CHEMICAL ENGINEERING TRANSACTIONS

VOL. 67, 2018

A publication of AIDIC

The Italian Association
of Chemical Engineering
Online at www.aidic.it/cet

Guest Editors: Valerio Cozzani, Bruno Fabiano, Davide Manca
Copyright © 2018, AIDIC Servizi S.r.l.
ISBN 978-88-95608-64-8; **ISSN** 2283-9216

DOI: 10.3303/CET1867060

“Offshore Directive” on Major Accidents: a Barrier-based Safety Management System Built on Shared Ontologies and Taxonomies. Real Applications in Italy

Luca Fiorentini[a], Giovanni Pinetti*[a], Rosario Sicari[a], Marta Farinella[a], Luca Marmo[b]

[a] TECSA S.r.l.
[b] Politecnico di Torino
giovanni.pinetti@tecsasrl.it

According to European “Offshore” Directive (2013/30/EU) by the next July, 19th safety cases (Relazioni Grandi Rischi - RGR, Major Accidents Report) should be submitted to the Authorities Having Jurisdiction (AHJ) in order to maintain the license to operate. By the preparation of RGRs the Owner should identify all the hazards connected with the installation, assess all the major risks, identify the acceptable/tolerable risks according to a defined ALARP criterion for human life and environment. Taking inspiration from real applications in Italy, this paper intends to highlight:

- the importance of a coherent assessment framework based on rule sets to manage all the information gathered during the various stages (also to facilitate the assessment conducted by the AHJ and the selected independent third-party inspector);
- the advantage coming from the use of a collector cloud-based IT system to manage data during assessment and to update them in the future leveraging the MOC process (also enforced as a specific requirement of the directive) across several installations and assets with a barrier-based management system.

1. Introduction

For the plants described in a Major Accident Report, the EU “Offshore” Directive intends to verify that:

- All hazards are identified;
- All major accidents are assessed;
- The overall risk level is acceptable, according to an ALARP criterion.

In order to reach these goals, Italian government proposed a detailed framework to structure the document, as described in the guidelines (hereafter “GL”) to the Legislative Decree 145/2015. According to these GL, the core of the report is a detailed risk analysis, as next described. The example here presented has been realized taking into account not only the legislative prescriptions, but also the requests from the Operator to have a high added-value solution to manage the outcomes. An *ad hoc* solution has been provided to satisfy this necessity.

First of all, the GL encourages the grouping of different plants, in order to reduce the number of safety cases. Grouping is permitted for plants operating in the same area, when logistics and emergency are managed from a unique control base. In this case, the risk assessment is performed only for the most representative plant of the group (i.e. the one having a higher risk). By the way, considering the necessity to know the critical control measures and to develop a detailed action plan for each platform (even those grouped in the same safety case), the risk analysis has been extended to all the plants of the same group, not only to the most representative. This approach was taken to overcome this hidden limitation of the methodology proposed by the official GL, which do not cover this “grey” part.

Please cite this article as: Fiorentini L., Pinetti G., Sicari R., Farinella M., Marmo L., 2018, “offshore directive” on major accidents: a barrier-based safety management system built on shared ontologies and taxonomies. real applications in italy., Chemical Engineering Transactions, 67, 355-360 DOI: 10.3303/CET1867060

2. Methodology for risk assessment

RGR is a document based on four different pillars of information: identification and description of the installation, safety management system in place, safety level and emergency management. According to the GL given by the AHJ, safety level should be identified via a specific quantitative risk assessment that evaluates: safety criteria adopted during the design phase, historical experience, risk assessment, performance standards and identification of critical elements for safety and environment. Risk assessment is a crucial issue of the workflow.

According to the official GL, assessment should be conducted with different levels of detail (simplified, average, detailed), depending on three factors.

- Presence of H_2S;
- Type of hydrocarbon (Oil or Gas);
- Processing of the substance onboard.

