



How do organizational structures impact operational safety? Part 1 – Understanding the dangers of decentralization



Gilsa Pacheco Monteiro^{a,*}, Andrew Hopkins^a, Paulo Fernando Frutuoso e Melo^b

^a Australian National University, School of Sociology, Canberra, ACT 0200, Australia

^b Graduate Program of Nuclear Engineering, COPPE, Federal University of Rio de Janeiro, Av. Horácio Macedo 2030, Sala G-206, 21941-914 Rio de Janeiro, RJ, Brazil

ARTICLE INFO

Keywords:

Organizational structure
Culture
Operational safety
Decentralization
Centralization
Major accidents

ABSTRACT

This paper (Part 1) is about the influence of organizational structures on the way major accident risks are managed. It discusses how decentralization, meaning the dispersion of decision-making autonomy within the company, undermines operational safety. A case study is presented, and three real situations experienced by an oil and gas company are described, revealing how the decentralized structure contributed to the negative outcomes observed in each case. The examples demonstrate the need for an operational safety structure with a higher degree of centralization and a greater independence from business pressures. Then, in a separate paper (Part 2) following on from this discussion, the authors propose a design strategy to strengthen the operational safety function. In the suggested structure, a more centralized and independent control of risks is achieved, without losing the ability to quickly identify and effectively address the safety issues at the asset level.

1. Introduction

Man-made disasters in different high hazard industries have proven the influence of organizational factors in the development of such accidents. Failures in the acquisition, analysis and flow of relevant information have contributed to an inadequate understanding of the operational risks, leading to a poor decision-making marked by a risk-blind or even a risk-denying that is only perceived in a retrospective view of these catastrophes.

Information flows and decision processes cut across a company's structure and are largely dependent on the organizational design. The structures in place directly affect the ability an organization has to identify, make sense of, and escalate whatever bad news there may be about safety to top-level managers who have the power and authority to effectively respond and act on them. This paper is mainly concerned with improving the understanding on how structures affect catastrophic risks management. A better comprehension on this organizational factor can enable major hazard companies to identify their design weaknesses and act on them before these vulnerabilities contribute to accidents.

In the oil and gas industry, the influence of organizational structure was recognized as a contributing factor to the British Petroleum (BP) Texas City refinery accident, in 2005. The BP US Refineries Independent Safety Review Panel concluded that:

“BP’s decentralized management system and entrepreneurial culture have delegated substantial discretion to U.S. refinery managers without clearly defining process safety expectations, responsibilities, or accountabilities” (BP, 2007, p.94).

The BP's decentralized system to manage process safety deserves further explanations. Hopkins (2008) clarifies that:

“A decentralized structure means that decisions about how a particular site will operate are made, as far as possible, at the site or local business level rather than at head office” (Hopkins, 2008, p.91).

Hence, establishing safety as a decentralized function means that the decisions that could impact the management of major hazards at BP facilities were made at business unit level, with little or even no influence or oversight by the corporate safety experts. Now, add to this decentralized management system, a lack of understanding about process safety and its differences from personal safety, and it is possible to visualize the state of organizational confusion established within the company where it was not always clear who was responsible for process safety related issues.

Another major accident where the BP organizational structure acted as a contributing factor was the Gulf of Mexico blowout, in 2010, frequently referred as the Macondo disaster. According to Hopkins (2012),

* Corresponding author at: Graduate Program of Nuclear Engineering, COPPE, Federal University of Rio de Janeiro, Av. Horácio Macedo 2030, Sala G-206, Centro de Tecnologia, Cidade Universitária, Ilha do Fundão, 21941-914 Rio de Janeiro, RJ, Brazil.

E-mail addresses: gmonteiro@nuclear.ufrj.br (G.P. Monteiro), andrew.hopkins@anu.edu.au (A. Hopkins), frutuoso@nuclear.ufr.br (P.F. Frutuoso e Melo).

“At that time, BP was among the most decentralized of the major oil and gas companies. It consisted of a series of relatively autonomous regional business, only loosely tied together at the corporate centre in London” (Hopkins, 2012, p.100).

Hopkins (2012) argued that this decentralized structure subordinated engineers to line managers. In so doing, any best practice proposed by a base-level asset engineer would be immediately balanced against production and cost reductions by the base-level manager to whom the engineer was directly subordinated. Since the engineering argument was not assessed by a more senior technical expert, positioned at a higher hierarchical level, the best practice suggested could be discounted too readily, degrading the quality of engineering decision-making that contributed to the blowout in 2010. At that time, the BP corporate staff was reduced, and its experts were put in a position of only providing safety guidelines to the company, without checking how these practices were deployed at site level, leading, according to Hopkins (2012), to global variations in the standards applied within BP’s facilities.

