R.I.S.K.

Risk Integrity Safety Knowledge, Inc.

Procedural PHA

Typically, a Process Hazard Analysis (PHA) is applied to the equipment in a process. The operating and maintenance procedures are considered only tangentially and not explicitly. Many sites, especially those with non-steady state or batch operations, can benefit from examining specific operating procedures using a Procedural PHA.

A Procedural PHA applies a HAZOP or What-If technique to the steps in a procedure to identify hazards and ways to mitigate the hazards. Performing a PHA of the written steps of a procedure can be used to identify critical steps and hazards that may have been missed during development of the procedure and seen as a final test of the procedure. Procedural PHA are useful during final design stage reviews to identify hazards in critical procedural steps in the new process. The purpose is to identify and evaluate those accident scenarios resulting when a procedure is not followed and to ensure appropriate safeguards are in place.

Benefits

Procedural PHAs may be more beneficial in analyzing activities such as:

- batch processes,
- heavily procedural driven processes, such as unloading/loading procedures,
- complex valve configurations,
- high hazard activities with high active failure potential (i.e. Start up, Shutdown procedures), and
- by-passing independent protection functions.

Procedure heavy processes often lack clarity, by nature. For example, “Open ##-Valve slowly” - What does slowly mean? What happens if it is opened too quickly?

Additionally, some procedures require certain safeguards to be in bypass mode. Therefore, it is imperative for the site to understand if there are sufficient safeguards still in place during the operation in question.

Procedural PHAs are also useful in examining procedures when writing or updating to verify if sufficient IPLs are in place. Since a large portion of major accidents occur during non-routine operations, using a Procedural PHA to review those operations can help identify hazards and missing safeguards.

When identifying human factors related causes associated with a procedure many of the safeguards may not be independent of the cause, thus invalid. The real question becomes if the procedure is robust enough to mitigate risk associated with its execution. Procedural PHAs can identify potential pitfalls inherent to the procedure. Perhaps steps are out of order. Perhaps an additional verification step needs to be added to have an extra set of eyes check before moving on. Perhaps wording is vague which could lead to confusion. All of these things can be identified during a procedural PHA.

Trying to generically capture procedural related causes during an equipment based PHA can lead to trying to ‘one-size-fits-all’ potential consequences that could occur. Conducting a procedural PHA can drive a more precise cause-

consequence pairing and thus ensure correct safeguards exists or good recommendations are made to cover the risk gap.

Using an equipment based PHA to identify procedural related results often creates unrealistic scenarios, especially in a dual HAZOP-LOPA or straight LOPA setting. Trying to analyze the effects of a release generically in the PHA can lead to poor identification of actual likely causes and/or over/underestimation of consequences. Looking specifically at the procedure in a procedural PHA helps define the essential steps, and again might provide insight as to where additional safeguards or additional people should be inserted to prevent loss of containment. Conducting a procedural PHA helps bridge the gap between a more realistic "1 in 10 human cause leading to release" and "fire, personnel injury" for every cause.

Approach

Procedural PHAs are done the same way a regular HAZOP is done. You break down the procedure into smaller pieces and analyze them using guidewords. In a Procedural PHA the procedure steps become the nodes or system/sub-systems and the design intent is the content of the step to be performed.

Guidewords (for HAZOP) or questions (What-If) are applied to identify possible failures in following the procedure that could result in possible hazards or releases by skipping steps or inadvertently performing a step inaccurately. Guidewords or questions are also used to identify procedural deficiencies or incompleteness.

In Chapter 9 of the "Guidelines for Hazard Evaluation" [3rd Ed, 2008, AIChE/CCPS], the CCPS text on PHAs provides direction on performing analysis of procedures. Essentially the same concept goes into analyzing a procedure as does a process, however, you use different guide words. Note that it is often acceptable to group 2 or 3 steps together that have the same parameters, much like pieces of equipment would be grouped in a PHA for equipment.