The presence of H_2S always forces a “detailed analysis”. Instead, if H_2S is not present and the plant treats gas, a “simplified analysis” is sufficient when there is no process on board, otherwise an “average analysis” must be conducted. Finally, if H_2S is not present and the plant treats oil, an “average analysis” is sufficient when there is no process on board, otherwise a “detailed analysis” must be conducted. Simplified and average assessments result in a risk matrix application while the detailed assessment results in the evaluation of the IRPA index. The difference among the three levels of analysis rely also on the method used to perform the frequency and consequence evaluation: the simplified analysis considers only qualitative methods to evaluate frequency and consequences; in the average analysis, frequencies are evaluated quantitatively; finally, in the detailed analysis, a full quantitative risk assessment is required. However, for already existing plant, which was always the case, an average analysis is always considered sufficient, as stated in the GL.

The risk analysis always moves from an initial preliminary hazard analysis (PHA) based on HAZID and, differently from the risk assessment requirements for Seveso III onshore installations, fault tree and event tree assessments are replaced by a single method known as “Bow-Tie” (BT). BT is referenced both in ISO 31000, ISO 31010, ISO 13702 and in ISO 17776 international standards and is the official method of the IADC guidelines (such as the “Health, Safety, Environment Case Guideline for Mobile Offshore Drilling Units”) by the most important drilling operators, in which the BT is the key element of the structured hazard identification and control process (SHIDAC).

According to the specific requirements of the GL, BT risk assessment has been improved in order to:

- obtain a quantification of threats and consequences;
- incorporate a measure of the “human factor”.

Each technical element/escalation factor and conditional modifier in the BT diagrams has been quantified using the AIChE-CCPA approach to Layers of Protection Analysis (LOPA) while “human factor” related components have been quantified via a specific human reliability assessment (HRA) conducted via the Spar-H method by the U.S. Nuclear Regulatory Commission (Doc. N. NUREG/CR – 6883, 2005).

2.1 The proposed workflow

Data collection

The very first step to develop such a complex document is to collect all the required information, data, and documents. To do so, a specific cloud platform has been developed to allow the upload of documents from the Operator and the download for the Consultants, in a well-defined structure, enabling also remote workflows for approval and feedback. All the documents, digitally protected from misuse, have been copied for a back-up.

Hazard identification (HAZID) and BowTie

Once the required information was available, every plant has been subdivided into homogeneous areas, depending on the involved hazards, substances, and presence of personnel over a certain threshold, whose loss of life would have caused an increase of the consequence level in the risk matrix. The homogeneous areas cover the entire offshore plant, ensuring consistency in the next step of the risk assessment. Once identified the areas, the HAZID has been carried out by the analysts, using the guidewords provided by the ISO 17776 to drive the identification through multiple hazards (excluding the ones about “occupational safety”, which are part of a different legislative prescription). During the HAZID, all the possible unwanted losses of controls have been listed, and their possible causes and final consequences (i.e. the incidental scenarios) have been identified, together with the preventive and mitigative barriers. The results have been then converted in form of Bow-Tie, a powerful tool to show, in a single shot, all the information coming from the preliminary hazard identification, merging together a fault and an event tree. It is clear that, in a very complex field like the offshore oil and gas industry, it is easy to identify multiple causes, primary barriers, consequences, escalation factors and secondary barriers. Therefore, a typical Bow-Tie is full of branches and it is more like the one in Figure 1. The Figure is voluntarily unreadable, but it clearly shows how complex the analysis has been.

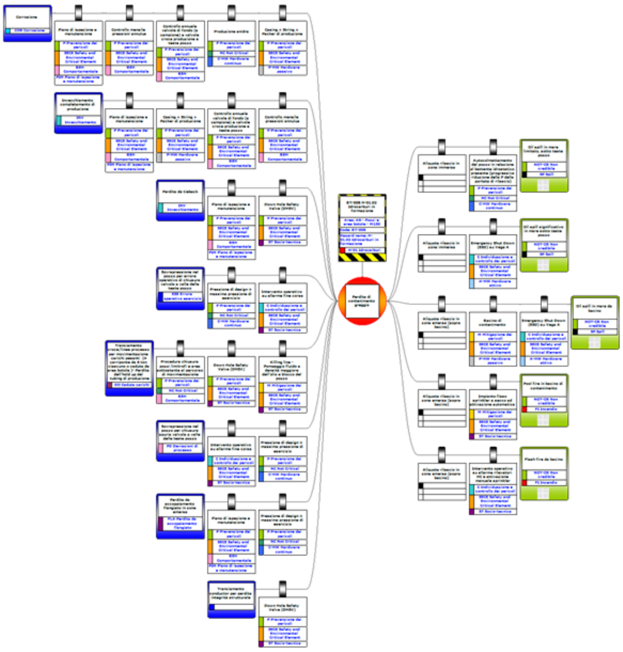

Figure 1: Example of a Bow-Tie developed for the Italian application of the Offshore directive

