Are Your Credits Worthy?

James R. Lay, P.E.
Lisa A. Long
Michael L. Marshall, P.E.
Jeffrey J. Wanko, P.E., C.S.P.

U.S. DOL – OSHA
200 Constitution Ave, NW
Washington, DC 20210
Lay.Jim@dol.gov
Long.Lisa@dol.gov
JWanko@dol.gov
Marshall.Mike@dol.gov

Prepared for Presentation at
8th Global Congress on Process Safety
Houston, TX
April 1-4, 2012

UNPUBLISHED

Are Your Credits Worthy?

James R. Lay, P.E.
Lisa A. Long
Michael L. Marshall, P.E.
Jeffrey J. Wanko, P.E., C.S.P.

U.S. DOL – OSHA
200 Constitution Ave, NW
Washington, DC 20210
Lay.Jim@dol.gov
Long.Lisa@dol.gov
JWanko@dol.gov
Marshall.Mike@dol.gov

Keywords: safeguard, credit, PHA, controls

Abstract

Chemical and petrochemical manufacturing processes have potential for high consequence, low frequency events. Process Safety Management (PSM) programs should identify and eliminate or control the conditions leading to the catastrophic hazards associated with these events. In recent years, industry has increasingly turned to quantitative or semi-quantitative risk assessment tools to prioritize and manage the hazards they have identified. Risk assessment, whether qualitative, quantitative, or semi-quantitative, is a powerful tool when used properly; however companies must ensure that the safeguards for which they take credit are robust enough to truly manage hazards.

This paper discusses possible inconsistencies in process hazard analysis (PHA) claims. If a PHA claims credit for a good mechanical integrity (MI) program, what happens when that MI program has numerous deficiencies or violations? When a PHA bases a failure scenario frequency on industry historical experience, how does the site know that this experience is actually applicable to their processes? When a safeguard is challenged, is it available on-demand? What are the consequences if a claimed safeguard does not perform as designed/credited?

1. Introduction

A process hazard analysis (PHA) is a critical part of a process safety management system. Both qualitative and quantitative PHAs may vary in quality and are rarely precisely duplicated. While this is to be expected, employers must do everything they can to ensure that the PHA team has successfully identified hazards, evaluated controls, and documented or recommended valid safeguards. Ensuring adequate safeguards requires the employer to assure that the team has:

- verified assumptions during the PHA,
- verified safeguard robustness and auditability, and
- acknowledged uncertainties in the process.

2. Verifying Assumptions during the PHA

During a PHA, a team of experienced employees identify hazards, evaluate controls, and identify and/or recommend additional safeguards. Whether the PHA is qualitative or quantitative, the team must ensure that they place value on safeguards that adequately protect against the identified hazard. In addition, the team must ensure that the safeguards are effective and auditable.

2.1 Take Credit for Safeguards vs. Controls

CCPS [1] defines a control as, "*A mechanism used to regulate or guide the operation of a machine, apparatus, process, or system*." The key here is that a control should maintain a process, for example, within its normal operating range. This concept is very important, but often missed, especially during qualitative PHAs. It is not uncommon for the PHA team to list a control as a safeguard.

Safeguards are protective mechanisms or systems meant to keep initiating events from proceeding to loss events when controls fail to keep a process operating within its normal range. CCPS [2] defines a safeguard as, "*Any device, system, or action that would likely interrupt the chain of events following an initiating cause or that would mitigate loss event impacts*." Employers need to ensure that PHA teams understand the difference between controls and safeguards.

It is not uncommon to see "mechanical integrity program" listed as a safeguard in a PHA—an example of taking credit for a control rather than a safeguard. Mechanical integrity programs, designed to maintain equipment operability, are therefore considered controls and not safeguards. PHA teams need to evaluate the failure of controls, in this case a mechanical integrity program. This means asking the question: what happens if the mechanical integrity program is weak or if maintenance lags behind schedule? Will the control be effective? Will it be compromised?

