MARY KAY O'CONNOR PROCESS SAFETY CENTER

TEXAS A&M ENGINEERING EXPERIMENT STATION

20th Annual International Symposium

October 24-26, 2017 • College Station, Texas

Safety Instrumented Bypass Management

Amol V. Deshpande, CEng, TUV FSEng

Senior Process Safety Engineer

TOTAL Petrochemicals & Refining USA Inc.

Houston, Texas, USA

amol.deshpande@total.com

1. Abstract

Proper management of Safety Instrumented Function (SIF) bypasses during process plant operation can be challenging and could compromise process safety if the SIF is bypassed longer than its allowable maximum time interval.

Safety bypass procedures are usually written on site to comply with OSHA 1910.119 and IEC61511. However, in practice, safety bypass management can be difficult due to a lack of readily available process safety information, lack of operator awareness and the existence of a production throughput oriented culture.

For many operating sites, process safety information (PSI) is only available in Process Hazard Analysis (PHA) reports. Commercial databases are available which display process safety information and make it readily available to operations and maintenance to properly implement and handle safety bypasses. An alternative approach is the creation of an in-house process safety database to provide easily-accessed process safety information.

This paper will present a case-study on how TOTAL-Port Arthur Refinery developed and implemented such a system. The paper will include our flow chart for bypass approval, how we perform a bypass risk assessment and how we developed our SIS database.

This SIS database has also proven useful for ‘operator training’ on the risks associated with the process unit and the available safeguards to manage those risks.

Keywords:

Safety Instrumented System, Safety instrumented Function, Safety Instrumented Bypass

2. Introduction

Safety instrumented function (SIF) acts as a preventive barrier to reduce the unmitigated risk. SIFs are automatic prevention barriers and do not require any manual intervention. Safety instrumented functions comprise of sensors, logic solver and final elements. SIF has a defined executive action to bring a process to a safe state.

SIFs are often bypassed during

- proof testing or
- start up procedures or
- instrument failure.

Even with a bypass management procedure in place, it is not sufficient to meet the requirement of IEC61511-1 standard due to the lack of information about:

- predefined mitigation measures until SIF is in bypass
- consequence and severity related to the SIF
- other independent protection layers

Robust procedure and process safety information plays an important role in the management of safety bypasses. When a bypass is invoked, process safety information like consequence and severity type help to carry out the risk assessment to reflect mitigation measures and approval information.

3. Example of Safety Instrumented Bypass

Consider a gasoline tank overfill scenario where miss-routine in to another tank is an initiating event, due to human error.

In the event of tank overfill, pool fire consequence is due to the presence of immediate ignition sources around the tank (Figure 1).

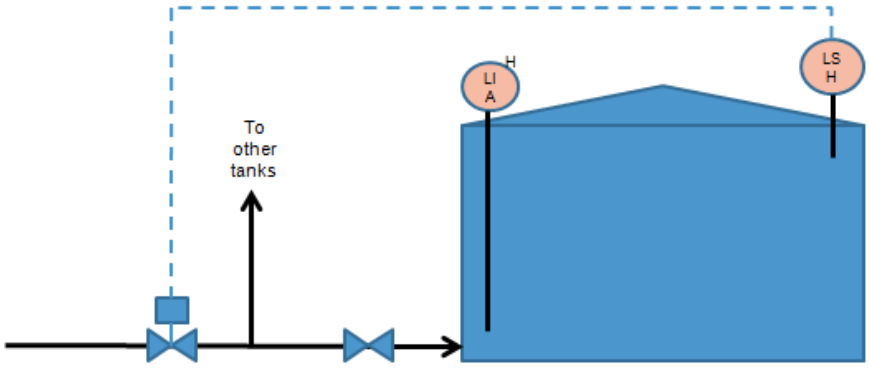


Figure 1: Tank Overfill Scenario

Risk Assessment:

For this scenario, TOTAL's risk matrix is used to carry out the risk assessment.

- Likelihood L5 represents once per 10 year frequency of an initiating event.
- Severity S3 represents one onsite fatality

Independent protection layers to prevent tank overfill

- (LI-A) Tank high level alarm with an operator response to terminate flow going into the tank.
- (LS-H) SIL-2 safety instrumented function to trip filling line valve

