IPL/CMS- Integrity Management of Non-SIS Independent Protection Layers after the LOPA

Ron Nichols
aeSolutions
10375 Richmond Avenue, Suite 800
Houston, Texas 77042
Ron.Nichols@aesolns.com

Prepared for Presentation at
American Institute of Chemical Engineers
2014 Spring Meeting
10th Global Congress on Process Safety
New Orleans, LA
March 30 – April 2, 2014

IPL/CMS- Integrity Management of Non-SIS Independent Protection Layers after the LOPA

Ron Nichols
aeSolutions
10375 Richmond Avenue, Suite 800
Houston, Texas 77042
Ron.Nichols@aesolns.com

Keywords: Non SIF IPL, Identification, Selection, Implementation, Life-cycle management, MOC, Security.

Abstract

This paper discusses the identification, selection, implementation and management of Non-SIF IPLs through the process lifecycle.

1. Layer of Protection Analysis

Layers of Protection Analysis (LOPA) in conjunction with the Process Hazard Analysis (PHA) is now a key tool used by the chemical, oil and gas industries to assist companies in identifying, implementing and managing the critical safeguards needed to achieve their risk tolerance targets. The LOPA is used to identify the number of Independent Protection Layers (IPLs) and their integrity needed to reduce the likelihood to an acceptably low frequency that an initiating cause will progress to an undesired consequence.

2. Lifecycle Management of IPLs

Since the acceptance of ISA 84.00.01/IEC-61511, the life cycle management of safety instrumented systems is now being implemented throughout industry. The required safety integrity level (dependability) for the safety instrumented functions (SIFs) are obtained by closing the LOPA gaps between the existing mitigated event likelihood (MEL) and the company's target mitigated event likelihood (TMEL). Often a SIF is combined with non-SIF IPLs to achieve the risk reduction gap closure, reducing the SIL requirement assigned to that SIF.

To maintain acceptable risk targets, all IPLs, not just SIFs, must be managed through the lifecycle of the process. This is because many LOPA gaps are closed by only non-SIF IPLs and the SIL assignment for many SIFs depend on the use of non-SIF IPLs used in that LOPA.

3. From IPL Identification through Lifecycle Management

IPL identification begins in the PHA where the worksheet captures the deviation initiating causes, hazard consequences (without credit for active safeguards/IPLs), consequence severity and existing IPLs (engineered and administrative safeguards). Based on the company's LOPA selection criteria, consequences assigned either high severity or high risk are selected for LOPA to determine if their MEL is adequate to meet the company's risk tolerance criteria. In the typical LOPA, the initiating cause has a frequency assigned and existing IPLs are identified and credited with a probability to fail on demand (PFD) for calculating the current mitigated event likelihood (MEL). LOPA quantifies if there is a gap between the MEL and the Target Mitigated Event Likelihood (TMEL) established to meet the company's risk tolerance requirements. If the LOPA finds a gap where the envisioned consequence is more frequent than the company's risk targets, the team will propose additional IPLs to close the risk gap or design changes to reduce the credible consequence severity. After identifying how many IPLs are needed to close a LOPA gap, existing IPLs must be validated as meeting the IPL criteria. If additional IPLs are needed to close a gap, they must be identified, validated to meet IPL criteria and implemented. After selected for implementation, all IPLs needed to meet the company's TMEL must be placed under a program for lifecycle management.

4. Requirements to Credit a Safeguard as an IPL

To classify a safeguard as an IPL it must meet the following criteria:

- Effectiveness/Specificity - this barrier by itself can prevent the cause from progressing to the undesired consequence.
- Independence - the IPL is independent from the initiating cause and other IPLs used in the LOPA to meet the targeted minimum event likelihood (TMEL) required by the company's risk tolerance requirements. Common cause failures between this IPL and the initiating cause or other IPLs will not defeat the protection.
- Dependability - the IPL can be relied on to function with an expected probability to successfully prevent the undesired consequence when placed in demand.
- Auditability - the IPL can be routinely audited/tested at an adequate frequency through the process lifecycle to maintain its' dependability.
- Access Security - there are controls in place that prevent unauthorized changes to the IPLs.

5. IPL Types

IPLs are often grouped into two categories: Preventative and Consequence Mitigation.

