

How Will the Approach to Industrial Risk Management in the Petroleum Sector Change in the Face of Increasing Complexity and Emerging Risks? The Iplom Experience

Luca Fiorentini^{a,*}, Gianfranco Peiretti^b

^aTecsa S.r.l., via Figino 101, 20016 Pero (MI), Italy

^bIplom S.p.A., via Navone 3b, 16012 Busalla (GE), Italy

luca.fiorentini@tecsasrl.it

Iplom is an Italian company operating in the energy and oil sector. As a Seveso company, Iplom has worked with specialist service companies like TECSA to improve the Safety Report over time. They have gone beyond just meeting formal requirements and have turned the report into a tool for assessment and decision-making. This paper aims to demonstrate that the forthcoming edition of the Safety Report will feature a concise and completely electronic "executive summary" in alignment with the "Safety Case" approach. The "executive summary" aims to become the central point of access to critical information concerning the industrial risk profile of Iplom's plants. This new approach allows, with obvious advantages, greater readability and comprehension by all those involved (including the competent authority). The complexity typical of the industrial sector, also related to emerging risks, can be managed in an informed manner and with a robust approach closer to field safety, where operators are. Through this approach, the "executive summary" becomes an updated representation of the risk profile based on the key elements (technical and organisational managerial) that contribute to a holistic strategy to guarantee safety for both known and emerging risks. Consequently, it is possible to have a synthetic representation of the plant's risk profile using data from the field through the numerous sensors installed in the plants monitoring the critical parameters of the industrial processes.

1. Introduction

The onshore oil and gas Seveso plants in Italy face new risks due to the energy transition process, intensifying the complex management challenges. Despite this growing challenge, the associated risks are still not effectively managed, structured, or robust, unlike the "Safety Case" approach. Safety reports are prepared periodically (every five years) for the relevant authorities, following a formal index provided by the regulator. However, they do not demonstrate to the plant owner that risks are "As Low As Reasonably Possible" (ALARP) and are not comprehensive. Even though a specific legislative decree (D.Lgs. 105/2015) defines the requirements for safety reports for onshore plants, limitations can still be observed after years of implementation. Currently, there is no defined risk acceptability criterion by regulation, and plant owners are not allowed to assess the acceptability of risks or their compliance with ALARP (As Low As Reasonably Practicable) conditions. The only guidance provided is that major accident events with a probability of occurrence lower than 10^{-6} occasions per year should not be discussed regarding consequences. Regulators have not yet recognised the ALARP approach, leading to conflicts in implementing internationally recognised standards, such as functional safety (e.g. IEC 61508 and IEC 61511) or risk-based inspections proposed by the American Petroleum Institute in 2026. The responsibility for determining acceptability lies with the governing authority. The operator only outlines the plant's conditions, backed by a quantitative risk assessment, without making a formal statement. Even when the regulator provides the safety report structure, it often feels like a list of tasks to complete rather than a coordinated set of elements leading to a safety assurance statement. Discussing all the elements involves a significant effort and often leads to duplicating information from various other official documents. The authorities have recognised these limitations (Marrazzo, 2021 and Vazzana, 2019), and working groups have been dedicated to implementing new requirements for Safety Case production. This paper will present the

proposed Safety Case methodology. Authorities started with a specific guideline for the offshore sector, where a more consistent approach with the international guidelines has been defined.

Embracing the challenges coming from this awareness, Iplom decided to elevate its risk management following the Safety Case approach and thus acting like a leading implementer in the Italian context. Indeed, in the next years, this approach will also be moved to onshore Seveso installations. It would be advisable that Safety Case preparation could be extended to other situations that would benefit from a formal statement of safety assurance, even if not related to Seveso, such as buildings fire Safety Cases and new energy production plants following the recent important will to fulfil a global energy transition. In the context of this paper, the Safety Case approach is concentrated inside the proposed “executive summary” for the next revision of the Iplom’s Safety Report. The main features and the content of the proposed Safety Case approach will be discussed in the next paragraphs.

2. The Safety Case approach

“Safety Case” is a term that, across multiple sectors as well described in Maguire, 2017, defines the outcome of a precise process aimed at the presentation, via a structured document, of safety considerations related to a specific socio-technical asset (a product, a site, a process or a system) including the demonstration that its major accidents events and their risks have been identified, can be considered minimised and ALARP (Melchers, 2001) and they will be communicated and managed accordingly, within a systematic approach (Kelly, 2004), coordinating the activities via the Safety Management System elements.