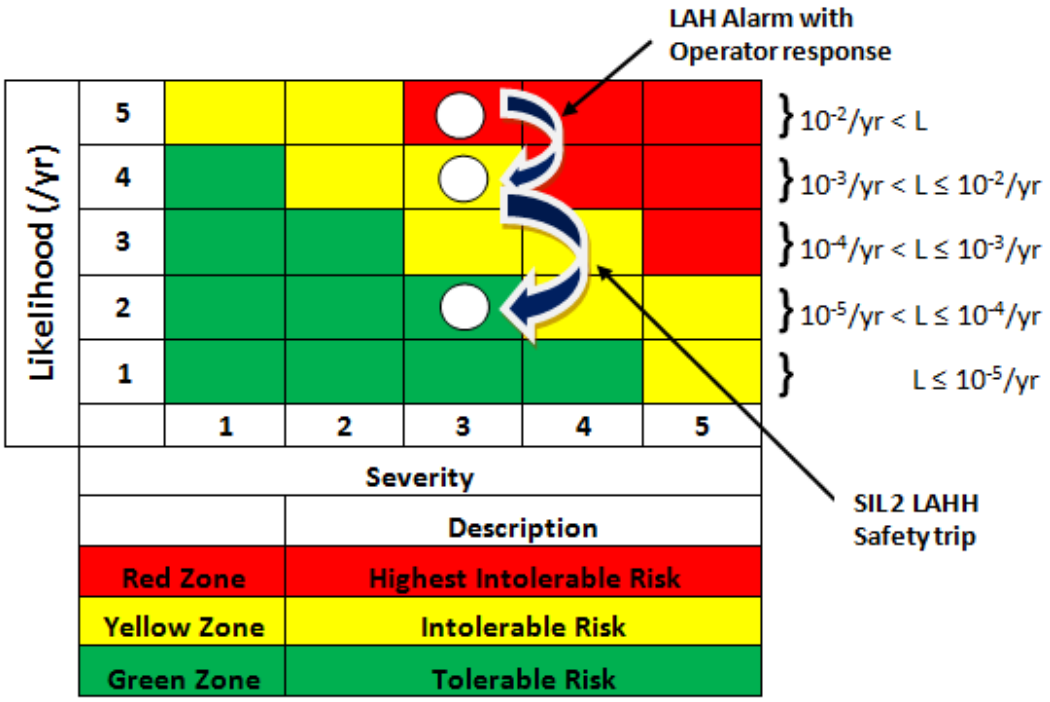


Figure 2: Tank Overfill Risk Assessment

If SIL 2 safety instrumented function malfunctions, then an operator could invoke safety bypass. The operator has to verify it is an instrument fault and not an actual demand on the safety system. After invoking safety bypass, the operator has to introduce additional mitigations during the mean time to repair period of an instrument, that can be qualitative, to reduce the likelihood of risk.

Additional mitigating measures could be:

- To validate the correct tank is lined up for the filling operation
- To verify change in the tank level in relation to the flow rate
- To validate product batch receipt against the available tank ullage
- Continuous monitoring of a tank level during the tank filling operation
- In the event of "Level Transmitter fault alarm" from Level Transmitter (LI-A) or (LS-H), the operator has to stop tank filling operation and investigate cause of an alarm
- For tanks with independent Level transmitter (LI-A) & (LS-H) installed, deviation between two levels are monitored to detect issues with the level instrumentation. Periodic checking of tank levels by operator during the tank filling operation also validates correct tank level.

Below is the graphical representation of additional mitigation measures introduced during mean time to repair by an operator.

