Evaluation, Visualization and Monitoring of Cumulative Risk Exposure Resulting from Safety Critical Hardware and Human Barriers Deviation

T Olusanya*[1], O Adeyemi*[2], O Olusanya*[3]

*[1] Principal Consultant, Melios, Aberdeen

*[2] Senior Consultant, Melios, Lagos

*[3]Principal Consultant, Cerebral Instinct, London

Identifying, understanding, and managing major risks is an integral part of operations within major hazard industries. In the UK and throughout Europe, this is typically achieved within a framework of goal-setting or prescriptive regulatory requirements. Safeguards required to protect against major risks or Major Accident Hazards (MAHs) exposures are known as Safety Critical Barriers (SCBs) and comprises of human and hardware elements or a hybrid of both.

If an SCB is unable to operate as intended, it is deemed as an impairment from its functional requirement and is subject to an operational risk assessment. Impairments can include degraded hardware systems, maintenance backlogs, overrides, poor operating discipline, etc. SCB impairments can result in increased exposure to MAHs and undermine an organisation's ability to demonstrate that operational risks remain as low as reasonably practicable (ALARP).

Operational risk assessments often focus on individual SCBs, and the impact caused by deviation from their functional criteria, as opposed to the aggregate risk exposure from all recorded deviations. The outcome of these assessments typically leads to implementation of temporary safety measures that do not consider the cumulative effect of all existing interim safeguards associated with other SCB deviations. Risk assessment of SCB deviations also tend to primarily consider hardware systems with limited or no attention given to cumulative risk exposures created by impaired hardware and human-based SCBs.

The significance of managing cumulative risk exposure is further emphasized by the fact that major accidents seldom occur from the loss of a single SCB, but rather from combined hardware and human barrier failures. For example, in the Texas City refinery incident, the investigation uncovered a string of failures that included procedural breaches and equipment malfunction. Unofficial procedures were followed as the raffinate splitter tower was over-filled and the high-level alarm for the tower was non-functional and did not sound (Kolokson, 2020).

Although guidelines exist for cumulative risk management, current approaches can be cumbersome, labourious and provide limited or no comprehensive inclusion, visibility, and monitoring of all contributing hardware and human-related SCB deviations. To illustrate this for a typical MAH facility, multiple changes are regularly made to equipment functionality to mitigate the impacts arising from a protracted delay to start-up. These changes are risk assessed individually with implementation of temporary mitigations. However, there is often a lack of visibility or understanding of the cumulative effect of all the changes. Frequently, there is the perception that a cumulative risk assessment would be complex and time consuming, resulting in the acceptance of a risk exposure that is not fully understood.

Accounting for cumulative risks in operations and effectively demonstrating ALARP, even when temporary controls are put in place to mitigate SCB deviations, therefore remains a challenge. Operators of major hazard facilities openly recognise this challenge. It is widely accepted that a true understanding of cumulative risk is imperative and invaluable for successful major risk management and operational performance. To achieve this a methodology must provide robust and verifiable means of assessing cumulative risk exposure without being too onerous. The methodology must connect to a variety of data sources (i.e., SAP®, Synergi®, Permit to Work, Override logs etc.) and account for all hardware and human-based SCB deviations.

This paper discusses an alternative approach to assessing cumulative risk derived from hardware and human SCBs deviations. This approach takes SCB impairments into account, including sub-elements and tasks that are necessary for the barriers to function as intended, and the interactions and dependencies between the sub-elements and tasks. The approach is consistent with industry guidelines and good practice publications. It utilises a custom algorithm that enables determination of cumulative risk ratings based on dynamic status of all SCB elements, the hazard management hierarchy principle, and credible and foreseeable scenarios related to identified MAH at a facility.

The methodology has been developed into a digital tool. It enables monitoring and visualization of cumulative risk exposure. It also enables dynamic barrier management, while helping organisations to focus attention on those SCB deviations associated with cumulative risk exposures and the main contributors to major accident risk reduction. This methodology deepens understanding of major accident cumulative risks, helping to maintain it at or below their acceptable thresholds throughout the life of a facility. It also provides an intelligent, and comprehensive means for effective and dynamic ALARP demonstration.

The cumulative risk digital tool has already been deployed on several MAH facilities where it has been proven to be an effective and reliable means to develop a representative cumulative risk profile. Ultimately, this has enabled organisations to achieve informed, risk-based decision-making related to resource planning, allocation, and deployment of measures to reduce their exposure and vulnerability to major risks.

Introduction

Current industry position on Cumulative Risk

Understanding, assessing and effectively managing cumulative risk is widely acknowledged in the high hazard industry, particularly in the oil and gas industry, as critical to robust demonstration of safety and integrity of operating assets.

In the United Kingdom (UK) upstream oil and gas industry for example, concerns around limited consideration and visibility of cumulative risk management are well established. Prominent industry stakeholders such as the offshore safety regulatory body, the UK Health and Safety Executive (HSE) and the leading representative body for the UK offshore oil and gas industry, the Oil and Gas UK (OGUK) have both expressed the need for owners of oil and gas installations to demonstrate how cumulative risks are addressed in major accident hazard management.

In its Asset Integrity Key Programme 4 (KP4) publication the UK HSE, under the Process Integrity findings, advises Duty Holders that *where a Safety Critical Element (SCE) has more than one Operational Risk Assessment (ORA), the consequences should be considered in combination to ensure they do not unduly increase risks to the installation* (UK HSE, 2013). The OGUK in its Cumulative Risk Guideline publication states that *the significance of the threat from cumulative effect of a number of deviations has become more apparent in recent years* (OGUK, 2016).