The Safety Case approach can be condensed into three words: demonstration, structured, and synthetic.

2.1 Demonstration

The Safety Case summarises and declares the demonstration, supported by specifically selected evidence, that the risk profile satisfies the ALARP condition for the identified and minimised risks in a specific domain and given a specific context (to be described briefly in the Safety Case itself), operating in defined modes. The demonstration should reference any eventually applicable requirements from regulations, standards and RAGEPs and discuss their application and actual compliance. Demonstration is often supported by specific notations such as the Goal Structuring Notation (Spriggs, 2012).

2.2 Structured

Safety Cases should have a clear hierarchical structure that allows the reader to understand the workflow that has been adopted and to identify the input data and the results with particular emphasis on the ALARP demonstration. In some cases, their structure follows specific requirements given the applicable regulation to the specific domain. The importance of the structure is also connected with the possibility of using the contents of the Safety Case for the communication of results to internal and external stakeholders, for training activities of different classes of students (management people, field operators, external contractors, etc.) and for inclusion of people in the Safety Case formation process itself towards an “operationalisation” of the Safety Case, as suggested in (McDade, 2021). Structure assures consistency among Safety Cases (e.g. across the years or multiple different assets) and supports the formal statement of the operator (as a declaration). A well-defined structure enables the maintenance of the Safety Case during time (it should be updated regularly and modified, when necessary, as a living document).

2.3 Synthetic

Safety Cases should focus on a single domain or a specific pool of domains (e.g. if the Safety Case’s intended use is for major accident events safety assurance, it should not refer to occupational safety and health issues). For the specific selected domain, they must briefly, through the hierarchical structure, set out the demonstration through the appropriate evidence, referring, if necessary, to external documents (Maguire, 2017). It is not advisable to copy the entire body of evidence in the content of the Safety Case, while it is fundamental to have precise references to documents under control.

2.4 The Claim Argument Evidence (CAE) and the Goal Structuring Notation (GSN)

The proposed Safety Case is essentially a structured argument, supported by a body of evidence, which provides a compelling, understandable, and valid case that the system is safe for the given application, eventually through specific processes, in a given environment considering the human factor. The Safety Case contains a structured argument (rationale) demonstrating that the evidence is sufficient to show that the system is safe. The argument should be commensurate with the potential risk, the inherent system complexity, the novelty of the approach or technology, the uncertainty of the context of use, the human factor issues, etc. The distinction between claims, arguments, and evidence is very important because it provides a common language

and notation, helps build a logical structure, and allows for focus on each component and their relationship, thus enforcing the reasoning, helping the communication, and facing the challenge.

The CAE (Bloomfield & Netkachova, 2014) and GSN (Spriggs, 2012) are well-established graphical notations that can achieve these objectives practically. Both standards are continuously updated. The core node types are broadly equivalent to CAE and GSN notations (claim: goal; argument: strategy; and evidence: solution). The goal type in GSN is certainly a claim, as per the GSN standard. Moreover, for both the notations, the nodes are linked to show lines of support for each argument element, and each branch ends with evidence, solutions, or data. As shown in Figure 1, the two notations use different shapes, and the GSN has many more elements. However, this does not mean that one method is more efficient than the other; the CAE puts more emphasis on supporting the narrative. Even if the arrow direction is different, the semantics are the same.

One of the most obvious differences between the methodologies is that while CAE notation explicitly uses colour to identify elements, GSN notation, conceived many years earlier, favours black-and-white diagrams. This choice facilitates the sharing of information, although in today's world, it is common and practical to have documents, even on paper, in colour. The planned use of colour ensures better understanding, especially for non-experts.

The CAE approach is used for the proposed "executive summary", as shown in Figure 2.

