Lifecycle Management of Protection Layers and Safeguards

Jack Chosnek, PhD, PE
Knowledge*One* LLC
PO Box 451629, Houston, TX 77245
jc@knowledge1.net

Prepared for Presentation at
American Institute of Chemical Engineers
2019 Spring Meeting and 15th Global Congress on Process Safety
New Orleans, LA
March 31 – April 3, 2019

Lifecycle Management of Protection Layers and Safeguards

Jack Chosnek, PhD, PE
KnowledgeOne LLC
PO Box 451629, Houston, TX 77245
jc@knowledge1.net

ABSTRACT

From project inception to continuous plant operation a stream of safety studies will be conducted on the process, and the identified hazards will have to be either eliminated or reduced to an acceptable risk level. This risk level needs to be maintained at an acceptable level throughout the lifecycle of the plant. As changes occur and time passes the safeguards and protection layers start getting disconnected from the intent of the safety studies. This happens for many reasons but mainly because on proposing and implementing the layers of protection, the assumptions and intent made during the study are not explicitly attached to the specification of the equipment, instrumentation, or procedures. This is aggravated when the recommendations coming out of a study are implemented in a different manner as the recommended one or a totally different solution is adopted. Furthermore, the same equipment may be part of different safeguards in different studies.
A Hazards Register would contain all the pertinent information related to the risks assessed during all the safety studies performed by the company, whether a PHA, or a MOC review, or an incident investigation. The resolution of each hazard should be available in the Register, and not only the latest resolution but also its evolution (history) starting from the original study. In order to be effective, the Hazards Register should be easily accessible, be capable of simultaneous use by all plant personnel, have appropriate security, and be fully and effortlessly searchable. It should also automatically provide metrics that allow to manage outstanding recommendations and automatic recalculate relevant risk information (e.g., cumulative probability of failure on demand, pfd, from a LOPA study). It should be able to import data from any type of safety study and to export all or part of the data for other uses (e.g., instrument specifications). Such a system was successfully used in a very large project in which over 9,000 safeguards and their justifications were managed. At the end of the project the Hazards Register was transferred to the operating company for continued management of the process risks.

Introduction

Managing the risks of a process is a task that starts at the conceptual stage and continues throughout the design, startup, operation of the process, and decommissioning of the plant. Thus, we have to continuously manage the risks through the life cycle of the process. But the risks keep changing as we define in more detail the equipment and instrumentation of the process during the design, or introduce changes as a result of a desire for process improvement, or a change in operation. The nature and severity of the risks will also change when we analyze them and implement measures for either avoiding them, or minimizing or mitigating them.

Whichever method we use for safety studies, we will start with identifying the hazards, defining a potential cause for a process deviation that will make the hazard become an event, determining the consequence of that event, and then we will identify what safeguards exist to prevent or mitigate the consequence. If we use risk-based process safety we will also want to describe the risk by assessing the severity of the consequence and the probability of that occurring given the identified safeguards. During the analysis we will make assumptions and develop some logic that supports the description of the found risk. We may want to reduce the risk and therefore we will recommend and implement additional safeguards. So, there is a lot of information that lets us understand the risk and find commesurate ways to control it.
As time passes this information evolves and the basis for its creation becomes faint. This may lead to adding, modifying or removing necessary safeguards adopted from safety studies, as the reason for these safeguards being there is hidden or forgotten. Thus, a tool is needed for the long-term maintenance of the assumptions and logic for all the control schemes, instrumentation loops and equipment specs that make up the safety infrastructure of the plant.

The Evolution of Risk Assessment in the Life Cycle of the Plant or a Project

Any process design will undergo safety studies to determine the hazards of the process and the means to control them. Most of the time this is done through PHAs using many different methodologies. If the company practices risk-based process safety, this may be followed by a LOPA and/or a QRA, if the consequence level demands it. When performing the PHA oft times recommendations are made to mitigate the risk resulting from a given cause that leads to a specific consequence (we will call it a cause-consequence pair or c-c pair for short). The recommendation will generally propose adding or modifying safeguards (or even changing equipment to make that part of the process inherently safer). If a LOPA is performed in order to evaluate the risk in more detail, the same c-c pair may produce a more detailed safeguard, which can be an independent layer of protection (IPL) with its own rules [1, 2, 3]. Those rules will dictate, depending on the desired risk reduction and independence from other instrumented protections, a Safety Integrity Level (SIL) for the IPL. We then specify instrumentation that is part of a Safety Instrumented System (SIS) and which gets documented in the SIS archives of the plant. The same applies to a non-SIS layer of protection or safeguard, except that the documentation is in another place. This applies as well as to procedural (administrative) safeguards, where only the required actions will become a part of an SOP and their basis may not be documented in any place except for a PHA report. Unless we document very well the reason behind a layer of protection (and are able to find it at any time), we are destined to defeat it at some point in time.

