MARY KAY O'CONNOR PROCESS SAFETY CENTER
TEXAS A&M ENGINEERING EXPERIMENT STATION

19th Annual International Symposium
October 25-27, 2016 • College Station, Texas

Using Data to Build a Picture of Safety

Alfred Ward, M. Mostert

RiskPoynt - 4100 East Mississippi Avenue Denver, 17th Floor, Colorado 80246, USA

Email – michael.mostert@tpsco.com, al.ward@tullowoil.com

Abstract

Process Safety Management (PSM) involves a number of key elements from a technical prospective 'Plant', operational management 'Processes' and the human element 'People'. All major incidents can be traced back to the failure in the management of these elements and can be attributed to these elements being managed in silos. PSM plays an integral role in delivering efficient, reliable, cost effective and safer facilities.

While PSM has been recognised by many in the Oil &Gas sector, PSM has evolved significantly over the past three decades. Citing key incidents such as Piper Alpha, Longford, Texas City and Macondo have lead regulators such as BSEE 250, EU Offshore Safety Directive 2013/30/eu, UK HSE Safety Case Regulations 2015 and COMAH 2015 to work with operators, industry bodies such as API, UKOOA, IOGP etc. and technology providers to find solutions that demonstrate an asset's integrity and safe operating status. These various stakeholders are driving the need for standardisation in PSM yet are met with the challenge of data proliferation and growing complexity of relating data elements' impact on overall safety status. Emerging as a standard method of conveying asset integrity health is the use of barrier models as a solid approach to improving PSM, resulting in more favourable safety outcomes. The following article is a case study that addresses the next generation of PSM leveraging, complex data, visualisation and the barrier model.

Maximising utilisation of key data sources such as maintenance management systems, operating data control systems for the delivery of PSM enable standardisation in line with the aspirations from the likes of API with 754 Process Safety Key Performance Indicators, Energy Institute Process Safety Management Frame Work, IOGP 415 Asset Integrity and 456 Process Safety Leading Key Performance indicators. These are a few of the recent guidelines created in response to the need to improve both understanding at all levels of the sector and enable means to measure the effectiveness of the PSM.

The following deals with one of the most difficult areas of PSM, the demonstration of the effectiveness of mitigation control measures applied when part or parts of an operating envelope

are compromised. This could be a defective safety critical escalation control barrier, lack of competency in the operating team or a design that fails to deliver and work arounds having to be introduced to maintain safe operations.

Introduction

During the design phase of a facility or process system, there is considerable scope to remove or minimise hazards and maximise process safety to a level that is as low as reasonably practical (ALARP).

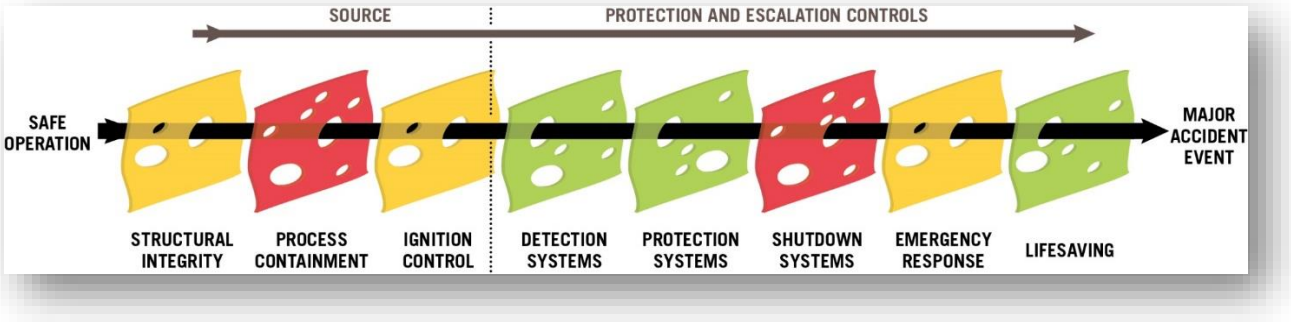
For most operations however they do not have that opportunity, as many installations are aged (with more than 70% of oil production coming from assets older than 10 years), UK HSE KP4 Aging Asset program, typically part of a joint venture, recent asset acquisition or if they are green field, are in pre-start up phases where design decisions have been set in concrete.

The challenge is once a facility is operational, there is a finite maintenance budget that needs to be applied to an ever-changing operation. Dynamic production targets, continuous aging of facilities and the changing levels of competency by shift, POB restrictions, material availability, logistical challenges of equipment delivery methods must be considered.

