 Approach 2: Risk Based – Qualitative – Generic

- Use a sample of qualitative risk assessments, such as a qualitative What-If, HAZOP or FMEA.
- Identify the scenarios which could result in a Major Accident.
- Select the safeguards against major accidents.
- Validate the list of safeguards generated by the risk assessment against API 14C for process components to generate tables of SCE.
- Apply table(s) across all similar process components across all facilities.

See Example in Appendix D.

2.3 Approach 3: Risk Based – Semi-Quantitative – Generic or Facility Specific

- Use semi-quantitative risk assessments, such as a semi-quantitative HAZOP, FMEA or LOPA.
- Review the risk assessment for scenarios which could result in a Major Accident.
- Select the all "credited" safeguards or independent protection layers (IPLs), which required a reliability of 90 per cent or greater from each of those scenarios.
- Validate the list of credited safeguards or IPLs against API 14C, or Bow-Tie studies to capture any mitigative safeguards that may not be identified in studies such as HAZOP, LOPA or FMEA.
- Generate a facility-specific list of SCE process components.
- This approach could also be done generically using typical risk assessments for similar facilities.

2.4 Approach 4: Risk Based – Quantitative – Facility Specific

- Utilize semi-quantitative risk assessments (such as a semi-quantitative HAZOP or LOPA) and full QRA from each facility (if available),.
- Review the risk assessment for scenarios which could result in a Major Accident.
- Select safeguards or independent protection layers (IPLs), which required a reliability of 90 per cent or greater from each of those scenarios.
- From the QRA (if available), pull a list of all mitigative safeguards that were considered to provide risk reduction.
- Generate a facility-specific list of SCE components from both sources.

2.5 Summary

Safety Critical Equipment prevents and mitigates the effects of a major accident. The systematic identification of SCE is necessary to ensure adequate inspecting, testing and maintenance programs are in place. The four approaches in this document provide operators choices for identifying SCE according to their own needs and conditions.

Appendix A. Definitions

Note: Several definitions are provided for some terms. Use the definition that best reflects your operating environment.

Asset Integrity (CAPP from OGP)

Asset integrity is related to the prevention of major incidents. It is an outcome of good design, construction and operating practice. It is achieved when facilities are structurally sound and perform the processes and produce the products for which they were designed. The emphasis is on preventing unplanned hydrocarbon releases that may, either directly or via escalation, result in a major incident. Structural failures may also be initiating events that escalate into major incidents.

Hazard

A situation, condition or thing that may be dangerous to the safety or health of workers.

IPL/Safeguards – Independent Protection Layers

An independent protection layer (IPL) is a device, system, or action that is capable of preventing a scenario from proceeding to its undesired consequence independent of the initiating event or the action of any other layer of protection associated with the scenario.

In order to be considered an independent protection layer (IPL), a device, system, or action must be

- effective in preventing the consequence when it functions as designed
- independent of the initiating event and the components of any other IPL already claimed for the same scenario
- auditable; the assumed effectiveness in terms of consequence prevention and PFD must be capable of validation (by documentation, review, testing, etc.)

Major Accident

a) an event involving a fire, explosion, loss of well control or the release of a dangerous substance causing, or with a significant potential to cause, death or serious personal injury to persons on the installation or engaged in an activity on or in connection with it;

(b) an event involving major damage to the structure of the installation or plant affixed to it or any loss in the stability of the installation causing, or with a significant potential to cause, death or serious personal injury to persons on the installation or engaged in an activity on or in connection with it;

(c) the failure of life support systems for diving operations in connection with the installation, the detachment of a diving bell used for such operations or the trapping of a diver in a diving bell or other subsea chamber used for such operations;

(d) any other event arising from a work activity involving death or serious personal injury to five or more persons on the installation or engaged in an activity on or in connection with it; or

(e) any major environmental incident resulting from any event referred to in paragraph (a), (b) or (d)

Major Accident Hazard (MAH)

A situation, condition or thing that may result in a major accident.