A change in risk also occurs when a change in the plant occurs. The change will go through the MOC process and obviously an MOC safety study will be performed. In order to be successful, the safety study will need to review the hazards identified during the process' PHA, and the protections that were identified at the time, plus the mitigations recommended by the PHA team. In addition, the safety study will have to review any previous modifications of the equipment and instrumentation, that is, search the MOC database to see if any of the existing layers of protection are not impacted.

An additional challenge is that recommendations made by any of the teams, be it a PHA or an MOC (or an incident investigation), sometimes doesn't get executed as the team proposed, as a better solution

may be implemented once there's more time to think and come up with a potentially better design. When this happens, chances are that the implementation will only refer to the PHA report, or MOC number, and there will be a disconnect between the cause of the event and the implemented solution. It is very common to create a new document in order to track implementation of the recommendations and this document will increase the gap between the implementation and the understanding of why the recommendation was needed.

The effect of all this is that, as time goes by, the process safety reason for a certain process configuration gets lost. A new safety analysis may totally miss the underlying safety need for that configuration as the need may have been identified a couple of iterations before and it may not be obvious at the present time. This gets complicated even more when there are interlocks that activate various valves (for example a plant shutdown) but one of the valves is also part of a control loop that has a different safety function (SIF) from that of the shutdown. The plant shutdown may be obvious after some analysis, but the other SIF may not be that obvious. At some point in time a decision could be made to reduce the SIL rating of the loop because it is unnecessary for the shutdown, but by doing this the risk reduction for the other safety function may be compromised.

It all depends on how the safety documentation and the process documentation are interrelated. The following documents would need to be consulted for a proper risk estimation in case of a change in the process:

1. PHA report
2. MOC database
3. Safety study of the MOC (if not integrated into the MOC database)
4. Cause and Effect Table
5. Instrument list containing instrument specifications.
6. Incident investigation reports if there had been any incidents in the plant.
7. Action-tracking table to see if there are unimplemented safety recommendations.

And, of course, up-to-date P&IDs that reflect all the actual control schemes and other protections, be it SIS, DCS, or other.

All this information can be easily integrated in a Hazards Register, which is a dynamic database that can also serve as a tracking device for all safety recommendations. The Hazards Register ought to also include a historical record of all the resolutions that were ever made with respect to safety studies or changes affecting safety systems. Such a database was created and its capabilities are described below.

The Hazards Register

The Hazards Register is a database with all the causes and consequences that were ever identified in a plant, including its grass-roots design project. These c-c pairs will have unique identifiers that will allow them to be tracked throughout the life cycle of the plant. The history is preserved. In order to avoid errors created by compilation of data, all the data is imported directly from most commonly used PHA/LOPA software, or from any spreadsheets used in safety studies. The only required manual entries

are the name, date and type of the source safety study (PHA, LOPA, MOC, etc.). If desired, additional information can also be entered, such as study team composition, remarks, etc., without limitations.

The data elements that the Hazards Register includes for each c-c pair are:

- C-c unique identifier (created automatically on entering the data by importing or otherwise)
- Source study name, type and date
- System (e.g. Operating Unit, plant area)
- Subsystem (e.g. Compressor system, Cold Box, Final Purification, etc.)
- Process deviation/keyword used in PHA for the c-c pair
- Consequence (Hazard)
- Cause
- Consequence severity level
- Type of consequence severity (e.g. economic, safety, environmental, etc.)
- Safeguards or IPLs
- Frequency of initiating event (LOPA)
- Frequency and type of enabling event (LOPA)
- Frequency and type of modification event (LOPA)
- PFD (Probability of Failure on Demand) for each IPL
- Probability (calculated from PFDs or entered from Risk Matrix)
- Risk (from risk matrix)
- Mitigated risk
- Reference (e.g. P&ID or other)
- PFD gap
- Recommendation or Action Plan
- Owner (for tracking purposes)
- Target date of implementation (for tracking purposes)
- Resolution (the latest resolution for the item will show, but all the resolutions from the beginning can be seen by clicking a button)
- New safeguards/IPLs resulting from recommendation(s)
- SILs of each of the new IPLs
- Final cumulative PFD (calculated automatically)
- Documentation description
- Status (open, closed, deferred, in progress, etc.). Milestones are defined by the user. Past due items, that is items not closed by target date, will show in red.
- Comments

That is, all the information contained in a PHA and LOPA plus some. But everything is electronically imported to avoid errors. A main table (see Fig. 1) is a list of the c-c pairs with all the data above and is fully searchable. If a c-c pair from a HAZOP, for example, which was imported into the program, was taken further into a LOPA which was then also imported into the program, the database will create a link between the two identical c-c pairs. At the click of a button you can switch between one and the other. All the data can be easily searched, filtered, sorted and exported. Excel spreadsheets and Adobe Acrobat reports can be created at the click of a button.

