Safety Case Management in the United Kingdom Offshore Industry – Verification of Safety and Environmental Critical Elements, and Risk Management through Predictive Bow Ties

Dr. Ian Stanley
Shell International B.V., Aberdeen, United Kingdom, I.Stanley@shell.com
Adjunct Associate Professor, University of Queensland, Brisbane, Australia

The content of this paper was developed during PhD (University of Aberdeen) and subsequent personal research and work prior to the Author joining Shell International B.V.. The contents therefore do not necessarily reflect the views of Shell International B.V. and the Author asserts their moral right to be identified as Author of this work.

Abstract: This paper outlines the development and pending use of a new variation of Bow Tie modelling which incorporates live operational data (corrective and planned interventions) from Computerised Maintenance Management Systems (CMMS) into Bayesian Learning processes. This variation provides longer term probabilistic risk management analyses hence allowing the early scoping of interventions to mitigate future predicted "As Low As Reasonably Practicable" (ALARP) impairments. This provides additional proof to the Competent Authority that risks are being proactively managed based on Asset Specific performance data.

1. INTRODUCTION

1.1. UK Offshore Safety Case Management

In the United Kingdom (UK), the safety management of offshore oil and gas production installations is primarily governed by the Offshore Installations (Offshore Safety Directive) (Safety Case etc.) Regulations 2015 [10]. The adoption of the Safety Case regime was a key outcome of the Cullen Inquiry [2] into the Piper Alpha disaster in 1988. The Safety Case is a comprehensive document that demonstrates the Duty Holder (typically the owner or operator of an installation) has identified all major accident hazards (MAH), assessed the risks, and has put in place adequate control measures and management systems to manage these risks.

An inherent philosophy in migrating to the Safety Case regime was the transition from prescriptive safety management legislation and regulations to a goal setting regime, i.e. setting out what must be achieved but not prescribing how it is to be accomplished. These actions effectively require the Duty Holder to demonstrate that identified MAH risks have been reduced to ALARP (As Low As is Practicable) [9] where the cost of further mitigation is deemed "grossly disproportionate" to the benefit gained. For UK Offshore the ALARP region is between 10^{-6} and 10^{-3} events per year. It is a condition of operation that the Safety Case is accepted by the Competent Authority, and in the case of the UK offshore oil and gas sector this is the Offshore Major Accident Regulator (OMAR).

Duty holders must review their Safety Cases at least every five years, or whenever a material change occurs that could affect major accident prevention. In the intervening period, a verification process (as outlined in the Safety Case) is employed whereby an Independent Competent Person (ICPs) is appointed to confirm that an installation's Safety and Environmental Critical Elements (SECE's) [22] are suitable and dependable throughout their lifecycle. Therefore, ensuring major accident risks are controlled as described in the operator's Safety Case.

Within the Safety Case, two methods are generally applied to demonstrate ALARP and their subsequent influence on Safety Management Systems (SMS), viz. Quantitative Risk Assessments (QRA) and Bow Tie models. This paper firstly delivers a high-level overview of these two processes, their role in the

Safety Case, and the associated verification of SECE's. The second part of this paper, given the physical size and detail contained in the Safety Case, offers insight to a developing methodology (a variant of Bow Ties and incorporating QRA) for keeping the Safety Case live, providing predictive and probabilistic risk capability, and for the pragmatic real time communication of risk.

1.2. QRA – Quantitative Risk Assessments

QRA methodologies are well described and outlined in [7,8,10,12] which includes additional analyses such as Computational Fluid Dynamics (CFD) for predicting blast overpressures and subsequent structural integrity impairment due to ignition of leaked gaseous hydrocarbons. In short, the QRA aims to identify the major threats to life and to quantify them as risks expressed in terms of:

- TRIF – Temporary Refuge Impairment Frequency (per annum) – the annual frequency with which the TR (a zone of safety) will be impaired by smoke and hazardous atmosphere) within its specified endurance time from MAH hydrocarbon events;
- PLL – Potential Loss of Life (per annum) – number of predicted fatalities per year on the installation;
- IRPA – Individual Risk Per Annum – the annual probability of fatality of an individual member of an employment category.

Potential MAH's to be considered in the Safety Case are [5]:

(a) a fire, explosion or the release of a dangerous substance involving death or serious personal injury to persons on the installation or engaged in an activity on or in connection with it;
(b) any event involving major damage to the structure of the installation or plant affixed thereto or any loss in the stability of the installation;
(c) the collision of a helicopter with the installation; the failure of life support systems for diving operations in connection with the installation,
(d) the detachment of a diving bell used for such operations or the trapping of a diver in a diving bell or other subsea chamber used for such operations; or
(e) any other event arising from a work activity involving death or serious personal injury to five or more persons on the installation or engaged in an activity in connection with it;

It is noted that there is a requirement for a "suitable and sufficient" [13] QRA in ALARP demonstration before the QRA can be accepted. The Competent Authority therefore requires strong justification for assumptions and handling uncertainties in the QRA, with the expectation of clear, self-contained arguments supported by data. Traditionally, these QRA analyses are based on industry wide data as opposed to Asset Specific Data.

For MAH's where the release of a dangerous substance might be involved, the QRA is based on potential release (and ignition potential) frequencies for each isolatable section and is derived by counting the equipment items (vessel, pipework and fittings etc.) in each section and combining the counts with generic release frequencies for each of those items. The results for these analyses are aggregated for individual MAH ALARP demonstration, and where applicable aggregated for total asset ALARP demonstration akin to the top event in Bow Ties.