This article examines how quality data and information (not quantity) plays its part by presenting a picture of common understanding about what the real risks are for a given facility.

The article explores the inclusion of interdependencies into the risk assessment process to further strengthen and validate that same picture – thus stating "Yes I am safe to operate TODAY".

Overview of the Barrier Model



The barrier model concept has been around for many years. Above is a display of 8 barriers that functionally represent complex systems. The idea is that the health of each barrier presents the robustness of the plant, processes and people aligned to safety critical elements and performance standards.

These relate back to the initial design phase and safety cases when the plant's original HAZOP, HAZID, LOPA's and specific BOW TIE analysis were conducted; all of which attribute to major accident hazard identification.

But when a business is in full operational mode – the challenges switch from design to day to day reality. Therefore, if a barrier effectiveness has been compromised during operation, its colour changes. Amber indicates a moderate level and Red is an unsatisfactory level. At some point, and this is the crux of the matter, engineering, operations, maintenance and business leadership accept the decision to voluntarily shut down or to continue to operate with mitigation and recovery plans, providing they are all in place and well managed.

As with all software visualisation tools, the underlying data is critical. The basis for observation of failure remains the operational risk assessment. In some systems risk is categorised as process safety related issues (keeping energy away from people) and operational risk (changes to the operating envelop that takes you out of a design and compliance safety margin). Other categories include deferment and deviation (when work is formally deferred and the risk documented) as well as human factors (shift rotations effecting competency for example).

The operational risk record can be a very complex live document as it describes the risk, which barrier or SCE element is impaired, specific equipment impacted, the details normally noted and broken into multiple hazards, including mitigation summary and recovery plan as well as engineering sign off (onshore support) and offshore leadership team agreement. These records are highly scrutinised, challenged, argued and agreed to, so it's not unusual that it may take weeks to bring a record into approval.

As operators become proficient in the identification and description of hazards and the qualification of scoring the risk profile (using a risk matrix based on consequence, severity and likelihood), they can then set themselves a target for managing the risk to a residual level (ALARP) by mitigation control activities and the reliance on existing safety critical systems (i.e. take credit for existing barriers such as a fire suppression system, structural integrity physical barriers etc.)

This is where things become interesting. When a risk record is established, and the mitigation measure involves for example a level alarm but that level alarm has not been routinely inspected, can the operator now rely on such a mitigation plan?

Say for example a Hydrogen Sulphide (H2S) detector is currently off-line, this places more reliance on the GDS (Gas Detection System) to pick up HC detections to trigger an automatic shutdown. Based on a risk assessment there is now identified failure potential in one section of the plant, putting greater reliance on other systems to keep people safe. It's therefore practical for software systems that manage operational risk data to show the interdependencies and feedback to users during the creation and review of a risk assessment.

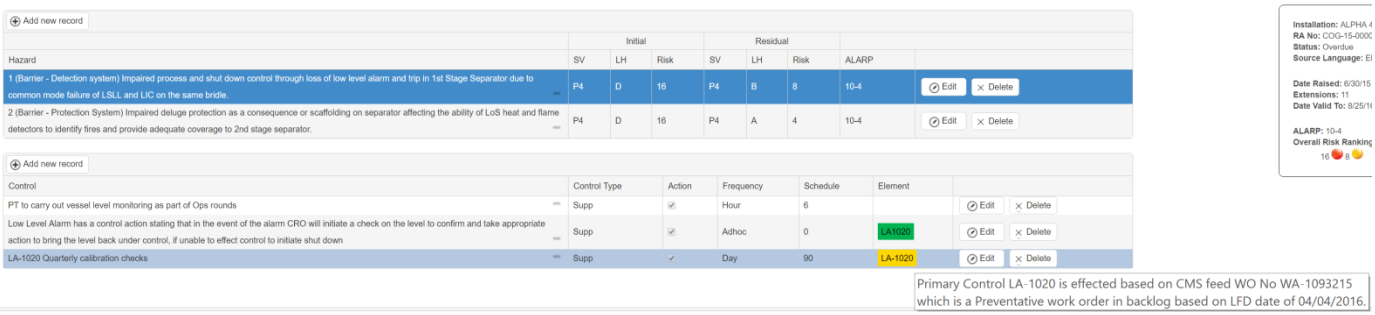
Below are 2 separate examples, one showing how mitigation management identifies dependencies on control elements whilst the other is the visualisation of hard wired dependencies – based on the effect one safety critical element has on another.