Some may claim an annual audit as a safeguard to protect against an MI program failure. For an audit to be a valid safeguard it must be rigorous enough to identify gaps in the audited program. We have seen cases in which an employer's annual PSM audit verified that inspections had been completed on approximately 1% of process equipment—hardly a rigorous evaluation. In situations such as this, it is common to see a PHA take credit for an MI program as a safeguard,

and compliance officers to find numerous problems with the program resulting in citations. In this case, it could be argued that a deficient MI program compromises the validity of the PHA. Employers should classify MI systems as controls and put rigorous systems in place to protect against program failure.

In addition to MI, PHA teams often mistakenly classify procedures, training, and equipment design as safeguards.

Commonly, PHA teams list "operating procedures" and "training" as safeguards. Normal operating procedures and training describe measures operators take to keep a process inside its normal operating range, and therefore, are considered controls and not safeguards. PHA teams should never cite normal operating procedures and training as safeguards on a PHA.

PHA teams sometimes credit equipment design as a safeguard. If the equipment is designed to contain the process within the normal range, then it is a control and not a safeguard. A good example of this is a basic process control system (BPCS). Instruments that operators use to respond to normal process variations and keep a process inside its normal operating range are not safeguards. An example of a safeguard, in this case, might be redundant instrumentation with a separate and independent alarm.

2.2 Verifying Safeguard Adequacy

PHA teams rely on a substantial amount of judgment, which is expected and often adds value. However, the team should be careful in making assumptions about safeguards; they should ensure that the safeguards are both effective and auditable. Below are some examples of things to remember when choosing safeguards.

Emergency and other procedures and associated training that operators employ after a process is out of control can be considered safeguards. In cases where a PHA team takes credit for emergency procedures and training as safeguards, the PHA team should verify that:

- procedures accurately reflects operating practices,
- operators are able to follow and perform the procedure,
- operators have been properly trained on the procedure, and
- systems exist to keep the procedures up-to-date.

In the case of verifying procedures, input to the PHA team from operators that actually perform the procedures in question is valuable. CCPS [4] provides an example of a 10-step operator response/procedure to a safety alarm on a reactor system. This example illustrates all the steps needed to be considered and successfully implemented in order to prevent a loss event and consider operator action a safeguard.

Equipment designed to operate when the process is outside of the normal range can be considered a safeguard. One example of this type of equipment is a relief valve. When taking credit for relief valves, the team should verify that:

- a mechanism exists to ensure that it was designed properly;
- a method exists to ensure that the design is current based on changes that may have occurred over time with the up and downstream equipment that is related to the relief valves;
- a system exists to ensure the relief valve(s) cannot be rendered inoperable, for example, by intervening block valves;
- a mechanism exists to ensure that the proper relief valve is installed; and
- inspection and testing takes place to assure the integrity of the valves.

Keep in mind that the most cited violations in OSHA's Refinery National Emphasis Program included employers not assuring relief valve availability during process operation. Relief valves could be rendered inoperable due to closed intervening block valves or failure to ensure that intervening block valves were maintained in the open position. In these cases, the designed safeguards are inadequate because the intervening block valves, without strict administrative control, provide the opportunity for relief system failure.

PHA teams often cite dikes around process equipment and tanks as mitigating safeguards. Mitigating safeguards act after a loss event occurs and reduces the loss event impacts. [3] While mitigating safeguards are not fully protective, they do reduce an event's severity and it is reasonable to take credit for them. In this example, it is important that the PHA team verify that a dike is effective. Some items the team should consider and verify include the:

- dike integrity is verified and monitored,
- dikes can contain 110 percent of the largest credible spill,
- procedures to assure tank and dike drains valves are closed when not in use (e.g., when draining accumulated rain water),
- control of ignition sources around the dike area; and
- adequacy of foam supplies for the materials contained in the diked area..

PHA teams cite block valves and emergency valves as safeguards in PHAs. In these cases, the PHA team needs to consider whether the:

- valves will work when needed,
- valves are tested,
- testing is effective, and
- valves are located in a place where they can be safely accessed and used.

