Health & Safety

Bypass Management Practice

Content Owner	Director, Process Safety		
Custodian	H&S Programs & Projects		
H&S Discipline	Process Safety		
Program	Bypass Management		
Subject Matter Expert	Niki Phillips, niki.phillips@cenovus.com		
COMS	See COMS Standards		
Document Number	CEN-EHS11071		
Version	1.0	**Review Cycle**	3 years
Revised Date		**Issued Date**	September 11, 2015

Version	Description	Date	Sign Off		
			Requester	Reviewer	Owner
1.0	New Document Issued	June 18, 2015			

Table of Contents

List of Tables

1.0 Purpose

The purpose of the Bypass Management Practice is to evaluate and mitigate risk for ALL occurrences where safety critical equipment is bypassed, and to ensure the bypass is performed in a safe and controlled manner.

2.0 Scope

This Bypass Management Practice applies to all Cenovus worksites, work activities and equipment. The Practice includes contracted work activities and contracted equipment.

3.0 Bypass Management Process

3.1 Identification of Engineered Equipment Safeguards

Safety critical equipment is defined as any engineered device or control (safeguard) that is required to ensure a process or equipment is operated within designed safe operating limits or to prevent or limit the effects of a hazard with a potential risk ranking of High or Extreme . Safety critical equipment includes the following:

- DCS or PLC shutdowns and interlocks
- Mechanical shutdowns (Pressure Switches, Level Switches, etc.)
- Pneumatic shutdown systems (for gas compressors, etc.)
- PSVs, PVSVs and Rupture Disks
- Emergency Shut Down Valves (ESDVs)
- Emergency Blow Down Valves (EBDVs)
- High Integrity Pressure Protection Systems (HIPPS)
- Safety Instrumented Systems (SIS)
- Car Seals on safety critical manual valves
- Gas blanketing and inerting systems
- Fire and Gas Detection systems
- Fire Pumps and associated starting systems
- Fire Water system valves
- Automatic fire suppression and extinguishing systems
- Manual fire water systems
- HVAC, Exhaust Fans and Louvres
- Burner Management Systems (BMS)

- Heat Tracing and Insulation
- Flare and blowdown systems
- Vents, Overflows, Flame Arrestors and other physical protection elements
- Mechanical over-speed trips, vibration switches, etc.
- Temperature controls and safety devices on catalytic gas heaters (or similar equipment)
- Electrical safety and protection devices including overcurrent protection devices and ground fault circuit interrupters
- And any other equipment that has been identified as required to ensure operating process conditions are maintained within safe operating limits, or to prevent or limit the effects of a major accident hazard (major release, fire or explosion with a rank of 'Extreme' or 'High' on the Cenovus risk matrix)

Note that some safeguards may also apply to Camps and other infrastructure.

3.2 Types of Safety Critical Equipment Bypasses

3.2.1 Temporary Bypasses

Safety critical equipment may only be temporarily bypassed for the purposes of safe start-up, testing, maintenance or repair. In the case of fire detection sensors, these may also be temporarily bypassed during hot work or flash photography, where such work may cause false equipment shut-down.

Only the minimum number of safety critical equipment that can be adequately monitored should be taken out of service. As soon as the task is completed, the safety device or devices must be placed back in service.

If a safety critical equipment bypass could cause an abnormal operation to occur, the requirements of Section 3.3.2 of the Cenovus Energy Process Hazard Analysis Manual must be followed.

3.2.1.1 Bypasses on Isolated Equipment

In some cases, safety critical equipment bypasses are applied to process equipment that may be positively isolated for long periods of time. In these cases the bypasses are applied to prevent the shutdown of the equipment caused by process parameters that are normal during isolation but undesired when operational (ex. low pressures, low levels, low flows). During this period of equipment isolation, the hazard that the safeguard is protecting against may no longer exist, or the risk is significantly reduced. Therefore, during this period the risk associated to the safeguard bypass shall be managed as follows:

1. A bypass risk assessment shall still be required, but shall only focus on potential impacts to equipment and processes that are still in operation (i.e. does the bypass affect more than the isolated equipment?). It is not necessary to provide alternate safeguards for the bypassed safety critical equipment providing positive isolation is in place and no additional hazards have been identified.