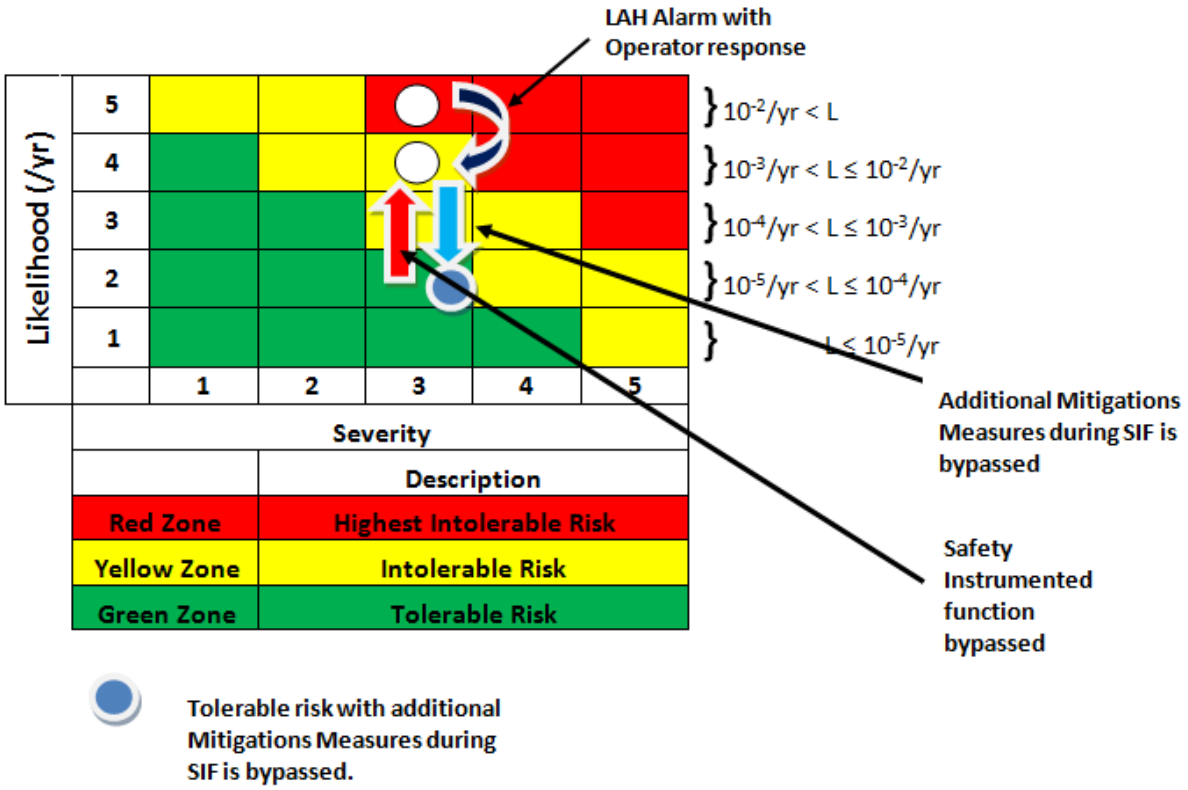


Figure 3: Safety bypass risk assessment with additional mitigating measures

4. Case Study at TOTAL Port Arthur Refinery, USA

As part of continuous improvement program to achieve operational excellence, bypass procedure was reviewed.

Following are the issues typically encountered during the management of safety bypasses:

a) Lack of proactive approach in identifying mitigation measures
b) Lack of bypass classification information i.e. safety, environmental or asset bypass.
c) Lack of operator competence and training on the usage of bypass procedure.
d) Difficulties in the management of paper based bypass procedure, due to the possibility of multiple paper copies at different locations (copies with board operator, shift supervisor and outside operator) showing different statuses of the safety bypasses.

4.1.Improvements to the management of safety bypass

Safety bypass procedure is modified with the following improvements

a) Safety trips are identified by referring to the Process Hazard Analysis (PHA) studies and safety documentation.
b) Information on additional mitigation measures are collected from experienced operators and validated with their supervisors.
c) In-class and computer based training on revised bypass procedure in conjunction with SIS database information is provided to the operators.
d) Identification of safety critical equipments on site as well as on DCS to make operations aware of critical equipments related to the safety trips.
e) An electronic bypass form rather than paper based forms
f) Development of SIS database which has predefined information on independent protection layers, consequence and type of severity, and additional mitigation measures

4.2.Revised Bypass Procedure

Safety trips are in place to prevent abnormal operational conditions. Abnormal operational condition is defined as 'It is a developing plant condition which is abnormal and which has the potential to evolve into a 'high risk' situation in which a safety instrumented system could potentially be activated.'

4.2.1. Safety bypass can be further classified into following types:

Maintenance bypass: It is used in order to allow repair or routine on-line testing and operability checks of a 'safety instrumented system' to ensure its continued functionality and reliability to operate on demand

Operational bypass: It is used to provide an opportunity to maintain a continued operation where an instrument fault or failure has been confirmed.

Permissive bypass: In certain procedural situations such as a unit or equipment 'start up', bypass has to be used as a 'permissive' to allow one or more input parameters of a 'safety instrumented system' that is in a 'tripped' status to reach the values required to enable a 'reset' of that system.

4.2.2. Following are the occasions when the bypass may need to be used:

a) Planned Bypass

Routine on-line checks or testing of the instrumented systems. Bypass risk assessment shall be carried out and all specified risk control measures put in place before the bypass is used for tasks within this category.

b) Unplanned bypass (Abnormal Operational Conditions)

i. Abnormal controlled operational condition

An ‘abnormal controlled operational condition’ is a developing process upset which has the potential to lead to a trip. If the situation has developed from a ‘known’ cause and has a well practiced method of quickly mitigating the risk and re- stabilizing the operation, the ‘controlled’ use of bypass may be used in such circumstances. The appropriate approval and authorization is required when its use is clearly identified within a recognised practice and or procedure.

For example: Instrument fault

Despite any history or experience of an instrument’s poor reliability, a fault or failure should not be automatically assumed. All suspected faults or failures must first be confirmed by other signs, signals and symptoms prior to bypass being used.

In cases where the circumstances and potential consequences of an instrument fault allow a bypass, ‘Bypass Risk Assessment’ shall be carried out and the specified risk control measures will be put in place before the bypass is used.

ii. Abnormal uncontrolled operational condition

An ‘abnormal uncontrolled operational condition’ is a process upset where the cause is unknown and therefore no method of address is immediately available or known and a process of investigation and diagnosis is required to identify the cause. Bypass shall never be used for “uncontrolled abnormal operational condition”

c) Permissive bypass

When the trip function of a safety instrumented system is in an activated state and is therefore preventing the continuation of a start-up or other operational procedure, the use of bypass may be required as a ‘permissive’ to allow one or more of the safety instrumented system input parameters to reach the values required to enable its ‘reset’.

In such cases, it is not necessary to complete bypass risk assessment form because the trip is already in an ‘activated state’ and the increased monitoring, checking and focus is required as key control measures. Key control measures will already be in place due to the procedural start-up requirements.