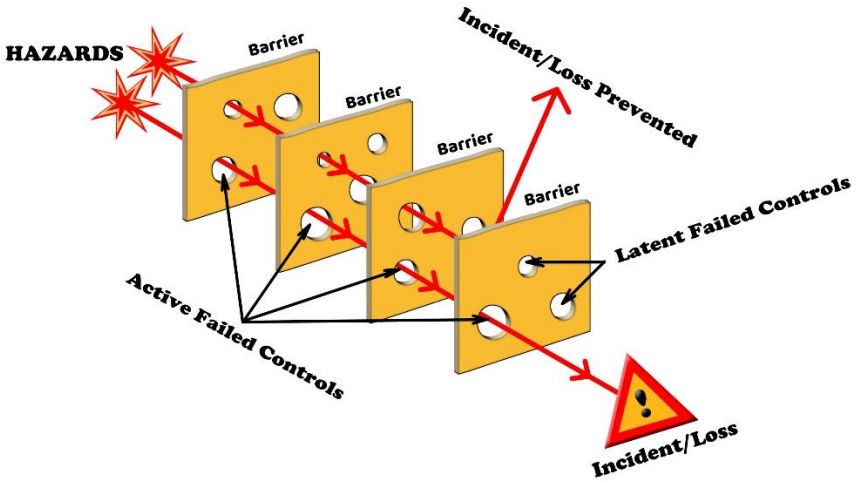
The predominant opinion in the oil and gas industry agrees that current risk management practices such as the use of ORA and other allied methods for managing SCBs impairments or deviations is not adequate for cumulative risk management. This is because it focuses on assessment of individual barrier deviation and the implementation of remedial measures without considering inter-dependencies of multiple barrier deviations and the cumulative exposure they create.

To address concerns around cumulative risk created by multiple SCBs deviations, different methodologies have been proposed and published. These methodologies range from the use of complex mathematical model to simplified tools that help to monitor barrier degradation. This paper introduces an approach that lies between the spectrum of proposed methodologies, accounts for interactions and interdependencies among impaired human and hardware SCBs, connects with relevant data sources, enables dynamic monitoring of barrier health status and their impact on overall exposure to major risks, and provides a reliable platform for managing cumulative risk exposure.

Previous Accident and Cumulative Risk Contribution

Evidence from various accident investigation reports supports the industry position on the significance of managing cumulative risk exposures. It shows that major accident events often result from a combination of failures where the holes or deficiencies in a series of barriers line up as illustrated by Figure 1 rather than from a single barrier impairment. The deficiencies or holes at each layer of protection are constantly increasing or decreasing based on management decisions and operational deviations (Reason, 1997). The following major accident examples shows how layers of protections can progressively be weakened with little or no visibility of the vulnerability caused by these barrier deficiencies.

Figure 1: Swiss Cheese Barrier Concept



Caribbean Petroleum Company (CAPECO) Tank Terminal Explosion

The accident occurred in Puerto Rico during offloading of gasoline from a tanker ship to the CAPECO tank farm onshore on night of October 23rd, 2009. A 5-million-gallon aboveground storage tank (AST) overflowed into a secondary containment dike which caused the gasoline spray to be aerosolized (forming a large vapour cloud) and ignited after reaching the ignition source. It resulted in damage to 17 out of the 48 storage tanks, other equipment onsite and leakage of the petroleum products to the environment. (CSB, 2010).

The investigation found that that numerous technical and systemic failures contributed to the accident. Multiple layers of protection failed within the level control and monitoring system at the same time in addition to a lack of independent safeguards. The incident was also attributed to multiple deficiencies in the safety management system in addition to failures of the hardware barriers. For example, there was a lack of formal procedures for tank filling operations for operators and managers, disregard for standard operating procedures, an insufficient integrity program for safety critical equipment and a poor culture of not closing out safety critical actions from audit and inspections (CSB, 2010).

Texas City Refinery Explosion and Fire

On 23 March 2005, an explosion erupted at BP's Texas City refinery, which led to 15 fatalities, 180 injured and $3billion in damages and legal settlements (Kalokson, 2020). The incident occurred during the startup of an isomerization unit when a raffinate splitter tower was overfilled; pressure relief devices opened, resulting in a flammable liquid geyser from a blowdown stack that was not equipped with a flare. The resulting vapour cloud was ignited resulting in an explosion and fire. (CSB, 2007).

A litany of barrier failures that included procedural breaches, poor communication at shift handover and equipment malfunction was found during the investigation. Unofficial procedures were followed as the raffinate splitter tower was over-filled and the high-level alarm for the tower was non-functional and did not sound (Kalokson, 2020). The investigation found that Texas City management did not emphasize the importance of following procedures as evidenced by its lack of enforcement of the Management of Change (MOC) policy, its acceptance of procedural deviations during past start-ups, and its failure to ensure that the procedures remained up-to-date and accurate (CSB, 2007). In its fatal accident investigation report the company emphasized that following the procedures would have prevented the explosions and fire on March 23 (BP. 2005).

Piper Alpha

On 6 July 1988, an explosion occurred from ignition of a low-lying cloud of condensate. The explosion occurred in the gas compression module of the Piper Alpha Platform. The ensuing event resulted in167 fatalities offshore. The detailed report that followed highlighted a series of failings bothering on both equipment and management system failures (Cullen, 1990).

These examples show a consistent pattern in the failings that eventually led to the accident events and reinforce several key facts:

- human and hardware barriers are fundamental to effective risk management
- there are interactions and dependencies between human and hardware barriers and that should be considered in major risk management
- risk exposure is dynamic risk and influenced by organisational and operational factors and their cumulative impact must be monitored and managed.
- organisations need to assess and maintain good visibility of the impact of progressive deterioration of both human and hardware barriers.

