Auditing IPLs
Using Safety Critical Functions Manuals

10th Global Congress on Process Safety
New Orleans – March 2014

BLUEFIELD
PROCESS SAFETY

Mike Schmidt bio

- **Principal of Bluefield Process Safety since 2008**
- **Joined Union Carbide in 1977**
- **Began work in process safety, following tragedy in Bhopal in 1984**
- **Joined faculty at Missouri S&T in Rolla in 2009, teaching on safety and risk**
- **Work includes**
  - **Facilitating PHAs, LOPAs, RTC establishment**
  - **SIS conceptual design, SIL verification calcs**
  - **PSM compliance and audits**

Auditing IPLs
Using Safety Critical Functions Manuals

10th Global Congress on Process Safety
New Orleans – March 2014

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**

A LOPA identifies IPLs

- **To be considered IPLs, safeguards must be:**
  - **Effective**
  - **Independent**
  - **Auditable (and audited)**
- **LOPAs typically address**
  - **Effective**
  - **Independent**
- **Need a mechanism for auditing IPLs**

LOPAs and “safety critical”

- **LOPA scenarios with severe consequences are safety critical**
- **IPLs credited in safety critical scenarios are all safety critical**
- **IPLs not credited in safety critical scenarios are not safety critical**
- **If everything is safety critical, nothing is safety critical**

Safety Critical Functions Manuals

- **Practical method of identifying, documenting, and ensuring the maintenance of safety critical functions**
- **A basis for auditing**
- **Two parts**
  - **Report: scope, purpose, and instructions for use and upkeep**
  - **Datasheets: identify, document, and maintain each safety critical function**

SCFM Datasheets

- **Three key categories of information**
- **Four types of safety critical functions**

Categories of information

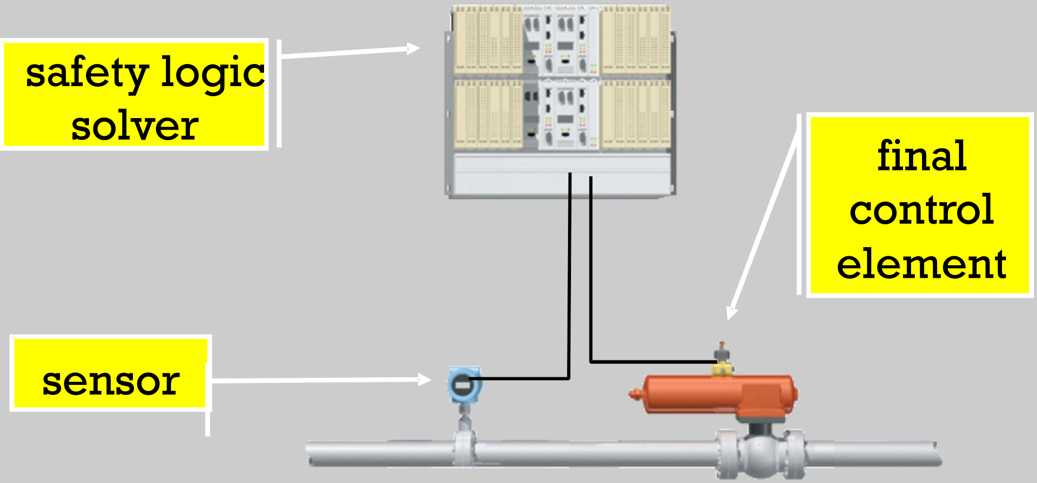
- The hazard prevented, how the function prevents it, references
- How personnel should respond to a demand on the function
- Inspection, testing, and maintenance requirements