Preventative

Preventative IPLs will prevent the cause from progressing to the undesired consequence. Examples of preventative IPLs include alarms that initiate operator intervention, standard operating procedures (independent of the cause) that can prevent the consequence from occurring, basic process control interlock functions and safety instrumented systems.

Consequence mitigating

Consequence mitigating IPLs often referred to as consequence mitigation systems (CMS) reduce the severity of the undesired consequence to a level that meets the companies risk tolerance. Examples of CMS include pressure relief devices, dikes and instrument activated deluge systems.

6. Efficient Documentation for the IPL Lifecycle

The efficiency of the IPL implementation work process improves when the documentation and procedures for information capture, validation, selection and integrity management are integrated through the different phases. The IPL implementation process can involve different teams and stakeholders operating over an extended period of time. Developing an IPL implementation documentation protocol for consistent capturing of the key information and standardizing the work practice between different individuals or teams early in the process improves the efficiency of the IPL implementation and subsequent lifecycle management.

7. IPL Documentation during Initial PHA/LOPA study

For the initial PHA and LOPA studies, it is helpful for the company to provide a protocol to capture key information in the PHA Worksheet that can be efficiently referenced. Consistent capture of key details of the initiating causes and existing IPLs in the PHA worksheets assists later teams through the steps of IPL identification, validation, selection, implementation and lifecycle management.

Examples of initiating cause details to capture in the PHA worksheet can include:

- BPCS Control Loop: Tag numbers of instrument inputs and outputs, P&IDs where the input and output instruments are located.
- Human Operations: Frequency the step is routinely performed, reference to document number and Step # for that operation, reference of procedure for independent checks of the procedure, guidance on probability of failure.

Examples of IPL information to capture in the PHA Worksheets can include:

- BPSC or SIF: Instrument tag numbers inputs/outputs, logic solver ID (if multiple), P&IDs the instruments are located on.
- Alarms: Instrument tag number, setpoints and reference to documented operator response requirement.
- SOP: Document number and step for the action that prevents the progression to the undesired consequence.

7.1 IPL Register

While the numbers of instruments, procedures and other safeguards used on a site can be enormous, the fraction classified as IPLs is relatively few. The development of a central IPL register can be a useful tool to aid the implementation, management and update of the site's IPLs. This register can provide a cross reference to the PHA/LOPA source(s) that uses the IPL and reference to the documents that support the IPL's validation.

7.2 Assigning PFD to IPL

To provide consistency across different PHA/LOPA teams, procedures should provide the teams with a common set of IPL dependability values (PFDs) with a reference to any literature source and guidance on their selection. The following are some common sources of published sources for dependability values used in industry:

- Oreda
- Exida
- Nureg
- CCPS.

7.3 Team Development of Probability of Failure on Demand (PFD) Values

Where no published PFDs are available, it is useful for the site to provide guidance for an IPL study team to develop and document PFDs based on the site's operating experience or maintenance records.

8. IPL Validation

8.1 Consequence Severity Verification

During the IPL validation step, performing a more rigorous consequence assessment may allow a severity reduction to the hazard reducing the number or even need for IPLs. The use of these tools may not be available or practical for use during the initial PHA/LOPA study resulting in the team assigning an overly conservative consequence severity. Often the use of these tools is driven by the challenge to provide adequate IPLs to meet the TMEL for the identified consequence. Some examples of more rigorous consequences modeling tools include:

- PHAST
- HYSIS/ Aspen
- Computational Fluid Dynamics.

9 Confirming Existing and Proposed IPLs Meet Design Criteria

During the validation stage, the IPLs are reviewed to confirm compliance with the following IPL requirements:

9.1 Independence

Independence between the initiating cause and IPL(s) or between different IPLs used to mitigate the event likelihood must be confirmed. If the site procedure allows two BPCS credits within a single LOPA then:

- The BPCS inputs and outputs must not be shared between the initiating cause and an IPL or between the two different IPLs.
- The IPLs or initiating cause must not share common sensors, elements, or I/O cards.

9.2 Effectiveness/Specificity

The IPL should provide documentation supporting how this IPL can by itself prevent the initiating cause from reaching the undesired consequence, such as:

- PSV documented with design basis and calculations to support sizing meets required relief rate for the consequence identified in the LOPA.
- Response times for the operator response to alarms are studied and documented to show there is adequate time to diagnose the event and take the required actions to prevent the undesired consequence
- BPCS interlock response time and outputs are adequate to prevent the undesired consequence
- Dikes are adequately sized to hold the contents of the loss of containment.