Environmental studies

The environmental risk assessment requires a preliminary step to study the intrinsic vulnerability of the environmental receptors in case of oil spill. By the combination of the receptors' vulnerability and the severity of the damage, the GL provides the resulting level of consequence to be used in the risk acceptability criterion (i.e. the environmental risk matrix).

Frequency estimation

The frequency estimation is undoubtedly one of the most important step of the risk analysis, providing the numerical values that must be used when applying the risk acceptability criteria (i.e. the safety and environmental risk matrixes). Basically, it is possible to distinguish two elements of the BT that need to be quantified: the causes and the barriers. By their combination, according to the rule of the LOPA analysis, you obtain the frequencies of the final consequences (right-side of the BT). To evaluate the frequencies of the initial causes (left-side of the BT), the data of the statistical-historical rupture have been associated using the databases in Table 1. Once the frequency of statistical-historical rupture has been obtained for every homogeneous area, the frequency of the causes, as identified during the HAZID, is obtained considering their contribution, expressed in percentage according to the OGP 434-5. In particular, the following categories of causes have been considered: corrosion, ageing, natural events, operative error in operation and maintenance, dropped object, ship collision (OGP 434-16), helicopter crash (OGP 434-22), process deviations, and loss of containment from pump seal or from flanged coupling. If necessary, fault trees have been adopted to calculate the frequency of those peculiar causes. The loss of structural integrity has been taken into account too, using OGP 434-13 (Structural risk for offshore installations).
The evaluation of the Probability of Failure on Demand (PFD) of the barriers depends on the type of barrier. The distinction about the barrier types depends on who is in charge to detect, decide, and act, as shown in Table 2. When a human failure event is part of the failing barrier, the human failure probability has been evaluated through the Spar-H method; when a technology failure is involved, specific databased have been used to obtain the relative PFD (like “exida” and “Oreda”). When these two factors were contemporary present, they have been combined in “and/or” logic combination, depending on the specific context.

Table 1: Databases used to determine the frequencies of the causes

Title	Document	Institution
Process release frequencies	N° 434-1 March 2010	International Association of Oil&Gas Producers (OGP)
Riser and Pipeline release frequencies	N° 434-4 March 2010	International Association of Oil&Gas Producers (OGP)
Storage incident frequencies	N° 434-3 March 2010	International Association of Oil&Gas Producers (OGP)
Blowout frequencies	N° 434-2 March 2010	International Association of Oil&Gas Producers (OGP)
Mechanical lifting failures	N° 434-8 March 2010	International Association of Oil&Gas Producers (OGP)
Ship/Installation collisions	N° 434-16 March 2010	International Association of Oil&Gas Producers (OGP)
Structural risk for offshore installations	N° 434-13 March 2010	International Association of Oil&Gas Producers (OGP)
Aviation transport accident statistics	N° 434-11 March 2010	International Association of Oil&Gas Producers (OGP)
Human factors in QRA	N° 434-5 March 2010	International Association of Oil&Gas Producers (OGP)
Guidelines for quantitative risk assessment	Purple Book	TNO
Failure rate and Event data for use within Risk Assessment	28/06/212 HSE UK	HSE UK

Table 2: Barrier types

Barrier type	Detect	Decide	Act
Passive Hardware	N/A	N/A	N/A
Active Hardware	Technology	Technology	Technology
Active Human	Human	Human	Human
Hardware + Human	Technology/Human	Technology/Human	Technology/Human
Continuous Hardware	N/A	N/A	Technology

Moreover, additional tags have been used to categorize the barriers, distinguishing between the Safety and Environmental Critical Elements (SECE) and the not-critical barriers, as well as among the different goal of a barrier: hazard prevention, hazard detection and control, hazard mitigation, or evacuation, escape and rescue functions.