Major Incident

An incident that has resulted in multiple fatalities and/or serious damage, possibly beyond the asset itself. Typically initiated by a hazardous release, but may also result from structural failure or the loss of stability that has caused serious damage to an asset (note this is intended to incorporate terms such as 'Major Accident' as defined by the United Kingdom's Health and Safety Executive (HSE).

Process Safety

Process safety is a disciplined framework for managing the integrity of operating systems and processes handling hazardous substances. It is achieved by applying good design principles, engineering, and operating and maintenance practices. It deals with the prevention and control of events that have the potential to release hazardous materials and energy. Such incidents can result in toxic exposures, fires or explosion, and other releases of hazardous energy that could ultimately result in serious incidents including fatalities, injuries, property or environmental damage, lost production.

PSM – Process Safety Management

Process safety management (PSM) is a systematic analytical tool for preventing the release of highly hazardous chemicals (as defined by CSA Z 767.). Hazardous chemicals include toxic, reactive, explosive and highly flammable liquids and gases. It is a comprehensive management that aims to decrease the number and severity of incidents relating to highly hazardous chemical releases. PSM standards are established by a combination of federal and national standards, directives and their interpretations, integrated technology, organizational and operational procedures, management practices, design guidance, compliance programs and other similar methods.

SCE – Safety Critical Equipment

Process Safety Critical Equipment — equipment, instrumentation, controls, or systems whose malfunction or failure would cause or contribute substantially to the release of a hazardous material or energy or whose proper operation is required to mitigate the consequences of such release (CSA-Z767-17).

Appendix B. Safety Critical Equipment Background and Key Legislation in Other Jurisdictions

B.1. UK Origins

The term “Safety Critical Elements” originated from the Piper Alpha disaster that occurred in the UK North Sea on July 6, 1988. Following his investigation, Lord Cullen’s report led to a change in the previously prescriptive legislation, introducing a risk-based safety case regime including the requirement for operators to identify their own Safety Critical Elements.

A suite of new legislation has since been introduced from the 1990s, including Offshore Installations (Safety Case) Regulations 2005 (SCR) and Offshore Installations (Design & Construction) Regulations 1996 (DCR).

DCR introduced the concept of safety critical elements with legal definition as:

“Such parts of an installation and such parts of its plant (including computer programs), or any part thereof –

- The failure of which could cause or contribute substantially to; or
- The purpose of which is to prevent, or limit the effect of a major accident.”

SCR introduced the requirement for major hazard assessment as well as identification and documentation of mitigative measures to prevent and/or control major accident hazards (MAH). The identified MAHs would then form the basis for determining Safety Critical Elements to be covered by the verification scheme. Performance criteria to maintain asset integrity were also introduced; Functionality, Availability, reliability, Survivability, Interaction, Dependency (FARSID).

The safety case based approach currently followed in UK, Europe and other regions comprises the steps of:

1) Safety assessment to identify the Safety Critical Element, which can include:
    a) HAZOP to identify risk scenarios and levels of control.
    b) Bowtie analysis that helps provide structure to key elements of an MAH.
    c) Summary of Operation Boundaries (SOOB); validation of shut-down keys and actions of the Safety Critical Element to prevent deviation from safe operating envelopes and thus prevent MAH.

2)List of Safety Critical Elements
    a) Performance standard and verification scheme including functional performance definition and testing,
    b) Independent and Competent Person (ICP) Verification, including witness tests, inspections, audits, review of records.

B.2. US Regulations

The primary legislation addressing Safety Critical Elements is API RP 14C “Recommended Practice for Analysis, Design Installation and Testing of Basic Surface Safety Systems for

Offshore Production Platforms" (March 2007). This was incorporated as US law within 30 CFR 250.1628(c).

API 14C is recognized as being very prescriptive with respect to the safety shutdowns and safety devices required for the equipment from wellhead to custody transfer to the pipeline companies. It also mandates rigorous testing of the safety devices to ensure required functionality. It does not address implementation of any safety system or framework.

Whilst the title indicates application for Offshore Facilities, API RP 14C is also being applied to onshore.