The major difference is that it is not as clear where to break down the steps. Additionally, it may not be appropriate to create different nodes. Some procedures can be evaluated as one node, each step or phase change being a "what it" and analyzing them using the different deviations. Other procedure may be so complicated that different steps or phases become different nodes. Like a standard process hazards analysis, the complexity of the process will determine the path you take.

It is important to take note of things like temperatures, ("cooking") time required, ramping up/down times and or temperatures, valves that are too far apart for one person to manage in the time required, valving line-ups that are too complex to manage in the time allotted when grouping. Often, these changes in parameters are good places to separate steps.

The deviations are different and are related to steps in a procedure. Some may be the same that you are used to seeing. Here are a few to consider:

- Missed step
- Performing incorrect step
- Steps completed out of order
- Valve opened too far
- Too much time
- Too much mixing
- Wrong material
- Rate of heating to quick/slow
- Too much heat

- Not enough heating
- Wrong materials added
- Wrong concentration
- Others may be added as deemed appropriate to how, why, when, where, who, and order of steps

Risk Ranking may or may not be completed due to the reliance on human based safeguards, knowing that you may be in a position to always fall short of enough safeguards.

It is imperative that you discuss how you intend to address the risk ranking with management to have agreement on crediting human based safeguards as some companies allow more leniency in utilizing human based safeguards.

When conducting a Procedural PHA, there are two possible approaches:

1. You can make recommendations as you would in a standard PHA that identifies the changes, additions, deletions that are recommended, along with the reason why and the outcome is a recommendation list to update the procedure.

2. The outcome can be the actual procedure. If it is a new draft procedure, the recommendations can be used to develop the procedure with cautions, hazards, recommended tools, etc. When this is done, the recommendations are used to track changes to the procedure and the procedure is red-lined by a team member, much like drawings would be red-lined during a PHA when an error is found.

Batch Processes

For batch processes a natural place to group steps are based on next stage of the batch process. With batch processes, you may often cover the same piece of equipment several times. However, not all safeguards will be relevant for each step of the batch. Some may be temperature based, others pressure, therefore, you may only use a few of the deviations per step.

With batch processes it is important to remain aware of potential reliance on a computer generated operation. It is important to identify and address what part of the procedure is human driven and what part is computer driven.

For example, when you have a completely computer generated batch process, the questions become,

"What if a valve sticks open (or closed) during X phase? "

However, if it is partially human driven (i.e. the operator adds material X1011 at step 4) then you have questions like,

"What if too much (little) material is added?"
"Can the material be added at the wrong point of the process?"

If the entire batch is human driven, then run through all of the deviations.

Human Heavy Processes – Loading/Unloading

Historically, there have been several incidents and near misses during loading and unloading. Loading/unloading presents a whole set of different hazards than a "normal" procedural PHA. As such, there are several pieces of information to look for before even beginning.

1. Does the site use a single trucking company for delivery or a variety?
2. How many steps and people are involved in placing and receiving an order of material? Think about the purchasing process, the Bill of Lading, weighing the truck etc. These may become part of a safeguard identifying multiple people involved.
3. Does the trucking company have its own safeguards? Are they a requirement per DOT, and/or a requirement as part of their contract? Can they be counted by the site for credit? (Usually not.)
4. Is the material be loaded/unloaded to a classified area? How is the area classification maintained?
5. How is the truck secured? Who secures it?
6. Is the truck driver involved in the loading/unloading? If not, where do they remain during the process?

There are several other elements involved in looking at loading/unloading which are often covered in the procedure and therefore included in the PHA. These items listed above are just some of the things that are often overlooked.

During a PHA for loading/unloading, depending on the process, you may use both standard deviations and procedure-based deviations.

<u>Example Loading/Unloading Incident from Chemical Safety Board (CSB) Case Study</u>:

This photo is from a CSB investigation of the Oct 2016 incident at the MGPI facility in Kansas. There was a massive release of toxic chlorine gas into the atmosphere. It was due to a chemical reaction between sodium hypochlorite (bleach) with sulfuric acid. In the incident a delivery operator unloaded sulfuric acid into the bleach tank due to a wrong connection to the inlet ports of the various filling lines. The ports were all placed close together, included incompatible chemicals, and were not clearly labelled. The facility relied on the plant supervisor to identify the correct port and to unlock the port. In this incident both the sulfuric acid port and the sodium hypochlorite ports were unlocked at the same time.