Consequence analysis for “human life”

For every scenario classified as potential major accident, whose frequency of occurrence was bigger than a credibility threshold, a computer assisted simulation has been performed to evaluate the consequences for human life, in terms of damaged areas, also taking into account the survivability of the escape routes and evacuation systems. Combing the damaged areas and the adopted vulnerability models, a risk level is assigned for every single scenario.

Risk assessment for “human life”

Once the scenarios affecting the human life have been assessed, the risk tolerability verification has been carried out considering the cumulated risk. This means that for every deck of the offshore installations, all the consequences having the same impact (i.e. the same level of consequence) have been taken into account and their frequencies combined to obtain the overall frequency that a consequence happen with a specific magnitude. The combination of the “overall frequency” and selected magnitude are the inputs for the risk matrix and the tolerability verification. These steps are repeated, for the same deck, changing the magnitude level. The cycle is then re-executed for every deck. The division in decks was suggested because it helps to consider the domino effects from a lower deck to an upper deck.

Consequence analysis and risk assessment for “environment”

Similar to the consequence analysis for “human life”, computer assisted simulations have been performed also for environmental major accidents. The goal was to evaluate the consequences of an oil spill on the three environmental receptors, taking into account also wind and sea currents. In particular, the simulation provided the estimation of the time required to the oil spill to touch the coast, when no barrier is working. A cumulation criterion has been adopted also for environmental risks.

ALARP

Those risks falling in the “ALARP” region of the risk matrix, require an “As Low As Reasonable” study. Basically, a cost-benefit analysis has been performed to understand if the costs of an eventual additional barrier compensate the benefits coming from its application. However, if the additional barrier is “simple” or its installation is established by law, or it has been already installed with positive feedback in other plants, then no ALARP study is performed and the additional control measure is installed without a cost-benefit analysis. Otherwise, a qualitative approach is used to help the Operator in the choice of implementing a new barrier or accepting the existing risk level.

SECE

From the generic list of the barriers that have been identified through the risk analysis, the subset of the Safety and Environmental Critical Elements (SECE) is extracted. In particular, the elements satisfying at least one of the following features are considered SECE:

- The failure of the element might cause a major accident;
- The failure of the element might contribute to cause a major accident;
- The objective of the element is to prevent a major accident;
- The objective of the element is to mitigate a major accident.

Every SECE is then described by the FARSI performance criteria: Functionality, Availability, Reliability, Survivability, and Independence. At the end, the third party verification guarantees the respect of the legal prescriptions for the whole risk assessment.

3. Taxonomies and cloud-based management system

Rule-sets have played a crucial role in each stage of the assessment, in particular to establish a common language based on several taxonomies to make the approach uniform and guarantee the consistency of the data in the future (where a specific process safety management system, PSMsys, will guarantee the continuous update of documents, information towards a live ‘risk register’ of major accidents).

Data from the risk analysis making the BT can be seen as records in a database. These elements are causes, barriers, hazards, consequences, top events, and escalation factors. A structured taxonomy has been used to categorize them, to immediate distinguish credible scenarios from not credible ones, grouping them among spills, fires, explosions, toxic releases, structural damages and immediate loss of human life (this category has been included to consider the major accident coming from the loss of control of the helicopter). This capability translates into the possibility to immediately extract the required information, such as SECE, or SECE aimed in hazard prevention, or SECE aimed in hazard prevention in a specific homogeneous area, or to easily list the credible scenarios, the ones involving fires, the not credible ones involving explosion and so on. The infinite possibility to combine the filters and sorting the results provide a tangible help to both the Owner and the AHJ, which can easily access to an infinite range of data. For example, this was made for SECE (Safety and Environment Critical Elements) to be divided into specific categories (preventing hazards, controlling hazards, mitigating hazards and elements related with evacuation and escape routes); those have been coupled with the taxonomy used by ISO 13702 in order to build a specific ontology related with systems able to control and mitigate fires and explosions and they have been described in terms of functionality, availability, reliability, survivability and independence. Moreover, a cloud-based IT system allows to access to this powerful source of information, including organizational units, taxonomies on causes, consequences, barriers, reports with filtering and sorting capabilities, action tracking, audit, HAZID, and an user-defined Wiki section containing the safety reports, the technical references, the HAZIDs, and the document links. A screenshot of the cloud-based platform is shown in Figure 2.