9.2.1 Dependability

Adherence to appropriate recognized and generally accepted good engineering practice (RAGAGEP) is useful to support the PFD credit given during the initial LOPA. The following are some common RAGAGEP providing guidance on the design of IPLs that can support their dependability and auditability:

- PSV: Boilers ASME I, Unfired Equipment ASME VIII, API 520, API 521, API 5210/5210A,
- PVSV: NFPA 30, API 2000,
- BMS: NFPA 85, NFPA 86, NFPA 87, API 556
- SOPs: 29 CFR 1910(f)(1)(i)(D), HSE Human Factors Toolkit
- Alarms ISA 18.2, NUREG/CR-1278,
- Deluge: NFPA 15,
- Explosion Prevention NFPA 69,
- Explosion Venting: NFPA 68
- etc.

9.3 Eliminating or Modifying IPLs

If during the validation process identified IPLs are determined to be invalid, then recommendations must be made to modify or replace IPLs as needed to close the gap. The company should define a protocol to replace or modify IPLs that includes:

- Written Management of Change Procedures and Practices
- Who is involved in accepting and approving the change, i.e. stakeholder/team composition?
- What is the documentation procedure and how will the original PHA/LOPA be updated?

10 Final Selection of IPLs

From experience, the final selection of IPLs to be implemented and managed through the process lifecycle involves team meetings that include the original PHA/LOPA team and the facility controls/SIS engineer. The team reviews the IPL options and makes final IPL selections based on the following criteria:

- Operability
- Process Safety time
- Maximum allowable Response Time
- Hardware Fault tolerance for SIFs
- Financial analysis

This team meeting also provides the opportunity to close the recommendations associated with consequences reduced by performing a more rigorous consequence assessment or by implementing inherently safe design change.

The output of this meeting is the IPL list for implementation and management that provides their basis for criticality or design.

10.1 Excess IPLs

Occasionally more IPLs are identified by the team than are needed to close the TMEL gap. This can occur if multiple valid IPLs are identified during the PHA/LOPA or if a SIF integrity level design is driven by a higher gap scenario reducing the number of supporting IPLs needed to close the risk reduction gap.

How will your procedures handle excess IPLs?

- Will all IPLs be kept or only those needed to close the gap?
- What will be done with excess IPLs removed from the IPL list; deleted or converted to non IPL Safeguards?

10.2 IPL Priority

For consistency between the different PHA/LOPA teams and through IPL management, the company may wish to provide a philosophy of priority for selecting IPLs. For example:

- Prevention versus Mitigation,
- Engineered response verse operator response etc.

11 IPL Integrity Management (Auditability) through the Process Lifecycle

11.1 Auditability/Integrity Management Procedures

After IPL selection, the company must place the IPLs under a testing program (auditing) to support their dependability. This testing program must include:

- Defining test frequency and maintenance priority
- Documenting test results in maintenance system
- Defining corrective action requirements for test results showing nonconformance, e.g.:
- Firewater pumps don't pass test
- PSV fail testing, nozzles repeatedly found plugged
- Alarms nonfunctioning or defeated
- SOP refresher testing fails
- Defining maximum time allowed to repair and steps for authorization to operate with deficient IPL, or risk gap, until repair is made.

11.2 RAGAGEP that Supports IPL Testing

Adherence to a RAGAGEP for testing IPLs can provide a good basis to support the safeguards dependability. The following are examples of a few RAGAGEP that provide guidance on inspection and testing of IPLs:

- PSV: ASME 576
- BMS- NFPA 85, NFPA 86, NFPA 87, API 556
- SIF-ISA 84.00.01/IEC-65111.

Where there is no guidance from RAGAGEP, the site should develop a procedure/protocol to define appropriate testing that each IPL needs to support its' dependability.

To meet the requirements of 29 CFR1910.119for engineered and administrative safeguards, the site must have written management systems to identify the IPL auditing tests, schedule the required tests, maintain test records and initiate the required correction of nonconformance.