1.3. Safety and Environmental Critical Elements (SECE's)

A SECE is defined "as any part of the facility, plant, or computer program, the failure of which could cause, or contribute substantially to, an MAH; or the purpose of which is to prevent or limit the effect of an MAH" [5]. They are therefore critical in overall Safety Case management and in ALARP demonstrations. As outlined in the Introduction, and in addition to the Safety Case being reviewed least every five years, SECE's are subject to verification process (as outlined in the Safety Case) by an Independent Competent Person (ICPs) to ensure they are suitable and dependable throughout their lifecycle.

The frequency for the verification of SECE's is not set by a single universal table or regulatory body. It is determined by the specific operator as part of their Safety Case. The frequency depends on the scale, size, and risk profile of the facility and its equipment. Verification activities by the ICP are based on the following attributes:

- **Witness Testing**: Directly observing safety tests, such as checking the closure time of a fire damper or the activation of emergency systems.
- **Inspection and Auditing**: Physically inspecting hardware and reviewing maintenance and testing records to ensure they meet performance standards.
- **Documentation Review**: Verifying initial suitability through design and specification documents, material certificates, and previous "Certificates of Fitness".
- **Personnel Interviews**: Interviewing offshore staff to confirm they understand the operational limits and maintenance needs of safety-critical equipment.

The associated SECE performance standards are categorised through the FARSI Framework [5] which specify criteria across the following five categories:

- **Functionality**: What the SECE must specifically do (e.g., "The valve must close fully within 30 seconds of an emergency signal").
- **Availability**: The proportion of time the SECE is required to be operational (e.g., "99.5% availability for the firewater system").
- **Reliability**: The probability that the SECE will operate correctly on demand (e.g., "1 failure in 1,000 demands for the emergency shutdown system").
- **Survivability**: The ability to function during or after a major accident (e.g., "Passive fire protection must withstand a jet fire for 120 minutes").
- **Interdependency**: Any other systems required for the SECE to work (e.g., "Emergency lighting requires the UPS to be functional").

The FARSI Framework, from a Reliability aspect, focusses on Probability of Failure on Demand with minimal consideration of SECE equipment failing whilst in active service i.e. between verification activities or Proof Test intervals.

For an ICP to attend an offshore asset for executing SECE verification activities, transport via helicopter and multi-night accommodation on the asset is often required. Given the demands on flights and availability of accommodation, the confined nature of offshore hydrocarbon processing equipment, and the physical number of SECE's to be validated, to meet the spirit and intent of the Safety Case necessitates prioritization (ranking) and establishing frequency of verification activities. Some guidance is provided for SECE ranking [5] with the following equation and factors applied:

$$SCE_{Criticality} = F_n \times C_q \times R_n \tag{1}$$

- The MAH management functional role of the SECE (F_n)
- The consequence of failure of the SECE (C_q).
- Inherent redundancy (R_n)

with the resulting SECE criticality score leading to a ranking of High, Medium, or Low. This ranking provides a defendable methodology for the scheduling of verification activities. Risk Assessment Matrices (RAM) can also be used in the risk ranking process, however recent literature e.g. Bratvold [26] indicates that this methodology is less than ideal as probabilities and consequences can be easily distorted.

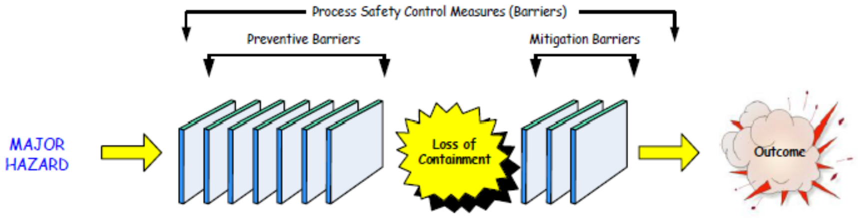
1.4. Bow Tie Methodology

The formal adoption of a systemised transparent barrier approach to risk management in the UK Offshore Oil and Gas Industry (and leading to the adoption of the Bow Tie methodology in Safety

Cases) arose following the Cullen Inquiry into the Piper Alpha disaster [2]. It was determined that a fundamental understanding of associated hazards and risks was required for effective offshore safety management. The concept of the "barrier approach" originated with Reason [23] and the Swiss Cheese Model.

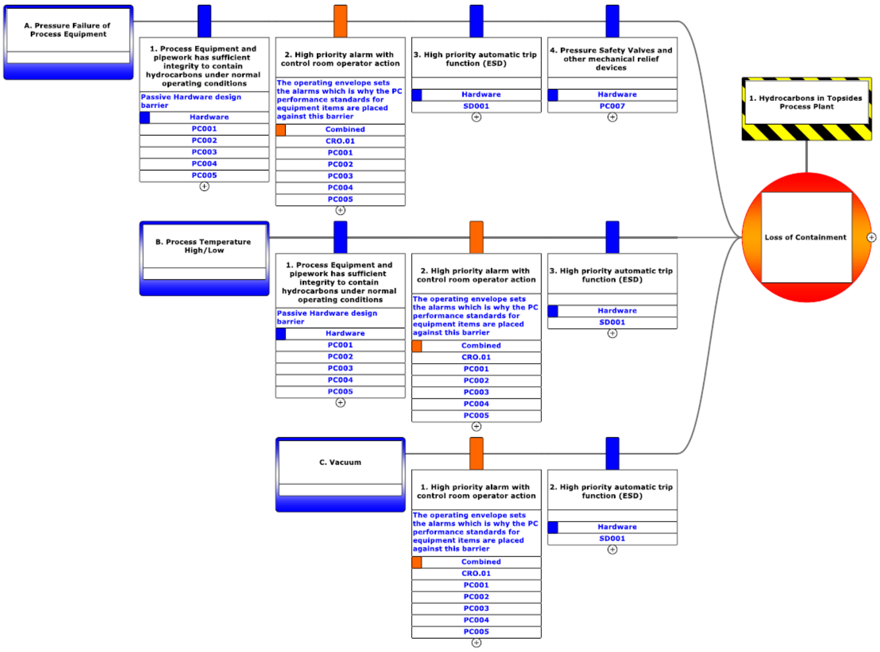
The development of Bow Ties has recently been formalised in [1]. The fundamental aspect of the Bowtie methodology lays in the production of a graphical representation of the risk of the hazardous event (the Top Event) and its potential consequences. The left-hand side of the diagram presents the individual cause(s) (Threats) of the hazardous event - this can be thought of as a Fault Tree. The right-hand side represents escalation pathways to various possible consequences and can be considered an event tree. Risk reduction measures are indicted as Barriers [1]. Figure 1 [11] is the UK Health and Safety Executives Regulatory Model with barriers indicating layers of protection provided by SECE's.