Four types of functions

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

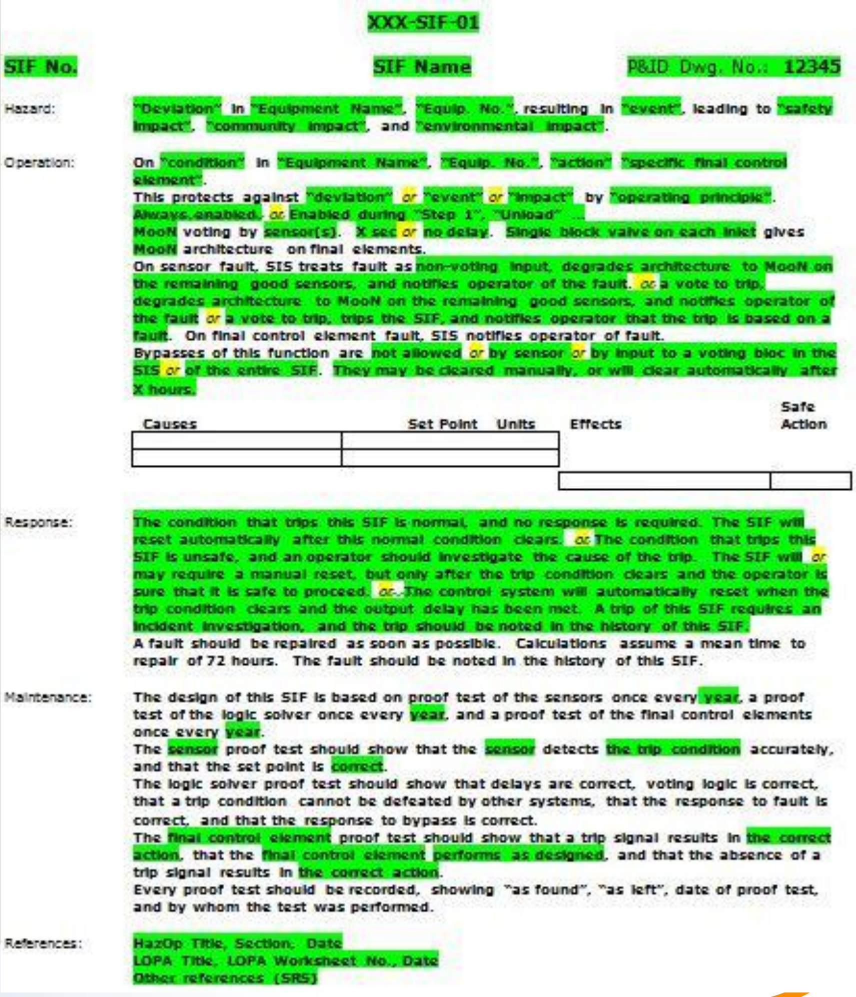
SIFs

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



SIF Datasheet

- **Identity**
- **Hazard**
- **Operation**
- **C&E**
- **Response**
- **Maintenance**
- **References**



XXX-SIF-01

SIF No. **SIF Name** P&ID Dwg. No.: **12345**

Hazard: "Deviation" in "Equipment Name", "Equip. No.", resulting in "event", leading to "safety impact", "community impact", and "environmental impact".

Operation: On "condition" in "Equipment Name", "Equip. No.", "action" "specific final control element".
This protects against "deviation" *or* "event" *or* "impact" by "operating principle".
Always enabled. *or* Enabled during "Step 1", "Unload" ...
MooN voting by sensor(s). X sec *or* no delay. Single block valve on each inlet gives MooN architecture on final elements.
On sensor fault, SIS treats fault as non-voting input, degrades architecture to MooN on the remaining good sensors, and notifies operator of the fault. *or* a vote to trip, degrades architecture to MooN on the remaining good sensors, and notifies operator of the fault *or* a vote to trip, trips the SIF, and notifies operator that the trip is based on a fault. On final control element fault, SIS notifies operator of fault.
Bypasses of this function are not allowed *or* by sensor *or* by input to a voting bloc in the SIS *or* of the entire SIF. They may be cleared manually, or will clear automatically after X hours.