The analyses performed by Hopkins on both BP accidents (Hopkins, 2008, 2012) have clearly revealed the connection between what went wrong and the organizational structure, leading to the main hypothesis herein discussed: that a decentralized safety structure undermines operational safety¹. Findings from investigations of catastrophic scenarios in other high hazard industries provide additional evidence that support this hypothesis. At this point, it is worth exploring some findings from the Columbia Accident Investigation Board (CAIB, 2003).

Columbia disintegrated in 2003 while re-entering the earth’s atmosphere, claiming the lives of all its seven-member crew. The accident occurred 17 years after Challenger shuttle was destroyed during its launch, killing another seven astronauts. The Columbia Board identified that the structure of NASA (National Aeronautical and Space Administration) did not provide effective checks and balances and did not have an independent safety program. The Board concluded that only significant structural changes would enable NASA to adjust its organizational culture and improve safety of shuttle operations. After evaluating best safety practices and looking to the model adopted by the U.S. Navy Submarine and Reactor Safety Programs, the Columbia Board recommended the adoption of an organizational approach that separated the technical authority from the functions of managing schedules and costs (CAIB, 2003). The Board was highly influenced by the nuclear navy model. After all, like NASA, the U.S. nuclear navy operated risky technologies with little or no margin for errors. But unlike NASA, the nuclear navy program has strived for accident-free performance and have, by and large, achieved it, revealing the characteristics of the so-called High-Reliability Organizations (HROs).

The establishment of an independent Technical Engineering Authority was then recommended by the Columbia board. This

¹ Operational safety is the safety branch that focus on the prevention, mitigation and response to major accidents. Within the Oil and Gas Industries, the expression “process safety” (API, 2016; IOGP, 2011) is also commonly adopted. While these terms are sometimes used interchangeably, operational safety is a broader concept that encompasses process safety. Accident scenarios that do not meet the criteria to be reported as “process safety events” (API, 2016; IOGP, 2011) can be considered within the scope of operational safety. Examples include collisions between a production platform and an external vessel; leakages and fires at a drilling rig while not operating “in hole” (IOGP, 2011); loss of stability or loss of position of offshore platforms, among others. It is also worth mentioning that the term operational safety is commonly applied in other high hazard industries, such as the nuclear segment, although no definition is provided in the IAEA Safety Glossary (IAEA, 2016). For all these reasons, the concept of operational safety is adopted in this paper. Thus, from this point on, the term “process safety” will be used only when describing the structure of the company selected as a case study, since this is the term applied by this organization.

function, set up at the top of the organization, should have no connection to or responsibility for schedule or costs. The Technical Authority should be the sole “owner” of technical requirements and waiver capabilities and should independently verify launch readiness (CAIB, 2003). This means that the Technical Authority was not merely relegated to a centralized and independent function with oversight responsibilities. Rather, it had a decision role to guard the organization against decisions that might compromise safety.

The impacts of a decentralized structure on risk management were also identified in the investigations of the accident at the Fukushima Daiichi Nuclear Power Plant, a facility owned and operated by TEPCO (Tokyo Electric Power Company). In 2011, this facility experienced a severe nuclear accident. Although triggered by an earthquake and a subsequent tsunami, both of unprecedented magnitudes, the accident was considered a man-made disaster (NDJ, 2012, p.9). According to the Fukushima Nuclear Accident Investigation Commission (NAIIC),

“The risk of a potentially severe accident never appeared in TEPCO’s list of risks. TEPCO explained this glaring omission by arguing that nuclear safety was supposed to be dealt with by its on-site plant department, hence such risks were not to be recorded in the records of the central risk management meetings” (NDJ, 2012, p.44).

“As the nuclear power business became less profitable over the years, TEPCO’s management began to put more emphasis on cost cutting and increasing Japan’s reliance on nuclear power. While giving lip service to a policy of “safety first,” in actuality, safety suffered at the expense of other management priorities” (NDJ, 2012, p.44).

After the accident, TEPCO went through a nuclear safety reform that established an independent internal safety assurance function, directly reporting to the board of directors. This new division was created to independently monitor and advise the nuclear power division on the management of nuclear accident risks (TEPCO, 2013, p.8).

In the light of the Fukushima Daiichi accident, the International Atomic Energy Agency (IAEA) recognized the need for a systemic approach to safety, which would represent a new way of thinking about safety in the nuclear field (IAEA, 2013). This type of approach must be capable of considering the interrelationships and interactions among different actors, which include the staff at nuclear power plants, the corporate experts at the headquarters, the regulatory body, among others (IAEA, 2013). And the way these interactions will occur will be largely influenced by the manner through which the organization is structured.