API 14C describes a safety-analysis approach based on a number of traditional hazards-analysis techniques such as failure-mode-effects analysis (FMEA) and hazard-and-operability studies (HAZOPS). The purpose of a safety analysis is to identify undesirable events (overpressure, leaks, liquid overflow, gas blow by, underpressure, excess temperature, direct ignition, and excess combustion vapours in firing chamber) that might pose a threat to safety and define reliable protection measures that will prevent such events or minimize their effects should they occur.

Potential threats to safety are identified through proven hazards-analysis techniques that have been adapted to hydrocarbon-production processes. Recommended protective measures are common industry practices proved through many years of operating experience. The hazards analysis and protective measures have been combined into a "safety analysis" for onshore and offshore production facilities.

The 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 standing alone, 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.

A safety analysis is required to:

- Determine which undesirable event could be associated with each component
- Which safety devices are required for the protection of the component
- What responses the safety devices must make to ensure adequate protection.

The safety analysis comprises of safety analysis tables (SATs), safety-analysis checklists (SACs) and safety-analysis function evaluation (SAFE) charts.

SACs provide a guideline for eliminating redundant devices while maintaining the required level of protection. API RP 14C requires that two levels of protection is always in place.

SATs indicate which devices are needed on each component and SACs determine which devices may be eliminated and what conditions must be met when eliminating the device. Neither SATs nor SACs indicate what the devices do or how the devices interrelate from one component to another.

SAFE charts are used to evaluate the function of each safety device and to document precisely what each safety device does. For example, the SAFE chart not only shows that a flowline PSH shuts off inflow, it indicates how it shuts off inflow (e.g., through the closing of a particular well's surface safety valve).

SAFE charts also indicate everything else that happens when a PSH trips. SAFE charts provide a mechanism for considering every component in the facility and then, for each component, to fully account for each required safety device. SAFE charts are used to ensure that the facility is as fully protected as it should be and also can be used as a troubleshooting tool.

The major benefits of this analysis are:

- Concise, easy-to-audit documentation
- Minimized subjective decisions
- Consistent results

API 14C Appendix C addresses Support Systems such as ESD, fire/gas/flame/smoke/heat detection, ventilation, containment systems & sumps, Sub-surface safety valve systems (SSSVs), and flare systems. These are described as 'essential systems that provide an level of protection to the facility by initiating shut-in functions or reacting to minimize the consequences of released hydrocarbons'.

API 14C Appendix D specifies Testing and Reporting Procedures for each of the safety devices/systems identified.

B.3. Canadian Regulations

There are no overarching regulations driving Safety Critical Elements within Canada, however, at provincial level, ABSA addresses pressure related Safety Critical Elements within AB-525. The regulation states that *Safety Critical Elements* are equipment (such as instrumented shutdowns and pressure relieving devices) and process parameters that can have an impact on the Maximum Upset Pressure determined in the Overpressure Risk Assessment (ORA).

AB-525 requires that an ORA must use an organized, systematic and documented approach conducted by qualified personnel through a multi-disciplinary team. The process used for ORA must be based on recognized standards and good engineering practices (WRC-498, ANSI/API 521, ANSI/API-520, etc.). AB-525 requires that the ORA

shall include a list of Safety Critical Elements utilized in the determination of the Maximum Upset Pressure.

For other, non-pressure related Safety Critical Elements the primary guideline addressing identification and testing is Canadian Society for Chemical Engineers (CSChE) Process Safety Management Standard (PSM) which refers at a general level, to Safety Critical Elements in Element 6 'Process & Equipment Integrity':

"Each facility shall:

a) Identify equipment that is critical for process safety; and
b) Establish predictive maintenance schedules for monitoring, inspection and performance testing of equipment critical to process safety to enable cost effective correction of problems before they develop to the critical stage"

Another source of guidance impacting the Canadian energy sector is The Association of Oil & Gas Producers (OGP) – of which the Canadian Association of Petroleum is a member - which published 'Asset Integrity – the key to managing major incident risks' for new and existing upstream assets. It proposes use of the Swiss Cheese model using safeguards which include functional groupings of safeguards as detailed below in Table B-1; Prevention, Detection, Control and Mitigation. Following this grouping, the OGP guidance proposes additional evaluation to define safeguards at a system level, and then define the performance requirements, standards and testing for each safeguard.