Once the instrumented system parameters have all reached the ‘stable’ values required to enable its ‘reset’, the permissive becomes the bypass again and therefore must be immediately removed to enable the instrumented system protection.

4.3.Bypass Risk Assessment

Additional mitigation measures are implemented from SIS database and maintained during MTTR till instrument fault is rectified. If bypass continues to be in place after MTTR and not taken out then ‘extended use’ or a ‘long term strategy’ should be implemented.

a) Extended Use:

When the bypass is needed to remain ‘active’ beyond its defined ‘maximum permitted duration’ it is said to have had ‘extended use’. Authorization for the ‘extended use’ of the bypass shall only be granted by the appropriate level of authority for the site and shall be based on an assessment of the potential risk posed by the bypass extended use. Such assessments shall include the consideration of the risk control measures already in place as per ‘Bypass risk assessment’.

b) Long Term Strategy:

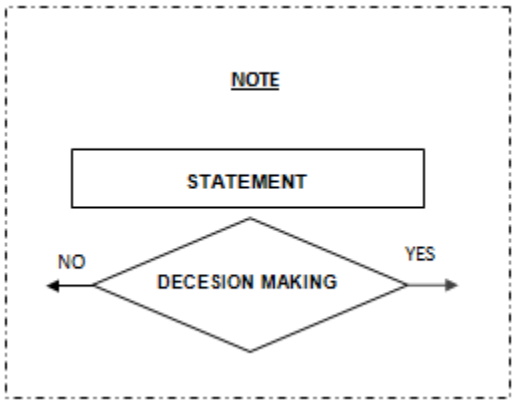
It is an authorized and approved plan of temporary measures or plant modifications that effectively implements an equivalent level of protection to that of the ‘safety instrumented system’ such that the continued use of the bypass on that system is no longer required.

c) Mean Time To Repair (Maximum Permitted Duration):

It is a specified period of time (60 hours) i.e. after 5 shifts, allocated to each bypass and which defines the maximum duration the bypass can be ‘active’ each time it is used (with the risk control measures in place), before authorization for an extended use or a long term strategy is required.

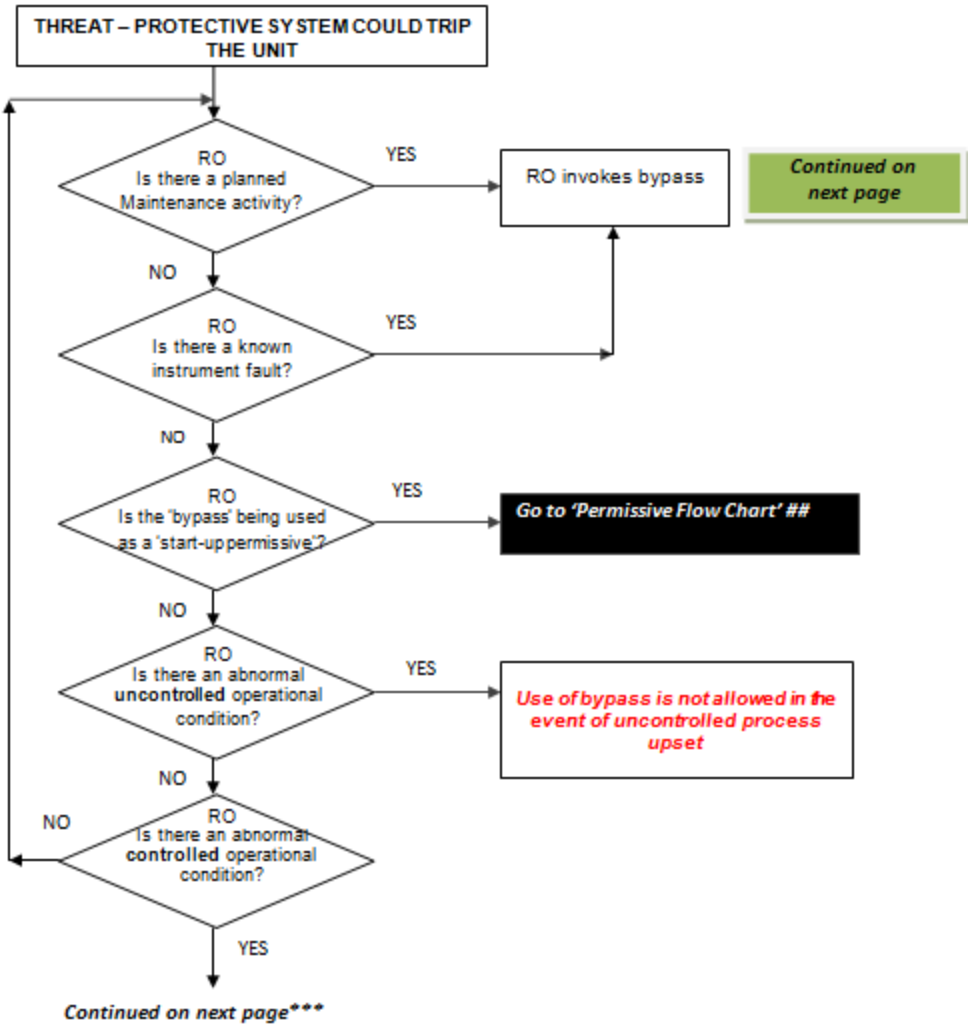
4.4.Flow chart for revised bypass procedure

