Practical implementation of “risk assessment” through Process Safety Management Systems

Marco Pagnini, Stefano Milanese
Arthur D Little S.p.A
Corso Sempione 66/A, 20154 - Milan, Italy
Alfredo Verna, James Perry
Arthur D Little Limited
Science Park, Milton Road, Cambridge, CB4 0XL, UK

A key element for Process Safety Management (PSM) systems is the so-called “Process Hazard Analysis”; as a matter of fact, many of the PSM elements includes an "understanding / evaluating risk" step, which needs to be fulfilled properly in order for that element to be robust and "fit for purpose". "Risk assessment" is often seen in abstract terms and left to the so called HSE and risk specialists instead of being perceived and carried out in a more pragmatic way, with the involvement of operational and maintenance personnel, as appropriate. As a result, some companies still fail to examine and evaluate with the necessary depth those risks linked to routinary and non routinary activities. The purpose of this paper is to show, through two real cases, what process safety “risk assessment” actually means in terms of day-to-day operations and how it can be tackled avoiding unnecessary bureaucracy and minimizing paperwork.

1. Introduction

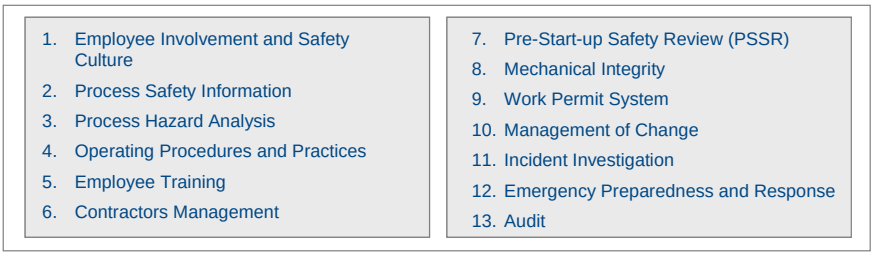
Many major oil & gas corporations have been reviewing their arrangements for managing Process Safety at their operational sites in the light of the observations and recommendations of Baker Report, following the 2005 BP Texas City refinery accident.
A Process Safety Management (PSM) can be considered effective when it allows a company to answer adequately the following questions:

- Have all hazards related to routinary/non-routinary activities been identified?
- Have the risks associated with those hazards been assessed?
- Have appropriate technical / organizational risk control measures been developed and implemented? Have they been communicated to the affected personnel?
- Are the risks as well as the integrity and effectiveness of the risk control measures reviewed on a periodic basis?

In this paper we use the term “risk assessment” in a wide meaning, i.e. the process of identifying the hazards, assessing the associated risks, introducing appropriate risk controls and confirming that they continue to operate as intended.

Lack or ineffective implementation of a sound and robust PSMS can lead to the uncontrolled release of hazardous materials or stored energy, with possible negative impacts on personnel safety, plant integrity and availability, environmental quality, image and reputation. In practice, PSM systems are based on a set of elements such as those in the US OSHA standard 29 CFR 1910.119 (as illustrated in Figure 1).

Figure 1: PSM Elements



Source: OSHA 29 CFR 1910.119

A key element for PSM systems is the so-called “Process Hazard Analysis” as process risks can be effectively managed only if they have been previously identified and evaluated. One of the major pitfalls in the implementation of an effective PSM system is the tendency, among many companies and stakeholders, to consider the "Risk Assessment" as an abstract and theoretical step which is normally delegated to the so called HSE and risk specialists, instead of being perceived and carried out in a more pragmatic way. Quite too often “hazard identification and risk assessment” are seen as a legal burden (e.g. *“something which should be done to comply with the Seveso Directive”*), and are often carried out with the aim of “ticking a box” rather than representing a sound basis for identifying, assessing and communicating the risks. By adopting this approach, that we can call “paper driven”, as opposed to “risk driven”, some companies still fail to examine and evaluate with the necessary depth those risks linked to routinary and non routinary activities such as isolation of lines/equipment for maintenance, temporary by-pass of safety interlocks, location of portable buildings within process areas, etc. The purpose of this paper is to show what process safety “risk assessment” actually means in terms of day-to-day operations and how it can be tackled in an effective way, avoiding unnecessary bureaucracy and minimizing paperwork. Focus will be given to practical examples of identification and evaluation of risks associated to key PSM elements. Real case histories taken from past PSM auditing activities conducted for several sites belonging to international energy companies have been used to derive suggestions to implement practical and effective solutions for identification and assessment of process safety risks.

2. Hazard identification and risk assessment in the context of a PSMS

In addition to the element “Process Hazard Analysis”, other PSM elements contemplate an "understanding / evaluating risk" step, which needs to be fulfilled properly in order

for that element to be robust and "fit for purpose". These elements include: 1) Work Permit Systems, 2) Management of Change, 3) Pre-start up Safety Review.
This is a further confirmation that identification of hazards and evaluation of risks should be seen as a process inherently linked to the operation of the plant during its lifecycle. In fact, an effective implementation of the above elements would ensure a proper management of risks related to normal (stable) operation of the plant, changes to the process and/or the organization, start up or shut down of the plant, routine and non routine activities.