Figure 1: Trajectory of an incident through a barrier / bow tie Diagram [11]



There is a presumption that barriers are independent, however following Macondo [15] this is challenged. Figure 2 is a Bow Tie extract (Left hand side only) from a typical North Sea Safety Case.

Figure 2: Example of Preventive Barriers (Left Hand Side) of a typical Bow Tie



The threat lines jointly lead to the Top Event (Loss of Containment e.g. Hydrocarbons), each of which have Preventative barriers. The Top Event can be similarly considered as the aggregation of relevant MAH's in the Safety Case QRA. The colouring of the Bow Tie has multiple meanings across Offshore Operators and this is now standardized in [1]. Similar attributes are found on the Right-Hand side of the Bow Tie. A typical notation used in the UK North Sea to distinguish the type of SECE's making up barriers is outlined in Table 1, and from here the associated Performance Standards of SECE's are established.

Table 1: Typical SECE Barrier Categories

Barrier Reference	Barrier Category	Functions
SI	Structural Integrity	Prevention
PC	Process Containment	Prevention
IC	Ignition Control	Prevention
DS	Detection Systems	Detection
PS	Protection Systems	Mitigation
SD	Shutdown Equipment	Control
ER	Emergency Response	Emergency Response
LS	Life Saving	Emergency Response

The Bow Tie model therefore is fundamental to providing transparency and line of sight for effective Safety Management Systems (SMS).

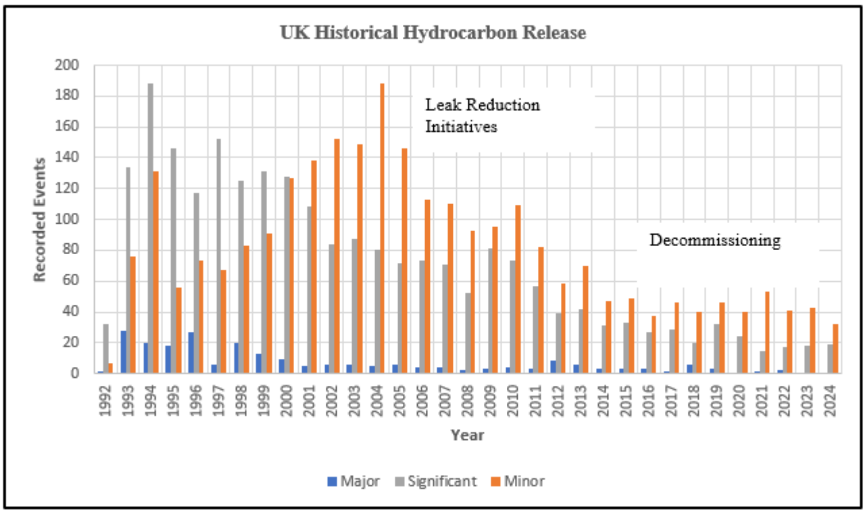
2. SAFETY CASE, SECE's AND UK OFFSHORE HYDROCARBON RELEASES

2.1 Demands on SECE's

The previous Section outlined the management of hazards through the Safety Case. However, to give one relevant example of demands placed on SECE's, Figure 3 outlines the recorded and notified UK Offshore Hydrocarbon releases [14] between 1992 and 2024. These releases are qualified as:

- Major - potential to cause catastrophic consequences if ignited
- Significant - could escalate to a major accident if not controlled
- Minor - low-level releases with minimal escalation risk

Figure 3: UK Offshore Hydrocarbon Releases [HCR]



The Piper Alpha disaster occurred in 1988, and with the subsequent introduction of Safety Case Legislation [10] and other initiatives, there has been (in general) an observable (and anecdotally causal) reduction in hydrocarbon releases between 2004 to 2014. However, from 2015 onwards with the progressive decommissioning of aging offshore production assets, the number of significant and minor releases have essentially remained static. It can therefore be inferred that demand on barriers and SECE's are now more frequent and onerous with possible impairment of associated performance standards.