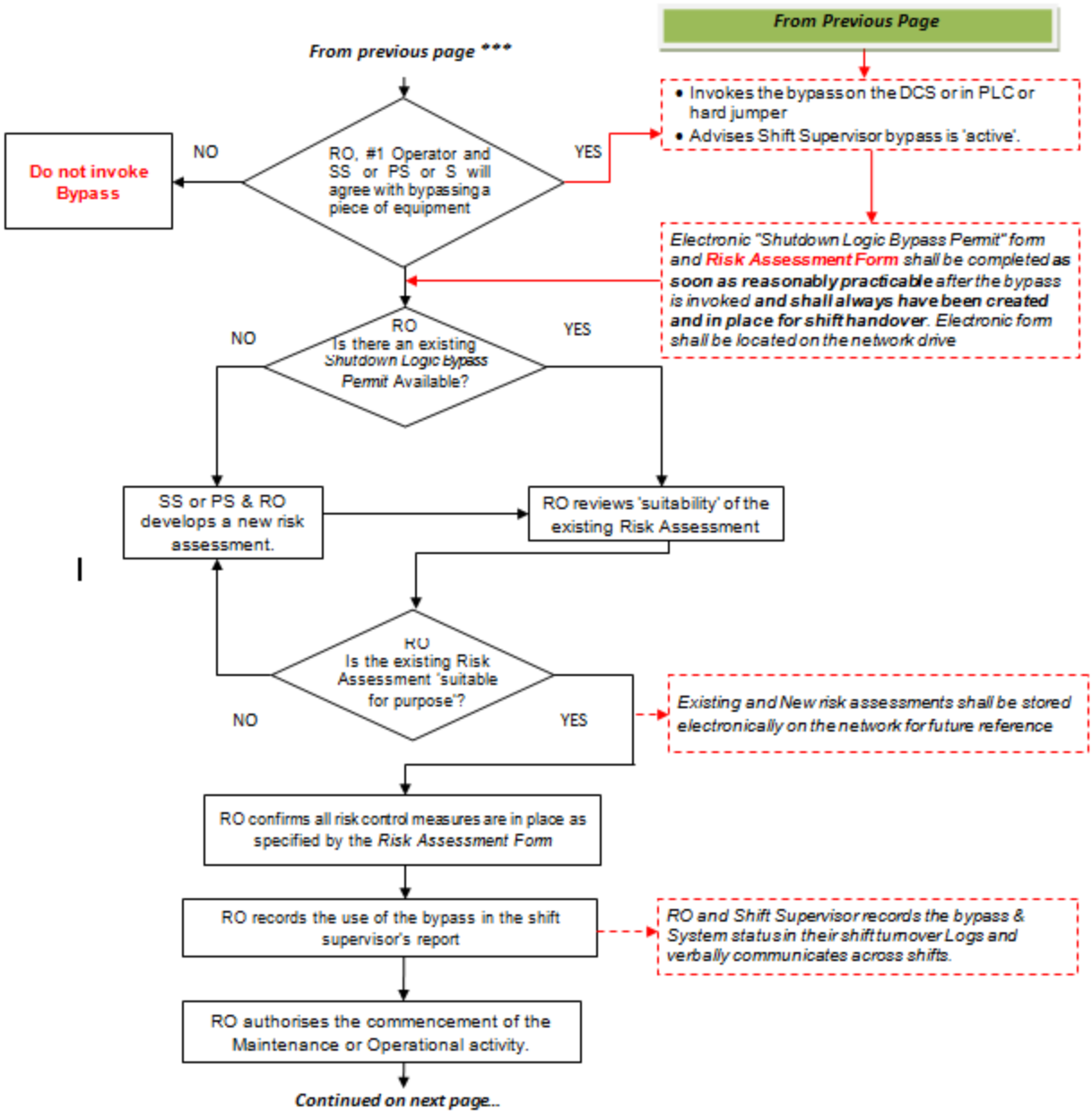
Flow chart shown below reflects the revised bypass procedure