This paper (Part 1) aims to identify typical structural characteristics that can be detrimental to operational safety. Following a conceptual discussion on different sorts of structure and their impacts to the decision-making processes, examples from a case study performed within an oil and gas company are presented. In the selected case, a high degree of decentralization could be observed to the safety function. Hence, the central idea of this paper (Part 1) is to present some operational safety issues experienced by this organization and discuss how these aspects can be connected to the decentralized design. Then, in a separate paper (Part 2), the authors promote a discussion on potential solutions that could be adopted to handle safety in a more centralized and independent approach even within a decentralized company organized into business units. In this process, we hope to expand the reader’s comprehension about this organizational factor and improve his or her ability to recognize the main characteristics of a complex organizational structure and their potential impacts to operational safety.

2. Key concepts – Decentralized versus centralized decision-making

Decentralized and centralized organizational structures are just two options that define a large spectrum of possibilities for organizational design. A critical structural variable is therefore the degree of

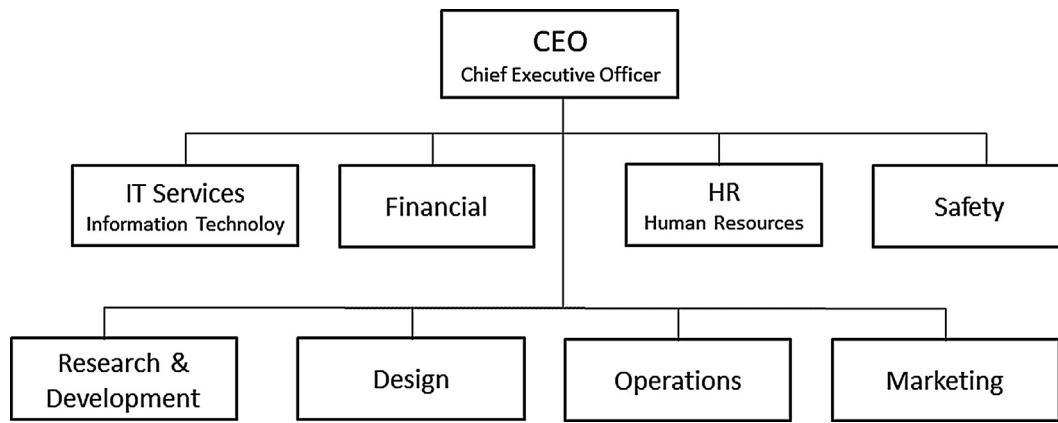


Fig. 1. Centralized or functional organizational structure (All figures in this article were constructed by the authors).

centralization, which means the extent to which the decision-making autonomy is dispersed or concentrated within the organization. This degree affects the way safety decisions are made and, consequently, their outcomes. The safety-related decisions of interest in this paper comprise the managerial decisions that require some sort of planning and investment and that, to keep the operational risks under effective control, may involve a sacrifice of long-term business goals due to short-term safety concerns.

In more centralized structures, also called functional organizations, decisions are made at the top. According to Duncan (1979), one key characteristic of this type of structure is the specialization by functional or technical areas that provide services to other departments but are answerable to the corporate levels, where decisions are taken. Since decisions are pushed up the hierarchy, a disadvantage of this structure emphasized by Duncan (1979) is that top-level managers may become overloaded, slowing the response time in the decision-making. Fig. 1 illustrates this kind of organization.

More complex environments require a structure capable of providing quicker response times. Decentralization is then a strategy commonly adopted. In large corporations, such as international oil and gas companies, the structure is often designed around several autonomous business units or assets. Decisions are transferred to these local assets which present their own technical or functional teams, subordinated to the asset manager. Each business unit come to possess all the authority and responsibility for schedules, costs, production and safety. The organization may be viewed as a set of individual companies linked together by a corporate center that establishes some general guidelines and goals to be deployed at asset level. This structure is illustrated in Fig. 2.

Another type of organizational structure that, according to Galbraith (2009), emerged from the aerospace industry in the 1960s, is the matrix. This type of structure is built around two or more dimensions, such as functions and products or regions. Dual accountability is a fundamental characteristic of a matrix structure, as illustrated for the safety function in Fig. 3, in which a business unit safety manager answers to the business unit leader but also to a corporate safety leader.

