Use of Live Barrier Models to Manage Risk

Rae-Ann Joseph, Team Lead – Process Safety, Atlantic LNG Company, Point Fortin, Trinidad and Tobago

Email address: Rae-annJoseph@atlanticlng.com

Keywords: Barriers, SCE, Asset Integrity, Risk management

Introduction

The goal of every operating facility should be to ensure its assets and equipment are operated safely, or without the threat of potential harm. Process Safety focuses on preventing and mitigating major accidents caused by the uncontrolled releases of hazardous materials by ensuring the right barriers are in place.

The Center for Chemical Process Safety (CCPS) [1] defines a barrier as a control measure or grouping of control elements that on its own can prevent a threat from developing into a hazardous scenario or can mitigate consequences once it has occurred. Barriers that prevent or mitigate major accidents are considered safety critical equipment (SCE) i.e., any part of a facility whose failure will either cause a major accident, or the purpose of which is to prevent or limit the effects of a major accident (CCPS 2018).

There are two main types of barriers - hardware and human. Hardware barriers include primary containment, process equipment and engineered systems designed to prevent major accident events (usually associated with loss of primary containment) and mitigate potential consequences of such. Human barriers are those that rely on the actions of people capable of carrying out activities designed to prevent loss of primary containment or process safety events, and mitigate any potential consequences of such (IOGP, 2018). Barrier Management is a systematic approach for managing hardware barriers to ensure they are functional, effective and available when required to prevent or mitigate against hazardous scenarios.

This paper focuses on use of a visual live barrier model to demonstrate hardware barrier effectiveness (or lack thereof). The model provides a cumulative risk profile based on barrier degradation across the facility, and this be used to guide risk-based decision making and prioritization of resources.

The steps to develop a live ‘Barrier Model’ are summarized below:

1. Identify major accident events (MAE) from risk assessments and develop MAE Bowties.
2. Identify hardware barriers from PHAs (process hazard analyses) and categorize using the hardware barrier and SCE groups in IOGP Report 415 Supplement: Standardization of Barrier Definitions.
3. Assess barrier effectiveness using data such as maintenance history, asset integrity inspections, root cause failure analyses, records of impairment and technical studies.
4. Use the data collated to ascertain barrier health as effective, partially effective or impaired and export to a live model to visualize cumulative risk. The barrier model can be built in-house or risk visualization software tools can be procured, developed and customized to meet customer needs.
5. Identify corrective measures to restore the barriers to their intended design and develop remedial action plans to reduce the cumulative risk posed by impaired barriers.
6. Monitor barrier health using well-defined metrics and take corrective action as needed.

Developing a Live Barrier Model

The Live Barrier Health model is based on the ‘Swiss cheese’ model concept (Figure 1), which asserts that no barrier can ever be 100% effective because ‘holes’ are always present. This is due to continuous changes in barrier health as a result of equipment deterioration, temporary bypasses, operational changes, maintenance lapses, as well as human factors over time.

Catastrophic process safety events such as Bhopal (1984) and the Texas City Refinery explosion (2005) are rarely caused by a single barrier failure but rather the failure of many barriers which did not perform as designed. Having multiple barriers reduces the likelihood that the holes align at the same time thus preventing the worst-case event from being realized. Minimizing the size of barrier hole, or extent of its defect reduces the likelihood of an incident.

The aim of the live barrier model is to identify and address gaps in the barrier performance, by minimizing the impact, or restoring to 100% effectiveness in minimal time. Only when these barriers are managed and maintained in such a way that they can perform as intended at all times, can a facility truly demonstrate that it is managing its operational risks successfully.