Causes	Set Point	Units	Effects	Safe Action

Response: The condition that trips this SIF is normal, and no response is required. The SIF will reset automatically after this normal condition clears. *or* The condition that trips this SIF is unsafe, and an operator should investigate the cause of the trip. The SIF will *or* may require a manual reset, but only after the trip condition clears and the operator is sure that it is safe to proceed. *or* The control system will automatically reset when the trip condition clears and the output delay has been met. A trip of this SIF requires an incident investigation, and the trip should be noted in the history of this SIF.
A fault should be repaired as soon as possible. Calculations assume a mean time to repair of 72 hours. The fault should be noted in the history of this SIF.

Maintenance: The design of this SIF is based on proof test of the sensors once every year, a proof test of the logic solver once every year, and a proof test of the final control elements once every year.
The sensor proof test should show that the sensor detects the trip condition accurately, and that the set point is correct.
The logic solver proof test should show that delays are correct, voting logic is correct, that a trip condition cannot be defeated by other systems, that the response to fault is correct, and that the response to bypass is correct.
The final control element proof test should show that a trip signal results in the correct action, that the final control element performs as designed, and that the absence of a trip signal results in the correct action.
Every proof test should be recorded, showing "as found", "as left", date of proof test, and by whom the test was performed.

References: HazOp Title, Section, Date
LOPA Title, LOPA Worksheet No., Date
Other references (SRS)

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?**

How personnel should respond

- **Steps to take: What actions should personnel take when there is a demand? What is the response to an alarm?**
- **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

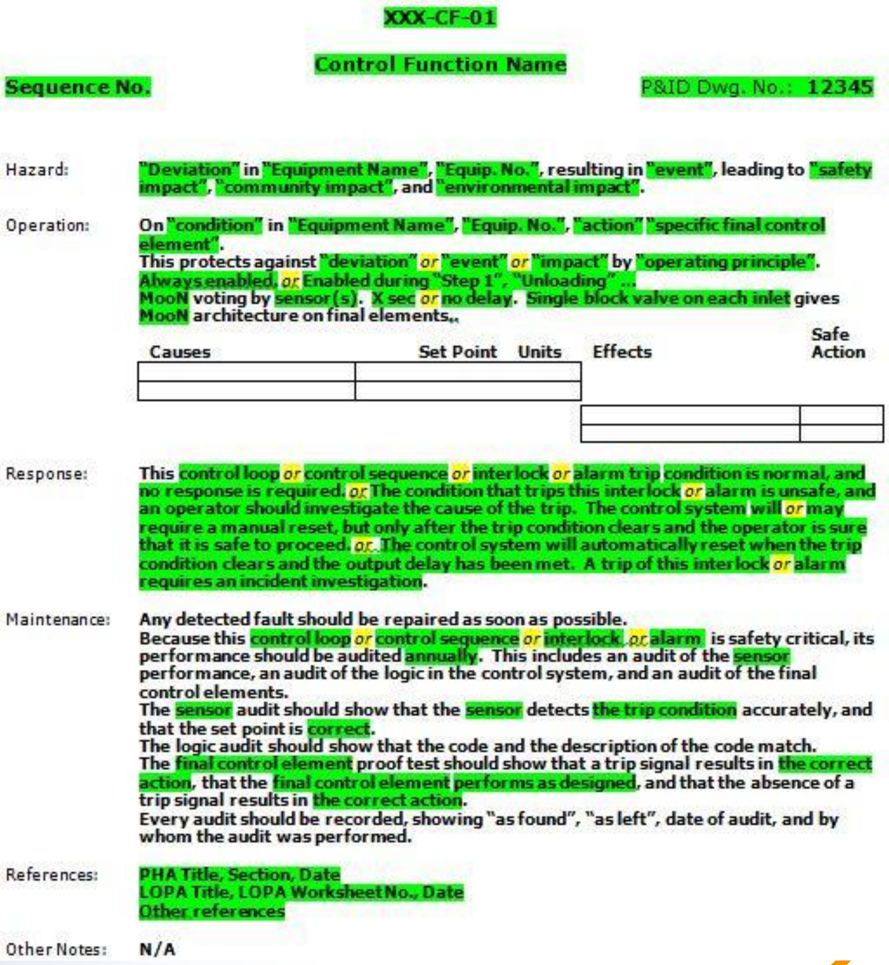
Inspection, testing, maintenance

- **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?**

Control Function Datasheet

- Identity
- Hazard
- Operation
- C&E
- Response
- Maintenance
- References



XXX-CF-01

Control Function Name

Sequence No.