2. The LOTO number or other isolation documentation reference number shall be recorded against each affected bypassed safeguard in the bypass documentation.

3. The bypass must be reinstated and the equipment safeguard tested (see 3.3.6) before the isolation is removed. Reinstatement and testing of each affected safeguard must be recorded in the bypass documentation.

4. If the bypass is in place for a long a period of time (60+ days), the related equipment / process and corresponding bypassed safety critical equipment shall be reviewed to ensure no equipment or process changes have been implemented that could affect the safeguard(s) when they are returned to service.

3.2.1.2 Equipment Permanently out of service

Isolated equipment may also be permanently out-of-service whereby it is not being used as part of the production process and it is positively isolated from all other production equipment or energy sources. Bypassed safety critical equipment for out-of-service equipment must be labeled "Out-of-Service". It is not necessary to provide alternate safeguards for the bypassed safety critical equipment providing positive isolation is in place and all hazards have been removed.

3.2.2 Permanent and Long-term Bypasses

Safety critical equipment may only be permanently bypassed as part of engineered changes to operating facilities.

Long-term bypasses on **in-service** equipment that extend beyond 7 days must also be managed as an engineered change within the Cenovus Management of Change (MOC) system. The only exception to this is long-term bypasses **on isolated** equipment; these may be managed through the site-specific process for bypass management until the isolated equipment is returned to service.

3.2.3 Prohibited Bypasses

Equipment safeguards as defined under OHS Code and/or required by equipment standards or vendor specifications for safe operation may **NOT** be bypassed, tampered with, over-ridden or removed unless the equipment is undergoing maintenance. In this case Lockout/Tagout must be used to ensure positive isolation of hazardous energy and all equipment vendor requirements shall be followed.

Bypassing, isolating, or removing process safeguards during upset/abnormal operating conditions in order to maintain production is **strictly forbidden**.

3.2.4 Water Based Fire Protection System Impairments

Where water based fire protection systems including sprinkler and water spray (deluge) systems, foam systems, fire pumps, water storage, water supply and distribution mains are installed, a fire protection impairment system shall be implemented to manage bypasses.

The impairment system shall comply with the requirements of the provincial Fire Code and the National Fire Protection Association (NFPA) Standard 25.

For fire system impairments, emergency services (if they are on site) or in some cases the local Fire Marshall, must be informed at the start of the impairment and when the impairment has been resolved.

3.3 Process Requirements for Bypass Management

All permanent and long-term bypasses of safety critical equipment shall be managed through the Cenovus Operational Management of Change process.

All temporary bypasses of safety critical equipment shall be managed either through the Cenovus Operational Management of Change process, or through asset-specified and documented processes. Examples of such asset-specific processes include the Christina Lake and Foster Creek Safety Bypass Tools, and asset-specific Car Seal Management procedures.

Asset-specified safety critical equipment bypass processes shall include the following elements:

- The scope of work covered by the process
- Identification of scenarios where temporary safety critical equipment bypasses are allowed
- The maximum duration a temporary bypass is permitted to be in place
- Completion of a risk assessment for operation with the safety critical equipment bypassed
- Identification of the original purpose or design intent of the safety critical equipment
- Identification of alternate protection(s) in lieu of the bypassed equipment, including the process parameters to be monitored for the duration of the bypass
- Identification of testing requirements to ensure the safety critical equipment functions properly once returned to service
- Notification requirements for workers affected by the bypass
- Identification of the responsible authorities for review and sign-off of the bypass
- A documentation system accessible to all workers for information about current bypasses, and for auditing purposes

Further information on these requirements is outlined in the following sections.

3.3.1 Scope of Equipment Safeguard Bypass Process

Assets may create separate processes for the various safety critical equipment bypasses that occur within their facilities. All bypass processes must clearly indicate the safety critical equipment that is in scope of each process, and the specific scenarios where bypass is permitted. Examples include processes specific to DCS and PLC shutdowns, fire and gas detection systems, and car seal management.

The number of safety critical equipment bypassed at any one time shall be kept to a minimum.