To illustrate the above point, an employer took credit for isolation valves to contain a possible release of hydrocarbons in a refinery. This sounds reasonable, however, the PHA team failed to consider the location of the isolation valve. In order to close the isolation valve, an operator climbed three 15-foot ladders and walked across a hot pipe. Obviously, this isolation valve was ineffective as a safeguard during emergencies.

Finally, the PHA team should always walk through the process. During the walk-through, the team may notice things that are either wrong or not captured in a P&ID or other process safety information. For example, they may notice an inaccessible isolation valve, a dead leg in a line, a potential to trap material and build pressure in a line, or, an incorrect P&ID.

3. Lifecycle of Safeguards

Once identified, whether through PHA or other means, a safeguard must remain available for use when required. Assuming the employer determined that the safeguard is designed appropriately for the service and installed correctly, maintenance and operations programs must rigorously act to ensure safeguards are available when conditions require.

PHA teams and employers make many assumptions and do not necessarily evaluate the entire lifecycle of a safeguard. The mere presence of a safeguard offers protective value for which the PHA team takes credit. However, there are perils with this means of evaluating safeguards and their effectiveness.

There are many examples of incidents involving safeguards that were ineffective when challenged. For example, safeguards that are not maintained may not provide the protection credited to the safeguard by the PHA team.

In one incident, an employer relied on an emergency cooling water system to provide reactor cooling if the primary cooling system were unavailable. When the primary cooling system failed and cooling water stopped, the employer found the emergency cooling system disconnected and unable to provide critical cooling water in a timely fashion. Minutes after the employer discovered the disconnected system the reactor exploded killing four workers. While a PHA team may have taken credit for the emergency cooling system, they did not account for failure of the system ensuring that the safeguard was functional.

In a second incident, a steam-heated mix tank processed a flammable mixture. During normal operations, an operator monitored temperature of the tank contents and cut-off steam manually. For emergencies or if the contents reached a critical temperature, the employer installed a temperature controller on the steam line with a temperature instrument monitoring temperature within a thermo well on the tank. However, unknown to the operator and the employer, the thermo well heat transfer fluid had dried and the reservoir bulb for the temperature device had been pulled from its intended location. These factors combined to make the temperature safeguard unreliable. On the day of the incident, the operator did not shutoff the steam flow at

the prescribed time and, when needed, the safeguard did not function. The mixture in the tank boiled, creating a vapor cloud that ignited. The flash fire killed one. A PHA may have given significant credit to the emergency temperature cut-off, however the cut-off device was not maintained and, although installed, did not function as needed on the day of the incident. PHA teams must understand and take into account the robustness of the management systems necessary to maintain safeguards.

The CSB investigated an incident involving emergency shutoff valves on a chlorine railcar unloading system [5]. When a chlorine hose failed, operators pushed a button to close the shutoff valves. Corrosion products had built up in the valves, which failed to close resulting in a large, offsite chlorine release. Operators had been testing the valves everyday by pushing the button, but never verified that the valves actually closed. PHA teams must evaluate test methods for field devices such as this and take into account how operations and management use test results to determine functionality of safeguards.

Even when the safeguards present are appropriate they must be maintained to be effective. Leaking block valves, delayed calibration and testing, postponed training and drills, poorly controlled process and procedural changes, and similar issues lead to safeguard ineffectiveness when called upon to prevent a potentially catastrophic incident. A well-known example of appropriate safeguards becoming ineffective is the BP-Texas City Refinery ISOM, following which the company identified up to 21 protective layers that failed to stop the incident from propagating to catastrophic consequences.[9]

These examples above clearly show that safeguards given protective value in a PHA require attention over the lifecycle of the safeguard. The lifecycle includes specification, design, installation, operation, ongoing maintenance, and auditing.

As in any quality cycle, auditing is an essential element to ensure controls remain robust. Where PHA teams specify administrative programs as a layer of protection they must do so based upon data showing the program is alive, well, and performing its intended function. An audit can verify that PHA team credits for administrative controls are appropriate and well-founded. For example, an audit team can verify a PHA team credit for an operator action in response to an upset condition. The audit team can verify the same information that the PHA team needs to ensure that an operating procedure pertinent to the operator's required action exists, is correct, and is understood (i.e., training has been provided) by the operators required to take the prescribed action. Management's role is to understand the credit given to safeguards and administrative programs and to ensure resources are available to maintain functionality.