P&ID Dwg. No.: 12345

Hazard: "Deviation" in "Equipment Name", "Equip. No.", resulting in "event", leading to "safety impact", "community impact", and "environmental impact".

Operation: On "condition" in "Equipment Name", "Equip. No.", "action" "specific final control element".
This protects against "deviation" *or* "event" *or* "impact" by "operating principle".
Always enabled. *or* Enabled during "Step 1", "Unloading" …
MooN voting by sensor(s). X sec *or* no delay. Single block valve on each inlet gives MooN architecture on final elements,.

Causes	Set Point Units

Effects	Safe Action

Response: This control loop *or* control sequence *or* interlock *or* alarm trip condition is normal, and no response is required. *or* The condition that trips this interlock *or* alarm is unsafe, and an operator should investigate the cause of the trip. The control system will *or* may require a manual reset, but only after the trip condition clears and the operator is sure that it is safe to proceed. *or* The control system will automatically reset when the trip condition clears and the output delay has been met. A trip of this interlock *or* alarm requires an incident investigation.

Maintenance: Any detected fault should be repaired as soon as possible.
Because this control loop *or* control sequence *or* interlock *or* alarm is safety critical, its performance should be audited annually. This includes an audit of the sensor performance, an audit of the logic in the control system, and an audit of the final control elements.
The sensor audit should show that the sensor detects the trip condition accurately, and that the set point is correct.
The logic audit should show that the code and the description of the code match.
The final control element proof test should show that a trip signal results in the correct action, that the final control element performs as designed, and that the absence of a trip signal results in the correct action.
Every audit should be recorded, showing "as found", "as left", date of audit, and by whom the audit was performed.

References: PHA Title, Section, Date
LOPA Title, LOPA Worksheet No., Date
Other references