12 Tools for IPL Validation

12.1 Checklist to Support the IPLs Validation Process

A valuable tool to provide the IPL validation team is a set of checklists to guide and document the requirements for the different IPL types. These checklists confirm and document the independence, effectiveness, dependability, auditability and security for the different IPLs being implemented. The following are examples of several IPL checklists to demonstrate the concept.

Table 1. Alarm SOP

Description	Guidance/Comments
Independence	
Verify the consequence severity was based on no active safeguards. The contribution of this IPL was not considered when assigning the severity.	
Confirm the alarm that initiates operator response is independent of the LOPA's initiating cause	If the cause is a BPCS failure there can be no shared instrument loops, including the I/O card. Define where this is documented.
Confirm the alarm and required operator action(s) are fully independent from all other IPLs credited in the same LOPA scenario(s).	Instrument inputs to other IPLs must be independent of this alarm. The operator actions must be independent of other IPL outputs to prevent the consequence. If two uses of the BPCS are allowed for either initiating cause and IPL or as 2 separate IPLs, they must not share the same I/O card.
Effectiveness/Specificity	
Verify the response time for alarm setpoint provides the operator adequate time to diagnose and take action to prevent the consequence.	Provide location of documented study supporting adequate response time.
Verify the operator actions for alarm response are documented	Reference the document detailing required response to the alarm.
Confirm the service which this Alarm's sensor(s) is in is not prone to problems from plugging, polymerization, fouling or external environmental conditions.	
Performance or Dependability	
Verify documented basis for Probability of Failure on Demand (PFD) used in LOPA calculation.	Reference source/basis for PFD.
If no published basis, provide documentation on how the team developed the PFD used in the LOPA.	Provide procedures on PHA/LOPA team PFD development and documentation for retrieval and reference.
Define required repair time for the alarm as needed to maintain dependability. If a backup alarm is identified as needed it is also placed under IPL management.	
Check if design is per a RAGAGEP	ISA 18.2

Description	Guidance/Comments
Auditability	
Verify the following: • The management system records the alarm setpoint. • The alarm's logic solver and sensors are identified in the sites management systems as safety critical. • That requirement for periodic testing of the alarm is specified • There is documentation linking this IPL to the consequence in the PHA/LOPA it protect against	Reference SOPs and work orders for managing alarm and response procedure testing.
The data sheet for this Alarm's sensor(s) is complete and available.	Document where are datasheets located to reference? How are they updated and who is the custodian?
Verify the operator actions to be taken in response to the part of a the periodic retraining program	Reference to the procedure listing the frequency for required operator retraining on this procedure.
The SOP(s) which describes the required Operator response to this Alarm is periodically reviewed by the department.	1910.119(f)(1)(i)(D)
Verify the alarm's sensors are calibrated and inspected in accordance with site procedures	Reference the site: Procedures for testing. Procedure to archive test results. Procedures to require correcting nonconformance.
Testing meeting appropriate RAGAGEP.	CFR 1910.119 (f)(3)
Security	
Verify the alarm setpoints are secure.	Alarms are not resettable by the operator without authorization and management of change.
All Software changes which impact this Alarm are reviewed and authorized under "Management of Change" protocol.	

Table 2. SOP

Description	Guidance/Comments
Independence	
Verify the consequence severity was based on no active safeguards. The contribution of this SOP or any other active IPL did not reduce the severity assigned to the consequence.	
This SOP, the related Operator Action and the final element(s) that the operator may use are independent of the LOPA scenario initiating cause(s).	Example: The primary operator response can't be to put a control valve in manual and close it to isolate the flow if the initiating event was a BPCS of a loop operating that valve.
This SOP, the related instruments in use during the execution of the steps or final elements related to the Operator Action are fully independent and separate from all other IPLs credited in the same LOPA scenario(s).	Example: The operator can't actuate a valve closed that is being closed by a BPCS interlock.
The potential for Common Cause Failure between this SOP and other IPLs credited in the same LOPA scenario(s) has been ruled out.	
Performance or Dependability	
The documentation source(s) supporting the Probability of Failure on Demand (PFD) selected for this IPL is referenced.	

