Now What?
After the LOPA is Done

2013 Mary Kay O'Connor Process Safety Center International Symposium

MISSOURI S&T
University of Science & Technology

BLUEFIELD PROCESS SAFETY

Presented by

- **Alex J. Sellers**
  - **Safety Consultant, Bluefield Process Safety, LLC, St. Louis, Missouri**
- **Michael S. Schmidt**
  - **Principal, Bluefield Process Safety, LLC, St. Louis, Missouri**
  - **Adjunct Professor, Missouri University of Science and Technology, Rolla, Missouri**

MISSOURI S&T

BLUEFIELD PROCESS SAFETY

Now What?

- **SIS Design:**
  IEC 61511 or ANSI/ISA S84
- **Confirm assumptions about IPLs made in LOPA remain true:**
  - **Effective**
  - **Independent**
  - **Auditable**
- **Mirror effort used for SIFs in SIS**
- **IPLs in LOPA → safety critical**

MISSOURI S&T

BLUEFIELD PROCESS SAFETY

What is safety critical?

- **OSHA does not define "safety critical" in the PSM Standard**
- **Generally understood to mean "functions that protect against major hazards"**
- **Vague understanding leads to a variety of definitions, uneven distribution**
- **If everything is safety critical, nothing is safety critical**

Features of "safety critical"

- **Limited to scenarios involving major hazards, *i.e.* catastrophic events**
- **Applies to**
  - **Safeguards that are relied upon to reduce risk of a major hazard to a tolerable level**
  - **Components, the failure of which can trigger a catastrophic event**

MISSOURI S&T

BLUEFIELD PROCESS SAFETY

LOPA and Safety Critical

- **Common features of "safety critical"**
- **Identifying scenarios that are candidates for LOPA**
- **Questions that LOPA answers**
- **"Safety critical" – some working definitions**

MISSOURI S&T

BLUEFIELD PROCESS SAFETY

Identifying LOPA Scenarios

- **High risk**
- **High consequence**
- **Instrumented**

Questions LOPA answers…

…when instrumented functions are proposed:

- **Is the proposed instrumented function necessary to reduce risk to tolerable levels?**
- **If it is necessary, may it be a BPCS function, or should it be installed in an SIS?**
- **If it must be installed in an SIS, what SIL should be assigned?**

Safety Critical – Definitions

- **SC scenario: One that results in a fire, explosion, or toxic release that leads to a catastrophic impact.**
- **SC function: Any safeguard credited as an IPL that is required to reduce the risk of a safety critical scenario to a tolerable level or any component or procedure, the failure of which has been identified as the initiating cause of a safety critical scenario**

Excess IPLs

- **Many LOPA scenarios list more IPLs than are necessary to achieve tolerable risk – Are all safety critical?**
- **Three approaches**
  - **All are safety critical**
  - **Inherently safer design hierarchy**
  - **Choose those that are easiest (or cheapest) to implement and maintain**

What to do?

"An organization must establish a system to periodically assess (audit) the elements (components and human interventions) identified as IPLs to ensure that the IPLs remain in service at the anticipated PFD."

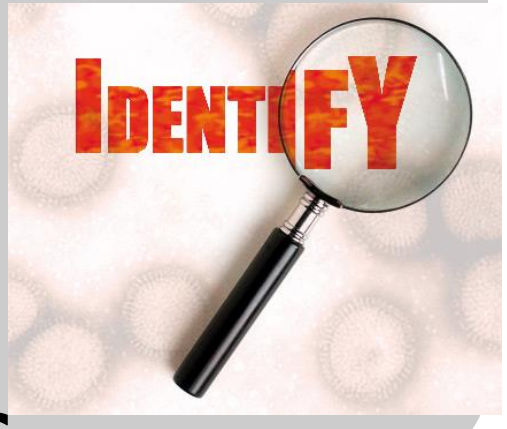
-Layer of Protection Analysis: Simplified Process Risk Assessment

What to do?

- **What should this "system" consist of?**
- **Three main parts**
  - **Identify**
  - **Maintain**
  - **Document**

Identify

- Go beyond creating a list kept by Engineering or Safety department
- Ensure all workers understand what is safety critical and why, including causes and consequences
- Greater awareness and understanding can change mindsets



Maintain

- **Ensure all functions are inspected, tested, and maintained to validate RRF assumed for each IPL during LOPA**

- **Above and beyond normal plant standard of care to differentiate and increase reliability of safety critical functions**

Document

- **Documentation of work done, training completed, and other data is especially important when it comes to safety critical functions**
  - **Verify that work/training is scheduled and has been completed**
  - **Measure and track progress**
  - **Record demands on safety critical functions**

Safety critical functions

- **Three key characteristics of safety critical functions**
- **Four types of safety critical functions**

MISSOURI S&T

BLUEFIELD PROCESS SAFETY

Three key characteristics

- **The hazard prevented, and how the function prevents it**
- **How personnel should respond to a demand on the function**
- **Inspection, testing, and maintenance requirements**