Other Notes: N/A

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

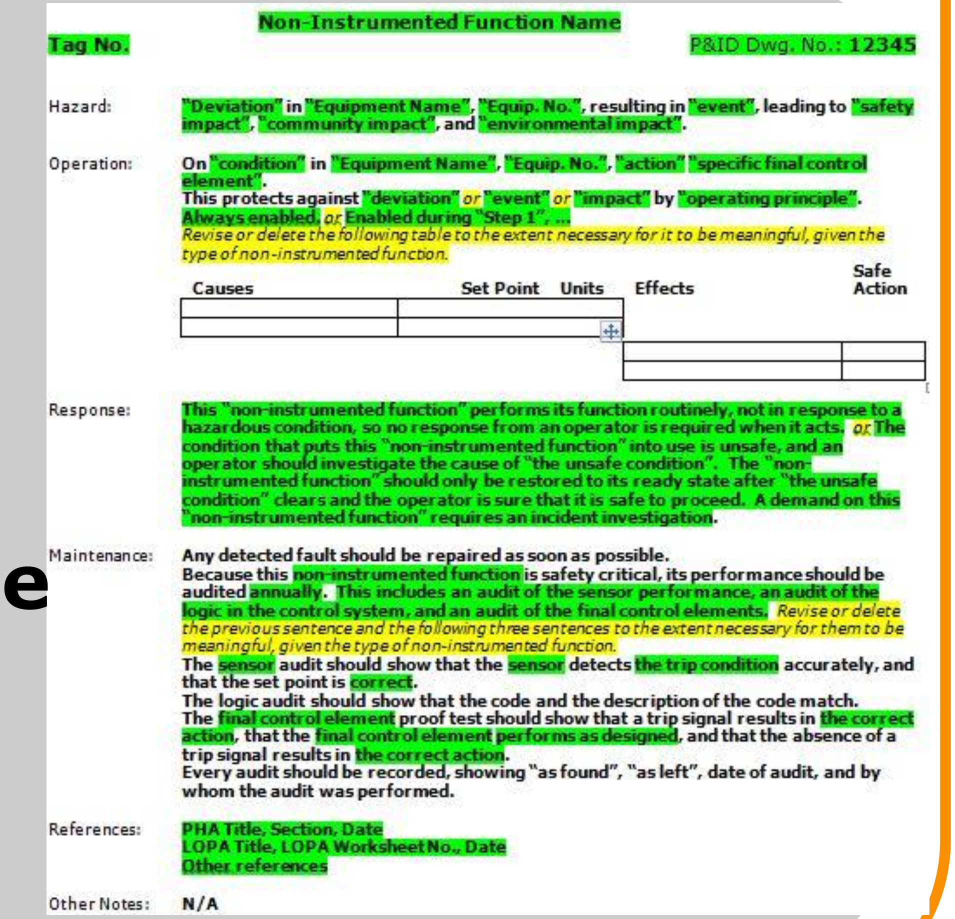
Inspection, testing, maintenance

- **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?**

NIF Datasheet

- Identity
- Hazard
- Operation
- C&E
- Response
- Maintenance
- References



Non-Instrumented Function Name

Tag No.

P&ID Dwg. No.: 12345

Hazard: "Deviation" in "Equipment Name", "Equip. No.", resulting in "event", leading to "safety impact", "community impact", and "environmental impact".

Operation: On "condition" in "Equipment Name", "Equip. No.", "action" "specific final control element".
This protects against "deviation" *or* "event" *or* "impact" by "operating principle".
Always enabled. *or* Enabled during "Step 1", ...