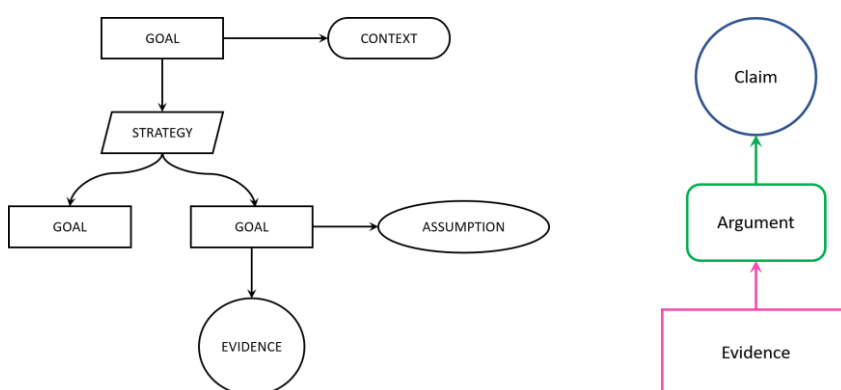


Figure 1 - GSN paradigm on the left (a) and CAE paradigm on the right (b)

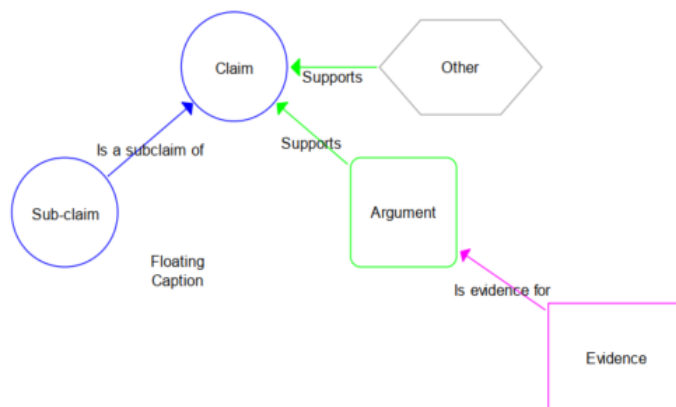


Figure 2 – CAE diagram

2.5 Patterns to reduce complexity

The structured analysis of Iplom's industrial safety makes it possible to identify modular and repeatable syntactic constructs of the Safety Case, which are the so-called "patterns."

The pattern is a portion of the Safety Case, or - in the CAE notation - a defined set of claims, arguments and evidence, characterised by the possibility of being replicated within the same Safety Case to analyse different sub-systems of the single general system, through the same analytical and structured approach, or the exact structure of claims, arguments and evidence, appropriately declined to depict the peculiarities of the specific sub-system analysed.

The possibility of using patterns derives, on the one hand, from the observation that the analysed socio-technical system (i.e. the industrial plant) is actually made up of technical and human sub-systems belonging to homogeneous families and, therefore, analysable according to the same "working scheme" that preserves the peculiarities of each sub-system; on the other hand, from the logical superstructure at the basis of the most modern approach to industrial safety which identifies quite standard risk control measures - the performance of which must, in any case, be calibrated and verified for the specific case.

2.6 The barrier-based approach to support the Safety Case development

The Safety Case becomes a structured recomposition of the various information available on risk management, using precise methodologies and notations for this purpose, such as those set out in the previous paragraph. It is noted that the adoption of a barrier-based approach to risk management is encouraged, as thanks to methods such as the Bow-Tie, it is possible to create functional links between the Safety Case evidence and the typical elements of a Bow-Tie diagram, such as barriers (Fiorentini, 2021). Furthermore, using this approach makes it even easier to visualise the risk analysis results and demonstrate the ALARP conditions possibly achieved, as stated in Fiorentini and Marmo, 2018.