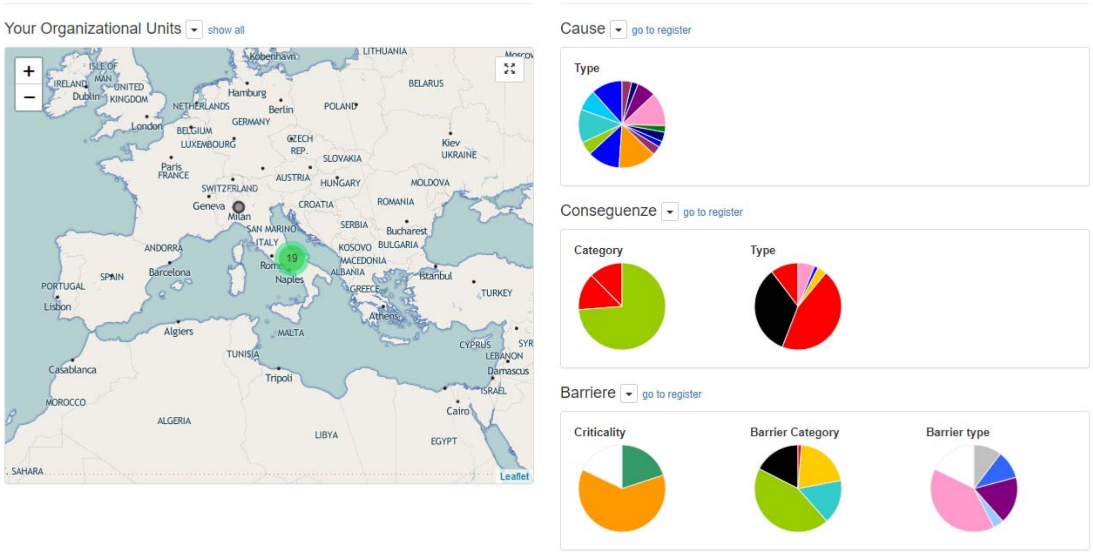

Figure 2: Screenshot of the cloud-based IT system: organizational units and pie charts on taxonomy

4. Conclusions

The activity conducted showed a lot of benefits and demonstrated how to manage all the requirements coming from the application of several regulations and standards in complex installations. As anticipated all the workflow has been supported by a cloud-based IT specific platform.

Application of the barrier-based management system resulted also in the possibility to collect information’s, data, documents, performance indicators, results to support the EU Directive requirements, to take better informed decisions, to real-time demonstrate to all the stakeholders the activities in place, the design intent with the intended results and the path to achieve those.

The possibility to employ an information technology system allows to measure maturity levels of the barriers and underline (installation by installation) the quality of them with specific and shared taxonomies and ontologies.

References

Bruce K. Vaughen, P.E., Kenneth Bloch. Use the Bow Tie Diagram to Help Reduce Process Safety Risks. CEP Magazine (An AIChE Publication); 2016.

CCPS. Guidelines for enabling conditions and conditional modifiers in layers of protection analysis. Wiley; 2013.

CCPS. Guidelines for initiating events and independent protection layers in layer of protection analysis. Wiley; 2015.

CCPS. Layer of Protection Analysis: Simplified Process Risk Assessment. New York: Wiley; 2011.

CCPS. Process Safety Glossary: Bow Tie Diagram. Available online at www.aiche.org/ccps/resources/glossary/process-safety-glossary/bow-tie-diagram; last access on April, 30th 2018.

CCPS. Project 237: Guidelines for Barrier Risk Management (Bow Tie Analysis), 2017 (in progress).

ISO 17776:2016. Petroleum and natural gas industries – Offshore production installations – Major accident hazard management during the design of new installations; 2016.

IEC 31010:2009. Risk management – Risk assessment techniques; 2009.

ISO 31000:2018. Risk management – Guidelines; 2018.

Luca Fiorentini, Luca Marmo. Principles of Forensic Engineering Applied to Industrial Accidents.
Wiley, Chichester UK; 2017.