Bypassing Critical Protections CoW Technical Standard

Version	Date	Approver
1.0	March, 31 2024	JO EHS Division

Introduction

This standard defines requirements for the bypassing of critical protections. It includes requirements for the management system and the operational activities that assure critical protections are bypassed, monitored, tracked, and returned to service in a manner which maintains the safe and reliable operation of safety critical systems to prevent or mitigate potential injuries, loss of containment, adverse environmental impact, equipment, or property damage. In the event there is a conflict between the requirements of this standard and local regulations, the more stringent shall apply.

Scope

This standard is applicable to equipment and/or facility critical protections where it is possible to apply a software and/or hardware bypass to temporarily block out, remove, isolate, override, inhibit, force, disconnect or otherwise disable a device or system such that it will not perform its designed function.

This standard applies to any bypass for the purposes of work or operational need including, but not limited to testing, maintenance (scheduled and non-scheduled), installation and commissioning of an engineering change, or startup of plant or equipment that requires a bypass of critical protections.

This standard is not intended to replace the Standard for Isolation of Hazardous Energy.

This standard is not applicable to testing, start up, and/or shut down overrides/bypasses that meet one of the following:

- Designed automatic functional reactivation after time delay (not to exceed 30 minutes).
- Designed automatic functional reactivation based on process variable condition (not to exceed 30 minutes).
- Permanent elimination or bypass of protective devices that are managed under the Management of Change (MOC) process.

This standard is not applicable for input instrumentation (i.e., sensor (H2S gas sensor), transmitter, etc.) testing and maintenance when **all** the following conditions are met:

- Viable means of constant communication between field and control room or control center personnel (Radio, GAI-Tronics, etc.);
- There are no additional active bypasses on the system, process, or piece of equipment.
- The bypass is performed as part of a documented inspection, testing, or preventative maintenance (ITPM) procedure, operating procedure, or operator routine duty that considers the hazards and details necessary mitigation(s) for each device bypassed; and
- The critical protection will not be in bypass for more than 30 minutes.

Requirements

The following sections provide minimum requirements for bypassing critical protections as well as supporting guidance to clarify the intent of those requirements.

- Requirements of this Standard **shall** be met.

1.	**Requirement:**	**JO shall define critical protections (both hardware and software) that may be bypassed, including at a minimum:** **a. Shutdown devices or systems (e.g., Interlocks (hardware and software), emergency block valves (EBVs), multifunction electrical protection devices, electrical control system (ECS) and mechanical key-interlocking systems).** **b. Fire and gas detection and fire suppression devices (e.g., LEL/H2S detectors, flame scanners, fire pumps, deluge systems, fusible links).** **c. Rotating equipment safeguards (e.g., vibration sensors, over speed trip, and similar systems).** **d. Pressure safety valves (PSV), blowdown valves (BDV), thermal relief devices, vacuum breakers, and associated valves.** **e. Integrity operating windows (IOW) critical alarms (e.g., IOW-safe operating limits (SOL)).** **f. Instrumented protective systems (IPS), which shall include, but are not limited to:** **i. Safety instrumented systems (SIS)** **ii. Alarms associated with independent protection layers (IPLs)** **iii. Basic process control system (IPLs)**
	Guidance:	Certain critical protections may be classified as safeguards. Unless otherwise established as critical protection, process alarms defined in CTC-COO-04000 or ICM-DU-5088 are not in scope for the requirements of bypassing a critical protection. For process alarms, follow the change methodology defined in CTC-COO-04000.
2.	**Requirement:**	**Bypassing, isolating, or removing critical protections in the following situations shall be prohibited:** **a. To maintain production during upset/abnormal conditions.** **b. To extend/defer the established inspection frequency of a critical protection.**
	Guidance:	JO should develop a list of critical protections that cannot be bypassed under any condition while the equipment/unit/process is in operation.