The matrix structure is a type of collaborative arrangement that can be applied by decentralized companies in order to provide a more centralized control of critical functions, such as safety. Nonetheless, in breaking the unit-of-command concept, it tends to create confusion and role ambiguities that often lead to a final arrangement in which the power, and even the legitimacy of one of the reporting lines are reduced. Usually, just one of the bosses selects the person to occupy the Business Unit Safety Manager position and establishes the goals to be pursued by this individual, whose performance is assessed afterwards, based on how well these goals were achieved. Besides the material rewards usually associated with these performance evaluations, it is possible to perceive some immaterial or psychological rewards connected to these assessment schemes that strongly influence the individual's behavior, such as the need for boss approval, the need to be recognized as making a valuable contribution, among others that transcend purely financial considerations (Hopkins and Maslen, 2015). The control of these rewards can explain the usual power difference observed between the two reporting lines of a matrix structure, where one works as the legitimate relationship and the other is not recognized with equal influence and even prestige. This imbalance of power between the two sides produces an "asymmetrical matrix", a type of structure more often observed in matrix organizations than the truly

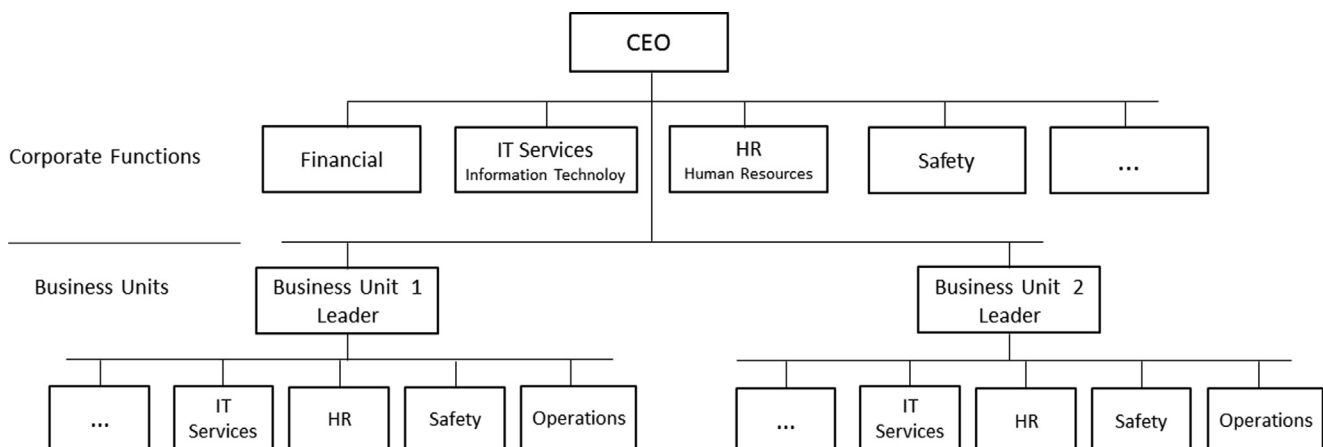


Fig. 2. Decentralized organizational structure.

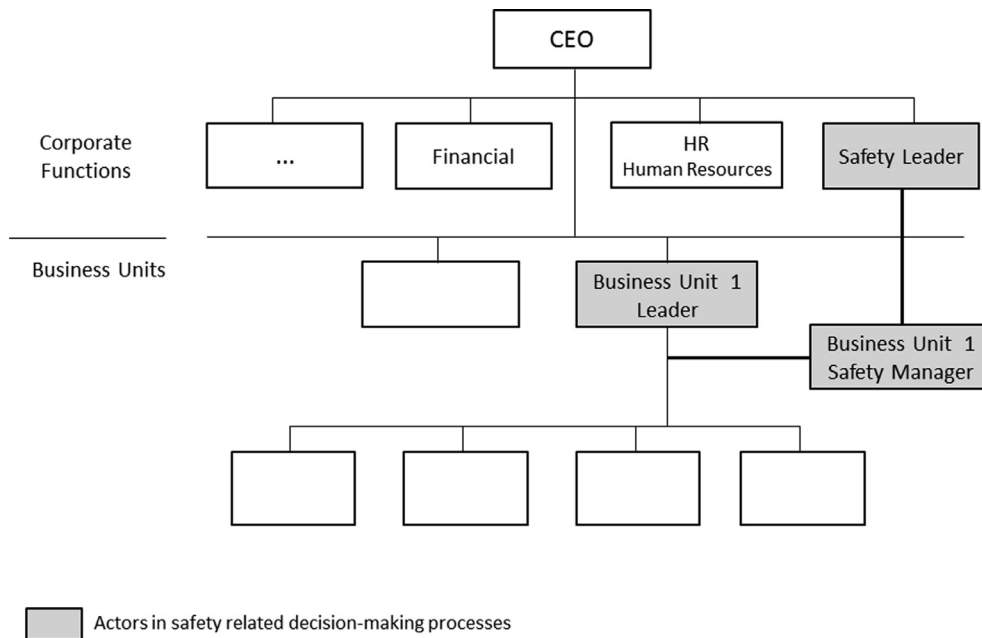


Fig. 3. Matrix organizational structure.

balanced structure depicted in Fig. 3.