Table B-1 Functional Grouping of Safeguards

Prevention	Detection	Control	Mitigation
Hydrocarbon containment	Fire (flame and smoke) detection	ESD system (including valves)	Firewater systems
Ignition prevention	Gas detection	Blowdown system	Passive fire protection
Structural Integrity		(Subsea) Isolation valves	Temporary refuge

None of the Canadian based guidelines or Regulations mentioned above specify testing methods/frequencies (as required in US) nor do they refer to verification of competency of persons completing the Safety Critical Element performance testing (as required in UK).

Appendix C. Resources and References

C.1. Resources

- BC: British Columbia Safety Authority
- AB: Alberta Boilers Safety Association
- SK: Technical Safety Authority of Saskatchewan
- MB: Manitoba Office of the Fire Commissioner – Inspection and Technical Services
- ON: Technical Standards & Safety Authority
- PQ: Régie du bâtiment du Québec (RBQ)
- NFLD: Service NL – Boiler, Pressure Vessel and Compressed Gas
- NB: New Brunswick Safety Code Services
- PEI: Boiler and Pressure Vessel Inspection
- NS: NS LAE – Technical Safety Division
- OGP International Association of Oil & Gas Producers: "Process Safety – Recommended Practice on Key Performance Indicators", Report No. 456, November 201
- CSA Z767 Process Safety Management
- IEC/ANSI

C.2. References

UK HSE SCE management and verification inspection expectations; SPC/ENFORCEMENT/183

http://www.hse.gov.uk/foi/internalops/hid_circs/enforcement/spcenf183.htm

Society of Petroleum Engineers ; Petrowiki: "Recommended methods for safety analysis"

http://petrowiki.org/Recommended_methods_for_safety_analysis

ABSA Owner-User Pressure Equipment Integrity Management Requirements AB-512

http://www.absa.ca/wp-content/uploads/2015/04/AB-512_OU_Pressure_Equipment_Integrity_Management_Requirements_IMR.pdf

Appendix D. Examples

Table D-1 Examples of Safety Critical Equipment Identified by one CAPP member using Approach 2: Risk Based – Qualitative – Generic

Safety Critical Equipment (SCE) Category	Safety Function or Purpose	Components (not limited to items listed)	Applicable Regulations/Codes/ Standards or Recommended Best Practices
Pressure Relief	To relieve excess pressure in order to maintain containment within a design envelope during a process upset condition or fire exposure.	Pressure Safety Valve (PSV)	Pressure Equipment Safety Regulation (PESR) SECT 38(1)(a)
		Pressure Vacuum Safety Valve (PVSV)	API STD 2000 (PVSV)
		Rupture / Bursting Disc	Pressure Equipment Safety Regulation (PESR) SECT 38(1)(b)
		Pressure switch / transmitters (For Pipelines ONLY)	CSA Z662 (For Pipelines)
Emergency Shutdown and Isolation	To reliably isolate hazardous process facilities/systems and limit the quantity of inventory released in the event of an emergency.	Emergency Shutdown valves (ESDV) and associated components (i.e. solenoid, actuator, switches, transducers, etc.)	API Std 521 - Guide for Pressure Relieving and De-pressuring Systems (ESDV) CSA Z662 & AER Dir 77 (Pipelines)
Emergency Blow-Down and Flaring	To rapidly reduce the high pressure flammable gas inventory from contributing to further escalation of an event by relieving the pressure within an acceptable period and ensuring disposal to a safe location.	Emergency Blow-down valves and associated components (i.e. solenoid, actuator, switches, transducers, etc.)	API Std 521 - Guide for Pressure Relieving and De-pressuring Systems (EBDV) CSA Z662 & AER Dir 77 (Pipelines)
		Flare stacks and associated components (i.e. instrumentation, sensors, alarms, etc.)	AER Directive 60 Upstream Petroleum Industry Flaring, Incinerating, and Venting