2.2 Issues pertaining to QRA and Bow Ties

The previous section outlined the potential increasing demands on SECE's and associated barriers for UK Offshore Oil and Gas facilities. This raises several issues which are outlined as follows:

1. The review of Safety Cases and the SECE verification processes are in fact "snap shots in time" of individual Equipment Item performance. For the Safety Case QRA revalidation process, generic industry hydrocarbon release data is typically adopted with minimal consideration given to the influence of ageing and degradation mechanisms. Can the QRA therefore, be considered "suitable and sufficient"?
2. In Bow Tie analyses (which are primarily pictorial) the barriers are assumed (or presumably designed) to be independent; however, it is conceivable that there are performance correlations [15] between barriers with (unless explicitly accounted for) the potential of some SECE's being common in separate threat lines. Beta factors related to Safety Instrumented Functions (SIF) [4,16,17, 24] can be adopted to model common cause failure within an individual barrier, with common cause failure between barriers excluded.
3. SECE's comprising a barrier are generally bundled into their Categorisation Groups (Figure 2 and Table 1) and considered independent. The barrier, which is a functional system, should therefore be considered as an arrangement of series and parallel SECE's (based on overall individual criticality and redundancy), with the reliability of the barrier determined via standard computational means.
4. When considering hydrocarbon leaks (Figure 3), barrier SECE's such as fire and gas detectors are typically allocated by zones to safeguard specific equipment. Along with considering their contribution to barrier reliability in series and parallel configurations, there is also the potential for a certain percentage of these SECE's in a zone to be in a failed state before the associated barrier is deemed to have failed. This is not necessarily considered in QRA analyses.
5. The verification process is to establish if SECE's meet their associated Performance Standard at the time of verification. It is noted that SECE's can experience mechanical failure between verifications rendering them impaired. The frequency of verification activities is partly established to accommodate this phenomenon, however the overall cumulative risk across the barrier is not currently considered. This fails to take into consideration the implications of SECE failure on a system wide (or individual barrier) basis impacts, or in the provision of longer-term predictive analyses thus enabling proactive risk management.
6. In keeping with the desire to enable longer-term predictive analyses and enabling proactive risk management, there are several impediments to the effective and efficient inclusion of CMMS data for the live management of the Safety Case and associated Bow Ties. Anecdotal evidence suggests that in the UK offshore oil and gas industry, the average number of SECE's listed in an Asset's CMMS is in the order of 20%. For a typical offshore oil and gas installation, this equates to around 9,000 individual equipment items being listed as SECE's, all of which are to be subjected to verification processes (and reporting to the Competent Authority) by an ICP.
7. Cursory observations of CMMS systems conclude that Functional Location Structures (FLOCS) and allocation of SECE's often do not map directly to the parts count in the associated QRA, or to the threat lines in Bow Ties. In addition, 1) the physical number of SECE's often far exceeds that included in QRA and Bow Tie modelling, with a large portion of those listed not having any form of defined SECE function, and 2) the FLOC structure often excludes equipment items (e.g. pipeline flanges) which are critical in QRA analyses.

Ultimately, beyond demonstrating ALARP to the Competent Authority, the main purpose of the Safety Case, supported by QRA and Bow Tie analyses, is to communicate risk clearly so that informed safety management decisions can be made. Safety Cases are inherently large and complex documents, and their intent can therefore be overlooked by operational staff, as seen in the Nimrod incident [6] and Macondo [3,20,27]. These issues, together with those outlined above, raise two key questions: when and where does the risk of SECE failure become intolerable in the context of a MAH, and what interventions can be identified and implemented sufficiently early to reduce predicted future risk?

2.3 Gap closure requirements

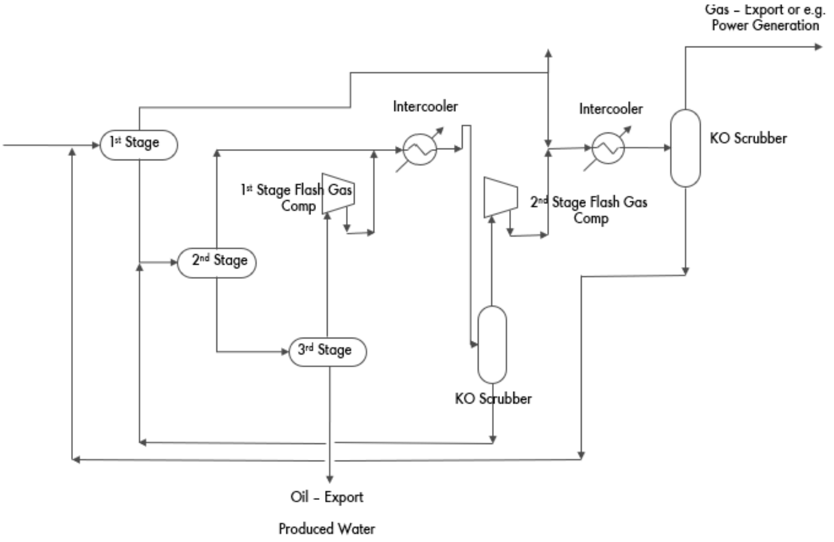
To address the issues and questions raised in the previous section, and others related to suitable and sufficient QRA's, the ensuing sections outline how SECE's can be modelled in a more granular and probabilistic manner which enables predictive analyses. Live data from CMMS systems is incorporated into this probabilistic modelling using Bayesian Updating processes, whereby a live Safety Case is enabled.

3. HYBRID BOW TIE

3.1 Offshore Oil and Gas Separation

Demonstrating how a Hybrid Bow Tie is constructed is best served with a direct industrial example, and one which reflects the demands on SECE's as outlined in Figure 3. The example adopted is a typical MAH (Jet/Pool Fire or Explosion in Oil Processing) considered in UK offshore oil and gas Safey Cases, and centers around the release (and subsequent ignition) of hydrocarbons in the separation and processing stage (Figure 4). In this process, fluid, which is a mix of hydrocarbons in the form of crude oil and gas (plus reservoir water) are separated into their constituent product streams for processing and subsequent export. Arrival pressure at the 1st Stage separation vessel is typically in the order of 30 bar (400psi). Within the 1st Stage Separation vessel, and subsequent 2nd and 3rd Stage Separation vessels, the fluid stream undergoes pressure reduction, whereby entrained hydrocarbon gas is "flashed off" from the crude oil resulting in stabilized products for additional processing before export.