3. What a weak risk assessment process can lead to

Whilst numerous techniques exist for hazard identification and risk assessment studies, companies need to understand that the evaluation of those risks may require different approaches as the final objective varies. The bottom line is that all risks should be identified and assessed, so as to ensure that they are properly controlled.
Weather the evaluation involves a fully quantitative approach or other simpler methodologies (such as risk matrix, informed engineering judgment, etc.) depends on the final objective of the analysis and complexity of the system/activity being examined.
There are a number of common operations / activities happening in a process plant which require a risk assessment step. These include, for example, isolation of lines/equipment e.g. for maintenance, temporary by-pass of safety interlocks, location of portable buildings within process areas, plant modifications (e.g. installation of a bypass around a valve or equipment), loading/unloading of hazardous materials, etc.
Many of these situations are not normally subject to a risk assessment as part of the Safety Case, nevertheless it is plenty of case histories related to accidents which occurred due to the incorrect management of such activities and, in many cases, due to a lack or inadequate understanding and evaluation of the risk involved.
The following two real cases derived from our experiences in performing process safety audits in some refineries and petrochemical plants can better illustrate what we mean by practical, pragmatic and effective risk assessment and what can go – and indeed went – wrong if this is not performed properly.

3.1 Case History 1 - Isolation of lines / equipments

Situation
In the present situation one of the three bottom pumps of a vacuum distillation column with multiple connections - other than suction and discharge lines - needed to be isolated for maintenance (See figure 2A – Complex pump to be maintained). Prior to remove the body of the pump, the procedure required the pump to be flushed with flushing oil; then the pump could be drained, isolated and dismantled for maintenance. The Vacuum Distillation Unit was installed in the early 70's. A HAZOP study was conducted in the past, however did not focus on operability issues such as maintenance.

Typical hazards/risks
A key hazard is represented by the potential for loss of containment of heavy hydrocarbon residue at temperature nearly or above the autoignition temperature which would result in a fire in case:

1. Issue 1 - all connections which need to be isolated are not properly identified and the operator fails to isolate them all (e.g. forgets to close the manual valves on the hot warm-up by-pass line – ref. to valves # 3 and # 4 in Figure 2B)
2. Issue 2 - the applied isolation method is not adequate for the heavy hydrocarbon residue at temperature nearly or above the autoignition temperature.

Moreover, from an operability point of view, missing or delaying the flushing of the pump would result in difficulty in removing the solidified hydrocarbon product.

How risks should have been assessed / controlled

Issue 1 - Isolation of complex equipment: for a complex system all precautions should be taken to minimize the operator error during the isolation procedure. These include:

- Drafting of a detailed sketch numbering all valves/blinds to be open/closed or inserted/removed (See Figure 2B). For complex equipment or equipment located in a very dense process area the provision of real photos showing the actual location of specific valves could be attached to the work permit together with the sketch.
- Development of a short clear sequence of operation to guide the operator; the sequence should clearly describe the correct order / timing in which the actions need to be conducted (e.g. a – closure of suction, discharge and hot warm-up by-pass valves 1 ,2 ,3 and 4; etc.).

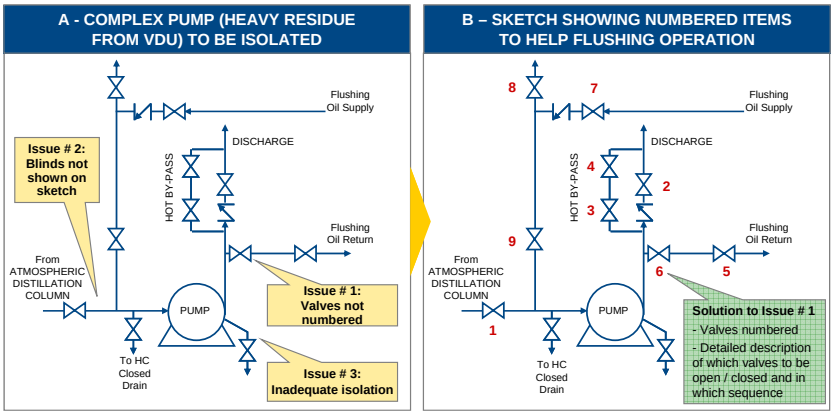
The involvement of maintenance personnel together with operation, contractor (if appropriate) and HSE staff is essential, as the combined knowledge and expertise of a multidisciplinary team will minimize the chance of overlooking a hazard or selecting an inappropriate risk control measure.

Issue 2 - Adequacy of existing isolation: prior to issuing a work permit, the adequacy of the existing isolation configuration should be evaluated, taking into consideration the nature of the fluid e.g. heavy residue and the operating conditions e.g. nearly or above autoignition temperature.