Safety Critical Equipment (SCE) Category	Safety Function or Purpose	Components (not limited to items listed)	Applicable Regulations/Codes/ Standards or Recommended Best Practices
Emergency Shutdown and Evacuation	To continuously monitor locally for the presence of flammable or toxic gases, or for excessive heat, smoke or fire/explosion providing the means to give earliest possible warning to limit the potential consequences and personnel exposure	Fire / Flame / Smoke Detector	Fire Detection Design Specification
		Heat / Thermal Detector	Fire Detection Design Specification
		Combustible Gas Detector	Practice for the Development of Emergency Shutdown Systems
		Toxic Gas Detector (Chlorine, oxygen, H2S, benzene)	Practice for the Development of Emergency Shutdown Systems
		ESD 1&2 Push Buttons	Practice for the Development of Emergency Shutdown Systems
		Associated beacons, horns, and solenoids	Fire Detection Design Specification
Critical Process Systems	To maintain hazardous inventories (hydrocarbon, toxic/corrosive) within the safe operating limits of pressure, temperature, level and flow. Failure of these systems can be catastrophic.	<u>Fired Heaters and Boilers</u> (Failure can lead to the fired heater and boiler combustion, explosion, fires and overheating. Exclude building heaters – covered under building ventilation) Associated instrumentation, as required by code (i.e. combustion safety controls, flame arrestors/fire-check) Associated Shutdowns, as required by code.	CSA B149.3 Code for field approval of fuel-related components on appliances and equipment

Safety Critical Equipment (SCE) Category	Safety Function or Purpose	Components (not limited to items listed)	Applicable Regulations/Codes/ Standards or Recommended Best Practices
		Compressors and Gas Turbines (Failure can lead to large leaks and failing catastrophically. Exclude air and instrument air compressors.) Associated trips and shutdowns (i.e. vibration, temperature, pressure, etc.) Associated isolation valves	ASME PTC (10)
		Pumps (Failure can lead to large leaks and failing catastrophically. Include all pumps containing or moving flammable or highly corrosive commodity.) Associated trips and shutdowns (i.e. vibration, temperature, pressure, etc.) Associated isolation valves	ASME BPVC (8.2)
Emergency Power Systems	To provide reliable and secure power source to allow continued operation of safety critical and safety related equipment for a defined period in the event of a loss of main and emergency power.	Emergency Generators (including switchgear)	Alberta Fire Code 2006
		Uninterruptible Power Supply (UPS) Systems (including transfer switches)	Uninterruptible Power Supplies (UPS)
		Emergency light panels	Alberta Fire Code 2006
		Batteries	Uninterruptible Power Supplies (UPS)

Safety Critical Equipment (SCE) Category	Safety Function or Purpose	Components (not limited to items listed)	Applicable Regulations/Codes/ Standards or Recommended Best Practices
Building Ventilation	To provide positive pressure forced ventilation to non-hazardous enclosed areas in order to prevent the ingress and accumulation of toxic/flammable gases or smoke and escalating a release by creating an explosive atmosphere. To maintain a safe breathing atmosphere during a release.	Exhaust fans (required by Area Classification)	Practice for the Development of Emergency Shutdown Systems
		HVAC (A/C Units, Air handling units, building heaters, louvers, etc.)	Building HVAC
		Acid and Fume scrubbers	Alberta OH&S Code
		Hood vents (e.g. sample boxes, laboratory)	Site Laboratories
Flexible Hoses and Expansion Joints	No safety function however they have a higher failure probability than piping *shall be used only under exceptional circumstances*	Flexible hose (including metal braided hoses, flex rubber hose, elastomer, Teflon, dresser couplings, etc.)	Flexible Hose Assembly
		Expansion Joints	Expansion Joints
Tanks and Vessels (containing flammable or toxic commodities)	To prevent loss of containment and gas blow-by or low suction to downstream process	Level indication (i.e. level transmitters, level switches, etc.)	AER Bulletin 2016-19 for LSHH (or HLS = high level shutdown)
		Associated components (i.e. alarms, shutdowns, etc.)	
Personal Protective Equipment	To provide suitably rated and certified equipment for use in the event of a	Hand-held Radios	Alberta OH&S Code
		Portable Gas Detectors	Gas Detection Training