Review of Current Cumulative Risk Management Approaches

Cumulative risk management involves achieving an updated information about dynamic risks through merging of SCBs (technical, operations, human and organizational) deviations existing within a facility (Syeda, 2009). Management of each deviation individually may not ensure that the cumulative risk of many deviations acting together is effectively managed. Cumulative risk management covers the proactive management of multiple deviations and the risks from them including their interaction (OGUK, 2016).

The following is a review of some industry approaches for managing barrier deviations and cumulative risk.

Barrier Deviation Management Methodologies

Operator of major hazard installations in the oil and gas industry deploy a range of programs to manage impaired SCBs and other defects. These programs include ORA or similar process such as Safety Critical Risk Assessment (SCRA), Safety Critical Element Impairment Risk Assessment (SCEIRA), Safety Critical Element Failure (SCEF) and Deviation Control Risk Assessment (DCRA). Temporary management of change procedures may also be used in such situations UK HSE).

According to the UK HSE, the effectiveness of such systems is a key component of risk control in that the system will be used as part of the process in deciding whether affected plant or equipment may remain in use and, at the extreme level, whether an installation, or parts thereof, may continue in operation. An ineffective system may

allow significant shortcomings to be allowed to persist, erroneous conclusions to be reached or reinforce the results of non-evidence based decision making (UK HSE). Where ORAs are used to manage barrier deviations, the safety regulator advises that:

- there should be a means of determining how individual ORAs may impact on each other to affect the hazard management process and overall risk level.
- there should also be consideration of other matters that will affect the risk, for example safety critical maintenance backlog, operational restrictions, weather conditions, etc

It admits that assessment of the overall risks taking into account key influencing factors is challenging but advises that there should at least be some system, which considers the overall impact of multiple assessments.

Pitblado (2016) also reports on some published examples for manging barrier deviations. Some of which include Manual of Permitted Operations which maps all anticipated activities and defines barriers that must be functional in format similar to a cause and effect chart. A BSCAT Incident Investigation tool which uses an incident Bowtie showing all the barriers involved in an incident, those that worked and the barrier that failed or performed below expectations.

While these SCB deviation management techniques can be effective, they are often heavily weighted towards monitoring the integrity of hardware systems or SCEs and, as highlighted by the UK HSE are limited in providing indication of the adverse overall exposure caused by multiple barrier defects.

Cumulative Risk Management Approaches

Cumulative Risk Model

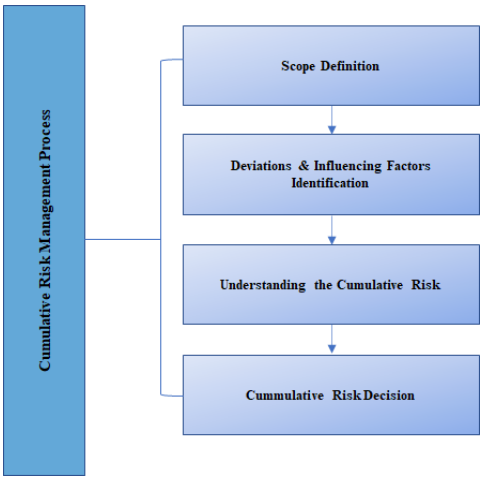
Blacklaw (2013) describes a cumulative risk assessment barrier model used within BG Group's upstream asset. The methodology is based on the Swiss Cheese model concept which postulates that accidents occur when the holes or defects in the layers of protection align. The holes can be created by degradation, malfunction, fatigue, delayed maintenance, changes in operating and conditions etc. The tool draws data from Permit to Work and Computerised Maintenance Management System (CMMS) and combine the data to provide a traffic lighted risk profile for each installation.

Although at face value the methodology described appears to offer useful insights into the organisation cumulative risk exposure, it is inherently limited as it focuses primarily on hardware systems and is based on a simplified barrier concept which does not consider all foreseeable accident paths or scenarios that could lead to a major accident and the interdependencies of associated SCBs.

OGUK Cumulative Risk Guideline

The OGUK Guideline on Cumulative Risk (OGUK, 2016) includes a workflow for assessing and managing cumulative risk. The process is grouped into four main steps, broadly illustrated by Figure 2.

Figure 2 Cumulative Risk Management Process



Scope definition requires that all deviations and influencing factors that might affect the system being considered are included in the assessment. once this is agreed, deviations are identified which can be hardware, human or process. To undertake the third step in the process, some degree of filtering may be required especially where there are large number of deviations. The filtered deviations are then grouped, interactions between them identified, and associated cumulative risk assessed. The final steps involve a collective decision to establish if the cumulative risk has been adequately addressed and what remedial measures should be implemented if necessary.

The Guideline advises that whatever method is chosen to assess cumulative risk there must be sufficient certainty in its outcome. At the very least, the process should enable a veritable and pragmatic basis for making informed decision on cumulative risk acceptability. Recommendations are made on three types of assessment methods which are: using expert judgement, scoring system and quantitative approach. Merits and demerits of each method is also outlined. To determine whether risk is tolerable or ALARP the guideline states that, in most cases a qualitative or semi-quantitative approach is appropriate.

Other Cumulative Risk Methodologies

In a presentation on addressing Cumulative Risk (Mansfield, 2018), six practical approaches based on the OGUK Guideline were mentioned with each offering different levels of sophistication regarding cumulative risk assessment. Two of the methods involves a review of information on SCE data sources such as backlogs, ORAs, Performance Standards etc. and status assessments of SCEs e.g., via dashboards respectively. A third approach uses the concept of major accident hazard bowties while the fourth one is based on the so called “Hot Spot” assessment where SCE status in a location on the installation is examined. The last two methodologies offer a more refined representation of cumulative risk as it entails various combination of the other suggested approaches.