Description	Guidance/Comments
Specificity	
This SOP is designed to fully prevent the LOPA scenario consequence(s).	Document basis for action of this SOP preventing the consequence The procedure is of sufficient detail to support consistent execution by any operator.
There is ample time for the operator to execute the procedure as intended and described.	An independent operator reviewing in the field on rounds has enough response time for a slow developing event Independent person performing checklist verification prior to start up verifies actions of prior operator
Auditability	
The SOP(s) which describes the required Operator response to this Alarm is periodically reviewed by the department.	
The SOP is inventoried on the IPL register. The affected personnel receive required training and periodic retraining The SOP receive periodic review and authorization to verify it is current and effective.	CFR 1910.119 (f)(3)
Security	
Changes to the procedural steps in this SOP are reviewed and authorized under "Management of Change" protocol.	

Table 3. BPCS IPL

Description	Guidance/Comments
Independence	
Verify the consequence severity was based on no active safeguards. The contribution of this BPCS Interlock or any other active IPL did not reduce the severity assigned to the consequence.	
The failure of this BPCS Loop's logic solver, sensors and control elements are independent of the LOPA scenario initiating cause(s).	
This BPCS Loop's logic solver, sensors and control elements are fully independent and separate from all other IPLs credited in the same LOPA scenario(s).	If two BPCS loops are allowed for the LOPA (e.g. initiating cause and IPL or as 2 separate IPLs) they must not share the same I/O card.
Performance or Dependability	
Verify documented basis for Probability of Failure on Demand (PFD) used in LOPA calculation.	Reference source/basis for PFD.
Design is per a RAGAGEP.	
Specificity	
Document how BPCS Interlock is designed to fully prevent the LOPA scenario consequence(s).	
When de-energized, this BPCS Loop's control elements will transition to their "safe" states for the credited LOPA scenario(s).	

Description	Guidance/Comments
The service which this BPCS Loop's sensors and control elements perform do not have records of instrumentation problems from plugging, polymerization, fouling, or external environmental conditions.	
When this BPCS Interlock detects the hazardous process excursion, it can fully transition its control elements to their safe states within the Maximum Allowable Response Time.	
Define required repair time for the BPCS as needed to maintain dependability.	
Auditability	
This BPCS Loop's logic solver, sensors and control elements are properly documented as IPL's per the site's procedures.	
The data sheet for this BPCS Loop's sensors and control elements are complete and available.	
This BPCS Loop's sensor(s) and control element(s) calibration and proof tested procedures are complete and available.	
This BPCS Loop's calibration is in accordance with site procedures and records are well maintained, current, available and includes both "as found" and "as left" conditions.	
This BPCS Loop's proof test records are well maintained, current, available and includes both "as found" and "as left" conditions.	
Security	
All Software changes which impact this BPCS Interlock are reviewed and authorized under "Management of Change" protocol.	
This BPCS Loop's logic block, sensors and control elements are only bypassed with heightened administrative controls and the bypassed state is clearly indicated on the HMI and the bypass is authorized per site procedures.	

Table 4. Rupture Disk IPL

Description	Guidance/Comments
Independence	
Verify the consequence severity was based on no active safeguards. The contribution of this rupture disk or any other active IPL did not reduce the severity assigned to the consequence.	
The failure of this Rupture Disk is independent of the LOPA scenario initiating cause(s).	Condition that can plug the nozzle to the rupture disk (e.g. polymerization, freezing, coking).
This Rupture Disk is fully independent and separate from all other IPLs credited in the same LOPA scenario(s).	
Performance or Dependability	
The Probability of Failure on Demand (PFD) selected for this IPL is based on a published source	Document source for PFD
If this Rupture Disk is coupled with a Pressure Relief Valve, the interstitial space is monitored to detect leakage.	If the interstitial space is field monitored there is a procedure for routine monitoring and documentation of the interstitial space observations. If a pressure alarm monitors the interstitial space then this alarm receive periodic testing. Procedure initiates corrective action if the rupture disk is determined to be leaking.
If this Rupture Disk is in potentially freezing service, then measures have been implemented to counter these effects (e.g. heat tracing).	If nozzle and rupture disk are heat traced, then procedures or instruments are in place to detect its' failure
Procedure is in place to inspected/replace rupture disk if it is suspected to have been challenged.	
Design is per a RAGAGEP	ASME VIII, API 520, API 521
Specificity	
This Rupture Disk is only bypassed with heightened administrative controls. Valves to the rupture disk are under a management system	
This Rupture Disk is designed to fully prevent the LOPA scenario consequence(s).	Relief device design basis for the rupture disk includes the LOPA consequences it is protecting against.
The outlet of this Rupture Disk has been designed for safe discharge (e.g., sized for adequate flow, process sewer, above congested process equipment, to a flare header).	
Auditability	
This Rupture Disk is periodically removed from service, tested and inspected for signs of corrosion.	
If this Rupture Disk is installed in polymerizing or fouling service, or there are extreme external conditions, it is removed for inspection during a shutdown.	
The data sheet for this Rupture Disk is complete and available.	
This Rupture Disk proof test procedure is complete, available	