Safety Critical Equipment (SCE) Category	Safety Function or Purpose	Components (not limited to items listed)	Applicable Regulations/Codes/ Standards or Recommended Best Practices
	hydrocarbon or toxic release.	PPE	Personnel Protective Equipment Practice
Fire Suppression Equipment & Emergency Medical Services	To provide fire extinguishing or suppression capabilities, appropriate medical aid, and suitable equipment to protect or mitigate against the effects of fire, smoke and toxic exposures.	Fire Extinguishers	NFPA 10 - Portable Fire Extinguishers
		Hydrants	Alberta Fire Code 2006
		Automatic Sprinklers	Alberta Fire Code 2006
		Fire Pumps / Water Supply	Alberta Fire Code 2006
		Fire-water Control Valves	Alberta Fire Code 2006
		Fire Trucks and associated equipment (i.e. hoses, reels)	Alberta OH&S Code
		SCBA / SABA	Alberta OH&S Code
		Ambulances / EMS vehicles	Alberta OH&S Code
Chemical Safety Equipment	To provide appropriate medical aid against the effects of a toxic exposure.	Safety Showers	Alberta OH&S Code
		Eye Wash Stations	Alberta OH&S Code
Secondary Containment	To provides effective means of containment and drainage for released	Berms, bunds, dikes or walls	Directive 055 - Storage Requirements for the Upstream Petroleum Industry

Safety Critical Equipment (SCE) Category	Safety Function or Purpose	Components (not limited to items listed)	Applicable Regulations/Codes/ Standards or Recommended Best Practices
	hydrocarbon liquids and provide control of pool fire escalation scenarios.	Drains, sumps, valves and piping for draw-off	Directive 055 - Storage Requirements for the Upstream Petroleum Industry
		Associated components for safe handling (i.e. safety shields for flanges, pipe joints, expansion joints, acid walls/Plexiglas, etc.)	Alberta OH&S Code

Table D-2 Examples of Safety Critical Elements Requiring Further Analysis

Safety Critical Equipment (SCE) Category	Safety Function or Purpose	Components (not limited to items listed)	Applicable Regulations/Codes/ Standards or Recommended Best Practices
Safety Instrumented Systems	To provide an independent, reliable monitoring and response systems capable to initiate timely action to safely bring the facility/system to the most appropriate level of alert or shutdown by warning the Control Room Operator of abnormal conditions via automatic or manually initiated input signals.	Control valves and associated components (i.e. control loop including sensing device, etc.)	Pressure Equipment Safety Regulation (PESR) Section 38(1)(b)
Emergency Shutdown and Isolation	To prevent the accumulation or creation of a flammable mixture within a tank or vessel that can lead to a fire or explosion if ignition source is present.	Blanket gas purge valves (manual valves)	
Overprotection Credits	To provide reliable and secure isolation in order to prevent a pressure breach of the design envelope for which insufficient inventory relief exists	Pump impellors	ABSA AB 525 Overpressure Protection Requirements for Pressure Vessels and Pressure Piping
		Tank insulation	
		Vessels insulation, passive fire protection	
		Check valves	

Safety Critical Equipment (SCE) Category	Safety Function or Purpose	Components (not limited to items listed)	Applicable Regulations/Codes/ Standards or Recommended Best Practices
HIPPS (High Integrity Pressure Protection System)	To provide reliable and secure isolation in order to prevent a pressure breach of the design envelope for which insufficient inventory relief exists	All components indicated on P&IDs or datasheets, as part of HIPPS	Pressure Equipment Safety Regulation (PESR) Section 38(1)(b)