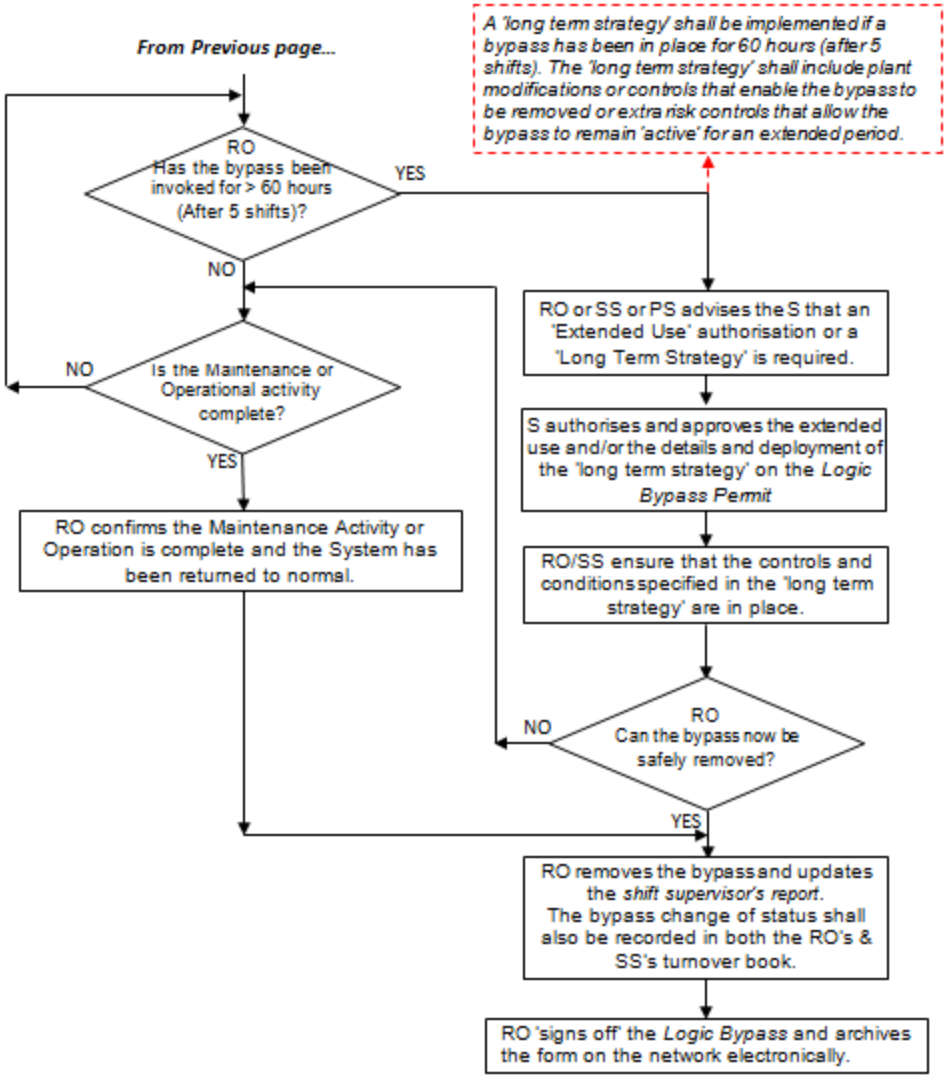


Acronyms:
RO: Responsible Operator
PS: Process Supervisor
SS: Shift Supervisor
S: Superintendent

FLOWCHART - "Bypass" procedure




From Previous Page
From previous page ***
• Invokes the bypass on the DCS or in PLC or hard jumper
• Advises Shift Supervisor bypass is 'active'.
RO, #1 Operator and SS or PS or S will agree with bypassing a piece of equipment
NO
YES
Do not invoke Bypass
Electronic "Shutdown Logic Bypass Permit" form and Risk Assessment Form shall be completed as soon as reasonably practicable after the bypass is invoked and shall always have been created and in place for shift handover. Electronic form shall be located on the network drive
RO
Is there an existing Shutdown Logic Bypass Permit Available?
NO
YES
SS or PS & RO develops a new risk assessment.
RO reviews 'suitability' of the existing Risk Assessment
RO
Is the existing Risk Assessment 'suitable for purpose'?
NO
YES
Existing and New risk assessments shall be stored electronically on the network for future reference
RO confirms all risk control measures are in place as specified by the Risk Assessment Form
RO records the use of the bypass in the shift supervisor's report
RO and Shift Supervisor records the bypass & System status in their shift turnover Logs and verbally communicates across shifts.
RO authorises the commencement of the Maintenance or Operational activity.
Continued on next page...


From Previous page...
A 'long term strategy' shall be implemented if a bypass has been in place for 60 hours (after 5 shifts). The 'long term strategy' shall include plant modifications or controls that enable the bypass to be removed or extra risk controls that allow the bypass to remain 'active' for an extended period.
RO
Has the bypass been invoked for > 60 hours (After 5 shifts)?
YES
NO
RO or SS or PS advises the S that an 'Extended Use' authorisation or a 'Long Term Strategy' is required.
S authorises and approves the extended use and/or the details and deployment of the 'long term strategy' on the Logic Bypass Permit
RO/SS ensure that the controls and conditions specified in the 'long term strategy' are in place.
RO
Can the bypass now be safely removed?
NO
YES
Is the Maintenance or Operational activity complete?
NO
YES
RO confirms the Maintenance Activity or Operation is complete and the System has been returned to normal.
RO removes the bypass and updates the shift supervisor's report.
The bypass change of status shall also be recorded in both the RO's & SS's turnover book.
RO 'signs off' the Logic Bypass and archives the form on the network electronically.