Description	Guidance/Comments
and includes both "as found" and "as left" conditions. It also includes inspecting and verifying the information on the Rupture Disk's tongue.	
Testing meets appropriate RAGAGEP.	
This Rupture Disk's inspection records are well maintained, current and available.	
Security	
If there are Maintenance valves in line with the rupture disk, they are on a periodic inspection to verify they are in the open position	
Change to the rupture disk requires MOC.	
If the process changes made can affect relief requirements, then the MOC updates relief device design basis, calculations and initiated changes as needed	

Table 5. PSV IPL

Description	Guidance/Comments
Independence	
Verify the consequence severity was based on no active safeguards. The contribution of this PSV or any other active IPL did not reduce the severity assigned to the consequence.	
The failure of this Pressure Relief Valve is independent of the LOPA scenario initiating cause(s).	
Performance or Dependability	
The Probability of Failure on Demand (PFD) selected for this IPL is based on a published value.	PFD is based on published source and nature of service (e.g. clean or fouling, risk of corrosion etc.).
All manual valves which can block this Pressure Relief Valve are managed (locked or car-sealed) open.	
If this Pressure Relief Valve is coupled with a Rupture Disk, a pressure gauge is installed in the interstitial space to detect leakage.	If the interstitial space is field monitored there is a procedure for routine monitoring and documentation of the interstitial space observations. If a pressure alarm monitors the interstitial space then this alarm receive periodic testing. Procedure initiates corrective action if the rupture disk is determined to be leaking.
If this Pressure Relief Valve is installed in polymerizing service or fouling service, or there are extreme external conditions, it is periodically inspected during a shutdown to verify that nozzles are open.	
Design is per a RAGAGEP.	
Specificity	
This Pressure Relief Valve is only bypassed with heightened administrative controls and the bypass is authorized per site procedures.	
This Pressure Relief Valve is designed to fully prevent the LOPA scenario consequence(s).	Design basis documents that the PSV is adequately sized for the LOPA consequences it is to protecting against.

The outlet of this Pressure Relief Valve has been designed for safe discharge.	
Auditability	
This Pressure Relief Valve is properly documented as an IPL per the site's procedures.	
The data sheet for this Pressure Relief Valve is complete and available.	
There is instrumentation which will indicate when this Pressure Relief Valve has been challenged. This Pressure Relief Valve is to be inspected if it is suspected to have been challenged.	
This Pressure Relief Valve's proof test procedure is complete and available.	
This Pressure Relief Valve is periodically removed from service, tested and inspected for signs of corrosion.	
Testing meeting appropriate RAGAGEP.	API 576
This Pressure Relief Valve's inspection records are well maintained, current, available and includes both "as found" and "as left" conditions.	
Security	
Change to the PSV requires an MOC	
If a process changes made can affect relief requirements, then the MOC updates relief device design basis, calculations and initiates required design changes.	
If there are maintenance valves in line with the rupture disk they are on a periodic inspection to verify they are in the open position	

12.2 Drill Down Audit of a Statistical Sample of IPLs

The "drill down" audit is a useful tool to validate the IPL management system effectiveness. The drill down audit involves periodic selection of a random sample of the different IPLs at the site. The audit trail selects a starting location to obtain the sample the IPLs, i.e. the originating PHA/LOPA to the IPLs documented or the site IPL register. The following outlines examples of drilldown audits for different IPLs.