The methodology described in this paper is based on major accident hazard Bowtie concept with interdependencies and interactions between SCBs modelled to create a veritable representation of cumulative risk profile of a major hazard facility.

Proposed Methodology for Cumulative Risk Management

The starting point of a typical risk management process is the identification of hazards. The risk associated with the hazards are then assessed and ranked using a Risk Assessment Matrix (RAM), Figure 3 is an example of a risk matrix. In the oil and gas industry, hazards carried forward for detailed analysis are known as Major Accident Hazards (MAHs). They fall within the MAH definition given in the UK HSE Safety Case Regulations (UK HSE, 2015) and/ or in the region of a RAM where the severity of the hazard consequence is considered too high and associated risk needs to be reduced to ALARP. See indicated region in Figure 3. The proposed methodology uses the list of MAHs derived from the hazard identification and risk assessment study as primary input.

Figure 3. Example Risk Assessment Matrix

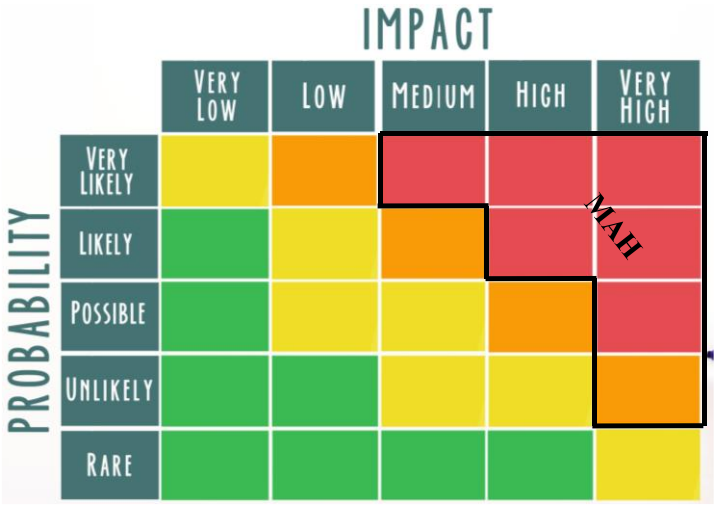
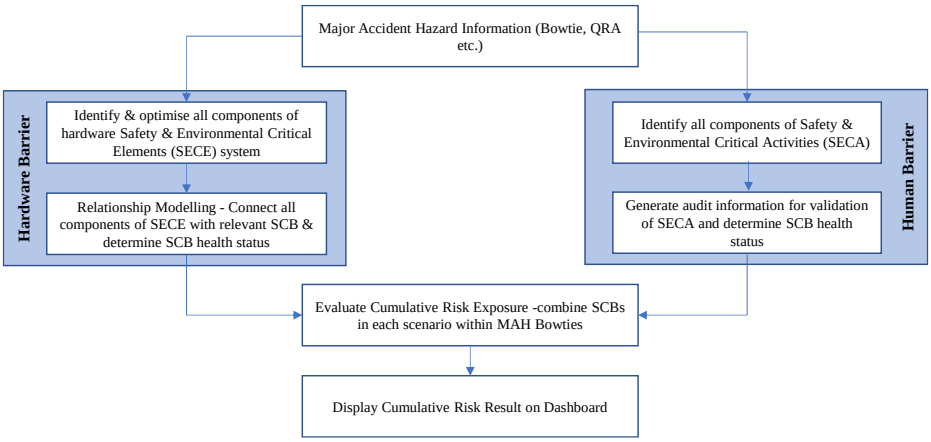


Figure 4 is a workflow schematic of the proposed methodology. Each step is explained in the following sections.

Figure 4 Proposed Cumulative Risk Assessment Methodology Workflow

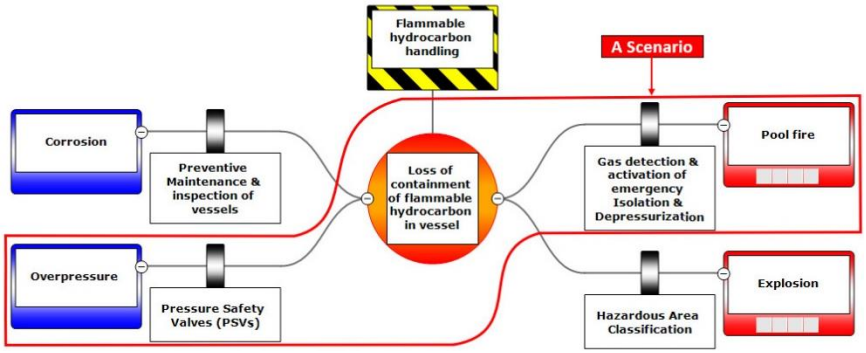


Major Accident Hazard Information

The level of detailed assessment applied to MAH is often driven by regulatory requirements, industry standard practice and company procedures. This can be qualitative, quantitative or a combination of both. Bowtie and Quantitative Risk Analysis (QRA) are examples of detailed safety assessment techniques for MAH, and they provide vital input information for cumulative risk assessment.

The first step in this approach requires reasonably foreseeable MAH scenarios to be identified and assessed, and Bowtie and QRA are well suited for comprehensive identification of scenarios. A Bowtie diagram displays possible accident paths (or scenarios) that could result in unwanted consequence. Each accident path includes a threat, a consequence, and the human and hardware barriers in place to protect against the threats or limit the severity of the consequences. Figure 5 is an example Bowtie with a scenario indicated.