Consider for instance, the asymmetrical matrix illustrated in Fig. 4. The solid line shown in this Figure is used to portray the final “one-boss” situation at asset level, while the dotted line represents the remaining communication line between the Business Unit Safety Manager and the Corporate Leader.

Comparing Fig. 3 (the truly balanced matrix) with Fig. 4 (the asymmetrical matrix with one boss at asset level), it is possible to visualize how the imbalance of power in this latter case has affected the organizational dynamics with respect to the safety related decision-making processes. In the asymmetrical structure illustrated in Fig. 4, the corporate involvement in these decisions is no longer perceived as a

requirement. The Corporate Safety Function becomes just an advisory group, involved only when the asset level asks for an expert opinion. As a result, major accident risks may end up being managed solely at business unit level without any type of control from the head offices.

The greater the personal prestige or expertise of the corporate safety specialists, the greater is the ability of the corporate function to influence the final decisions made at asset level, regardless of the formal situation. Accordingly, through a kind of a talent selection, the organization could use the power of expertise to fine-tune the power distribution between the two sides of a matrix. This strategy is suggested by Galbraith (2009). However, it does not ensure the formal authority that safety experts may need to avoid decisions with potential to

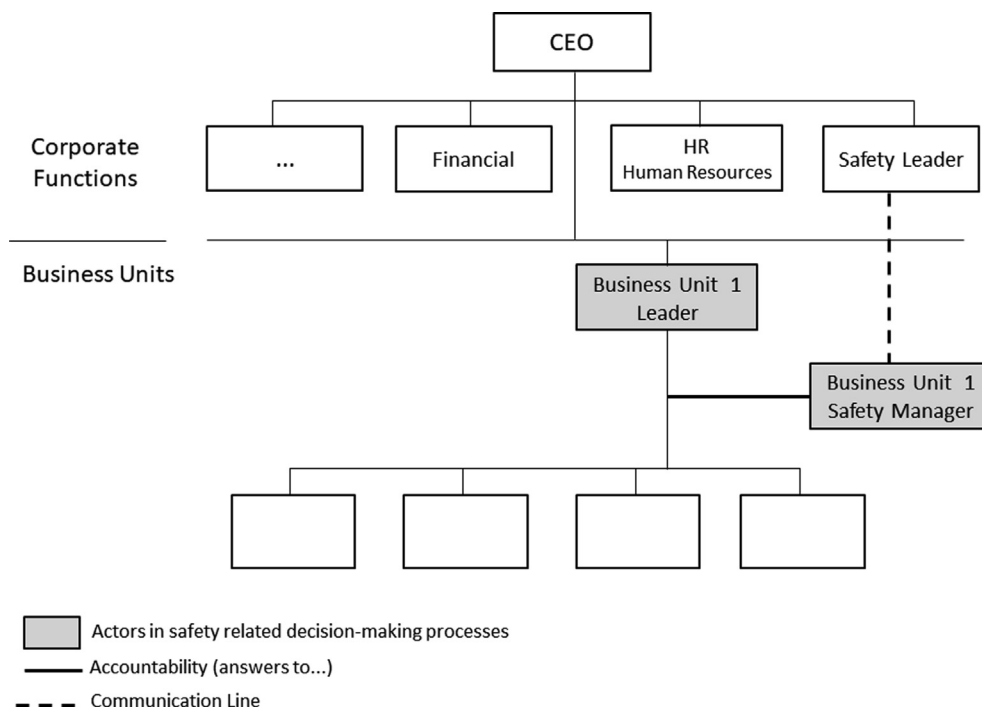


Fig. 4. Asymmetrical matrix structure– one boss at asset level.