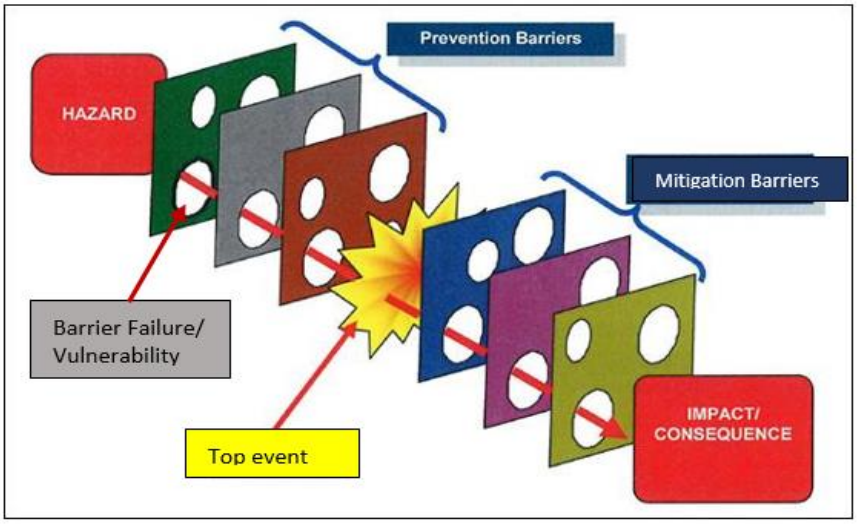

Figure 1: Swiss Cheese Model Diagram

Identify Major Accident Events

A major accident event (MAE) is defined as a hazardous event that results in one or more fatalities or even severe injuries; or excessive damage to structure, installation or plant; or large-scale, severe and/or persistent impact on the environment (CCPS 2018). MAE scenarios can be identified from facility process hazard analyses (PHAs) such as HAZOPs, HAZID. These PHAs / risk assessments can also be used to establish the barrier role or function and elements in hazard management.

Develop Bowtie diagrams

A bowtie diagram is a visual risk management tool that shows how various threats can lead to a loss of control of a hazard and allow this unsafe condition to develop into several undesired consequences [CCPS]. It also allows users to see which barriers prevent a top event such as a loss of primary containment (proactive) or mitigate consequences (reactive) e.g., fires and explosions. Figure 2 provides an illustration of a standard bowtie that can be used to depict an MAE.

It is important to note that at a detailed level, bowties can be used to highlight potential degradation mechanisms that undermine barrier health and to verify whether there is sufficient mitigations or measures in place to manage the risk introduced by a compromised barrier. A degradation mechanism or escalation factor is a condition that reduces barrier effectiveness, preventing it from fully performing as intended when required. Barrier degradation can be caused by human factors, mechanical failures, abnormal conditions or loss of utilities e.g., power, instrument air, cooling.