3.3.2 Bypass Duration

All bypass processes must indicate the maximum time frame allowed for temporary equipment safeguard bypasses to be in place.

This maximum timeframe may not exceed 7 days. If the bypass is required for more than 7 days the Cenovus Operations Management of Change process must be used. The MOC system allows for more rigorous review, approval and tracking of longer-

term bypasses, ensuring the inherent risk of such bypasses is appropriately managed.

Every effort should be made to limit temporary safety critical equipment bypasses to less than 12 hours. Certain work scopes may require a longer duration for the temporary bypass; it is recommended this not exceed 72 hours.

As soon as the task is completed, the protection device must be placed back in service.

3.3.3 Risk Assessment Requirements

The purpose of a safety critical equipment bypass risk assessment is to:

- identify hazards, hazardous situations or specific events that may arise due to the bypass condition;
- evaluate the risk associated with these hazards;
- evaluate safeguards that reduce the risk;
- determine the level of risk after safeguards are applied; and,
- determine if further safeguards are required to reduce the risk to an acceptable level.

It is important that the members of the bypass risk assessment team be experienced with the process or operation being reviewed. A bypass risk assessment requires an Operations Representative, a Health & Safety Representative, a Process Engineering Representative, a Process Controls and Instrumentation Representative and a designated Facilitator (who may also fill one of the previously listed roles).

If the bypass may result in certain operating conditions that pose high or extreme risks, the risk assessment must include appropriate technical experts and Operations leadership involvement to ensure effective decision making when planning for the work to be undertaken. This technical expertise may include Facility Integrity, Operations/Process Engineering, Process Safety Engineering or M&R Engineering.

The presence of one or more of the conditions listed below shall trigger participation from the previously mentioned technical support and the bypass must be reviewed and authorized by the facility Operations Superintendent:

- Breach or potential breach of the pressure system or tank
- Inability to prove positive isolation (as defined by OH&S)
- Large volumes of flammable liquids or toxic materials are involved
- Abnormal modes of operation - conditions where facilities are fully or partially out of service, emergency conditions exist, the operating mode is rarely used, construction or commissioning of facilities occurs or facility maintenance cannot be coordinated with equipment outages
- Freezing or hydrate conditions could exist

Where the risk is determined to be high, Operations Director or VP approval is required (as per Cenovus Risk Matrix) prior to proceeding.

3.3.5 Alternate Protection Requirements

Alternate protection methods shall be specified and functioning for the duration of all bypassed safety critical equipment. Examples of alternate safeguards may include:

- portable area monitoring systems in lieu of fixed building detectors
- use of temporary insulation until permanent insulation/cladding is installed
- use of a secondary redundant PSV when the primary PSV is out of service
- installation of a temporary replacement control valve or ESD when the permanent valve is out for repair
- modification of process parameters (pressure, temperature, flow) to reduce the likelihood of process excursions or releases

Any bypassed safety critical equipment that does not have an equal and redundant device to provide the same protection shall be continually monitored by a qualified person(s) at the location while the safeguard is bypassed, if safe to do so.

When a qualified person is monitoring bypassed safety critical equipment, that person is taking the place of that safeguard and must be able to manually provide the same level of protection as the safety critical equipment in a timely manner to prevent an undesirable event. They must also be able to do this without exposing themselves or others to unacceptable risk.

Qualified facility personnel shall determine the process, procedures and number of personnel required to provide effective monitoring for each piece of safety critical equipment that is bypassed. Effective monitoring can be conducted by one individual on more than one safeguard in the same general area provided the person can freely move around the general area of production equipment and effectively monitor more than one process simultaneously.

The number of personnel who monitor safeguards in lieu of automatic protection shall be kept to an absolute minimum. Any person asked to perform the function of safety critical equipment while that safeguard is bypassed shall know and understand the procedures regarding this type of monitoring, and shall be part of the risk assessment to determine whether they can safely complete the monitoring.