Figure 5 Example Bowtie with an Accident Path



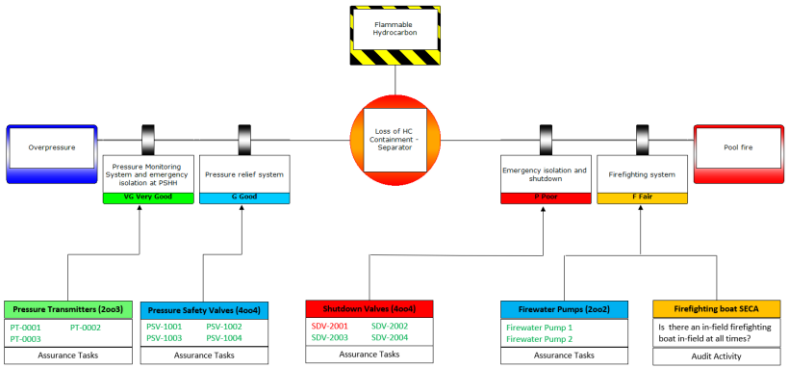
QRA identifies discrete process events and the hardware barriers provided to prevent a loss of containment or mitigate its impact. The information from QRA is vital input for a comprehensive and representative MAH Bowtie.

Hardware SCB Components and Optimisation

Hardware barriers are made up of Safety and Environmental Critical Elements (SECEs) their sub-systems and components or Functional Locations (FLOCs). Whilst these FLOCs are important, evidence from direct operating experience shows that not all are required for the SECE system to perform its safety critical function, and in some cases some FLOCs are excluded from maintenance priority because they are deemed not to be safety critical. Figure 6 illustrates the composition and hierarchy of a barrier on a Bowtie diagram. The hardware barriers comprise systems, subsystems, FLOCS, and assurance routines all required for the barrier to perform its safety function. A human barrier on the other hand consists of tasks that are performed by people to ensure the barrier delivers its required function.

This step of the process reviews all FLOCS and their assurance routines or maintenance activities, establish their core function, determine if they are indeed safety critical, and assess if the safety critical function they provide is relevant to the overall performance of the SECE system and connected barriers. The outcome is an optimised list of SECEs.

Figure 6 Barrier Composition



Relationship Modelling

The level of protection offered by a hardware barrier is at optimum when its constituent components are in good functional state. This protection diminishes as the components degrade until the barrier loses its safety critical function or becomes impaired if not restored. It is thus important to ascertain if the safety critical function of a component indeed contributes to overall performance of the parent and ultimately the barrier in the Bowtie, and if so, how this safety critical function is delivered to ensure that the barrier operates as intended. The delivery of this function can be as a standalone component or in conjunction with other related parts. Where there is a relationship a voting logic is used to help determine the health status of the barrier and to account for interdependencies including those between seemingly unrelated safety critical components.

An example of a pressure trip is given to illustrate this relationship modelling.

Pressure Trip Example

The ultimate function of a pressure trip is to protect against pressure excursion in a process system and restore the process back within safe operating parameters. A pressure trip, however, comprises of a pressure transmitter, a logic solver and a final element with all components required to achieve the intended safety function. The process system may also be designed such that the protection function is achieved in a voting configuration e.g., by two out of three (2oo3) pressure transmitters. Figure 7 is an example of a process system with three pressure transmitters acting in a 2oo3 (3x50%) voting logic.

Figure 7 Example Separation Vessel with Pressure Protection System

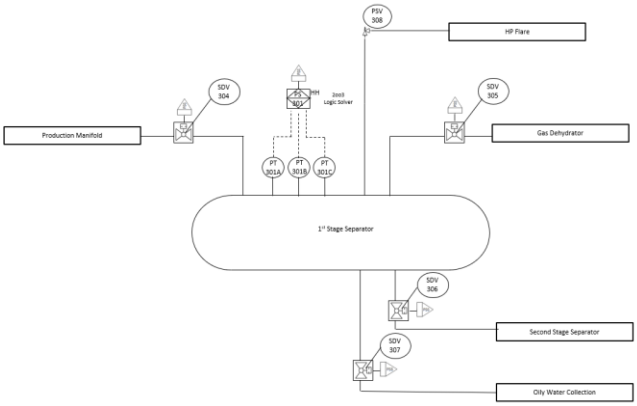


Table 1 shows how the pressure trip will be modelled while Tables 2, 3 and 4 show the possible barrier health statuses depending on the degradation of the components. In Table 2 all pressure transmitters are functional, as well as logic solver and final elements. Thus, the overall system has a very good status. In Table 3, one of the pressure transmitters is impaired. While this reduces the overall health status of the system, the safety critical function can still be performed since two transmitters are available to achieve the voting logic. In Table 3 the overall system is considered impaired because there are not enough functional pressure transmitters to meet the voting criteria.

The health status of each part can be affected by multiple factors which can be operational or organisational. These data sources which may include record of inhibits and overrides, deviation register, MOC register etc are reviewed and linked to respective part or sub-system.