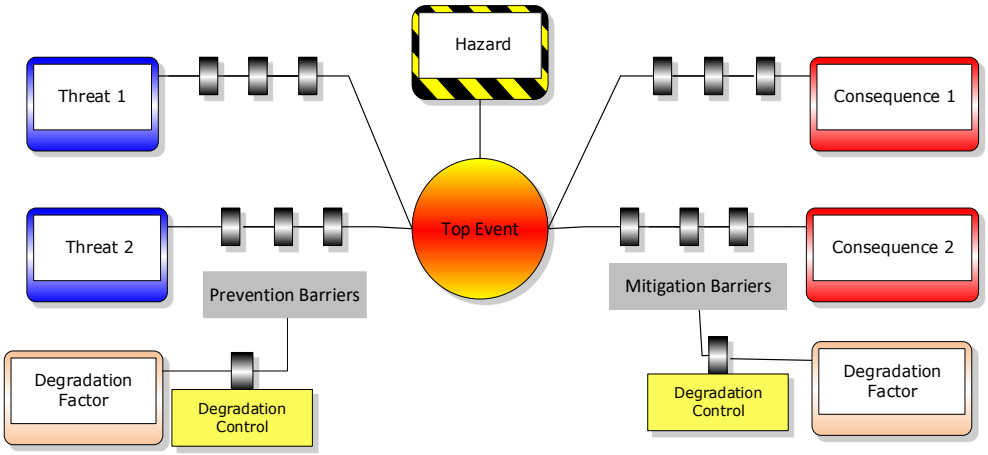

Figure 2: Illustration of a Standard Bowtie and its basic elements

Visualization of risk using a barrier model or bowtie offers one other key advantage over other risk management tools, i.e. demonstration of how well the facility proactively manages its risks. Barriers on the left side of the top event represent prevention (proactive) measures while barriers on the right display recovery or mitigation (reactive) barriers. A balanced and proactive approach should have sufficient, effective barriers between the threat and top event to prevent loss of control of the hazard. If the preventative barriers are inadequate this indicates heavy dependence on recovery barriers and a reactive approach to risk management, which is not as effective as a proactive one. When managing hazards, it is best to apply the principle of prevention is better than cure, or in this case, mitigation.

Identify and Categorize Safety Critical Hardware Barriers

Identify Safety Critical Hardware Barriers

Barriers on a bowtie can be human or hardware barriers, or a combination of both. The live Barrier model focuses solely on safety critical hardware barriers. To properly identify and tag hardware barriers as SCE, a structured and computerized asset register with current equipment data must first exist. The bowtie will show only equipment type at a high level e.g., for an overpressure scenario, one sees a PSV, or high-pressure trip is required to prevent a loss of containment. However, at a granular level in the CMMS and barrier model, the PSV is specific to a system or vessel and must be tagged as SCE in the facility's asset register. Facility HAZOPs and LOPA studies must be used to support the detailed tagging of SCE equipment

Assign SCE to a Hardware Barrier Group and SCE Sub-Group

After selecting and tagging equipment as SCE in the master equipment database, assign each an SCE sub-group under the umbrella of the eight hardware barrier groups (IOGP 2016) shown in Table 2. These SCE should be defined by their hazard management safety function as per the MAE scenarios in the risk assessment. Note: a facility is not required to have SCE in every sub-group and hardware barrier category. SCE barriers are designed and installed to address the specific hazards identified within the process, and can be managed at an elemental, group, or system level.

During the SCE identification process, use of a systematic naming convention is recommended that will help users easily identify SCE within the proper SCE Sub-Group and Hardware Barrier Group. For instance, if there are five (5) SCE sub-groups within Emergency Response (Hardware Barrier Code- ER), these will be assigned SCE sub-group codes ER-01, ER-02…ER-05 etc., with the final numeric count reflecting the number of sub-groups relevant to the facility.

The asset database administrator should be consulted with when making changes to the master database such as new system features e.g., a SCE checkbox, SCE hardware barrier and sub-group.

Table 1: IOGP Hardware Barrier Groups and SCE Sub-Group Examples

Hardware Barrier	SCE Sub-group examples
1. SI: Structural Integrity	Foundation and Surface Structures Heavy Lift Cranes & Mechanical Handling Equipment
2. PC: Process Containment	Pressure Vessels, Fired Heaters Piping Systems, Relief Systems
3. IC: Ignition Control	Hazardous and Non-Hazardous Area Ventilation Certified Electrical Equipment, Earth Bonding Purge Systems, Inert Gas Blanket Systems, Miscellaneous Ignition Control Components
4. DS: Detection Systems	Fire and Gas Detection Security Systems
5. PS: Protection Systems	Deluge and Sprinkler Systems Fire and Explosion Protection Systems Firewater Pumps and Firewater Ring Main Gaseous and Passive Fire Protection Systems Power Management System
6. SD: Shutdown Systems	Emergency Shutdown System, Depressurization System High Integrity Protection Systems (HIPPS) Isolation Valves, Process Emergency Shutdown Valves (ESDVs)

Hardware Barrier	SCE Sub-group examples
7. ER: Emergency Response	Primary Muster Areas, Evacuation Routes, Communication Systems Emergency Power, Uninterruptible Power Supply (UPS)
8. LS: Life Saving Equipment	Personal Survival Equipment (PSE) Rescue Facilities, Lifeboats

Develop SCE Performance Standards and Assurance Criteria

A Performance Standard is a measurable statement, expressed in qualitative or quantitative terms, of the performance required of a system, equipment, person or procedure and that is relied upon as a basis for managing a hazard (IOGP 2018). Performance standards determine equipment design specifications and requirements for maintenance and testing throughout the asset's lifecycle to provide assurance that the SCE can meet the performance criteria when called upon to act in a hazardous scenario. Figure 3 provides an example a Performance Standard for SCE sub-group, Active Fire Protection Systems, which falls under the Hardware Barrier group, Protection Systems (PS) with the necessary assurance checks.