Manual Valving Configurations

Many times, you will come across a series of complex valving configurations, such as a set of parallel dryers that also have a regeneration mode. When they are operated manually or partially manually, they can lead to errors during the valve switching.

When looking at a system like this, it is possible to set up two nodes (RISK's preference). One node for "normal operation" and a second for "regeneration" and assume one direction.

Then, a valve that is closed in normal operation and open as part of the regeneration phase can be reviewed as a "failed open" or "inadvertently left open" valve under the reverse flow or misdirected flow deviation and vice versa.

Another area of complexity that can be overlooked is when two valves must be (de)activated simultaneously, or nearly so, and they are too far apart for one operator to operate without calling out another person.

Example: Refinery procedure called for opening two manual valves that were about a mile apart with the potential for a train to go through the middle at the time of operation.

High Hazard Activities with High Failure Potential (Start-up/Shut-down/Recycle)

Start-up and shut-down activities account for large portion of incidents within industry, and yet, those two areas are often glossed over or not well documented.

Safeguards are often placed in bypass, or automatic valves placed in manual to facilitate start-up, recycle, regeneration, or shut-down activities.

Startup from a cold state may only happen once every 3-5 years. During that period of time, changes may have been made in the field that could impact startup or shutdown. Additionally, changes in feed composition might present new hazards during startup or shutdown.

The MOC process is designed to mitigate the concern, however, taking a holistic view of the procedure with all of the current changes in place BEFORE using them is a good idea.

Regulatory Requirements

From an OSHA, EPA and RAGAGEP perspective sites are required to review all modes of operation including non-steady state and that includes a review of procedures. Prior to the OSHA PSM regulation, OSHA published a guidance document[5] that said a human error analysis should address:

- Consequences of failure to perform a task.
- Consequences of incorrect performance of a task.
- Procedures and controls to minimize errors.

Since the OSHA PSM regulation was enacted, several OSHA documents, including citations, internal PVQ audit guidance documents, and NEP inspection guidance reference the need to review procedures for hazards. The EPA also recognizes the need to analyze procedures for the process. The guidance documents for Contra Costa County Health Services Industrial Safety Orders[1] include reference to performing Procedural PHAs.

Summary

Procedural PHAs are a useful and necessary tool for a comprehensive review of hazards. A full review of hazards associated with procedures is required by OSHA, EPA and local regulatory authorities. Contact RISK, Inc. if you would like us to facilitate a Procedural PHA for your site. We also offer training and mentoring.

Further References:

1. Contra Costa County Health Services Guidelines for PHA, http://cchealth.org/hazmat/pdf/iso/sect_b_ch_4.pdf

2. Guidelines for Hazard Evaluation Procedures, 3rd Edition, 2008, CCPS/AIChE

3. Handbook of Loss Prevention Engineering, 2 Volume Set, edited by Joel M. Haight

4. "Best Practices for Writing Operating Procedures and Trouble Shooting Guides", W. Bridges and Lauren Madden (REC Silicon), CCPS , Houston TX, April 2016.

5. "Necessity of Performing Hazard Evaluations (PHAs) of Non-normal Modes of Operation (Startup, Shutdown, & Online Maintenance)", W. Bridges and Mike Marshall (US OSHA), 18th Annual International Symposium, Mary Kay-O-Connor Process Safety Center, College Station, TX, October 2015.

6. "How to Efficiently Perform the Hazard Evaluation (PHA) Required for Non-Routine Modes of Operation (Startup, Shutdown, Online Maintenance)," W. Bridges and T. Clark, 7th Global Congress on Process Safety, Chicago, AIChE, March 2011.

7. Bridges, W.G., et. al., "Addressing Human Error During Process Hazard Analyses," Chemical Engineering Progress, May 1994