Table 1 Pressure monitoring system relationship modelling and key

Barrier Status	System Status	SubSystem Status	Part
Pressure Monitoring System and emergency isolation at PSHH	Pressure monitoring system (3x50%)	Pressure Transmitter A 1x100%	PT 301A
		Pressure Transmitter B 1x100%	PT 301B
		Pressure Transmitter C 1x100%	PT 301C

Voting Logic is represented as AxY%. where:
A = Number of Subsystems/Parts Available
Y = The Percentage coverage contribution each Subsystem/Part provides
If A x Y > 100%, The System provides Full Protection + Redundancy = Very Good
If A x Y = 100%, The System provides Full Protection = Good
If A x Y < 100%, The system provides Partial or no Protection = Fair / Poor

Part Key
Offline
Online

Barrier/System/Subsystem Key
Very Good | Fair
Good | Poor

Table 2 Pressure monitoring barrier with full protection plus redundancy

Barrier Status	System Status	SubSystem Status	Part
Pressure Monitoring System and emergency isolation at PSHH	Pressure monitoring system (3x50%)	Pressure Transmitter A 1x100%	PT 301A
		Pressure Transmitter B 1x100%	PT 301B
		Pressure Transmitter C 1x100%	PT 301C

Table 3 Pressure monitoring barrier with full protection

Barrier Status	System Status	SubSystem Status	Part
Pressure Monitoring System and emergency isolation at PSHH	Pressure monitoring system (3x50%)	Pressure Transmitter A 1x100%	PT 301A
		Pressure Transmitter B 1x100%	PT 301B
		Pressure Transmitter C 1x100%	PT 301C

Table 4 Pressure monitoring barrier without full protection

Barrier Status	System Status	SubSystem Status	Part
Pressure Monitoring System and emergency isolation at PSHH	Pressure monitoring system (3x50%)	Pressure Transmitter A 1x100%	PT 301A
		Pressure Transmitter B 1x100%	PT 301B
		Pressure Transmitter C 1x100%	PT 301C

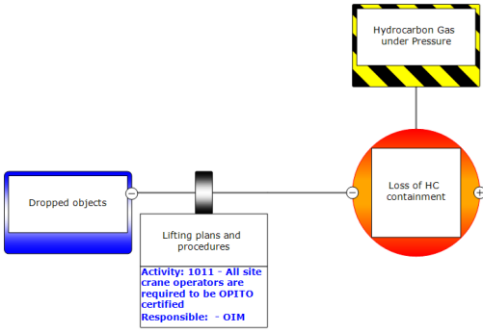
Safety and Environmental Critical Activity (SECA) Identification

SECAs are people and process elements required for assuring the effectiveness of activity based SCBs or human barriers. Human Barriers are those that rely on the actions of people capable of carrying out activities designed to prevent MAH and mitigate any potential consequences of such events (IOGP, 2016). SECAs are premised on the management system elements that support performance of human barriers.

SECAs are distinguished from activities performed to ensure continuous integrity of an SECE i.e., assurance routines or tasks. For example, maintenance and inspection tasks, or competence requirement for personnel performing inspection on an SECE. These activities are regarded as part of the scheme for SECE management rather than as SECA.

Safety critical tasks from the management system are extracted, reviewed, and linked to the relevant barriers. Example of SECAs include training and competency of an operator. Figure 8 is an example of a SECA. In this case a company has a requirement that all crane operators be OPITO certified. The activity is linked to human SCB, Lifting Plans and Procedures.

Figure 8 SECA Example



SECA Audit and Assurance

To establish the health status of human SCBs, survey questions are created based on industry or company specific people and process requirements. The survey questions are then used to audit the SECAs i.e., to assess if the SECAs are carried out.

Following the SECA audit, all responses received are reviewed and assigned a numerical rating between 1 and 0 corresponding to Very Good, Good, Fair, or Poor depending on the response. The ratings are defined as follows:

- Very Good - full compliance.
- Good - Non-compliance which is deemed to have only a minor impact on the level of protection offered by the applicable SCB.
- Fair or Poor rating of SECA is assigned depending on the level of impact a non-compliance has or potentially has on the protection offered by an SCB.

In the Figure 8 example the status will be assigned based on the audit questions as follows:

Survey Question: are all crane operators OPITO Certified?

The possible answers and ratings would be:

- All crane operators are OPITO certified – **Very Good**
- Some crane operators are not OPITO certified but have certifications from other recognized bodies and are supervised by personnel with OPITO certification – **Good**
- Some crane operators are not OPITO certified – **Poor**

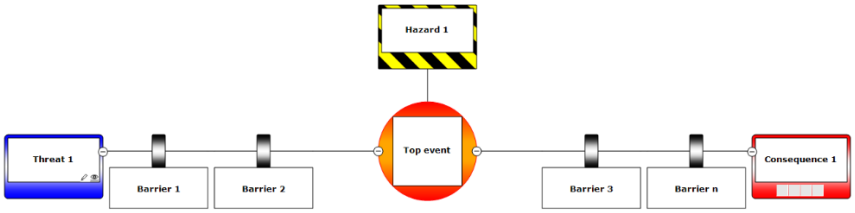
Cumulative Risk Exposure Evaluation

Once the health status of each barrier is determined and the appropriate score assigned the penultimate step involves evaluating the level of risk exposure or vulnerability to each scenario. To determine this exposure, barrier reliability and adequacy are combined as illustrated in Figure 9 and the equation below. In the context of this methodology, the health status of each barrier determines their **reliability** while their position in the hierarchy of controls determines their **adequacy**. Reliability and Adequacy are defined as follows:

SCB reliability is a measure of the health status of a barrier. It is an indication of how often a barrier will perform, on demand, relative to its performance criteria. SCB reliability is grouped into 4 states, namely, Very Good, Good, Fair and Poor with each category assigned a weighted score between 1 and 0.

SCB Adequacy is related to the barrier type in the conventional hazard management hierarchy and the safety critical function it is required to perform to protect against the development of an unwanted event. Barriers can be preventive, detection, control, mitigation, or emergency response. The higher the SCB is in the hierarchy of safeguards, the more adequate it is in protecting against a major accident hazard. Barriers are assigned a weighting between 1 and 0 depending on their type with preventive barriers having the highest weighting.