Figure 3: Excerpt from a Generic Performance Standard

PERFORMANCE STANDARD	**PS-XX ACTIVE FIRE PROTECTION SYSTEMS**		
Performance Objective	Provide fire water on demand to extinguish or limit the spread and effects of a fire.		
SYSTEM OVERVIEW			
To meet the performance objective, active fire protection systems are designed as per the design philosophy articulated under NFPA-59 code to provide adequate coverage for all conceivable major accidents and fire scenarios on the Facility. The system comprises: - A main fire water supply tank and a buffer tank with adequate volume reserved for firefighting and distribution to site locations via firewater ring main. - The firewater main pressure is maintained by two electrically powered pumps (one duty, one standby), that automatically start when ring main pressure drops below set pressures. Firewater is pumped from the firewater tanks through a ring-main distribution system to hydrants, monitors, deluge systems, and hose stations to provide fire protection coverage across the facility. - Supplementary firefighting equipment e.g. portable fire extinguishers and fire hoses			
FUNCTIONAL REQUIREMENT 1:			
Performance Criteria	**Basis**	**Assurance Task**	**Verification**
Firewater Pump Design Each pump shall be capable of supplying firewater at design capacity and pressure within 30 seconds of start signal and run for a period of at least 2 hours.	Firewater discharge pressure Firewater flow rate	Firewater Pump and Engine Function Test and Inspection per required frequency	Perform function test and ensure procedure adequately assures function under test. Review records to ensure pumps have been tested at the appropriate frequency and results recorded are acceptable.
Pump Activation The firewater system shall provide automatic audible and visual alarm or indication to operators when the: - - Firewater pump activates - Pump fails to start on demand	Equipment Design basis	1. Firewater Pump and Engine Function Test and Inspection per required frequency 2. Fire pump activation alarm on Control Panel	Review function test results and verify as acceptable or within limits. Review records to ensure activation alarms (audio/ visual) were tested at the appropriate frequency and results recorded.

Evaluate Barrier Effectiveness

For a barrier to be valid, it should be effective, independent and auditable. Barrier effectiveness was assessed by a cross functional team using objective criteria and verification methods such as auditing barriers against Performance Standards requirements, reviewing equipment maintenance history, equipment inspections, failure analyses and relevant risk studies. The effectiveness rating was determined based on the table below.

Table 2: Barrier Effectiveness Assessment Criteria

Effectiveness Score	Definition
Effective	A functional SCE device or barrier with no known defects that can impact functionality of the SCE device. The barrier performs its intended function when required and to the intended standard.
Partially effective	A functional SCE device with known defects that may impact SCE functionality in the near future (i.e. operating with defects).
Impaired	A non-functional SCE device i.e. not functioning per design and does not meet its performance standard.

Establish Objective Rule Sets

The effectiveness score assigned to each SCE sub-group and Hardware Barrier group was determined using objective evaluation criteria and pre-established quantitative and qualitative rule sets.

Qualitative Rule Sets

1. If a barrier is overdue for inspection or preventative maintenance, it is labelled “partially effective” once there were adequate mitigations are in place e.g. redundant equipment.
2. A temporary repair may generally be classed as impaired if it goes beyond the approved repair date and a healthy condition cannot be confirmed.
3. Reportable leaks on equipment and piping containing hazardous chemicals are classified as Impaired or Partially Effective, based on leak quantification levels.

Quantitative Rule Sets

When applying quantitative rules, it was assumed all barriers carry equal weight. However, in reality, preventative barriers play a more critical role because they help prevent accidents and may be assigned a heavier weighting if desired. The owners of the tool can choose to allocate more weight on specific SCE sub-groups establish rule sets based on absolute values or percentages of the total number of barriers at the Hardware barrier group or SCE sub-group level.