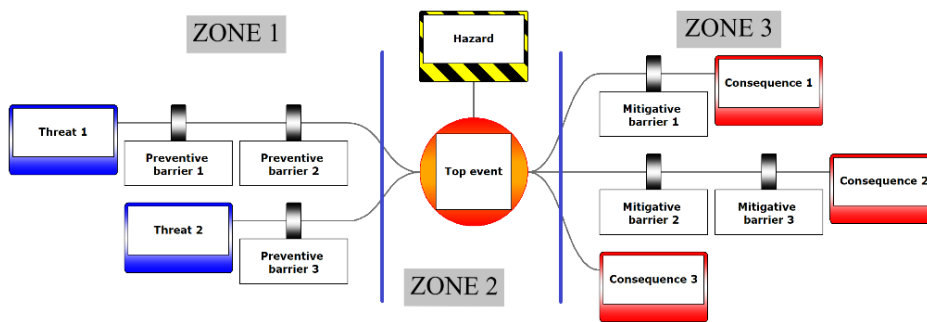


Figure 3 - Bow-Tie diagram structure

The Bow-Tie technique involves the development of logical flow diagrams in three distinct zones (Fiorentini and Marmo, 2018), as shown in Figure 3. "Zone 1" (Prevention) on the left side lists all potential causes (blue rectangles) associated with the unwanted event and the specific protection systems, akin to a simplified fault tree. The "Zone 2" (Top event) in the centre of the diagram identifies the specific danger (yellow and black striped rectangle) and represents the primary incidental event. It can evolve based on the dynamics of the incident in alternative scenarios. "Zone 3" (Protection) covers potential incidental scenarios like burning gas jets, explosions, flash fires, and protective systems to mitigate their effects. It's essentially a simplified event tree.

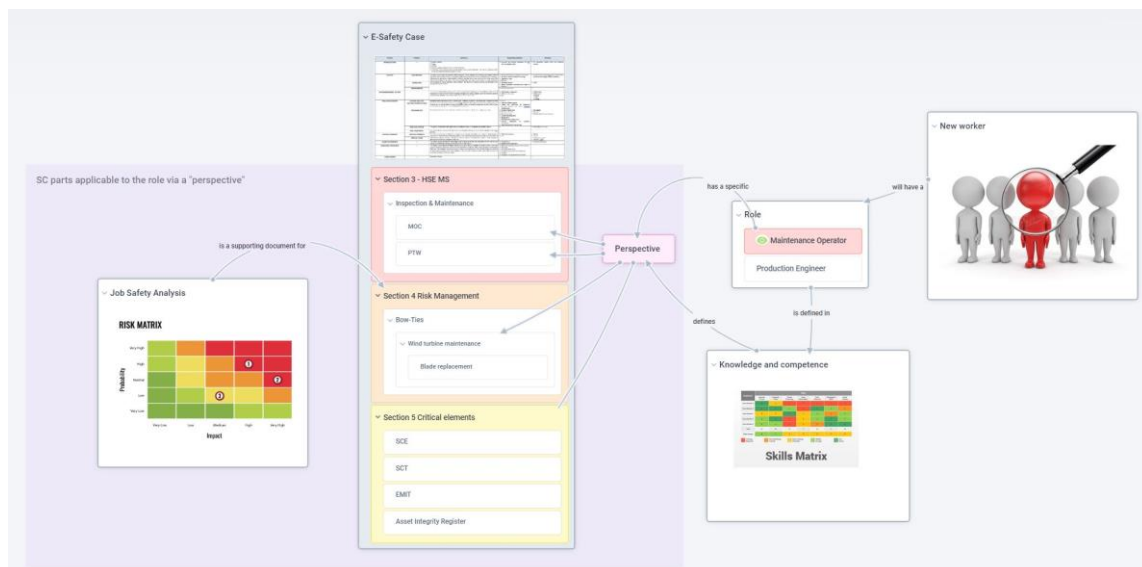


Figure 4 – Usable E-Safety Case

3. Contents of the proposed Safety Case

Based on the critical issues raised concerning the industrial complexity that characterises Iplom S.p.A. (multiple sites, complex industrial processes, plants in different territorial contexts) and emerging risks, it is proposed to summarise the salient risk management information according to a "Safety Case" approach, also leveraging the CAE or GSN notation and the Bow -Tie. This information can be summarised in an executive summary, to be delivered in electronic format (i.e. an E-Safety Case, see Figure 4), of which a possible table of contents (see Table 1) is proposed:

Table 1 Outline of the proposed Safety Case as Executive Summary of the Seveso Safety Report