Figure 9 MAH Scenario



Scenario Exposure Evaluation

$$\text{Scenario Exposure} = \text{Reliability} \times \text{Adequacy}$$

$$\text{Scenario Exposure} = (R_{B1} \times A_{B1}) + (R_{B2} \times A_{B2}) + (R_{B3} \times A_{B3}) + \cdots (R_{Bn} \times A_{Bn})$$

$$\text{Scenario Exposure} = \sum_{i=1}^{n} (R_{Bi} \times A_{Bi}) \quad \text{---------- (1)}$$

Where:

R_{Bi} = Reliability of barrier i,

A_{Bi} = Adequacy of barrier i.

Cumulative Risk Tolerability Evaluation

When all SCBs are functioning as intended the protection offered against a scenario is at its optimum or ideal. The reality, however, is that some barriers will be degraded, and the level of protection will be less than ideal. The difference between the ideal and actual protection can thus be expressed by the equation:

$$P_d = P_i - P_a \quad (2)$$

Where:

P_a = Summation of the actual protection all the SCBs offers against a Scenario

P_i = Summation of the ideal protection all the SCBs offers against a scenario i.e., all barriers operating as intended expressed as

$$P_i = \sum_{i=1}^{n} (R_{Bi} \times A_{Bi})_{ideal} \quad (3)$$

P_a = Actual protection against a scenario expressed as

$$P_a = \sum_{i=1}^{n} (R_{Bi} \times A_{Bi})_{actual} \quad (4)$$

A percentage ratio of the difference in protection (P_d) and the ideal protection (P_i) is then computed to determine the risk tolerability, i.e.,

$$Risk\ Tolerability\ (R_T) = \frac{P_d}{P_i} \times 100\% = \frac{P_i - P_a}{P_i} \times 100\% \quad (5)$$

Where $R_T \geq 40\%$, restoration of the failing SCB or at the very least implementation of appropriate mitigation is advised. Selection of the 40% or greater risk tolerability threshold is predicated on loss of the preventive SCBs. When a mitigation is implemented, the R_T is updated and exposure to the scenario falls within acceptable threshold.

When the R_T for all scenarios in a Bowtie are computed the highest percentage value is used as representative of the level of exposure to that MAH. The representative R_T thus represents the cumulative risk exposure as it takes account of all barrier deviations, barrier types and temporary mitigations for the MAH Bowtie.

Validation of Methodology

Validation is established through operational application of the methodology and retrospective evaluation of previous notable incidents in the oil and gas industry.

Operational Experience

The digitized application has been deployed across several major operating assets. The application which has been running for several years on some of these assets includes provision for automatic and manual data pick up from key repositories that contain information on barriers status. These sources include CMMS, action tracking registers, override/ inhibit register, deviation register etc. The tool also has a dashboard which displays cumulative exposure across multiple assets and drivers or influencing factors can be identified up to assurance routine or SECA tasks level.

Below are some of the feedbacks received from operational experience:

- Application enables, for the first time, a good understanding of the cumulative impact of SCB deviations, making visible link to MAH exposure, and enhancing risk-based decision making.
- Gaps in the maintenance management system which were hitherto unknown have been brought into focus helping the organisation identify where improvements are needed.
- The tool has been very useful in drawing the attention of asset and management personnel to barrier impairments that poses real risk exposure but have lost visibility and become latent due to operational exigencies.
- Encourage frank conversations between management and asset personnel on barrier deviations backlog and prioritisation
- Provides a basis for Specific, Measurable, Achievable, Relevant and Timebound (SMART) Key Performance Indicators (KPIs) that drive real safety benefit.

Retrospective evaluation of previous notable incidents in the oil and gas industry

The methodology was applied retrospectively to three previous major accidents in the oil and gas industry to determine if the cumulative risk created by the latent failures and underlying causes identified in the investigation reports would have provided the much needed visibility or at least reveal vulnerability to the major accident which could have prompted timely intervention and potentially saved lives.

Three previous cases of major accidents assessed were:

1. The FPSO Cidade de São Mateus (FPSO CDSM) Gas Explosion that occurred within the Camarupim oilfield in offshore Brazil on the 11th of February 2015. The accident was caused by a loss of condensate containment in the pump room which resulted in 9 fatalities and injuries to 26 workers, partial flooding, and the indefinite shutdown of two gas production fields (Garcia de Almeida, 2015).
2. CAPECO Tank Terminal Explosion and Multiple Tank Fires accident (CSB, 2010).
3. The Tesoro Anarcortes Oil Refinery Explosion that occurred on the 2nd of April 2010. Loss of containment due to High Temperature Hydrogen Attack (HTHA) in the heat exchanger of the naphtha hydrotreater unit (NHT) resulted in an explosion and a fireball that killed seven personnel and caused significant damage to the asset. (CSB, 2010).

For each of the major accident cases, investigation reports produced by the CSB were reviewed and a retrospective Bowtie diagram created. The threats, consequences, top events, and barriers were deduced from the investigation reports. Reliability and adequacy ratings for each barrier were then assigned and adjusted in turn to reflect their functional status as indicated in the investigation reports. This enabled the exposure level or Risk Tolerability (R_T) to be determined and displayed on a dashboard in the software. The results are presented in Figures 10, 11 & 12.