The main table will also automatically show statistics of all the table contents, both of those shown (after filtering) and of the total number of items. The statistics will reflect the milestones previously selected by the company (e.g., open, closed, in progress, deferred, etc.).

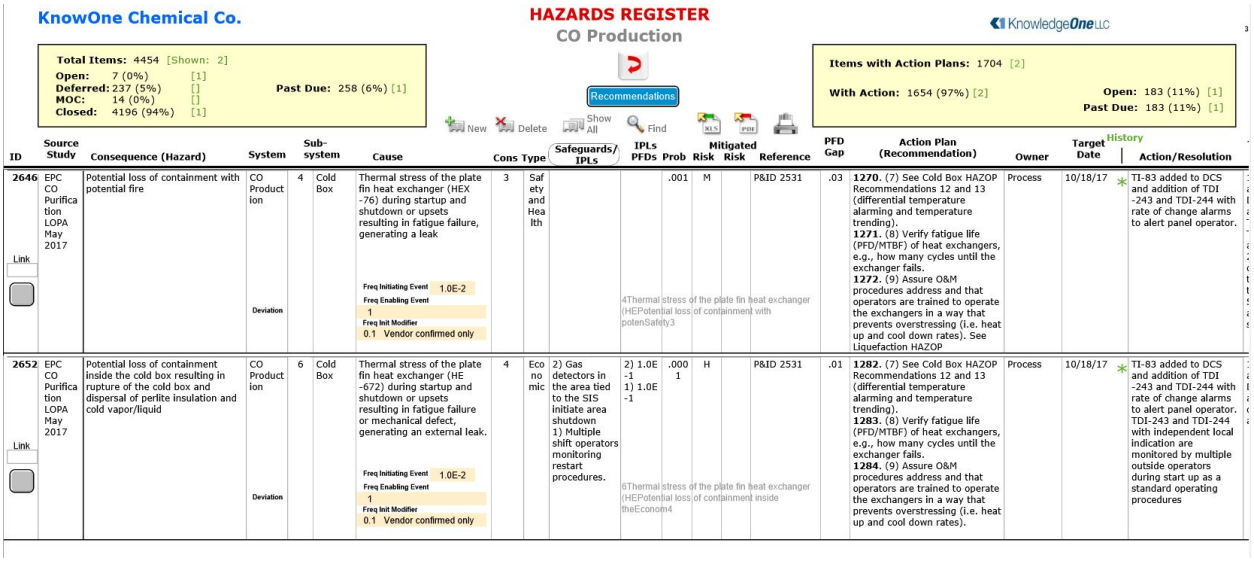

Figure 1. Hazards Register Main Table

Each c-c pair can be closely examined by clicking on the item ID which will take you to a detailed view as shown in Figure 2.

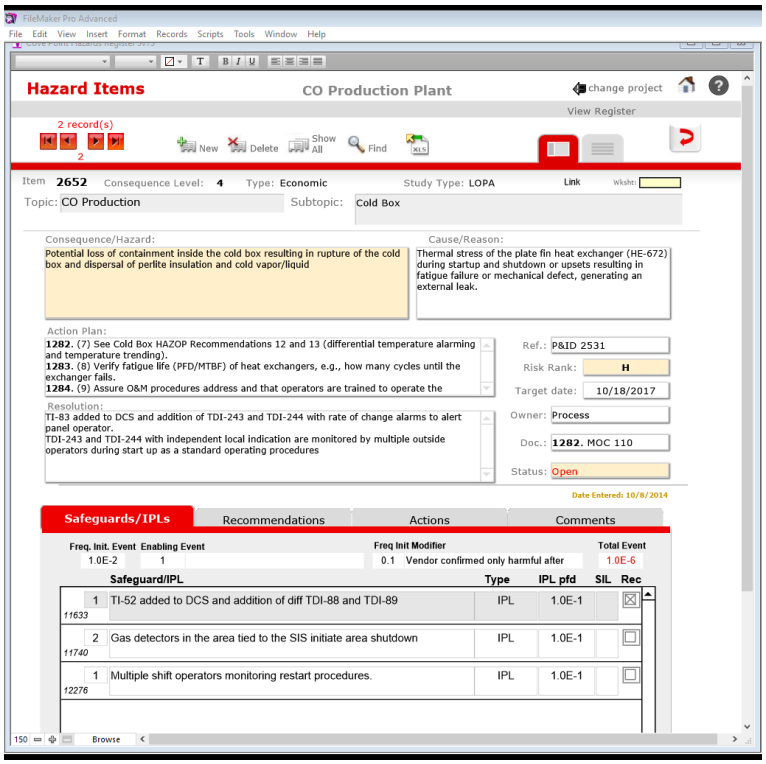

Figure 2. Item's Detailed View Showing Safeguards/IPLs

In this view, all the safeguards/IPLs can be seen and SIL values assigned. If a PFD has been entered, the program will calculate the cumulative (total event) PFD. If an IPL's PFD is changed, the cumulative PFD will be recalculated. If a safeguard or IPL came from a recommendation, it will be marked so, and it's possible to see the contribution of the recommendation to the total item's risk.