Figure 4: Process Flow Diagram: Typical Oil and Gas Separation and Export



In this separation process, there is potential for oil and gas to leak, and should there be an ignition source, Pool (oil) or Jet (gas) or fires, or explosions (gas vapour cloud) may eventuate. Leaks may occur from process piping (holes or flanges), compressor and pump seals, valves, vessel etc., with generic potential leak frequencies used in the QRA for ALARP demonstration.

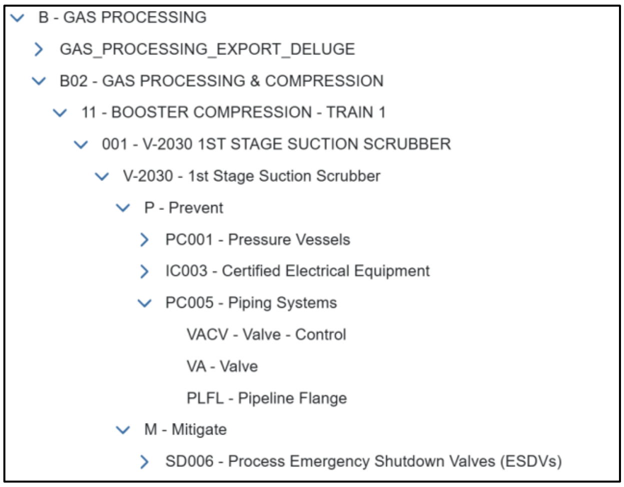
3.2 Hybrid Bow Tie Construction

The Asset's CMMS hierarchy is used as the fundamental structure of the Hybrid Bow Tie along with associated SECE references (e.g. Table 1). SECE's are further defined against specific main equipment items as:

- Prevent (**P**): Those of which failure is to be Prevented
- Prevent/Mitigate (**P/M**): Those which are to be Prevented or provide Mitigation to failure
- Mitigate (**M**): Those which provide Mitigation to failure of Prevent SECE's

Figure 5 outlines an example of structure applied to a Suction Scrubber (KO Scrubber) referenced in Figure 4. Effectively this structure creates "Mini Bow Ties" around main equipment items which are the main contributors to potential leaks. Creating these structures requires the physical relocation and insertion of FLOCS into appropriate groupings without breaking the necessary CMMS data link for live data feed. In essence, the traditional right-hand side of a Bow Tie is incorporated into the left-hand side to promote greater insight. The process of creating mini bow ties is greatly enhanced where originating FLOC structures are in accordance with ISO 14224 and associated taxonomies [18,19].

Figure 5: Typical Oil and Gas Separation and Export

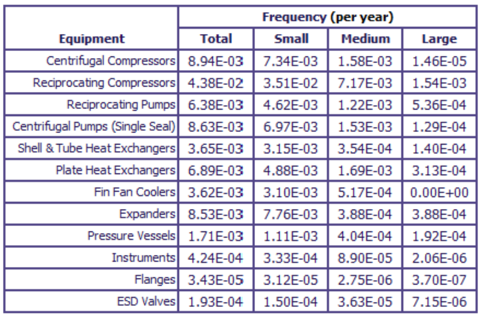


- B - GAS PROCESSING
  - GAS_PROCESSING_EXPORT_DELUGE
  - B02 - GAS PROCESSING & COMPRESSION
    - 11 - BOOSTER COMPRESSION - TRAIN 1
      - 001 - V-2030 1ST STAGE SUCTION SCRUBBER
        - V-2030 - 1st Stage Suction Scrubber
          - P - Prevent
            - PC001 - Pressure Vessels
            - IC003 - Certified Electrical Equipment
            - PC005 - Piping Systems
              - VACV - Valve - Control
              - VA - Valve
              - PLFL - Pipeline Flange
          - M - Mitigate
            - SD006 - Process Emergency Shutdown Valves (ESDVs)

In addition, the Safety Case QRA's often include equipment items (e.g. pipeline flanges) which are not included in the FLOC hierarchy. As these items are essential for ALARP demonstrations, additional groupings have been added e.g. Under PC005 – Piping Systems, an Object Type PLFL – Pipeline Flange has been included whereby a commensurate QRA part count is included in this structure.

The Object Types inserted under SECE references from CMMS have been included to provide a mechanism for inclusion of homogeneous and probabilistic quantification of leakage and other failure frequencies. Table 2 provides an extract example of some relevant leakage data.

Table 2: Typical Examples of Leakage Frequencies adopted in Safety Case QRA



	Frequency (per year)			
Equipment	Total	Small	Medium	Large
Centrifugal Compressors	8.94E-03	7.34E-03	1.58E-03	1.46E-05
Reciprocating Compressors	4.38E-02	3.51E-02	7.17E-03	1.54E-03
Reciprocating Pumps	6.38E-03	4.62E-03	1.22E-03	5.36E-04
Centrifugal Pumps (Single Seal)	8.63E-03	6.97E-03	1.53E-03	1.29E-04
Shell & Tube Heat Exchangers	3.65E-03	3.15E-03	3.54E-04	1.40E-04
Plate Heat Exchangers	6.89E-03	4.88E-03	1.69E-03	3.13E-04
Fin Fan Coolers	3.62E-03	3.10E-03	5.17E-04	0.00E+00
Expanders	8.53E-03	7.76E-03	3.88E-04	3.88E-04
Pressure Vessels	1.71E-03	1.11E-03	4.04E-04	1.92E-04
Instruments	4.24E-04	3.33E-04	8.90E-05	2.06E-06
Flanges	3.43E-05	3.12E-05	2.75E-06	3.70E-07
ESD Valves	1.93E-04	1.50E-04	3.63E-05	7.15E-06

Object Types (and their underlying FLOCS) carry with them essential CMMS data including planned and corrective maintenance actions. This data is essential for predictive analyses and in the application of Bayesian updating of underlying probabilistic quantification of leakage and other failure frequencies (Section 3.4).