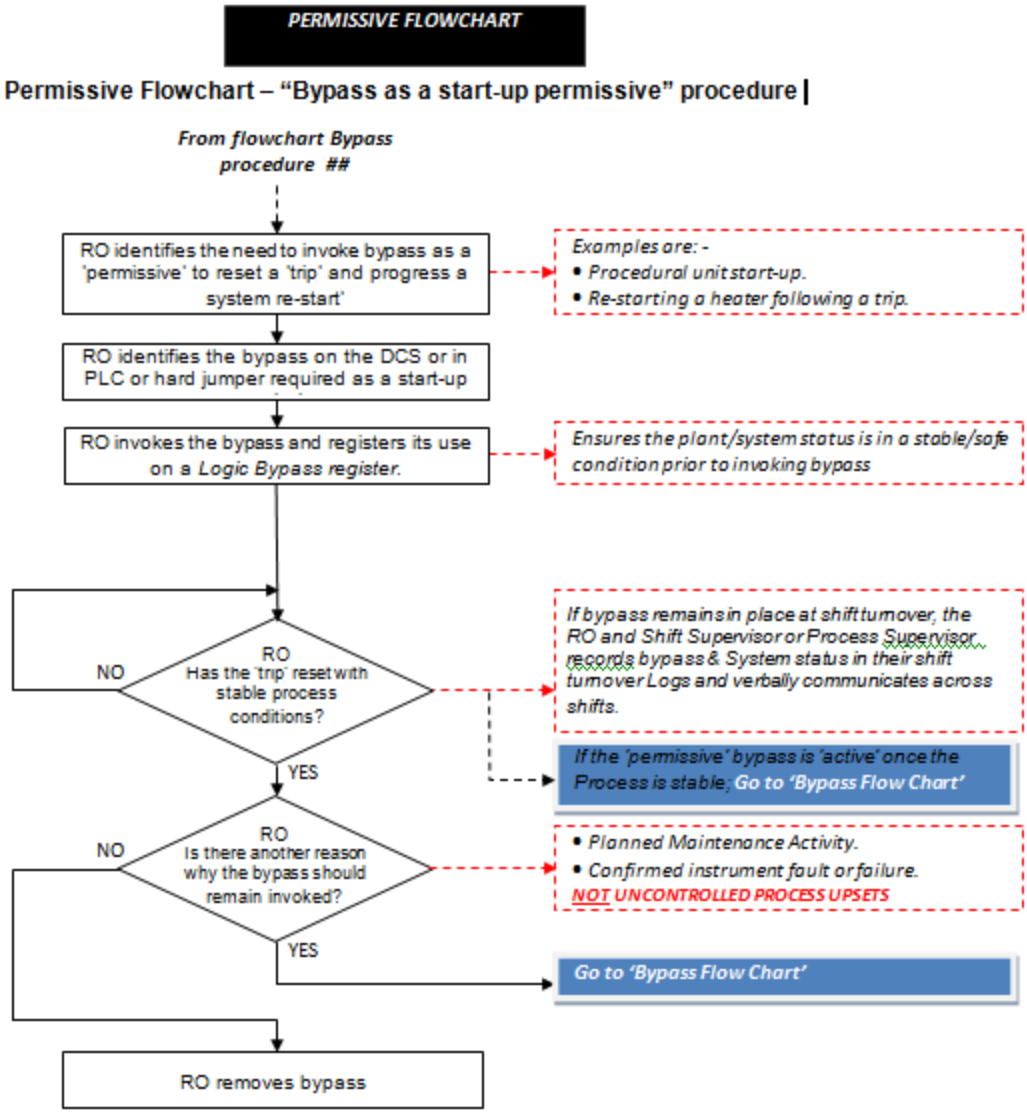


Figure 4: Flowchart for revised bypass procedure

4.5.Bypass Authorization and Risk Assessment Form

Bypass Number : Bypass Status:
Tag ID / Instrument details:
Bypass Type: ◯ Safety Bypass (SIS) ◯ Process Bypass (Non-SIS)

Type of Bypass(tick applicable):- Maintenance >		Procedural Operation >		Instrument Failure >
Reason for bypass:				
Work Order Number:				
Equipment affected by bypass:				
Does the bypass leave equipment without relief protection: Yes / No				
Safety & Environmental critical measure (SECM) : Yes / No				
Equipment Owner Signature: Date and Time:				

Shutdown system Logic Bypass Installation (To be completed by person installing bypass)
Tag or Identification Number of shutdown system device to be bypassed:

Location bypass installed: (DCS/ PLC/ Hard Jumper) If hard jumper, then following details required: Jumper (Tag#):	Jumpered at: Terminal Number:
Terminal Strip: Cabinet: Bypass Details:	Cabinet location:
Method bypass installed:	
Bypass Installer's name: Date & Time:	

While the bypass is in place, the following 'risk control' measures shall be put in place to maintain the risk potential of the system to the tolerable risk level Note: Refer SIS Database for SIS bypass mitigation measures if available	
1.	
2.	
3.	