Four types of functions

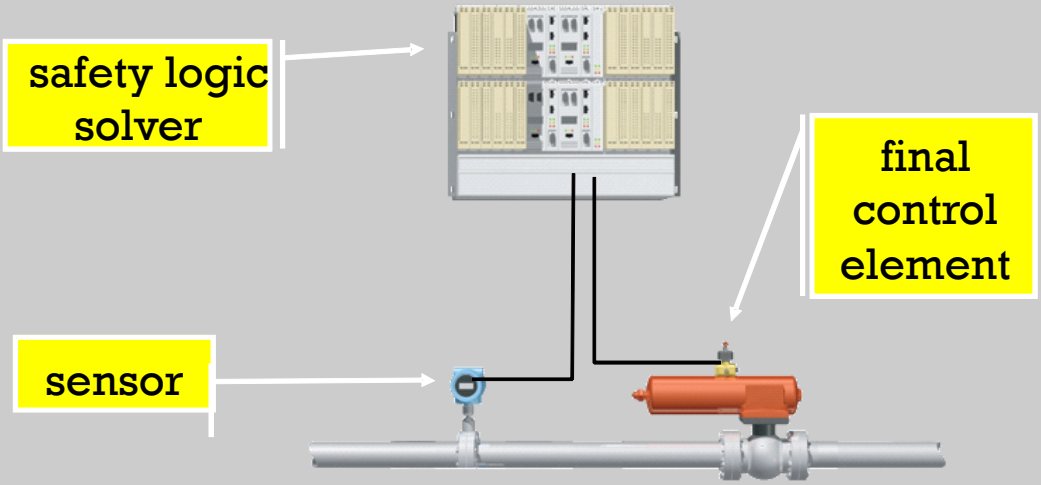
- **SIFs**
- **BPCS functions**
- **Non-instrumented functions**
- **Procedures and administrative controls**

MISSOURI S&T

BLUEFIELD PROCESS SAFETY

SIFs

- **SIFs are well covered in standards and hundreds of papers**



BPCS functions

How it prevents the hazard

- **Cause: What causes the BPCS function to experience a demand?**
- **Set points: What set points and conditions result in a demand?**
- **Effects/safe action: What should happen when the BPCS function responds to a demand?**

MISSOURI S&T

BLUEFIELD PROCESS SAFETY

How personnel should respond

- **Steps to take: What actions should personnel take when there is a demand?**
- **Incident report: Should an incident report be prepared when there is a demand?**

Normal control functions may serve as IPLs and require no response or report

Inspection, testing, maintenance

- **What should be tested?**
- **How should tests be done?**
- **How often should tests be done?**
- **What PM is expected?**

- **What is the method to schedule and issue work orders for inspection, testing, and maintenance?**

MISSOURI S&T

BLUEFIELD PROCESS SAFETY

Non-instrumented functions

How it prevents the hazard

- **Cause: What causes the non-instrumented function to experience a demand?**
- **Set points: What set points and conditions result in a demand or need to be maintained?**
- **Effects/safe action: What should happen when the non-instrumented function responds to a demand?**

How personnel should respond

- **Steps to take: What actions should personnel take when there is a demand?**
- **Incident report: Should an incident report be prepared when there is a demand?**

Some non-instrumented functions may serve as IPLs and require no response or report

Inspection, testing, maintenance

- **What should be tested?**
- **How should tests be done?**
- **How often should tests be done?**
- **What PM is expected?**

- **What is the method to schedule and issue work orders for inspection, testing, and maintenance?**

MISSOURI S&T

BLUEFIELD PROCESS SAFETY

Procedures and admin controls

MISSOURI S&T

BLUEFIELD PROCESS SAFETY

How it prevents the hazard

- **Written procedures: Is the procedure written?**
- **Identity: Is the procedure identified uniquely by name, procedure number, and revision?**
- **Hazard: Does the procedure specifically identify major hazard it protects against?**
- **Steps of procedure: Are the safety critical steps identified?**

MISSOURI S&T

BLUEFIELD PROCESS SAFETY

Training

- **Type of training: What kind of training is to be used?**
- **Understanding: How do personnel demonstrate their understanding of the training?**
- **Frequency of training: How often should personnel receive refresher training?**

Audits

- **Procedures: Are the procedures actually followed?**
- **Training: Is the training as frequent as required and do personnel understand it?**
- **Record retention: At least the last two audits, and most recent training records**

Safety Critical Functions Manuals

- **Practical method of identifying, documenting, and ensuring the maintenance of safety critical functions**
- **Two parts**
  - **Report: outlines the scope of the manual, the purpose of the manual, and general instructions for the manual's continued use and upkeep**
  - **Datasheets: Contains all information necessary to identify, document, and maintain each safety critical function**

MISSOURI S&T

BLUEFIELD PROCESS SAFETY

Safety Critical Functions Manuals

- **Electronic and/or hard copy**
- **Manual for entire plant or for each unit within a plant**
- **All "safety critical" information in one place, including all major process hazards in a facility**
- **Often linked to other documents and software systems — links should denote "safety critical"**

MISSOURI S&T

BLUEFIELD PROCESS SAFETY

Summary

- **Safety critical scenarios are LOPA scenarios with high consequences**
- **Safety critical functions are IPLs required to reduce risk of a safety critical scenario to a tolerable level**
- **Other components or procedures, the failure of which is the initiating cause of a safety critical scenario, are also safety critical.**
- **All safety critical functions, not just SIFs, need to be identified, documented, and maintained**

MISSOURI S&T

BLUEFIELD PROCESS SAFETY

Questions?

Missouri S&T

BLUEFIELD PROCESS SAFETY