Qualified personnel bypassing safeguards will be responsible for answering the following questions:

- What is the process variable to be monitored?
- What device will be used to monitor the process variable?
- How will the process be controlled?
- At what point must I react to prevent an undesirable event?
- Is there sufficient time available for the actions needed to return the process to a safe state?
- Will this procedure provide the same level of protection as the safeguard?
- How many people are required? If more than one person, what kind of communication will be used?
- How long can I effectively act as a safeguard before I need to be relieved (due to fatigue, distraction, etc.)?

Qualified operations personnel shall monitor the bypassed or blocked-out safety critical equipment until it is placed back in service. An operator is responsible for:

- Monitoring the function of the bypassed safety critical equipment;
- Directly monitoring the event while in bypass and not performing other duties;
- Assuring monitoring activity occurs at the location of the component, device or panel of the bypassed or blocked out safety critical equipment;
- Assuring monitoring is not interrupted for reasons such as breaks, lunch or other activities;
- Monitoring for abnormal conditions and taking corrective action (close inlet valve, ESD system, etc.) to prevent an undesirable event. The ability to manually initiate shut-in action in the event of an abnormal operating condition must be maintained to protect personnel, the environment and equipment.
- Where corrective actions are dependent on others taking action (ex. control room operator shutdown), reliable communication plan and protocols shall be developed, tested and maintained throughout the monitoring period.

3.3.4 Review and Approval of Bypasses

Review and approval of safety critical equipment bypasses must include, at a minimum, the Operations Area Lead and Operations Area Coordinator (or equivalent Operations roles). Additional review and approval may be required by area process engineering, panel operators, controls technicians, Health and Safety, technical experts and the Operations Superintendent as outlined in Section 3.3.4.

3.3.5 Notification Requirements

The operations personnel who execute the bypass shall notify all workers affected by the bypass when it is first executed and when it is removed. Affected workers shall include operations staff for the affected equipment, the permitting authority for the affected equipment (if different than operations), all affected maintenance workers, and any other staff who may be directly affected by the safety critical equipment bypass. Notification may be verbal where appropriate, and must also be included in all safe work permits issued for the affected equipment.

If the bypass extends beyond shift change, the affected incoming operations shift must be verbally notified and this notification must be recorded in the shift log. Any other affected personnel on the new shift must also be notified.

3.3.6 Testing Requirements upon Return to Service

All bypassed safety critical equipment shall be tested for proper function as soon as they are returned to service and prior to removing alternate safeguards. The testing requirements shall be based on the type of safeguard (mechanical, electrical, etc.), and may be included as part of normal maintenance procedures for safeguards that have been repaired or replaced.

Successful safeguard testing shall be documented as part of the bypass record.

3.3.7 Bypass Documentation

Site-specific safety critical equipment bypass documentation systems must incorporate all relevant information related to bypass management as outlined in this practice. Such systems must clearly indicate the review and approval process for bypasses, and must be accessible to all workers. In addition, safe work permits shall describe all bypasses and alternate protection methods relevant to the permitted scope of work.

Site-specific procedures related to bypassing of safety critical equipment shall be stored electronically and made accessible to all personnel.

4.0 Roles and Responsibilities

Roles and responsibilities specific to the Cenovus Bypass of Equipment Safeguards Practice are described below.

Table 1: Roles and Responsibilities

Role	Description
Operations Staff	• Participate in the bypass management risk assessments and bypass execution as required • Participate in bypass risk assessments, reviews and approvals as specified by site procedures • Manage duration of bypasses, alternate safeguards and bypass monitoring as required • Review all bypasses extending beyond the end of a shift at shift change
Process Control	• Review, approve, implement and remove bypasses where designated in the process
Process Engineering (or other competent engineer familiar with the equipment)	• Participate in bypass risk assessments, reviews and approvals as specified by site procedures • Steward long-term bypasses (7+ days) through the Cenovus MOC process • Provide subject matter expertise when requested by Operations teams
Health & Safety	• Provide subject matter expertise when requested by Operations teams
Process Safety	• Serve as Subject Matter Experts for this Practice • Provide subject matter expertise when requested by Operations teams
EHSR Audit	• Lead, organize and conduct audits to verify compliance, identify gaps and suggest improvement opportunities

5.0 Training and Competency

Competency describes the knowledge and skills required to successfully perform the technical aspects of a job. A worker must be able to demonstrate competency in safely performing work tasks or using equipment.