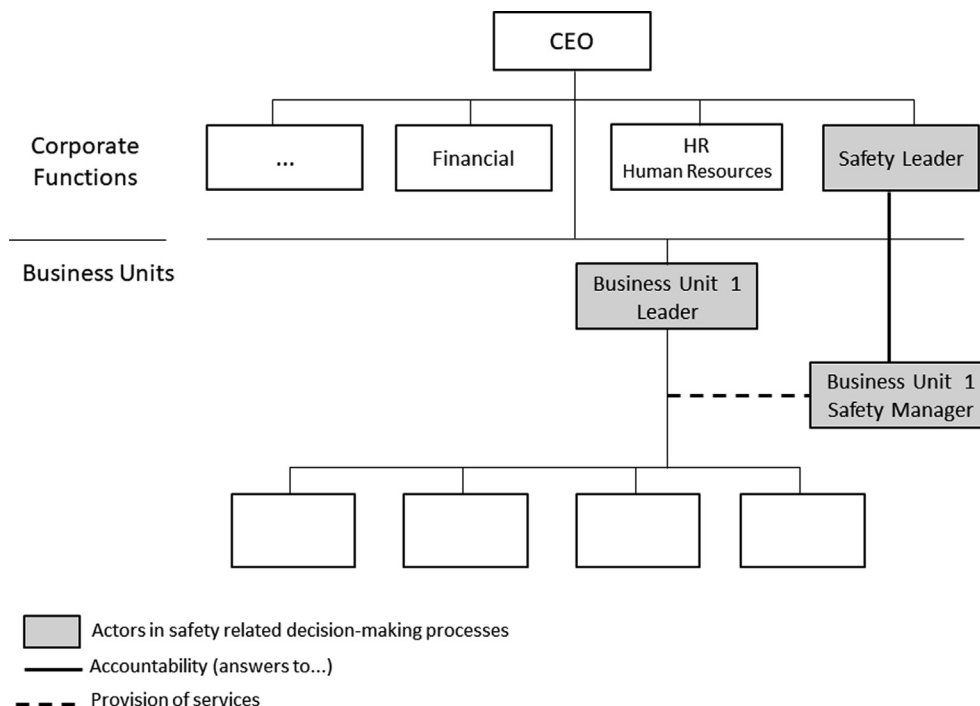


Fig. 5. Asymmetrical matrix structure– one boss at corporate level.

compromise safety.

But the imbalance of power between the two sides of a matrix structure can be appropriate if it stems from an organizational strategy to strengthen one of the dimensions (Galbraith, 2009). Consider, for example, the asymmetrical matrix illustrated in Fig. 5. In this case, the Business Unit Safety Manager is accountable to the Corporate Safety Leader, what makes the safety function more independent from business pressures and ensures the corporate involvement in critical safety related decisions at asset level. The dotted line has now a different meaning and represents the provision of technical services to the asset leader. But if the Corporate Safety function has the authority to intervene in the activities that can affect operational safety, it does not merely have an advisory or oversight role, but a decision-making role.

Structures define the level of independence and the authority assigned to the technical experts involved in the decision-making and this, in turn, affects the power of influence of these specialists, meaning the capacity these individuals have to act and affect another person's perceptions and attitudes. The lower the degree of centralization in the safety-related decision-making processes, the lower the power of influence of the technical experts, which may adversely impact the quality of engineering decisions adopted to manage the risks, leading, over time, to a “way of doing things” that amounts to a defective safety culture. More decentralized designs may produce safe outcomes, but these structures would be more likely to experience a less than rigorous decision at some point in some business unit, when the decision-maker faces a trade-off between production and safety. Certainly, other organizational design aspects and external actors (such as the government, regulatory agencies, researchers, contractors, among others) affect the way operational risks are managed, but the influence of the organizational structure on culture and on the prevention of catastrophic accidents cannot be overlooked.

At this point, it is possible to turn to the case study, which provides three real examples that reveal the dangers of decentralization.

3. How decentralization impacts operational safety – evidence from a case study

The organization selected for this case study is an oil and gas

company that has a highly decentralized safety function, thus providing a proper context to evaluate this paper's hypothesis. Fieldwork was conducted at the upstream segment of the company in the years of 2016 and 2017. The general information gathering techniques used were observation of formal and informal meetings, interviews and review of technical and administrative documentation. The objective was to collect real examples providing a picture of the impacts of decentralization to operational safety. The results are not limited to providing a qualitative description of the observed issues but include an analysis performed by the authors in order to connect each situation to the organizational design. It is also noteworthy that this work represents the collaboration between engineers and a sociologist.

This section is divided into two topics. The first describes the company's organizational chart and provides a discussion on relevant safety related structural aspects. The examples of real situations observed with this study are discussed in the second topic.

3.1. The case study – the organizational structure

The company has a business area focused on the oil and gas Exploration and Production (E&P) activities. As illustrated in Fig. 6, this business area is led by a Director who reports directly to the CEO of the company. The corporate level is divided into various departments that implement functions such as: Finance, Engineering, Corporate Services, among others. Safety is one of the services provided by the Corporate Services division, which has a department dedicated to HSE (Health, Safety, and Environment) activities.

The leader of the Corporate HSE department is therefore accountable to the Corporate Services Director. At the next level down, there is the E&P Corporate HSE department, an HSE division dedicated to the upstream segment of the Company, that is the E&P business area. Finally, an exclusively safety division is established within the E&P Corporate HSE department. Fig. 6 depicts all these corporate-level departments and highlights the divisions that are assigned with solely HSE activities.