Identification of risks that lead to ineffective barriers

Barrier degradation occurs for various reasons but mainly deviation from design intent, inadequate maintenance, failure etc. all of which undermines barrier performance. When assessing risk of a single barrier failure or degradation, one must consider all potential equipment integrity issues including asset integrity and operational risk.

Asset Integrity and Operational Integrity Risk

Asset Integrity risk stems from compromised equipment integrity based on defects from inspections or equipment failures. Asset integrity declines further when preventative maintenance tasks such as inspection, testing and maintenance of barriers are deferred. This can lead to SCE not meeting Performance Standards assurance criteria. Risk is also introduced from gaps in equipment design identified from engineering or risk studies. Some of these deficiencies developed over time due to facility wear and tear, or aging, or due to original design codes becoming obsolete. These require a long-term permanent solution and can be mitigated in the interim using temporary measures.

Operational integrity risk and challenges arise when there are deviations from design intent and exceedance of design limits, or repeated operation beyond safe operating limits.

Treatment of Risks Associated with Ineffective Barriers

The residual risk for various sources of impairment should be considered in the cumulative risk profile to provide a complete risk picture. Where barriers are ineffective, steps must be taken to minimize cumulative risk. For example:

1. Evaluate the risk of continued operation with the single barrier failure

2. Identify and verify possible interim risk reduction measures from facility PHAs or the MAE system bowties until the barrier can be restored to full function.
3. Apply pre-determined tolerability criteria for shutdown of systems or equipment, e.g., a minimum of two effective hardware barriers groups per threat on both sides of bowtie
4. Use an objective decision-making process on whether to continue operating with the impairment with mitigating measures, or halt operations and repair.
5. Develop remedial action plans which are endorsed and approved by leadership. The remedial plans should reduce the cumulative risk posed by impaired barriers. Greater emphasis should be placed on addressing defects in preventative barriers versus mitigative.
6. Routine verification of interim measures for the duration of impairment until the barrier is restored to full effectiveness.

Risk Mitigation

When identifying possible interim risk reduction measures to mitigate the emergent risk the following options should be considered for the proposed duration of the degradation until the impacted barrier can be restored to its function and design intent.

1. Temporary operating procedures
2. Increased frequency of monitoring and surveillance e.g. operator rounds
3. Increased frequency of inspection or testing
4. Use of a temporary repair or substitute measure e.g., portable fire and gas detectors or mobile fire-fighting equipment
5. Reduce demand on the system or restriction of activities that may increase risk e.g., reduce inventory, operating parameters, restriction of personnel
6. Limited work in the vicinity of the impairment e.g. SIMOPs
7. Total or partial shutdown of the process equipment.

Determine overall cumulative risk for the facility

The live Barrier model can provide a visual of cumulative risk by illustrating barrier effectiveness. While single barrier degradations may not seem significant, if the defects or gaps align as in a Swiss cheese model, there may be no effective barriers in place to prevent a hazard from progressing to major accident consequences. Seemingly minor defects in individual barriers can combine in an unforeseen manner and hinder their ability to perform as required.

Use of a live barrier model enables users to see how SCE, related roles and processes integrate to manage risks. More importantly, those in key leadership positions can see when there are gaps due to barrier degradation and help identify suitable degradation controls. Degradation controls minimize risk exposure by reducing the potential severity and likelihood of the defect.

SCE Performance Management and Review

When it comes to monitoring Barrier health, an organisation should select well-defined metrics that identify critical areas of weaknesses in its barrier management system and take prompt corrective action to address gaps. Guidance on selecting suitable SCE management KPIs (leading and lagging) can be found in industry guidelines such as API RP 754 - Process Safety Performance Indicators for the Refining and Petrochemical Industries.