4. PHA Uncertainties

PHAs play critical roles in process safety, but may be subject to significant uncertainties in hazard identification, frequency estimation, consequences assessment, and the evaluation of safeguard adequacy. In the 1990's, the Benchmark Exercise on Major Hazards Analysis

(BEMHA) in the European Union produced large differences in estimated risk (frequencies and consequences) between 11 teams evaluating a benchmark refrigerated liquid ammonia storage system.[6]. The follow-on Assessment of Uncertainties in Risk Analysis of Chemical Establishments (ASSURANCE) project involved seven well-qualified teams evaluating hazards in a hypothetical cryogenic ammonia storage facility. ASSURANCE examined the sources of uncertainties in risk assessments and found significant variation, typically two to three orders-of-magnitude, in the frequency and consequence estimates.[7] While this study was specific to quantitative risk assessments, the lessons learned from it may be applied to PHAs in general.

There are many possible ways in which uncertainty can enter into PHAs. Some examples of uncertainty in PHAs include:

- rejecting potential hazard scenarios as non-credible possibly due to the limited experience of the assessment team;
- relying on industry data that is not appropriate for a given facility;
- ignoring or rejecting process incidents at the facility, at sister facilities, or in industry as not applicable when, in fact, they are relevant to the design and/or operation of the process;
- overlooking hazardous configurations of equipment;[8] or
- overlooking changes in RAGAGEP and the affect on a site's risk assessment process.

Typically, scenarios qualitatively evaluated as having low consequences or risk will not make the cut for follow-on semi- or fully-quantitative evaluation. Serious hazards that are not identified or appropriately evaluated are less likely to be adequately controlled. Initiating event frequency estimates may not be realistic based on a number of factors such as:

- local experience, which may be too limited to offer effective guidance;
- published reliability or incident frequency data, which may have limited applicability to the process unit evaluated; or
- proprietary databases with uncertain provenance or applicability.

Assumptions made and uncertainties in knowledge concerning the exact condition of the process and surroundings can heavily influence the accuracy of consequence analysis and modeling, and thus a facility's assessment of scenario risk. Some of the numerous assumptions associated with consequence analysis and modeling include:

- highly hazardous chemical (HHC) discharge rate,
- discharge location,
- mass transfer,
- probability of ignition,

- location of personnel,
- meteorological conditions,
- dispersion model applicability and accuracy,
- explosion model accuracy,
- building damage response model applicability and accuracy,
- potential for knock-on damage, and
- effectiveness of shelter-in-place or evacuation procedures.

Again, these sorts of issues can affect both qualitative and quantitative risk assessments.

Evaluation of safeguard effectiveness can also be fraught. The increased use of rigorous quantitative or semi-quantitative methods (e.g., LOPA) to evaluate high hazard scenarios can, if properly conducted, identify common-mode failure mechanisms and help ensure that safeguards are effective, independent, and auditable. However, heavy reliance on procedural and administrative controls and basic process control systems may be leaving many facilities more exposed to serious process incidents. When crediting safeguards, PHA teams should consider that passive measures are generally more effective than active measures and that administrative or procedural measures are least effective.

While the 2005 BP-Texas City ISOM incident does not answer the question of how many safeguards employers need to control catastrophic hazards, it does answer the question about how many safeguards are required to function as designed when challenged. Since an "incident path" for a multi-causation incident like BP is extremely difficult to predict, the answer is simple—ALL safeguards must function as designed when challenged.