As Fig. 6 makes clear, the structure does not provide a safety position with direct report to the CEO. The highest safety position is two levels down. The position occupied by the safety head within the

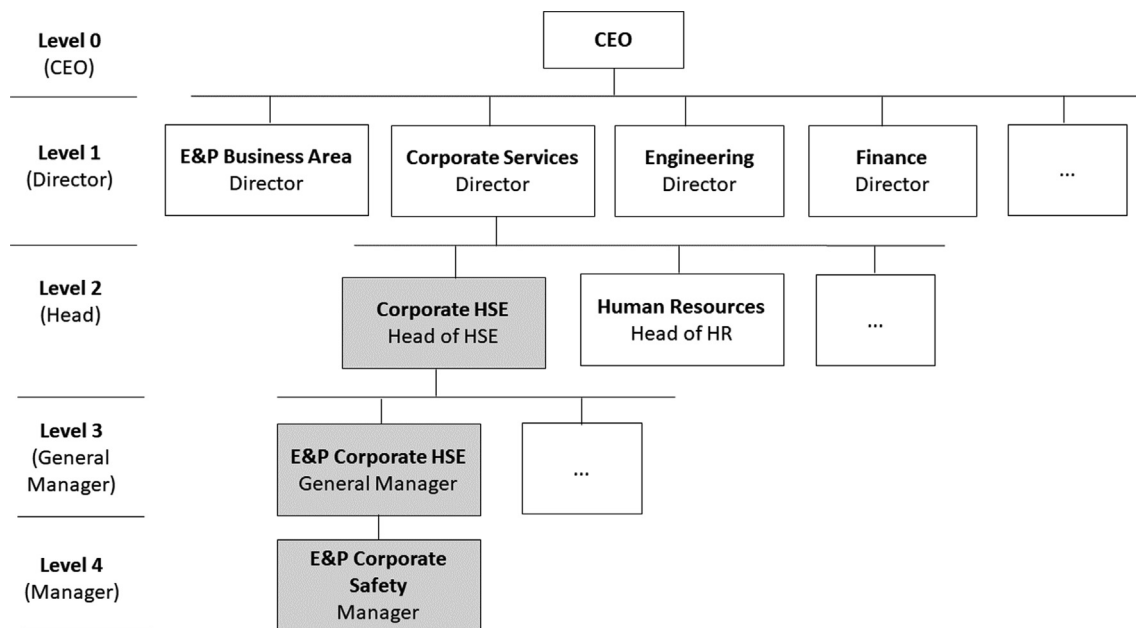


Fig. 6. The case study – the organizational chart at corporate level.

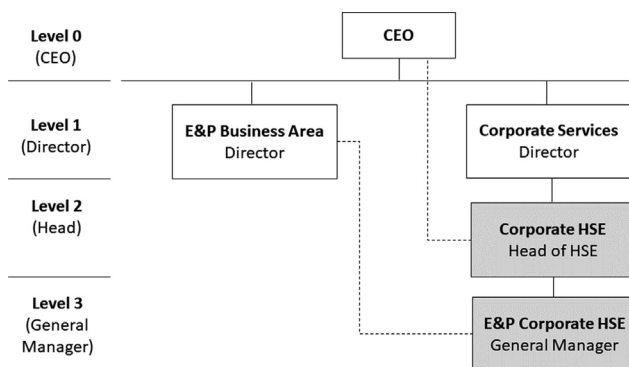


Fig. 7. The case study – the strategy of dotted lines for HSE.

organizational chart affects the power and authority this leader has to raise safety concerns at the top of the company and prevent decisions that, over time, may compromise operational safety. Prior to the Texas City refinery accident, BP had no such person and created this position after the Macondo disaster (BP, 2010), a lesson painfully learned. However, in the case study herein discussed, the need for a safety expert reporting directly to the CEO was recognized by the company, which adopted as a solution, a reporting line from the Head of HSE to the CEO. A similar strategy was adopted regarding the E&P Corporate HSE General Manager and the respective Business Area Director. This strategy is illustrated with dotted lines in Fig. 7.

Although the reporting lines illustrated in Fig. 7 can be perceived as an intermediate solution between the initial structure in Fig. 6 and the final mentioned strategy adopted by BP, the dotted lines do not provide the position power that may be required by the corporate HSE leaders when discussing safety issues with Business Areas' people located levels up in the organizational chart. These corporate HSE leaders have to rely on the power of expertise to guarantee that other competing goals do not prevail over safety. Besides that, the policy adopted by the company clearly states that business and operational managers are held accountable for identifying the hazards and managing the risks. In so doing, the company decentralizes the major accident risks management and reduces the corporate safety experts' role in the decision-making processes to an advisory role.

The Corporate HSE division is responsible for developing and

maintaining the safety policy, as well as the safety management system framework elements (such as Hazards Identification and Risk Assessment, Management of change, among others). This division is also responsible for defining the personal and operational safety indicators that will be adopted within the company. The E&P Corporate HSE department is responsible for developing safety standards for the Business Area and auditing the Operational Units to check for compliance with the safety management elements and regulatory requirements. However, standards and work processes established at corporate level are further detailed at Operational Units level. This allows variations in the standards and even in the computer-based systems adopted by the facilities, an outcome of safety decentralization that will be further discussed.