Revise or delete the following table to the extent necessary for it to be meaningful, given the type of non-instrumented function.

Causes	Set Point Units	Effects	Safe Action

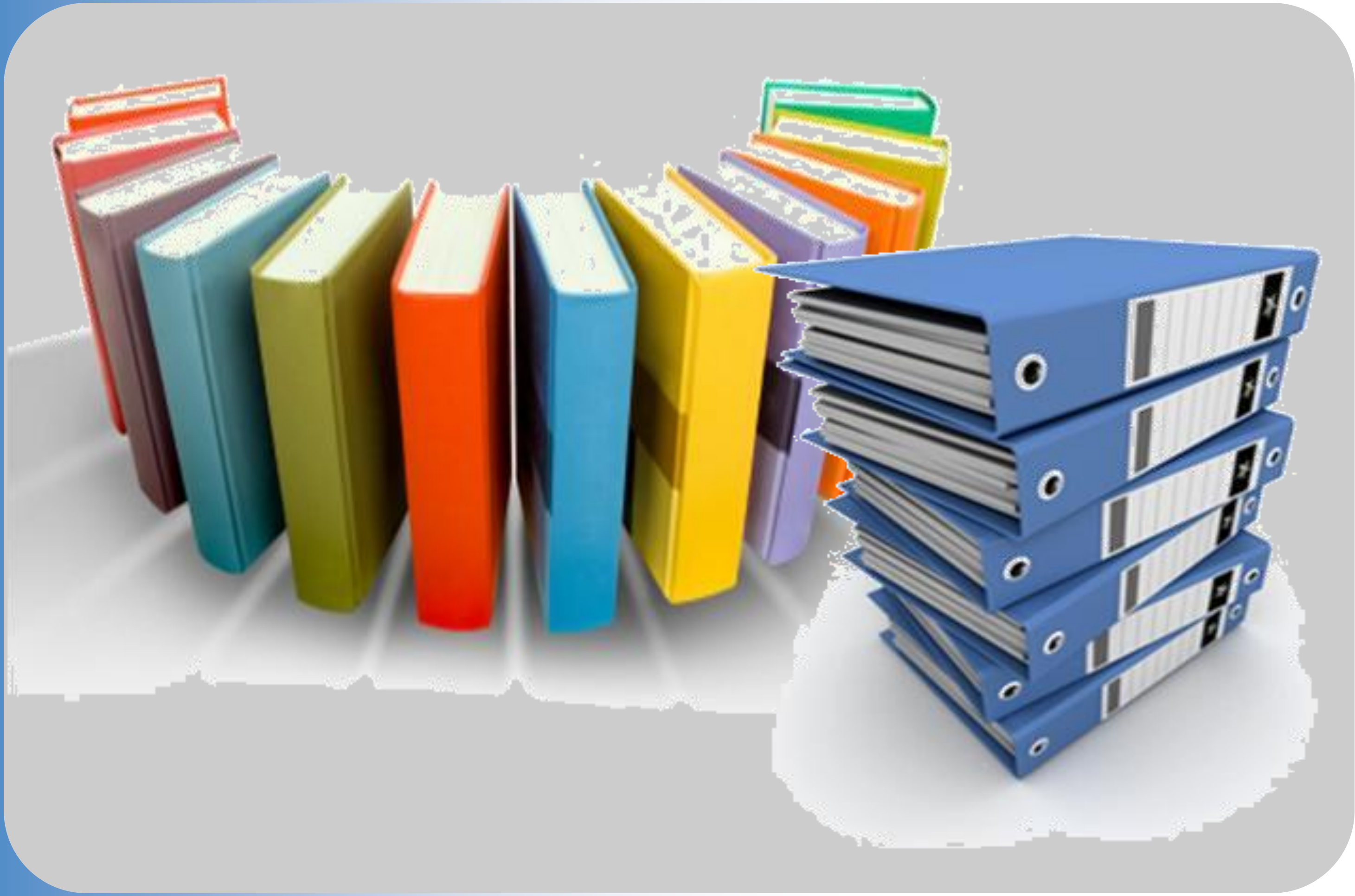
Response: This "non-instrumented function" performs its function routinely, not in response to a hazardous condition, so no response from an operator is required when it acts. *or* The condition that puts this "non-instrumented function" into use is unsafe, and an operator should investigate the cause of "the unsafe condition". The "non-instrumented function" should only be restored to its ready state after "the unsafe condition" clears and the operator is sure that it is safe to proceed. A demand on this "non-instrumented function" requires an incident investigation.