Some examples of pertinent KPIs or metrics include:

Leading Indicators for barrier health	Lagging Indicators for barrier health
• SCE with overdue inspection dates • SCE that failed inspection tests • % SCE PM Compliance	• No. of impaired barriers • SCE that failed to function on demand • % SCE Compliance

The model provides users with a snapshot of barrier health at a point in time. Users must also review trends over time to identify system vulnerabilities and susceptible areas and prioritize resources to reduce defects (systemic or equipment) and total risk. This is important especially for mature or ageing facilities which face a plethora of asset integrity concerns as the asset nears end of life.

Summary of Results

When selecting a live barrier model tool, the tool must be developed to benefit users at all levels of the organisation e.g. frontline personnel, engineers, management and communicate key areas of concerns effectively. It should provide a high-level overview of the facility and allow users to drill down to pertinent data as needed to investigate potential concerns. Figure 4 shows a facility comprising multiple business units, with impaired equipment in the Process Containment hardware barrier group on Unit 1, and potential Detection system issues on all units.

Further drill down of Unit 1 in the model (Figure 5) reveals that the main source of impairment lies within the SCE sub-groups for Piping systems and Relief systems. When frontline persons view the details, they may find instances of piping related impairments such as significant corrosion related repairs, leaks or overdue PSV testing on Unit 1. This will require verification of current condition and interim mitigations to ensure the unit remains safe to operate.