The provision of Object Type level also enables the opportunity of applying operational rule sets. For example, the failure of a single smoke or gas detector may not necessarily render the detection system fully failed, and therefore failure tolerance can be factored in.

3.3 Computations

Based on the structure shown in Figure 5, Object Types are initially modelled using exponential distributions with mean values such as those in Table 2. For rare **P** events with annual frequencies ≤0.01, the frequency may be treated as a failure rate to derive an exponential distribution, assuming a Poisson process (that is, independent events with a constant, memoryless rate). This differs from QRA, in which leak or failure frequency is treated as constant and deterministic over the Safety Case period. In contrast, reliability theory indicates that, provided no failure has yet occurred, the probability of failure increases over time; accordingly, Object Types are modelled using cumulative distribution functions (CDFs) (Figure 6). For **M** Object Types, typically Mean Time To Failure etc. data is used to establish CDF's.

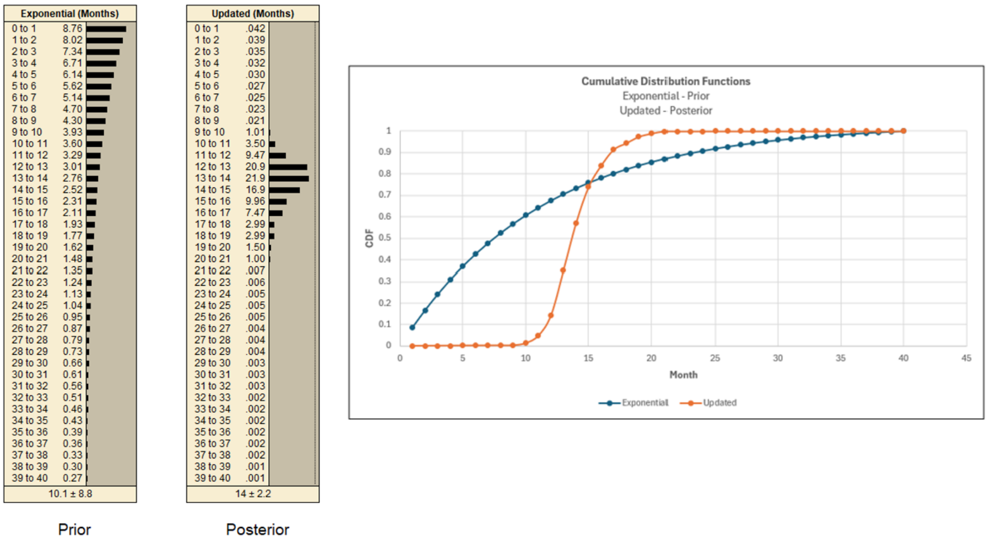
The Object Types are essentially considered to operate as a Series Configuration (OR Gate) with their computations cascading up to their respective **P** and **M** (and **P/M**) nodes. This continues up to the main equipment item (and up to system groups and top event) where the joint probability of failure is considered a combination of AND and OR Gates.

Where planned maintenance actions are incorporated, the respective CDF's revert to time zero at completion of the activity thus representing a return to virtually zero probability of failure. Where corrective actions are executed, the same revert to time zero applies and the corrective actions are incorporated in Bayesian learning (Section 3.4).

3.4 Bayesian Updating

As outlined in Section 3.2, Object Types provide a structure for homogeneous data analyses. This structure also enables a mechanism for enabling a Bayesian Updating process [25], whereby computational predictions become sharper owing to a reduction in underlying uncertainty of leak or failure rates through the incorporation of Asset specific data. Figure 6 (based on direct non-SECE operational corrective maintenance data) outlines the importance of this process where the CDF, a key attribute for predictive computations, provides more definitive time related risk insight.

Figure 6: Bayesian Updating and impact on Cumulative Distribution Function



Prior

Posterior

3.5 Typical Results, Predictive Capability and Decision Making

Figures 7 and 8 outline typical predictive leakage probability results. Figure 7 outlines the impact of future planned work orders (incorporating operations at SECE level) at a discrete point in time, whereby the leakage cumulative probability gets reset to time zero. These planned work orders can be rescheduled to test for top MAH sensitivity. The leakage cumulative probability plots (blue curve) appear linear at this scale – they are however asymptotic.