5.1 Training

It is expected that all personnel involved in this process will have training and the appropriate competency to perform their roles. Cenovus expectations related to this process are that all workers involved with Bypass Management shall review and sign off on this Practice.

6.0 Quality Assurance

6.1 Performance Measurement

Compliance with this practice and program effectiveness shall be assessed through program assessments and internal audits, or other measurement criteria as specified in the COMS Assurance Standard. Measurement can also be accomplished through the tracking of appropriate Key Performance Indicators (KPI).

Business functions or departments impacted by this practice must include compliance and program effectiveness verifications in their business assurance program. Performance will be monitored and reported within the responsible departments at least every three years.

6.2 Management of Change

The document owner will complete and document reviews of this practice, as follows:

- At minimum once every three years
- If there is a significant regulation or industry best practice change that indicates the need for review
- If an incident investigation indicates the causes were related to unclear or inadequate written instructions described within this practice

If frequent and multiple variances are required due to operational needs, the reason(s) will be investigated and the document owner will determine if there is a business need to update the practice.

If submitted MOC requests indicate gaps or significant improvement opportunities, the document owner will determine if there is a business need to update the practice.

Proposed changes to this practice can be directed to H&S Programs and Projects.

7.0 Glossary

Definitions and acronyms for safety documents are described in CEN-EHS243, H&S Definition and Acronym Standard.
The following definitions and acronyms are specific to this document:

Table 2: Terms and Definitions

Term	Definition
Bypass	To temporarily block out, isolate, override, inhibit, force, impair, jumper, disable or remove a device or system so that it will not perform its designed function, for the purpose of testing, maintenance and startup. For the purpose of this practice the words "bypass," "isolate," "override," "inhibit," "force," "jumper," "block," "disable," "remove' or any other term used to describe the temporary act of disabling safety critical equipment have the same meaning.
Effective Monitoring	Effective monitoring is, in effect, taking the place of the safety critical equipment. An individual must be able to manually provide the same level of protection as the bypassed critical equipment in a timely manner in order to prevent an undesirable event. (Leaving the area for breaks, parts, supplies or tools would compromise effective monitoring.)
Major Accident Hazard	A Major Accident Hazard is deemed to be an event such as a major release, fire or explosion resulting from uncontrolled operation of a facility, leading to fatalities or serious personal injury, significant damage to property, or to the environment. As per the Cenovus Risk Matrix, MAHs have high impacts and low likelihoods resulting in a risk rank of 'Extreme' or 'High'.

Table 3: Acronyms and Abbreviations

Term	In Full
BMS	Burner Management System
DCS	Distributed Control System
EBDV	Emergency Blow Down Valve
ESD	Emergency Shut Down
ESDV	Emergency Shut Down Valve
HIPPS	High Integrity Pressure Protection System
HVAC	Heating, Ventilation and Cooling
NFPA	National Fire Protection Association
PLC	Programmable Logic Controller
PSV	Pressure Safety Valve
PVSV	Pressure Vacuum Safety Valve

8.0 References

8.1 External Documents

The following external documents support this practice:

Table 4: External Document References

Document Type or Number	Document Title
Regulatory	Alberta Occupational Health and Safety Code, Part 22
Regulatory	Alberta Fire Code
(NFPA) Standard 25	Standard for the Inspection, Testing, and Maintenance of Water-Based Fire Protection Systems

8.2 Internal Documents

The following Cenovus documents support this practice:

Table 5: Internal Document References

Document Type or Number	Document Title
CEN125	Cenovus Risk Matrix
TR-50-PRC-00-035-01 / CVE-GEN-S-19	Cenovus Management of Change Standard
TR- 50-PRC-00-028-01	Cenovus Energy Process Hazard Analysis Manual
CVE-INST-R-01	Use of Safety Device Bypass Systems
FC0-0-00-OPS-COP-1215	Safety Shutdown Bypass Procedure
Christina Lake Production Practices	DCS Bypassing
Process Safety Practices	Safety Critical Elements Identification Practice