Figure 3 illustrates a guideline developed by an operator on the type of isolation to adopt, based on risk. In this case it was quite evident that a single manual isolation valve on a pump suction line was NOT adequate considering the fluid was a hot residue from the bottom of a vacuum distillation column. Whilst an upgrading plan should have been developed to reinforce the applied isolation based on the “risk level” as shown in Figure 3, immediate precautions should also have been taken to minimize the potential for loss of hot residue including, for example:

- Locking /car seal closed the valves on suction and discharge sides of the pump to minimize the potential for inadvertent opening of the operator
- Minimizing the length of time during which the pump is taken out of service e.g. giving higher priority to the maintenance activity
- Alerting all the operators of the risk involved in such type of isolation and ensure emergency procedures to be activated in case of leak are well understood
- Evaluating the need of additional fire-fighting equipment located in the vicinity of the area to ensure prompt intervention in case of leak of hot residue
- Limit / NOT permitting the conduction of other works in the vicinity of the area, to minimize potential for exposure of personnel to fire following a leak

Figure 2: Scheme of pump to be isolated



Source: Confidential Operating Procedure - Revised and adapted by Arthur D. Little

Figure 3: Isolation Methods

Category	Characteristics	Type	Scheme
I Intrinsic safe isolation	Complete separation between the section and the rest of the plant, which is working	**IA** Physical separation, with blind	
	Isolation with appropriate valves for safety	**IB** Double block and bleed, with blind and possible pressure control	
		IC Single block valve and blind, with possible bleed and pressure control	
II Controlled isolation	Isolation with double valve system and the possibility to control leakages	**IIA** Double block and bleed, with possible pressure control	
		IIB Single block valve and bleed, with possible pressure control	
III Not controlled isolation	Isolation with valves, without the possibility to control leakages	**IIIA** Double block	
	This isolation should never be used with hazardous fluids	**IIIB** Single block valve	

INCREASING RISK

F Working section E Isolated section Bleed Block valve

Source: Confidential Work Permit Procedure – Revised and adapted by Arthur D. Little

3.2 Case History 2 - Temporary modification of safety interlocks

Situation

One of the three analogic level transmitters on a cracked gas compressor KO drum failed giving an incorrect measurement. The three level transmitters were configured with a “2 out of 3” voting logic to trip the compressor in case of high high level in the KO drum. Following the by-pass of the faulty analogic transmitter, the trip logic was degraded to “2 out of 2” and had been kept in this configuration for months.

Typical hazards/risks

The change of the logic from a “2 out of 3” to a “2 out of 2” increases the likelihood of “failure on demand” of the interlock function, thus increasing the risk posed by the process such as compressor damage in case of liquid carryover (e.g. high level in the KO drum) and potential for cracked gas release to ambient resulting in fire / explosion.

How risks should have been assessed / controlled

Alternative measures to compensate the increase in risk should have been evaluated and implemented throughout the period during which the level transmitter was taken out of service and the logic configuration was modified, including for example:

- Establishing periodic field check (via level gauge) of the actual level in the KO drum e.g. 2-3 times per shift
- Minimizing the length of time during which the instrument is taken out of service e.g. giving higher priority to the maintenance activity
- Informing the chief of operation or even a higher level of the organization about the degraded safety conditions in which the plant is operated. For example the decision to configure the two remaining level transmitters in a "2 out 2" logic as opposed to a "1 out of 2" logic should have be taken at appropriate level in the organization
- Increasing the testing frequency of the remaining instruments / components of the interlock loop (at least for sensor and logic solver)
- Considering the reduction of the throughput / capacity of the plant
- Informing affected operators that the plant is being operated in a degraded safe condition, also to ensure awareness of the agreed risk control measures

This sort of evaluation should have been conducted involving people from operation, maintenance/instrumentation and process/technology departments, with adequate knowledge and experience. The process of selecting the most appropriate risk control measures can also be strengthened and made more objective by adopting a semi-quantitative assessment approach, e.g. adopting risk matrix in a "SIL analysis" fashion.

4. Conclusions

The paper underlines the importance of the "risk assessment" as one of the pillars of any PSM system, to ensure an effective management of risks related to facilities and routine / non routine operations involving hazardous materials. The two real cases presented in this paper demonstrate how a sound hazard identification and risk assessment process contributes to the safe and uninterrupted operation of process units and equipment. Hazard identification and risk assessment should not be limited to the design phase of a new plant or the periodic review of a Safety Case; since risk is inherent to all operation modes and activities, appropriate hazard identification and risk assessment techniques should be devised and applied to a variety of situations and circumstances. A key element to ensure the effectiveness of the assessment is the involvement of experienced personnel from operation, maintenance, process, technology and HSE as appropriate. A proper risk assessment is useful to determine if new risks are being introduced or existing risks are going to increase and what technical/organizational measures need to be introduced or strengthen to maintain the risk within the range of acceptability.

References

PSM performance benchmarking study conducted by Arthur D. Little (2007-2009).

OSHA PSM standard (29 CFR 1910.119), Process safety management of highly hazardous chemicals.

The Report of the BP U.S. Refineries Independent Safety Review Panel, January 2001.