		Examples of upset/abnormal conditions include: • Unplanned release of hazardous liquid or gas • Operations that exceed Upper/Lower Safe Operating limits and cannot be returned to Normal Operating Limits through procedural actions/controls. • Use of bypass to remain in a stable condition has been identified and approved as the safer alternative to initiating plant shutdown (e.g., a power outage in the plant where the best practice is to hold stable condition until power can be restored) • An unplanned release where bypassing an upstream critical function is necessary to control the downstream release • An electric motor tripped offline due to an overload condition that needs to be restarted before a normal reset procedure is followed
3.	**Requirement:**	**Bypass functions designed specifically for state transitions (e.g., start-up, shut down, regen, etc.) shall only be used during those operational states.**
	Guidance	Approved bypass functions for start-up operations should have either an Operating Procedure using CTC-COO-02000 or automatic method for restoring the critical protection to designed protection level after start-up.
4.	**Requirement:**	**Critical protections shall be bypassed only when necessary for a finite period of time. Bypassed critical protections that go beyond 72 hours shall then be managed per the Management of Change Process.**
	Guidance:	The 72-hour bypass limit starts with the first override application and DOES NOT stop or pause/re-start if the bypass is removed and then re-applied. JO should avoid grouping critical protections in large inspection/testing/maintenance campaign(s) that require JO to have critical protections in bypass for an extended period of time.
5.	**Requirement:**	**When planning the bypass of a critical protection, JO shall utilize existing technical information (e.g., risk assessments, etc.) to evaluate potential upstream and downstream impacts of the bypass and to determine the safeguards necessary to safely bypass the critical protection.** **a. When bypassing critical protections, a hazard analysis shall be performed in accordance with the Hazard Analysis SHEERS Standard.**
6.	**Requirement:**	**Only the minimum number of critical protections in a system shall be bypassed at any given time.**
	Guidance:	If bypassing more than one critical system, JO should determine if the MOC process would be a more appropriate solution for managing the temporary change.

7.	**Requirement:**	**Bypasses that require isolation shall be isolated in accordance with the Isolation of Hazardous Energy CoW Technical Standard.**
8.	**Requirement:**	**A bypass certificate or equivalent documentation (e.g., approved operating, maintenance, bypass, or inspection procedure(s) including required operator actions) shall be required for the bypass of a critical protection, shall establish the period of time for which the bypass is authorized, and shall include appropriate documented authorization.**
9.	**Requirement:**	**Work shall be authorized in accordance with the Work Authorization CoW Technical Standard.**
10.	**Requirement:**	**a. Bypassed critical protections shall be documented in a system of record (e.g., bypass register) that is maintained in the primary operations control center or equivalent.** **b. Entries in the bypass register shall include the period of time for which the bypass is authorized.** **c. JO shall establish the frequency in which the bypass and associated control(s) need to be acknowledged on the bypass register to verify that conditions being monitored have not changed or modifications are required to achieve the equivalent level of protection.** **d. JO shall establish a frequency and designate persons who shall be required to verify bypasses are in place per bypass register.** **e. The bypass register shall include:** **i. Name (description) of the critical protection being bypassed.** **ii. Start date/time and finish date/time.**
	Guidance:	Bypass registers may additionally contain the following information: • Responsible person • Controls/measures in place to provide equivalent protection • Upstream and downstream effects of the bypassed critical protection • Name of person(s) providing continuous monitoring • Record of who reviewed the control/measure providing the equivalent protection and when the review was done. • Name of person verifying the functionality of the bypassed critical protection once it is returned to service and date/time the verification was completed. Electronic bypassing critical protection logs designed in the control system along with electronic or manual registers are acceptable for use.