Figure 7: Timeline example for Predicted Leakage Cumulative Probability

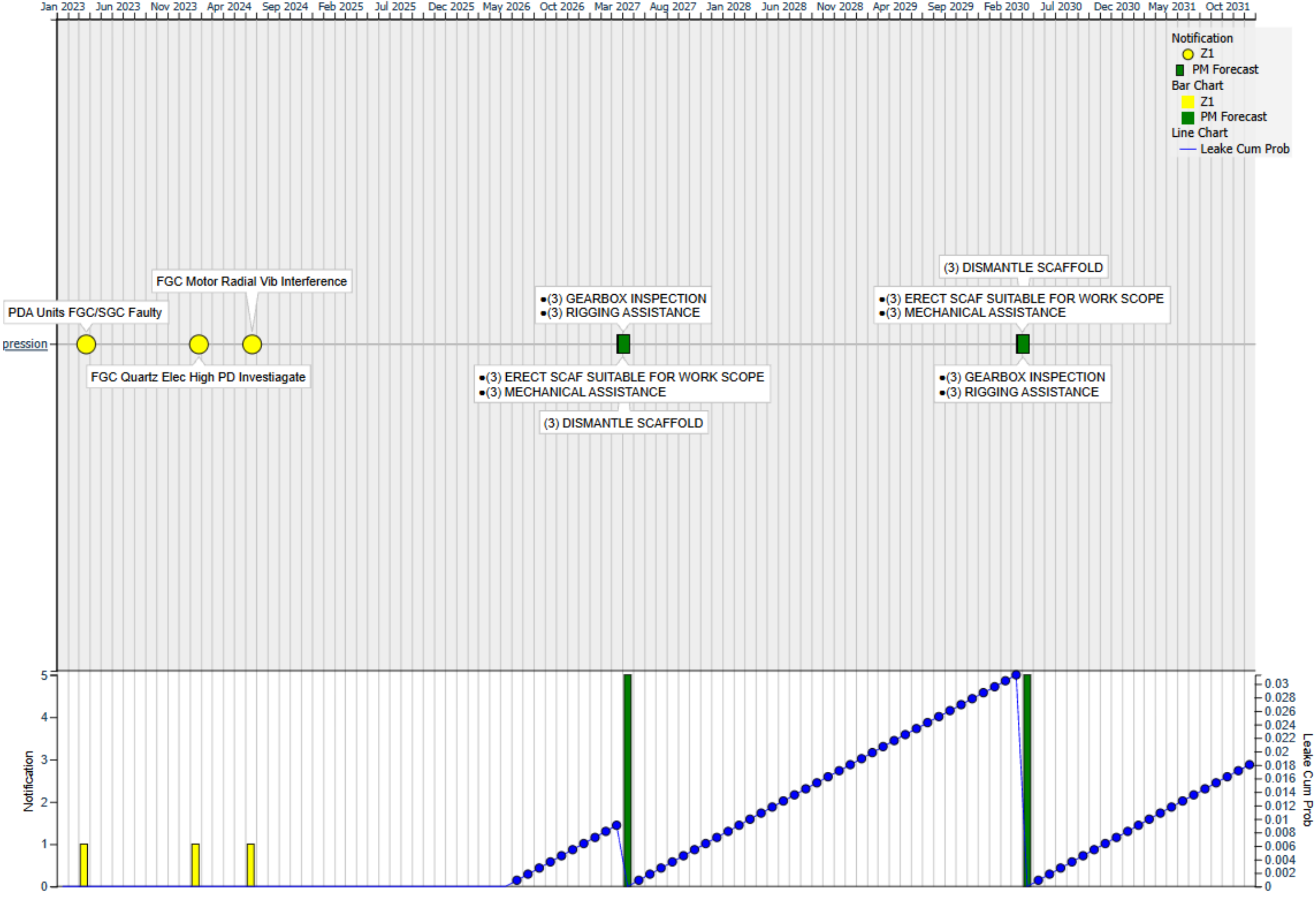


Figure 8: Topology example for Predicted Leakage Cumulative Probability

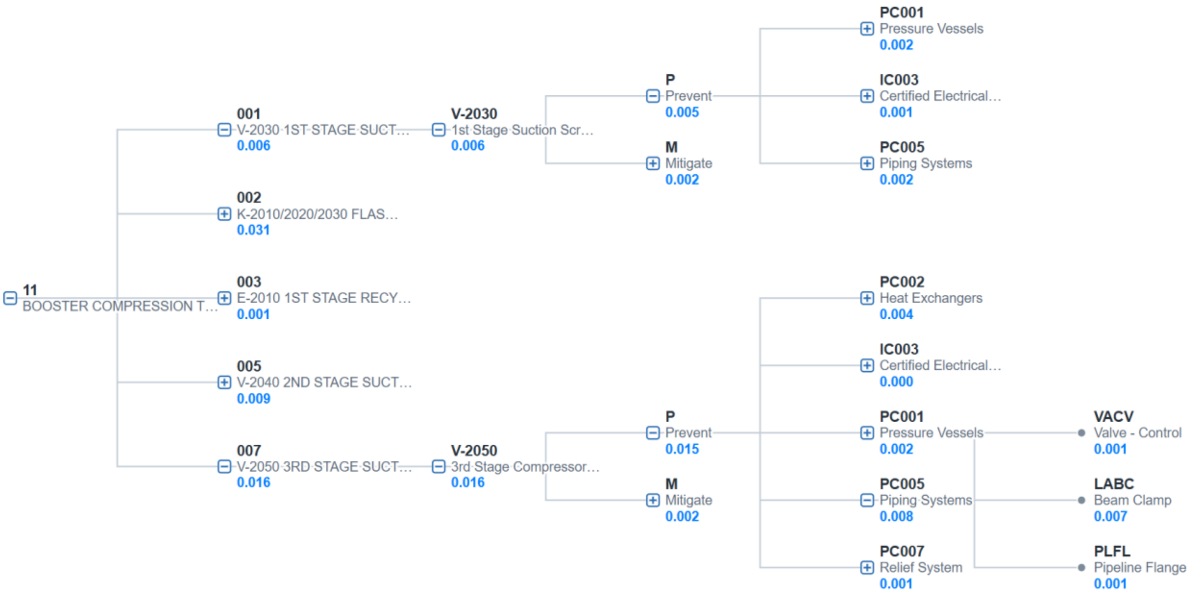


Figure 8 is a topology view of predicted Leakage Cumulative Probability at a discrete point in time. From here it is possible to ascertain the location and Object Types of predicted main contributors to ALARP impairment. It is at this (sufficiently early) stage where mitigation strategies can be scoped and implemented to reduce cumulative risk.