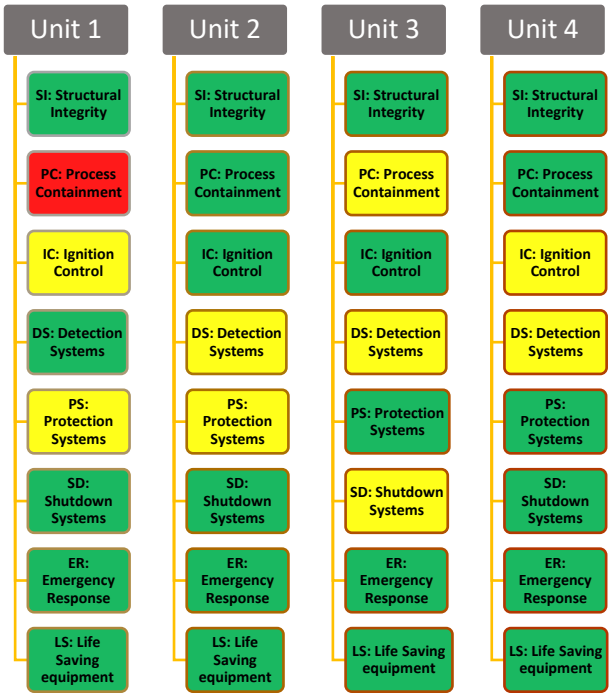

Figure 4: Facility Barrier Health Overview Showing Business Units

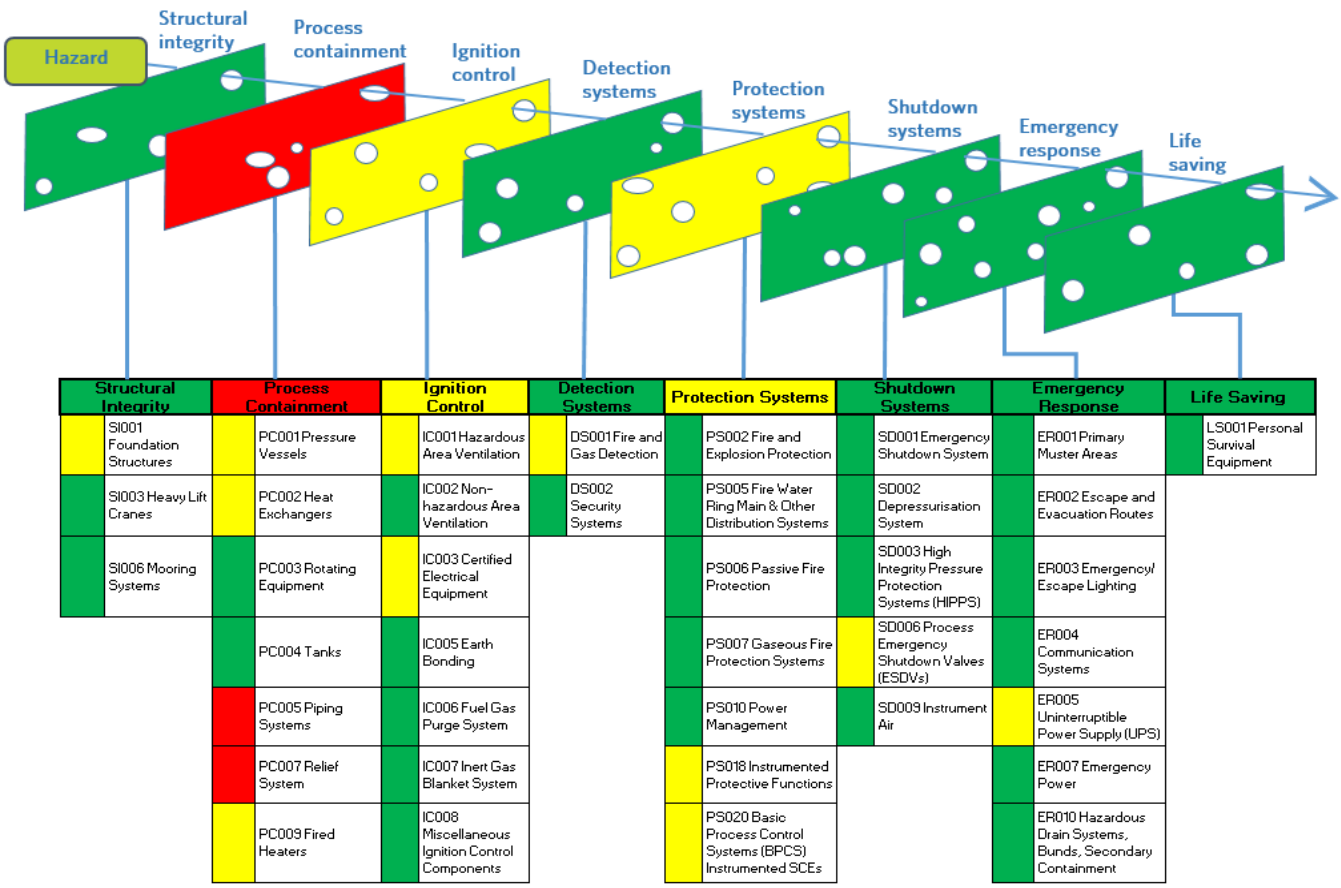

Figure 5: Detailed Barrier Health View of Train 1 Process Area

Lessons Learned

The journey to implement a live barrier model provided meaningful value to the organisation, but as is the case with most new initiatives, there comes key learnings that must be applied to ensure the success of similar future projects. Key lessons from this project comprise use of an effective change management process and understanding systemic challenges one may encounter along the way. For instance:

- Use and application of a clear and well-defined SCE identification and equipment tagging process at individual, unit and system levels. Failure to do this can lead to either inadequate oversight of SCE; incorrect assignment of equipment to SCE groups which means the appropriate maintenance and testing strategy may not be applied; or over determination of SCE at the unit level which increases the workload associated with preventative maintenance and assurance tasks.
- Early stakeholder engagement and buy in when making changes to existing processes owned by teams external to the implementation team.
- Identification of critical software features and performance criteria in the early project stages e.g. visual layout, ability to summarize data and generate reports of interest
- Verification of data accuracy and quality for digital based initiatives. The output of any tool is only as good as the input hence data used must accurately reflect SCE impairments for effectiveness.
- Realistic targets for achieving major project milestones. Our goal was to ensure there were zero ineffective barriers without approvals or interim risk mitigations in place. One must first understand and map out the required workflows and resources needed to support that objective, or set targets to reflect current resource levels.
- A detailed and agreed upon interfacing and handover strategy with clear roles and responsibilities for sustained embedding of the changes after the go-live or launch dates.