11.	**Requirement:**	**Bypassed Critical Protections shall be identified by a visual indicator (e.g., Human Machine Interface (HMI) symbology, tags/flags, Beacons, electronic flags for software) at the bypass, on the control system HMI.**
	Guidance:	JO should consider using automatic indication when critical protections are bypassed. (e.g., beacons, LED panel indicators, remote bypass indication, etc.) Physical bypass tags are only required on the device that is operated to bypass the critical protection (e.g., bypass switch, manual valve, etc.) Although logic forces and jumpers are highly discouraged, if one is used, then the physical bypass tagging requirement may not apply. However operational awareness should be employed (e.g., bypass document, force list or registers, etc.).
12.	**Requirement:**	**JO shall continually monitor bypassed critical protections without an equivalent and/or redundant device able to detect the same condition and respond appropriately. Monitoring shall be performed by a qualified person(s) able to manually provide a similar level of protection as the bypassed critical protection.**
	Guidance:	If an equivalent level of protection cannot be achieved by the person providing continuous monitoring, the JO should shut down the piece of equipment to perform the work. The equivalent protection to the bypassed critical protection should be functionally similar and provide a level of protection of comparable effectiveness to the critical protection bypassed. • For example, if the bypassed critical protection closes a valve, the equivalent protection should also close the same valve or another valve which would provide the same isolation, meaning the next upstream/downstream valve. Safety functions with multiple voting sensors/transmitters, that can be individually bypassed, can be considered equivalent, if the remaining sensors/transmitters provide similar alarming and/or trip capabilities. IPS sensors/transmitters that have a redundant non-IPS that monitors the same process condition can be considered equivalent.
13.	**Requirement:**	**JO shall develop a communication procedure to notify affected personnel and other impacted work crews on the status of bypassed critical protections that shall include at a minimum:** **a. Shift change/turnover** **b. Safety and/or operational precautions** **c. Completion of the bypass of the critical protection** **d. Verification that the critical protection is operational and returned to service**
	Guidance:	Use CTC-COO-05000 standard to manage communication strategies.

14.	**Requirement:**	**JO shall have a process for validating the reinstatement of critical protections when bypass is removed (e.g., procedures, beacon light, console indication).**
	Guidance:	Use CTC-COO-02000 standard to manage communication strategies.
15.	**Requirement:**	**Personnel conducting activities associated with the bypass of critical protections shall meet the competency requirements that apply to their roles in accordance with the Training and Competency SHEERS Standard.**
16.	**Requirement:**	**Documentation associated with the bypass of critical protections shall adhere to the JO record retention requirements.**

Appendix A: Terms and definitions

Term	Definition
Bypass	To temporarily block out, isolate, override, inhibit, force jumper, disconnect or otherwise disable a device or system so that it will not perform its designed function for the purpose of testing, maintenance, and startup or to maintain safe, reliable operation.
Bypass Register	A documented means of control and communication to account for the status of critical protections or systems that have been placed on bypass. Register should be maintained in the primary operations control center or equivalent and be visible and readily available for reference by any personnel in the control room regardless of role.
Critical Integrity Operating Window (IOW)	An established limit that if exceeded could result in rapid equipment deterioration, damage, or hazardous fluid release, beyond which troubleshooting and/or continued operation cannot be tolerated, and pre-determined actions are executed to return the process to a safe state.
Critical Protections	Devices or systems designed to protect personnel, the environment, process equipment, and properties from a process safety event. Functional critical protections are a vital component of safety systems that are designed and installed to increase the likelihood of safe, reliable, and environmental sound operations.
Independent Protection Layer (IPL)	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. An IPL requires verification of the following four characteristics: • Specific in preventing the hazard under consideration. • Dependable in that it must provide the same amount of risk reduction under any circumstances. • Independent from the initiating event and other layers of protection for the same hazard. • Auditable in that it must be periodically tested to confirm its availability and performance level.
Instrumented Protective System (IPS)	System of separate and independent combination of sensors, logic solvers, FEs, and support systems that addresses impacts related to health and safety effects, environmental impacts, loss of property, and business interruption costs.
Integrity Operating Windows (IOW)	Established limits for process variables (parameters) that can affect the integrity of the equipment if the process operation deviates from the established limits for a predetermined length of time.

Term	Definition
Safeguard	The hardware and human actions designed to directly prevent or mitigate an incident or impact.
Tag/Flag	An electronic, hanging, and/or removable placard specific to bypassing critical protections that identifies the critical protection as being bypassed.