The Shift Supervisor or Process Supervisor (or authorized deputy), shall sign below to confirm that the above measures are all in place and shall remain effective for up to a maximum of 60 hours (after 5 shifts), when authorization for 'extended use' or the implementation of a 'long term strategy' is required. See next page for details:

The Shift Supervisor has been made aware of the bypass and the risk controls required and has authorized the RO to sign below on their behalf. (tick when applicable)	

Print Name:	Signature:	Date:	Time:

All the time that the bypass is in place and effectively disabling the 'instrumented system', this completed form shall be kept posted at the panel console of the unit or area involved.

All Bypass movements shall be recorded in shift supervisor's report and also in the 'Shift Turnover Books' of the 'RO' and the Process Supervisor and effectively verbally communicated across shifts.

Renewal of Shutdown System Logic Bypass (To be completed by Equipment Owner)

	Date	Time	Equipment Owner Approval (Name)	Central Control Operator Approval (Name)	Supervisory Approval (Name)
Renewal 1					
Renewal 2					
Renewal 3					
Renewal 4					
Renewal 5					
Bypass Review					

After 60 hours (after 5 shifts), authorization for 'extended use' is required or a 'long term strategy' implemented.

'EXTENDED USE' AUTHORIZATION

Authorization is required from a Shift Supervisor or Superintendent for extended use of the bypass.

'Extended use' for	Hours	Justification:-		
Print Name:		Signature:	Date:	Time:

Note: When the period of 'extended use' has elapsed, a 'long term strategy' must be implemented.

LONG TERM STRATEGY

The implementation of measures to re-establish the integrity of the safety system such that the Bypass can be removed. The 'long term strategy' can be and implemented following the Management of Change standards and procedures

Details (including support document references)

(E.g. Additional Measures, MOC No, Work Notification etc.)
MOC Reference Number (where applicable):
Work Notification Reference Number (where applicable):

4.6.SIS Database

Following information is collected and made available to the operations personnel.

a) Description of a safety function
b) Other protection layers (such as alarm, DCS control, mechanical safeguard) which are considered during PHA study to mitigate risk before safety function is engineered.
c) Consequences and severity level of the unmitigated risk if safety function and other protection layers are compromised.
d) Instrument tags of the safety functions and its related equipment.
e) Safety Integrity level (SIL rating and Risk Reduction Factor) requirement of the safety function
f) Sensor voting logic and safe state description
g) Proof test requirement for safety function
h) Additional mitigating measure when safety function is in bypass

4.6.1. Development of SIS database has improved operational excellence as below:

a) Safety bypass management: Operators use safety bypass to bypass safety instrumented function during maintenance and operational activity. There is no discrimination between safety trips and basic process control trips. SIS database provides list of safety trips and its related Process Safety information

   When safety instrumented function is bypassed, operators can see which other independent protection layers (IPL) are considered as a safeguard during PHA for that safety instrumented function. With the available IPL information, operators can now validate IPLs related to ensure that they are not compromised and will be effective if there is a demand on them. SIS Database also identifies bypass variance which operator considers as additional mitigation measures.

b) Training: SIS database acts as a training tool for training operators. New or inexperienced operators can refer to SIS database to get familiar with additional mitigation measures as well as process safety information related to the safety instrumented function.

c) Management of change: SIS database information is useful during management of change process to carry out impact analysis

5. Summary

Robust safety bypass procedure along with SIS database not only improves operational excellence amongst operators but also improves safety culture. This approach also improves communication of safety bypasses during shift turnover. Improvements can be seen in management of safety bypasses across shifts. Competency of the operational personnel dealing day to day with the safety bypasses also improves.

Following points need to be addressed as part for the continuous improvement of operational excellence

a) Assessment of systematic errors during bypass management
b) Pre-defined mitigation measures for non-SIF and mechanical safeguards
c) Consideration of preventive maintenance for instruments used during mitigating measures
d) Management of independent protection layers related to safety instrumented functions

6. References

1. 29 CFR Part 1910.119, Process Safety Management of Highly Hazardous Chemicals,U.S. Federal Register, Feb. 24, 1992, http://www.osha.gov
2. ANSI/ISA-84.00.01-2004 Part 1 (IEC 61511-1: Mod). *Functional Safety: Safety Instrumented Systems for the Process Industry Sector – Part 1: Framework, Definitions, System, Hardware and Software Requirements*. The Instrumentation, Systems, and Automation Society. Research Triangle Park, NC.
3. TOTAL's DirSec08 Risk Matrix
4. 04-SIS-Mngmnt-Winter-Edition-2016, SIS Management Part 4: Bypass Management by Eloise Roche, SIS-Tech