Finally, there is the possibility of “Black Swan” high consequence / low frequency events stemming from scenarios not generally recognized or deemed to be of very low likelihood.[10] These uncertainties point to a need for caution when evaluating the extent to which hazards are actually being controlled. Employers should apply the principle of controlling serious hazards As Low As Reasonably Practicable (ALARP) to make sensible improvements to process safety even if it appears that the company’s meets its risk tolerance criteria. Companies should be slow to designate safeguards as superfluous or able to be run-to-failure. Mechanical integrity and management of change programs should be maintained at a high level of performance to prevent degradation of safeguards. A healthy skepticism should be applied when evaluating the effectiveness of procedural and administrative safeguards, and these should be rigorously considered as part of the facilities process safety audit program. Scenarios with potentially catastrophic consequences, in particular, should be viewed with a jaundiced eye, and appropriate measures, such as depopulation of exposed structures and the application of inherently safer design principles, where feasible, implemented.

The experience of multiple catastrophic incidents points to the need for multiple, intact, and effective safeguard layers in highly hazardous processes. Given the potential significant uncertainties inherent in process risk assessment, operating companies should be conservative in accepting hazard control as "adequate" and actively apply the principle of ALARP to ensure that incidents are reliably prevented.

5. Conclusion

PHAs and risk assessments are fraught with uncertainty. Predicting the likelihood and consequences of rare events, as shown in European studies, is not an exact undertaking. PHA teams and management, therefore, must ensure that those items for which there is certainty are managed, maintained, and audited. For the many items where there is uncertainty, PHA teams and employers should be conservative and apply ALARP to ensure catastrophic incidents are reliably prevented.

PHA teams cite and give credit to safeguards used to prevent or mitigate rare events and, within the context of the PHA, for reducing the likelihood or consequences of these events. The lifecycle of a safeguard includes the design/specification, installation, operation, maintenance, and auditing phases. Management commitment to safe operation must include understanding of the reliance of safeguards to act when required.

PHA teams cannot simply assume that the presence of a safeguard provides a protection layer. The PHA team, with management's commitment and knowledge, must address the systems and controls in place to ensure reliable and safe operation.

6. Disclaimer

This paper represents the views of the authors. Although it is based on OSHA programs, it is not an OSHA policy document.

7. References

[1] Center for Chemical Process Safety (CCPS), "Guidelines for Safe Automation of Chemical Processes, 1993

[2] Center for Chemical Process Safety (CCPS), "Guidelines for Hazard Evaluation Procedures", 3rd Edition, 2008, pg. xxvi

[3] Center for Chemical Process Safety (CCPS), "Guidelines for Hazard Evaluation Procedures", 3rd Edition, 2008, pg. 23

[4] Center for Chemical Process Safety (CCPS), "Guidelines for Hazard Evaluation Procedures", 3rd Edition, 2008, pg. 27

[5] "Investigation Report, Chlorine Release, DPC Enterprises, L.P., Festus, Missouri, August 14, 2002, Report No. 2002-04-I-Mo", May 2003 http://www.csb.gov/assets/document/DPC_Report.pdf (accessed January 17, 2012)

[6] Papazoglou, et.al.. "Uncertainty Quantification in a Probabilistic Safety Analysis of a Refrigerated Ammonia Storage Facility". Safety and Reliability '92, Petersen & Rasmussen, ed. Elsevier Science Publishers, LTD. Essex, England, UK, 1992. ISBN 1-85166-875-6. Pp. 78-79

[7] Lauridsen, et.al. "The ASSURANCE project, Final summary report", Riso National Laboratory, Roskilde, Denmark, 2002.

[8] Investigation Report LPG Fire At Valero – McKee Refinery, Valero Energy Corporation, Sunray, Texas, February 16, 2007, Report NO. 2007-05-I-TX", JULY 2008, http://www.csb.gov/assets/document/CSBFinalReportValeroSunray.pdf

[9] Lessons BP Learned from the Texas City Refinery Explosion, Broadribb, AIChE Loss Prevention Symposium , Orlando, FL, April 24/26, 2006, http://www.aiche.org/UploadedFiles/CCPS/Conferences/International/2006Presentation/Broadribb.ppt (accessed January 17, 2012)

[10] John F. Murphy, PE, "The Black Swan: LOPA and Inherent Safety Cannot Prevent All Rare and Catastrophic Incidents," ***Process Safety Progress,*** Volume 30, N0. 3, September 2011, AIChE.