Appendix B: Roles and responsibilities

Term	Definition	Responsibilities
Bypass Approver	Persons who are trained, competent and authorized to approve bypasses of critical protections.	Approve bypassed critical protections.
Bypass Executer	Persons who are trained, competent and authorized to implement bypasses of critical protections.	Implement bypassed critical protections.
Bypass Reviewer	Persons who are trained, competent and authorized to review and communicate the status of bypasses from the bypass log / register.	Review and communicate the status of bypasses from the bypass log / register.
Bypass Verifier	Persons who are trained, competent and authorized to physically verify the status of bypasses and update the bypass register / log.	Physically verify the status of bypasses and update the bypass register / log.

Appendix C: References

Internal References

CTC-COO-02000	Corporate Standard for Operating Procedures
CTC-COO-04000	Corporate Standard for Alarm Management
CTC-COO-05000	Corporate Standard for Management of Communication
CTC-FIRM-04000	Facility Integrity and Reliability Management for Instrumented Protective Systems
ICM-DU-5088	Design of Alarm Systems
ICM-DU-6187	Management of Functional Safety
CTC-FIRM-02XXX	Identification, Implementation, and Maintenance of an Integrity Operating Window System
MOC 03000	Management of Change

External References

American National Standards Institute

ANSI/ISA-18.2-2016	Management of Alarm Systems for the Process Industries
ANSI/ISA – 84.91.91.01 - 2021	Identification and Mechanical Integrity of Process Safety Controls, Alarms, and Interlocks in the Process Industry Sector
ANSI/ISA – 61511-1-2018; IEC 61511-1:2016+AMD1:2017 CSV	Functional Safety – Safety Instrumented Systems for the Process Industry Sector Part 1: Framework, definitions, system, hardware, and application programming requirements (IEC 61511-1:2016+AMD1:2017 CSV, IDT)
ANSI/ISA – 61511-2-2018; IEC 61511-2:2016	Functional Safety – Safety Instrumented Systems for the Process Industry Sector Part 2: Guidelines for the application of IEC 61511-1:2016 (IEC 61511-2:2016, IDT)

American Petroleum Institute (API)

Standard 521	Pressure-relieving and Depressuring Systems
Recommended Practice 14C	Recommended Practice for Analysis, Design, Installation, and Testing of Basic Surface Safety Systems for Offshore Production Platforms
Recommended Practice 14G	Recommended Practice for Fire Prevention and Control on Fixed Open-type Offshore Production Platforms

Recommended Practice 14J	Recommended Practice for Design and Hazards Analysis for Offshore Production Facilities
Recommended Practice 2001	Fire Protection in Refineries

British Standard Institute (BSI)

BSI BS EN 54	Fire Detection and Fire Alarm Systems

Bureau of Safety and Environmental Enforcement (BSEE)

BSEE NTL No. 2009-G36	Using Alternate Compliance in Safety Systems for Subsea Production Operations

Energy Institute (EI)

Element 16	Identification, Implementation and Maintenance of an Integrity Operating Window System – Management of Safety Critical Devices

International Association of Oil and Gas Producers (IOGP)

Report No. 415	Asset integrity – the key to managing major incident risks
Report No. 443	High Integrity Protection Systems – Recommended Practice
Report No. 459	Life-Saving Rules
Report No. 544	Standardization of barrier definitions – Supplement to Report 415
Report No. 638	Process Safety Fundamentals

International Society of Automation (ISA)

ISA-84.00.01-2004 Part 3	Functional Safety: Safety Instrumented Systems For the Process Industry Sector ─ Part 3: Guidance for the Determination of the Required Safety Integrity Levels ─ Informative
ISA-TR18.2.1-2018	Alarm Philosophy
SA-TR84.00.02-2015	Safety Integrity Level (SIL) Verification of Safety Instrumented Functions

National Fire Protection Association (NFPA)

NFPA 70	National Electric Code (NEC)

Occupational Safety and Health Administration (OSHA)

29 CFR 1910.119	Process Safety Management of Highly Hazardous Chemicals
29 CFR Subpart L	Fire Protection; 1910.164 Fire detection systems