DS&C Standard

Bypassing Critical Protections

Version	Date	Primary Author or Approver
1.0	September 2015	Scott Fife
2.0	July 2018	Scott Fife

Introduction

Bypassing Critical Protection procedures are designed to assure that safety critical controls and/or systems are bypassed in a manner that maintains the safe and reliable operation of safety critical systems to reduce the likelihood of injuries, equipment damage, loss of containment, property damage or adverse environmental impact. In the event there is a conflict between this standard and local regulations, the more stringent shall apply.

This standard is applicable to equipment or facility Critical Protections where it is possible to apply a software and/or hardware bypass to temporarily block out, 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 work 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 protection.

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

This standard is not applicable to testing and/or start up overrides/bypasses designed with automatic functional reactivation after time delay, permanent elimination or bypasses of protective devices that are managed under the Management of Change process.
This standard is not applicable for input instrumentation (i.e., sensor, transmitter, etc.) maintenance and testing when all the following conditions are met:

1. Constant communication between field and control room or control station personnel (radio, GAI-Tronics, etc.)
2. No other bypasses can be active in the area, system, or piece of equipment
3. The critical protection will be bypassed for no more than 30 minutes
4. A risk-based, documented testing procedure exists for each device bypassed

This standard defines the DS&C requirements for Bypassing Critical Protections.

Requirements

A written program for Bypassing Critical Protections shall be in place and include the following elements at a minimum:

A. Viable alternatives to Bypassing a Critical Protection shall be considered.

B. 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.

C. Bypass functions designed for use during start-up shall only be used for start-up scenarios.

D. Critical protections (both hardware and software) that may be bypassed shall be described, including but not limited to:

   1. Shutdown devices or systems (e.g., instrumented protective systems, emergency shutdown devices).
   2. Fire and gas detection and fire suppression devices (e.g., fire pumps, deluge systems, fusible loops).
   3. Valves that affect the availability of critical protections (e.g., LO/LC valves, fire water pump intake valves, etc).
   4. Equipment safeguards, over speed trip, fired equipment flame detectors and similar systems.

5. Pressure safety valves (PSV), blowdown valves (BDV), thermal relief devices, vacuum breakers and associated valves.
6. Integrity Operating Windows (IOW) critical category alarms (IOW-SOL).
7. Instrumented Protective Systems including but not limited to:
    i. Safety Instrumented Systems (SIS)
    ii. Safety Shutdown Systems (SSS), interlocks, equipment shutdown protections
    iii. Independent Protection Layer Alarms
    iv. Basic Process Control System IPLs
    v. Fire and Gas sensor alarms; with both automatic and manual response attributes

E. Bypassing, isolating, or removing critical protections during upset/abnormal conditions in order to maintain production or to extend/defer a critical protection device established inspection frequency shall be prohibited.

F. Only the minimum number of critical protections in a system shall be bypassed at any given time and additional safeguards shall be in place as evaluated during the hazard analysis or risk assessment.

G. A Permit to Work or equivalent documentation (e.g., approved operating and maintenance, bypass, or inspection procedure – including operator actions required) shall be required for Bypassing Critical Protections and shall establish the time period for which the bypass is authorized and include appropriate authorization signatures.

H. Critical Protections that are on bypass shall have a documented inspection/review at a frequency interval defined by the appropriate OpCo/BU/Facility Authority.

I. Bypassed Critical Protections shall be identified by a form of visual identification (e.g., Personal tags/flags provided to each qualified person, electronic flags for software) at the bypass or isolation point.

J. Bypassing Critical Protection personal tags/flags, bypass keys, bypass management systems and consoles, codes or cards shall be secured when not in use and shall only be used by authorized personnel.

K. Bypassed Critical Protections shall be recorded in a Bypass Register maintained in the primary operations control center or equivalent.

L. The OpCo/SBU/Facility shall define the process to provide effective, risk-based monitoring for each critical protection device or system placed in bypass.

M. Critical protections without an equal and/or redundant device to detect the same condition and respond appropriately shall be continually monitored by a qualified person(s) able to manually provide the same level of protection as the critical protection device.

N. A documented communication mechanism shall be in place for affected personnel and other impacted work crews on the status of bypassed protections, including, but not limited to:

1. Shift change/turnover
2. Safety and/or operational precautions
3. Bypass completion
4. Bypass return to service

O. A process shall be defined for validating the reinstatement of Bypassed Critical Protections.

P. Personnel assigned responsibilities in Bypassing Critical Protections shall be trained and competent.

Q. Training requirements and competency assessment for personnel authorized in Bypassing Critical Protections shall be documented.

R. The Bypassing Critical Protections Standard shall define the policy for record retention that meets applicable legal, DS&C and operating company requirements (or at least 6 months, whichever retention period is more).

Key Terms and Definitions

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 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. (e.g., flame arrestor, pressure safety valve, etc.).

Instrumented Protective System (IPS) – System of separate and independent combination of sensors, logic solvers, FEs, and support systems that addresses risk 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.

IOW-SOL – Critical alarm response to conditions that could result in rapid degradation of equipment integrity, potentially leading to an imminent loss of containment event as determined by the BU instruction for determining Integrity Operating Windows.

Tag/Flag – An electronic, hanging, and/or removable placard that identifies the status of a critical protection device. Tags should only be used on bypasses or temporarily out-of-service devices or components.

Table 1: Revision History

Version No. Change				
From	**To**	**Date**	**Summary of Changes**	**Approved by**
0.0	1.0	September 2015	Initial issuance of Standard	Scott Fife
1.0	2.0	July 2018	Alignment with approved 2017 Corporate update	Scott Fife