1) Mitigation management.

In many cases when the regulator audits a company, the auditor needs to see evidence of robust control measures in place for identified hazards. Operators also want that evidence to

demonstrate their residual risk profile. These controls enable operations to edge back into the safety and compliance zone.

The figure below shows an example of a low level alarm trip on a 1st stage separator. The level control is functioning; the level detector has not been routinely inspected as per the PM (preventative maintenance) schedule. Note the 3 controls in place for the hazard.



Control 1 - Manual Human Process - In the example above the Level indicator is suspected being out of calibration, this requires a person to carry out a visual check. While routine activities based on a schedule are part of the daily operational task list, what is new here is that the activity is linked to the risk assessment control itself. Without this link, it's impossible for operators to look over activity logs and match back to a specific risk assessment. This way the evidence is stored inside a single system for later reporting.

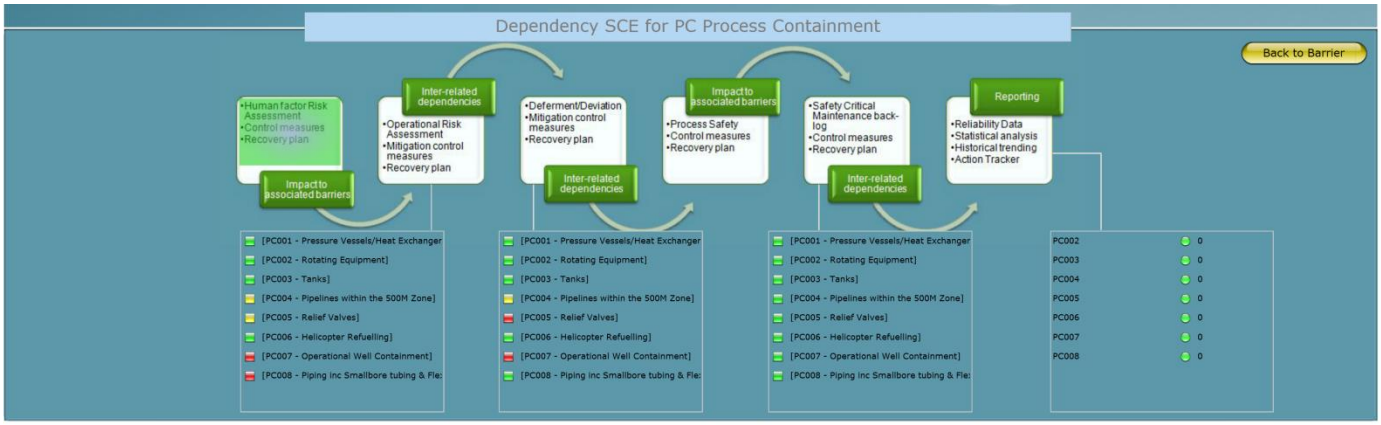
Control 2 – This level alarm is linked to the PI/DCS system which records the working status of the operating element. In this example the element is functioning (GREEN), and provides validation that the equipment being relied on is OK. However, if the element was not functioning, for example was emitting a SHUTDOWN signal, then the colour would be RED. In this case, the operations team are alerted to the fact and will have to make alternative choices on mitigation control. This backs up the evidence that relying on this control element is safe and robust and that the validation comes automatically via the integrated data feed.

Control 3 - Quarterly calibration checks. Here the system looks across the work management system (For example SAP PM, Oracle EAM or IBM Maximo) and identifies that an inspection work order that deals with calibration of the sensor is actually in backlog. Hence the effectiveness of the control element is a downgraded state (Amber). By integrating into the work management system, users are provided with further validation that controls are robust and dependable.

In summary, for this risk assessment, the operator knows to keep a closer attention on the HP Separator and avoid any over pressurisation and potential release. This in turn creates more discussion around why the PM was not complete, and now records are viewed in conjunction with a clear line of sight on what the potential failure points really are.