Figure 10: Cumulative Risk Exposure – FPSO CDSM Pump Room Explosion

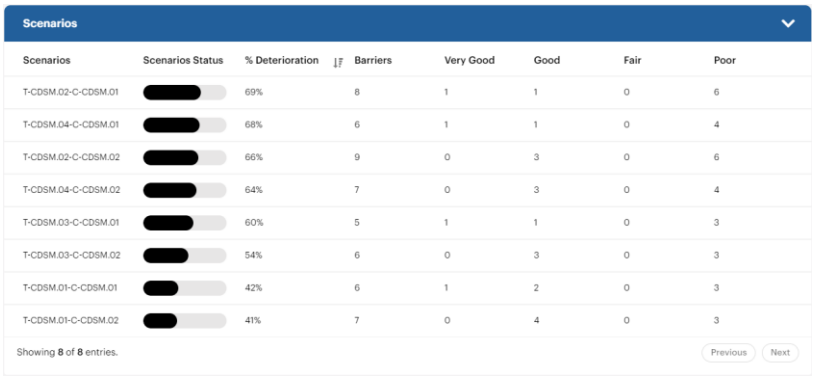
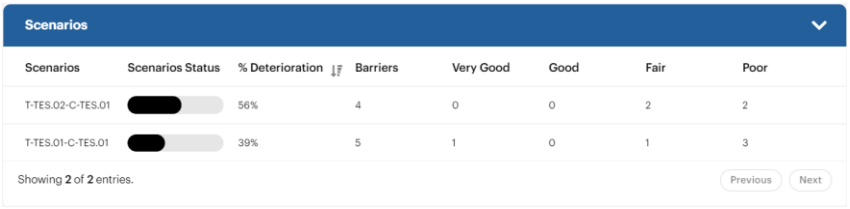


Figure 11: Cumulative Risk Exposure – CAPECO Incident

Figure 12: Cumulative Risk Exposure – Tesoro Anacortes Refinery Accident



Figures 10 and 11show that the R_T (indicated by % deterioration in the figures) exceeded the 40% threshold across all scenarios while in Figure 12 the R_T on one of the scenarios was 56%. These results show that the failing barriers would have been flagged and early warning of vulnerability to the major accident provided to frontline and management personnel if the application was deployed on these facilities. These examples demonstrate the value of understanding, evaluating, and maintaining visibility of cumulative risk imposed by impaired or deficient human and hardware barriers. The methodology provides a veritable means of managing

dynamic risks and connects interactions and dependencies to give a reliable and representative cumulative risk profile of a MAH asset.

Conclusion

A methodology for cumulative risk assessment has been developed that enables evaluation, visibility and monitoring of cumulative risk exposures created by human and hardware barrier deviations, and accounts for interactions and interdependencies across SCBs. The underpinning concept behind the methodology is consistent with established risk management techniques and with the OGUK Guideline on Cumulative Risk.

This approach provides robust and verifiable means of assessing cumulative risk exposure without being too onerous. It enables dynamic barrier management, while helping organisations to focus attention on main drivers of cumulative risk exposures. It helps to deepen understanding of major accident cumulative risk and has been shown to provide tangible and pragmatic risk reduction benefit for operator of major hazard installations.

Future Development

Whilst the methodology in its current form shows promising results there is opportunity for further refinement of the algorithm to enable inclusion of more variables such as threat frequency, threat category and 'smart automation' which will reduce human error in data processing and facilitate Predictive Analytics.

References

Blacklaw Alan, Ward AI, Cassidy Kevin, 2013, The Cumulative Risk Assessment Barrier Model, SPE 146255

BP, 2005, Fatal Accident Investigation Report, Isomerisation Unit Explosion, Final Report

CSB, 2007, Investigation Report, Refinery Explosion and Fire, US Chemical Safety and Hazard Investigation Board Report No. 2005-04-I-TX

CSB, 2010, Final investigation report, Caribbean petroleum tank terminal explosion and multiple tank fires, U.S. Chemical Safety and Hazard Investigation Board

CSB, 2010, Investigation Report, Catastrophic Rupture of Heat Exchanger (Seven Fatalities), U.S. Chemical Safety and Hazard Investigation Board.

Cullen, 1990, The Public Inquiry into Piper Alpha Disaster, Department of Energy, Volume I

Garcia de Almeida A, Silva B. F, Maurieli de Morais C. P, Nunes Ferreira N, Pires T. da Silva, 2016, Investigation Report of the Explosion Incident Occurred on 11/02/2015 in the FPSO Cidade de São Mateus, Brazilian National Agency of Petroleum, Natural Gas and Biofuels, (ANP), Rio de Janeiro, Brazil.

IOGP, 2016, Standardization of Barrier Definitions, Supplement to 415, Report 544

Kalokson Gurung, Laya Jayadeep, Janusz Siwek, Satyam Vora & David Zhou, 2020, Texas City Refinery Explosion – Safety out of focus, Loss Prevention Bulletin 275.

Mansfield D, Forster S, 2018. Perspectives on Addressing Cumulative Risk. AECC, Aberdeen.

Oil and Gas UK, 2016 Cumulative Risk Guidelines, Issue 1

Pitblado R, Fisher M, Nelson B, Flotaker H, Molazemi, K, Stokke A, 2016, Dynamic Barrier Management – Managing Safety Barrier Degradation IChemE Hazards 26 Symposium Series No 161

Reason J, 1997, Managing the Risks of Organisation Accidents

Syeda Z. H, 2009, Cumulative Risk Assessment to Analyze Increased Risk due to Impaired Barriers in Offshore Facilities, Texas A&M University.

UK HSE, 2013, Key Programme 4 (KP4), Ageing and Life Extension Programme, A report by the Energy Division of HSE's Hazardous Installations Directorate

UK HSE, 2015, The Offshore Installations (Offshore Safety Directive) (Safety Case etc) Regulations 2015, Guidance on Regulations

UK HSE, HID Inspection Guide Offshore, Inspection of Operational Risk Assessments