Maintenance: Any detected fault should be repaired as soon as possible.
Because this non-instrumented function is safety critical, its performance should be audited annually. This includes an audit of the sensor performance, an audit of the logic in the control system, and an audit of the final control elements. *Revise or delete the previous sentence and the following three sentences to the extent necessary for them to be meaningful, given the type of non-instrumented function.*
The sensor audit should show that the sensor detects the trip condition accurately, and that the set point is correct.
The logic audit should show that the code and the description of the code match.
The final control element proof test should show that a trip signal results in the correct action, that the final control element performs as designed, and that the absence of a trip signal results in the correct action.
Every audit should be recorded, showing "as found", "as left", date of audit, and by whom the audit was performed.

References: PHA Title, Section, Date
LOPA Title, LOPA Worksheet No., Date
Other references

Other Notes: N/A

Procedures and admin controls



How it prevents the hazard

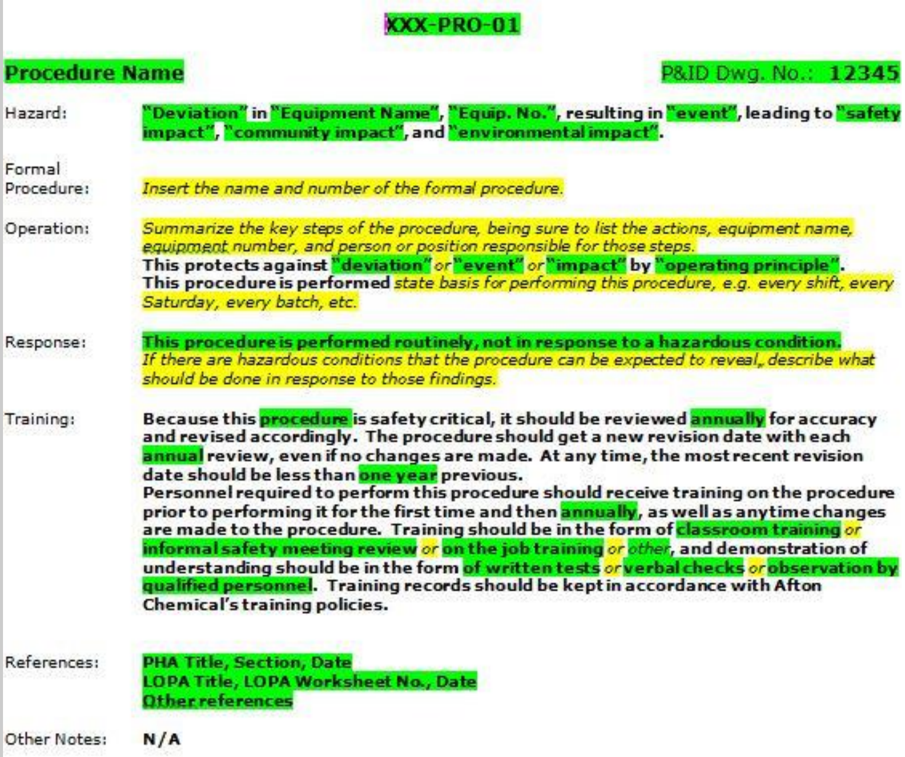
- **Written procedures: Is the procedure written?**
- **Identity: Is the procedure identified uniquely by name, procedure number, and revision?**
- **Hazard: Does the procedure specifically identify major hazard it protects against?**
- **Steps of procedure: Are the safety critical steps identified?**

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?**

Procedure Datasheet

- **Identity**
- **Hazard**
- **Procedure**
- **Operation**
- **Response**
- **Training**
- **References**



XXX-PRO-01

Procedure Name P&ID Dwg. No.: **12345**

Hazard: **"Deviation" in "Equipment Name", "Equip. No.", resulting in "event", leading to "safety impact", "community impact", and "environmental impact".**

Formal Procedure: *Insert the name and number of the formal procedure.*

Operation: *Summarize the key steps of the procedure, being sure to list the actions, equipment name, equipment number, and person or position responsible for those steps.*
This protects against "deviation" *or* **"event"** *or* **"impact" by "operating principle".**
This procedure is performed *state basis for performing this procedure, e.g. every shift, every Saturday, every batch, etc.*

Response: **This procedure is performed routinely, not in response to a hazardous condition.**
If there are hazardous conditions that the procedure can be expected to reveal, describe what should be done in response to those findings.

Training: **Because this procedure is safety critical, it should be reviewed annually for accuracy and revised accordingly. The procedure should get a new revision date with each annual review, even if no changes are made. At any time, the most recent revision date should be less than one year previous.**
Personnel required to perform this procedure should receive training on the procedure prior to performing it for the first time and then annually, as well as anytime changes are made to the procedure. Training should be in the form of classroom training *or* **informal safety meeting review** *or* **on the job training** *or other*, **and demonstration of understanding should be in the form of written tests** *or* **verbal checks** *or* **observation by qualified personnel. Training records should be kept in accordance with Afton Chemical's training policies.**

References: **PHA Title, Section, Date**
LOPA Title, LOPA Worksheet No., Date
Other references

Other Notes: **N/A**

Audits

- **Procedures: Are the procedures actually followed?**
- **Training: Is the training as frequent as required and do personnel understand it?**

Implementing an SCFM

- **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"**

Other criteria for inclusion

- **Organizational policy**
- **Regulatory requirements**
- **Causes**
  - **Components, the failure of which can trigger a catastrophic event, may be considered "safety-critical" and so included**
  - **Failure rate of these components already considered in LOPA, so inclusion is not needed**

Summary

- **An SCFM, consisting of general report and datasheets, is a way of tracking and auditing IPLs**
- **SCFM datasheet formats will differ for SIFs, Control Functions, NIFs, and Procedures, all of which are IPL types that can be included in an SCFM**
- **SCFM datasheets should include**
  - **Hazard and how function addresses it**
  - **How personnel should respond to demands**
  - **Inspection, testing, and maintenance**

Questions?