Section	Chapter	Summary
INTRODUCTION	--	This section defines: <ul style="list-style-type: none"> • Scope; • Context • Structure outline and demonstration of the logical flow. • Justification of the selected level of detail considering the extent of potential risks and the complexity of the activity and installation/process/system involved.
FACILITY	Description Operation Environment	This section should describe the facility and its operation. The facility includes the refinery, tank farms, pipelines, and loading/unloading facilities in port. It defines position and layout, as well as location-specific conditions. The operation should describe the activity in the scope of the Safety Case, including utility systems, personnel transportation, personnel welfare, logistics, diving operations, marine operations, and special operations. Maintenance and service activities are described in the HSE/Seveso management system section.
HSE MANAGEMENT SYSTEM (HSEMS)	--	This section will describe each pillar's major aspects of the management system(s). HSEMS (also Seveso management system) should include all the persons involved in the Refinery/Tank Farms and Pipelines activity, including managers, employees, operators, external contractors, and external support people (including emergency services, transportation services, etc.).
RISK MANAGEMENT	Hazard Analysis and Risk Identification Risk Analysis Risk Evaluation Risk Treatment	Extensive hazard analysis should be included for both installation/commissioning and operation. Hazards should be identified as general hazards for the entire facility, including external factors) or hazards specific to a part of the facility. Identified risks should be assessed, and this section should summarise the results of supporting analysis. This section should present the results of comparing risks with acceptability/tolerability criteria. This section should summarise the preventive and mitigative measures in place and the selection criteria.
SAFETY CRITICAL ELEMENTS (SCE)	Critical Elements Critical Tasks	This section includes identifying safety-critical elements and tasks. It should also describe the performance standards, inspection, and maintenance processes to provide assurance. SCEs will include flammable gas detectors, emergency shutdown systems, fire suppression systems, HVAC, emergency lighting, emergency means, etc.
ALARP STATEMENTS	--	This section should describe the methodology used to demonstrate that risks associated with the activities are reduced to the ALARP level, including discussing the ALARP criteria.
EMERGENCY RESPONSE	--	This section should outline emergency procedures, including suspending and abandoning activities. It should address how components at various locations, such as pipeline pumping stations, can communicate effectively. The emergency response plan should highlight any reliance on human intervention and external services (e.g. the marine authority for port operations and onshore fire brigades). Additionally, it should include details on resource coordination (including cooperation with competitors in nearby areas as part of the external emergency plan for major accidents).
CONCLUSIONS	--	Executive summary. Statement of fitness.

4. Conclusions

The need to manage growing complexity and emerging risks in reality at risk of a major accident has led the authors to highlight the need to equip complex industrial realities, such as those of Oil & Gas, with a streamlined,

structured and complete tool for the management of risks. This tool has been identified in the Safety Case to be condensed into an executive summary according to an approach already widely used in other industrial contexts. Thus, the document is configured as a connecting element between the Safety Report, the Safety Management System and the Prevention of Major Accidents. Furthermore, if used in electronic format, it offers itself as a sharing tool between the various stakeholders, including the authority having jurisdiction, helping to keep the representation of risks updated.

The executive summary contains the evidence of the changes that have occurred over the last five years or since the previous management review, together with the link to the dedicated insights (assessment of the human factor critical elements for safety and the environment), the evidence (including those related to fire safety management) and plans to substantiate and demonstrate the implementation of the Safety Management System for the Prevention of Major Accidents, as well as the emergency response plan and the personnel information/education and training plan.

This approach has been positively tested at the company Iplom S.p.A., characterised by multiple production sites, complex production processes, and an extremely extensive safety report.

References

- Bloomfield, R. E. & Netkachova, K. (2014). Building Blocks for Assurance Cases. Paper presented at the International Symposium on Software Reliability Engineering (ISSRE), 03-11-2014 - 06-11-2014, Naples, Italy
- 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.
- Fiorentini, L. (2021) Bow-Tie industrial risk management across sectors: A barrier-based approach. 1st ed. New York: John Wiley & Sons.
- Fiorentini, L., and Marmo, L. (2018) Sound barriers management in process safety: a bow-tie approach according to the first official AIChE—CCPS guidelines, *Chemical Engineering Transactions*, 67, 253-258. DOI: 10.3303/CET1867043.
- Kelly, T. (2004) 'A systematic approach to Safety Case management'. *SAE Transactions*, 113, pp. 257–266.
- Maguire, R. (2017) *Safety Cases and safety reports: Meaning, Motivation and Management*. 1st ed. London: Routledge.
- Marrazzo, R. (2021) ISPRAs experience in inspections of the Safety Management System for the Prevention of Major Accidents (in Italian).
- McDade, D. (2021) 'Operationalising' Safety Cases – How to share and use Safety Cases. Warrington: Risktec Inc.
- Melchers, R. (2001) On the ALARP approach to risk management. *Reliability Engineering & System Safety*, 71(2), pp.201-208.
- Spriggs, J. (2012) *GSN – The Goal Structuring Notation: A structured approach to presenting arguments*. London: Springer.
- Vazzana, F. (2019) Control activities in industrial plants subject to the Seveso Directive: impact on safety and environmental protection aspects (in Italian).