Ignition probabilities which are included in the Safety Case QRA to condition annual frequencies, have been excluded in these analyses as the focus of this paper is to demonstrate a new and numerically robust process for jointly addressing issues pertaining to CMMS, Bow Ties and QRA, and to provide a pragmatic way forward in delivering probabilistic safety assessments with predictive capabilities.

4. CONCLUSION

This paper highlights the development and a proposed way forward for managing and providing predictive probabilistic safety assessments. This methodology is commensurate with the "suitable and sufficient" aspects of UK Offshore Safety Case management, ALARP demonstration, and addresses identified issues pertaining to CMMS, Bow Ties and QRA.

A key aspect of the developed methodology, which draws upon robust probabilistic analyses, lays in the early identification and quantification of potential sources of diminished process safety, whereby mitigation strategies can be scoped and implemented (at a sufficiently early stage) to reduce predicted cumulative risk. The methodology also provides additional insight for the ranking and scheduling of verification activities by the Independent Competent Person to meet the obligations of the Safety Case.

References

[1] Center for Chemical Process Safety (CCPS) & Energy Institute (EI), 2018. Bow Ties in Risk Management: A Concept Book for Process Safety. Hoboken, NJ: Wiley / CCPS; London: Energy Institute.

[2] W.D. Cullen, The Hon. Lord, "The Public Inquiry into the Piper Alpha Disaster", 1990, London, HMSO.

[3] Deepwater Horizon Study Group (DHSG), "Final Report on the Investigation of the Macondo Well Blowout", Center for Catastrophic Risk Management (CCRM), 2011, University of California, Berkeley.

[4] Energy Institute (EI), "Guidance on Safety Integrity Level (SIL) Determination in Support of IEC 61511", 2014, London: Energy Institute.

[5] Energy Institute, "Guidelines for management of safety critical elements (SCEs)" ISBN 978 1 78725 155 7, Third edition January 2020.

[6] C. Haddon-Cave, C., An Independent Review into the Broader Issues Surrounding the Loss of the RAF Nimrod MR2 Aircraft XV230 in Afghanistan in 2006. 2009, HC 1025. London: The Stationery Office. ISBN 9780102962659**.**

[7] Health and Safety Executive (HSE), (n.d.), "ALARP Suite of Guidance" Health and Safety Executive.

[8] Health and Safety Executive (HSE), "Offshore Safety Case Assessment Manual (OSCAM)" 2006. Bootle: Health and Safety Executive.

[9] Health and Safety at Work etc. Act 1974, c. 37. London: HMSO.

[10] Health and Safety Executive (HSE), "Offshore Installations (Offshore Safety Directive) (Safety Case etc.) Regulations 2015", (SI 2015/398). London: The Stationery Office.

[11] Health and Safety Executive (HSE), "HID Regulatory Model", 2013, Bootle: Health and Safety Executive.

[12] Health and Safety Executive (HSE), "Status of Technical Guidance and Information on Design, Construction and Operation of Offshore Installations (Operations Notice 27)", 2012, Bootle: Health and Safety Executive.

[13] Health and Safety Executive (HSE), "A Guide to the Offshore Installations (Safety Case) Regulations", 1992, London: HMSO.

[14] Health and Safety Executive (HSE), "Offshore Hydrocarbon Release Statistics" Bootle: Health and Safety Executive.

[15] A. Hopkins, "Disastrous Decisions: The Human and Organisational Causes of the Gulf of Mexico Blowout", 2012, ISBN-10: 1921948779.

[16] International Electrotechnical Commission (IEC), 2016. IEC 61511: Functional Safety – Safety Instrumented Systems for the Process Industry Sector. 2nd ed. Geneva: IEC.

[17] International Electrotechnical Commission (IEC), "IEC 61508: Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems", 2010 2nd ed. Geneva: IEC.

[18] IOGP (International Association of Oil & Gas Producers), 2020. CFIHOS – Capital Facilities Information Handover Specification, Version 1.4. London: IOGP.

[19] ISO 14224:2016. Petroleum, petrochemical and natural gas industries — Collection and exchange of reliability and maintenance data for equipment. International Organization for Standardization (ISO), Geneva, 2016. Edition: 3rd edition.

[20] Oil & Gas UK, UK Deepwater Drilling: "Implications of the Gulf of Mexico Oil Spill", 2010, Written evidence submitted to the House of Commons Energy and Climate Change Committee.

[21] Official Journal of the European Union (OJEU), "Directive 2013/30/EU of the European Parliament and of the Council of 12 June 2013 on safety of offshore oil and gas operations and amending Directive 2004/35/EC", L178/66–L178/106.

[22] R. Potter and J. Holroyd, "Offshore critical barrier identification; management of their continuing suitability and their verification", Symposium Series No. 162, HAZARDS 27, 2017.

[23] J. Reason," Managing the Risks of Organizational Accidents", 1997. Aldershot: Ashgate Publishing.

[24] D.J. Smith, (2011). Reliability, Maintainability and Risk: Practical Methods for Engineers. 9th ed., 2017, Oxford: Butterworth-Heinemann, ISBN 978-0-08-102010-4.

[25] I. Stanley, "Improved Methods for Reliability-Based Structural Integrity Assessment of Steel Jacket Structures", PhD Thesis, 2005, University of Aberdeen, Scotland, UK.

[26] P. Thomas, R. Bratvold, J.E. Bickel, "The Risk of Using Risk Matrices", 2014, SPE Economics & Management. 6. 10.2118/166269-PA.

[27] U.S. Chemical Safety and Hazard Investigation Board (CSB), 2016. Investigation Report Executive Summary: Drilling Rig Explosion and Fire at the Macondo Well. Report No. 2010-10-I-OS. Washington, D.C.: CSB.