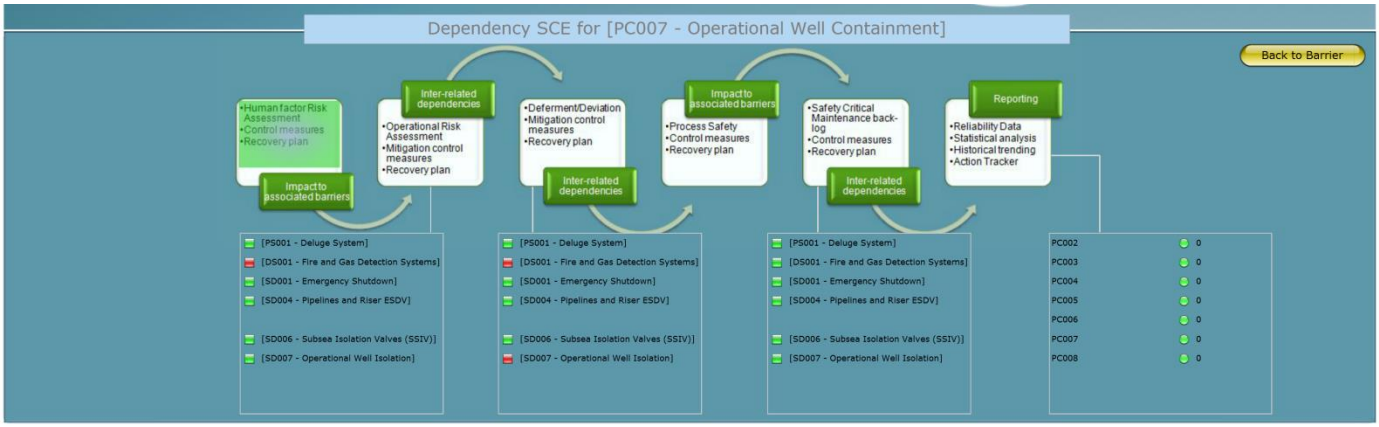
2 - Inter-dependency visualisation

Below is a visualisation example that shows no risk function is independent, by displaying dependencies along with the status of the lower level Safety Critical Elements, broken down in to the risk assessment categories and reliability data.



Process Containment dependency status is displayed, as each barrier is broken down into categories – separating operational and process safety, deferment, SC backlog and on the far right, barrier element availability is calculated based on the volume of inspections carried out and historical information taken from the work management system over the last 12 months.

Selecting any of the status elements will display more detailed information on the condition drivers.



The next figure shows the user selecting an impaired dependency and now the Inter-Dependencies are displayed using the same visualisation method. The implication here is that these safety critical elements are dependent on the PC007 SCE. If "PC007 – Operational Well containment" fails it will put greater dependency on the elements in the list. If all of those elements are also unhealthy and RED, then the model is showing the user a potential interrelated failure.

The Drilldown;

From figure 1.0 - Process Containment

Dependencies

- PC001 Vessels & Exchangers
- PC002 Rotating Equipment
- PC003 Tanks
- PC004 Pipelines
- PC005 Relief Valves
- PC006 Helicopter Refuelling
- PC007 Operational Well Containment
- PC008 Piping inc. Smallbore tubing & Flexible Hose
  Dependency Status
  - (HF) Human Factors
  - (OP) Operational Risk Assessment
  - (DF) Deferment of Safety Critical Maintenance
  - (PS) Process Safety Risk Assessment
  - (SCM) Safety Critical Maintenance Backlog
  - (AV) Availability

From figure 2.0 Inter-Dependency from PC007 Operational Well Containment by Area e.g., Well Bay

Inter-Dependencies Status	HF	OP	DF	PS	SCM
• PS001 Deluge	G	G	G	G	G
• DS001 Fire & Gas Detection		G	R	R	G
G					
• SD001 Shutdown System	G	G	G	G	G
• SD004 Pipeline and Riser Isolation		G	G	G	G
G					
• SD006 Subsea Isolation	G	G	G	G	G
• SD007 Operational Well Isolation		G	G	R	G
G					

Summary

By using a dedicated system for the management and control of operational risk, users are able to focus on the importance and relevance of those risks, bring out a common understanding between the various teams managing the facility.

Visualisation ensures that a wider audience of people have a common understanding of the asset integrity barrier health and this contributes to a strong safety culture. The simple visualisation by way of barriers enables people to “recall” that single picture in their minds – yes, today we are safe to operate.

Reference:

1. *BSEE Regulations 250*
2. *UK HSE Safety Case Regulations 2015*
3. *UK HSE COMAH 2015 Regulation*
4. *UK KP4 Aging assets*
5. *EU Offshore Safety Directive 2013/30/eu*
6. *API with 754 Process Safety Key Performance Indicators,*
7. *Energy Institute Process Safety Management Frame Work,*
8. *IOGP 415 Asset Integrity*
9. *IOGP 456 Process Safety Leading Key Performance indicators.*