There are other views, of all the recommendations and actions taken for each recommendation (with dates and name of implementer), and of all the resolutions, which are the explanations of how item was finally resolved. There's a resolution for every item, even if a recommendation wasn't made and even more important, if a recommendation was not followed upon. Although the latest resolution is the one that will be shown in the main table, all the history of the item from day one is available by clicking on the history button. Thus, the evolution of the reasoning of why the resolution stands as it is, is available, as well the justification for all the safeguards and IPLs that are part of the current process configuration. When making a change, it will be immediately obvious why a certain protection is in place. If a protection is removed or a new protection is added, the program will recalculate the risk.

Another very useful part of the Register is a list of all the safeguards/IPLs with their PFDs and SIL values (Figure 3). This list can be easily exported to Excel and serve as the basis for creating or checking the plant's instrument list as well as inspecting and maintaining the Cause and Effect table. Since it is fully searchable any instrument or device can be found, and its participation in more than one Safety Instrumented Function (SIF) at a time scrutinized.

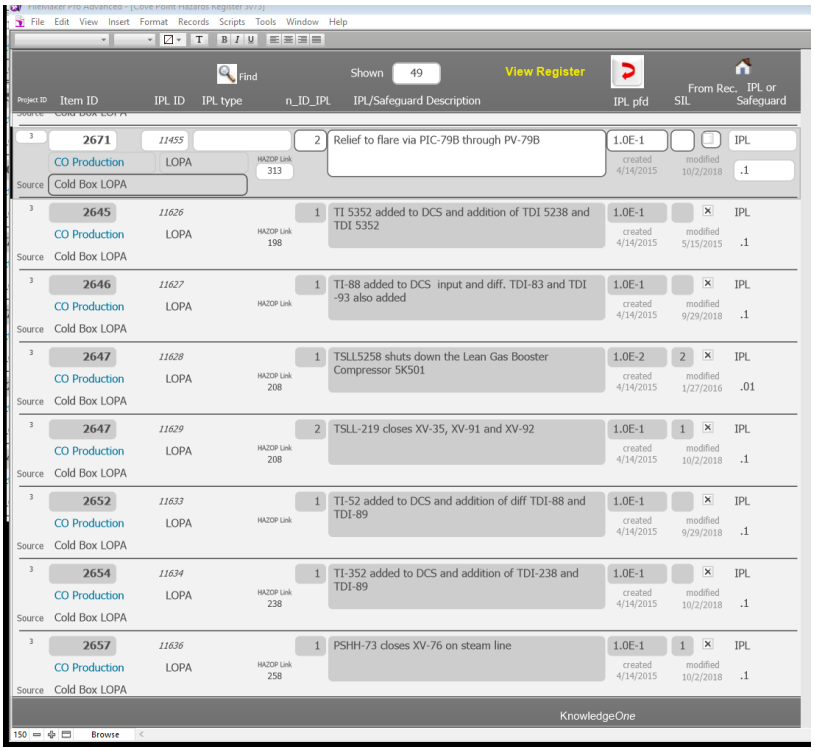

Figure 3. List of Safeguards/IPLs

In summary, the Hazards Register that was created maintains in one place all the hazards and related risks of the facility. The basis and reasoning for resolving the hazards through time is available since

when the first safety study was imported. This is essentially in order not to forget the intent of an instrument or protection layer which could be later be changed, unintentionally increasing the risk of the facility. Since it resides in a database with simultaneous access to all, and is fully searchable, all the data can be easily found and continually used to maintain a safe design throughout the life cycle of the plant.

This Hazards Register was successful used in a very large EPC project ($4 billion) that lasted over three years. The database contained about 2,300 c-c pairs and 9,000 safeguards/IPLs and it was used to track resolution of all these items. At the end of the project the data was incorporated in the new facility's information. The Register could be seamlessly transferred to the facility and continued to be used.

REFERENCE

1. CCPS, "Layer of Protection Analysis: Simplified Process Risk Assessment", October 2001.
2. CCPS, "Guidelines for Enabling Conditions and Conditional Modifiers in Layers of Protection Analysis", November 2013.
3. CCPS, "Guidelines for Initiating Events and Independent Protection Layers in Layers of Protection Analysis", February 2015.