<u>Auditing Alarm IPLs</u>

In a drill down audit, the following features are verified for Alarm IPLs:

- The setpoints are properly documented and set on the BPCS.
- These alarms are under management to prevent unauthorized changes and no history of unauthorized changes have been made.
- There is a PM in the maintenance/MI system to periodically test the alarm.
- The documented instructions for operator alarm response are reviewed and confirmed as current.
- These documented procedures have been periodically reviewed per site procedure.
- Operators are interviewed to verify their knowledge of the actions to be taken.

- The training program is reviewed to verify the training program includes both initial training and periodic retraining of the affected operators.
- Operator training records are reviewed to show the training of all affected operators is up to date.
- Maintenance records are reviewed confirming the periodic alarm tests have been performed and any corrective actions implemented for any nonconformance.
- Any changes to the alarm IPLs or associated initiating cause/consequences were correctly managed under MOC.

SOP IPLs

The sample of SOPs identified as IPLs are obtained for drill down audit to verify:

- These SOPs are periodically reviewed per site requirements.
- The training program includes these SOPs for both initial training and periodic retraining of the affected operators.
- Operator training records are reviewed to show that the training of all affected operators is up to date for initial and refresher training.
- Operators are interviewed to verify their knowledge of the actions to be taken.
- If gaps are found in the SOP or operator training, corrective actions are implemented to address nonconformance,
- Any changes to the SOP IPLs or the associated initiating cause/consequences were correctly managed under MOC.

BPCS interlock

The sample of BPCS interlocks identified as IPLs are obtained for drill down audit to verify the following:

- Inputs and outputs are properly documented and controlled to prevent unauthorized changes.
- The BPCS interlocks have a PM work order in the in the maintenance/MI system to perform a functional test.
- This test includes the testing of the input instrument to verify it activates the interlock at the correct setpoint.
- The test include verifying the outputs of the interlock correctly functions to prevent the event, i.e. the valve closes and is confirmed to isolate the flow, pump is shut down and flow is confirmed to be stopped.
- Records are reviewed confirming the tests have been performed and any corrective actions implemented for any nonconformance.
- Any changes to the IPLs or the associated initiating cause/consequences were correctly managed under MOC

PSV/Rupture disks

The sample of PSVs identified as IPLs are obtained for drill down audit to verify the following:

- The PSVs/Rupture disks have a have a PM work order in the in the maintenance/MI system to perform a functional test.
- There are records showing these tests have been performed per the required test interval.
- Records are reviewed confirming the tests have been performed and any corrective actions implemented for any nonconformance.
- Any changes to the IPLs or the associated initiating cause/consequences were correctly managed under MOC.

13 Access Security/MOC

The site must maintain the security of the IPL throughout its lifecycle. Systems must be in place that prevent unauthorized changes to the IPLs. For example:

- Alarms or interlocks on a BPCS are controlled to prevent unauthorized changes or disabling (e.g. password, key locks and physical locks to access equipment etc.) are in place to prevent changes.
- Systems are in place to manage change to SOP or alarm response procedures. SOPs are under MOC control and periodic auditing is performed to verify that procedures are understood and being followed. Training includes adequate understanding of role for this procedure in preventing the unwanted consequence and is trained as a mandatory action.
- Systems are in place to authorize the temporary bypass of IPLs and follow-up on their return to service.

When the site makes a change that affects a process, the site must assess if the changes affect the severity of consequence identified from the PHA/LOPA or any IPLs used to mitigate these consequences. The site should give guidance on what triggers a review of LOPA/PHA consequence from a MOC.

For MOCs the site should consider:

- How will the site flag that BPCS LOOP components, procedures, alarms, dikes, PSVs being affected are associated with an IPL?
- How the MOC/Maintenance systems will include these flags to assist the MOC process?
- How the MOC process initiates review of how the proposed changes affects the PHA/LOPA initiating causes or consequence severity that lead to IPL implementation?

14 Summary

- Non-SIF IPLs must be managed through the lifecycle of the process the same as SIF IPLs.
- Efficient flow through the process for IPL identification, validation, selection, implementation and integrity management is aided by procedures to define information capture, document work flow for IPL Identification, validation, selection and implementation.
- The IPL must be validated as part of the initial implementation and audited through its lifecycle to show compliance with the IPL requirements of independence, efficiency/specificity, dependability, auditing/testing and security.
- Tools are needed to identify and review the effect of MOC on the process IPLs and their originating LOPA.