Systemic Challenges and Observations

Use of the model improved barrier management culture and awareness significantly, but it also revealed systemic gaps and areas for improvement within interfacing functions e.g., maintenance management practices for SCE and non-SCE, turnarounds; and quality of data in the CMMS which posed potential risk due to unknowns, and skewed outputs in the barrier model. Observations of these gaps include:

1. Significant work order backlog points to potential challenges in work prioritisation or insufficient resources to meet the required manhours to liquidate the backlog.
2. Omission of SCE work from major turnaround scopes highlighted gaps in communication between TAR planning and interfacing teams, and inadequate scope definition, planning and scheduling. The impact is deferral of some SCE tasks to ensure timely startup.
3. Inconsistent labeling of SCE tags in various process areas on the facility. If equipment was not tagged as SCE, no inspection or maintenance strategy was in place to provide SCE assurance.
4. Entry and closure of work orders with insufficient details on equipment condition or failure.
5. Instances of duplicate or aged SCE work orders (5+ years old) cluttered the CMMS and skewed output in the live barrier model.
6. Gaps in collating reports or data for jobs done by third party contractors.
7. Uncertainty in terms of asset integrity ownership for certain joint/ common systems leading to inadequate oversight in some cases and eventual equipment failure.

Benefits

Use of a visual live barrier model to manage risk provided many benefits to the organisation not just in terms of risk management but overall continuous improvement efforts and improved clarification around roles and responsibilities and accountability for barrier management. More specifically:

1. A central hub to manage risk due to barrier degradations and impairments which provides a complete, cumulative visual of the facility's risk for front line employees and leadership.
2. Data to support timely, risk-based decision making in terms of work prioritization and scheduling, and allocation of resources for risk reduction projects.
3. Streamlined work management and planning processes for managing barrier health
4. Improved awareness of barrier management roles (detection, reporting, repair, risk mitigation)
5. Increased ownership from front line supervisors in addressing and reducing ineffective barriers.
6. Overall 90 % reduction achieved thus far in the number of ineffective barriers onsite.
7. The model served as a catalyst for continuous improvement initiatives to address some of the systemic challenges identified in the previous section.

Limitations

There are also limitations associated with use of this tool mainly around data quality and software or tool customization needs. Some examples of these include:

1. Absence of data in a computerized maintenance management system (CMMS) limits the facility's ability to create a robust live barrier health model or tool.
2. The output of the visualization tool is only as good as the data inputted. Quality of data entered in the model can skew results e.g. duplicate work orders, incorrect entry or closure of work orders, incorrect classification of work as corrective vs preventative, or shutdown vs normal operations.
3. Limited customizability of software tool features to meet customer needs. It is important for the client to communicate the critical features desired upfront during design and before procurement. Customization in the later stages can be costly and time consuming for both the vendor and client.

Conclusion

Effective risk management requires complete oversight and understanding of process hazards, how they lead to major accidents, and the barriers needed to manage the risk associated with these hazards. The primary objective of the live barrier model is to use real time data to assess and visualize barrier health, and manage emergent risks introduced by ineffective barriers on the facility.

A risk management strategy based on proven barrier health is an effective one as it helps provide assurance that barriers are in place and will perform as intended in a hazardous scenario. More importantly, users, specifically frontline personnel, managers and leadership are aware of key risks or areas of vulnerability when there are impaired barriers due to degradation. In turn, this empowers them to make timely, and strategic decisions to proactively manage and address risks on a facility.

References

1. Center for Chemical Process Safety (CCPS), *Bowties in Risk Management: A Concept Book for Process Safety*. American Institute of Chemical Engineers (AIChE), New York, NY & Energy Institute, Great Britain, (2018), pp xv-xxi
2. International Association of Oil and Gas Producers (IOGP) Report 415 Supplement: *Standardization of Barrier Definitions (*2016), pp 9-13
3. International Association of Oil and Gas Producers (IOGP) Report 415. *Asset integrity – the key to managing major incident risks* (2018), pp 14-16.