Consider now the E&P Business Area. The upstream segment is split into exploration and production activities, as well as other support functions. The Head of each one of these divisions is accountable to the E&P Director. Production operations are decentralized, being grouped into autonomous Operational Units in accordance with the geographical location where the activities take place. Each Operational Unit is led by a general manager and presents its own HSE department. Fig. 8 illustrates this E&P organizational chart, as well as the corporate HSE divisions, highlighting the departments that perform safety activities to the upstream operations. The significance of the Process Safety division depicted in Fig. 8 will be addressed later.

In order to achieve a higher degree of centralization for the safety function within the upstream production activities, a matrix structure was adopted, as illustrated in Fig. 9. However, as Fig. 9 makes clear, the matrix was designed without dual accountability. The safety manager of each Operational Unit continued to be accountable to just one boss, who is located at the asset level. The asset safety divisions were then connected to the E&P Corporate Safety department but through a dotted line that works basically as a communication line. The resulting structure is therefore, an asymmetrical matrix, such as the one illustrated in Fig. 4. This means that, as previously discussed in Section 2, the corporate safety function works mainly as an advisory and oversight group that provides safety standards and performs some audit activities but, in the end, safety-related decisions can be made at asset level with no involvement from the head offices. As a result, similar safety-related situations can be handled by the Operational Units through different strategies. It is reasonable to conclude that the adopted asymmetrical

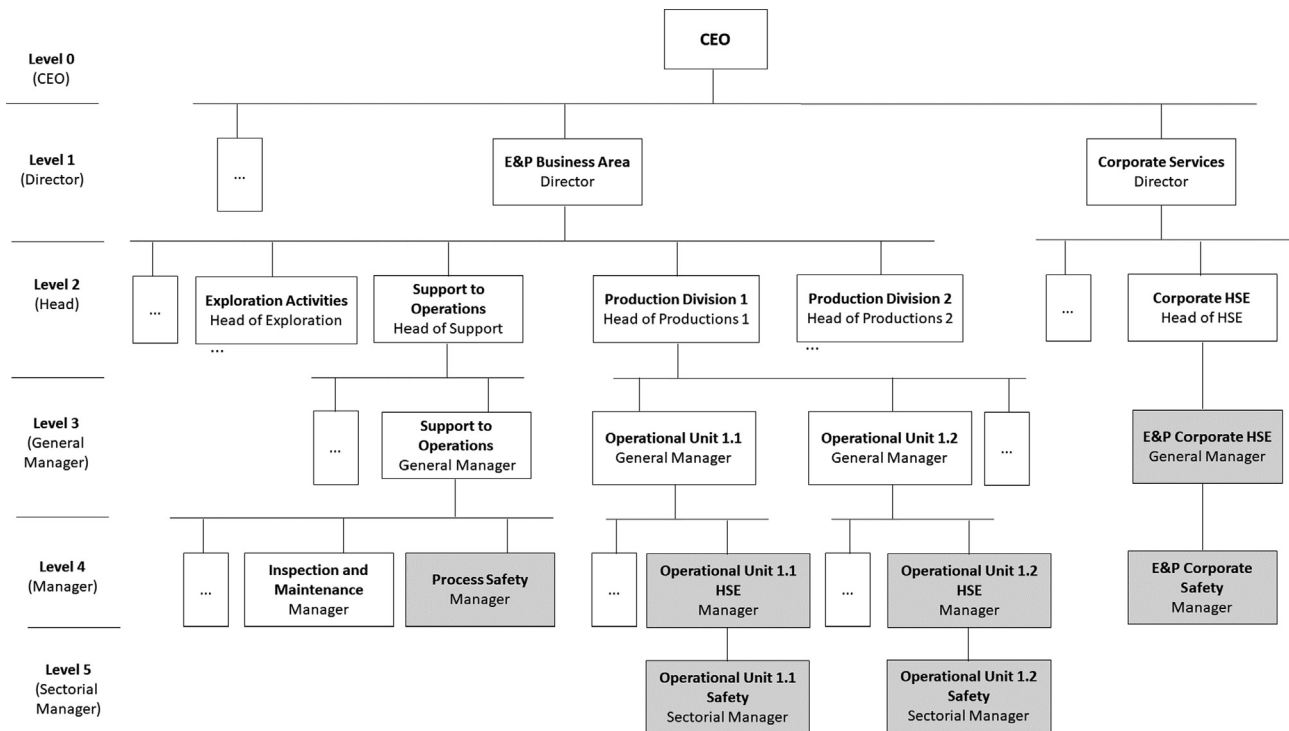
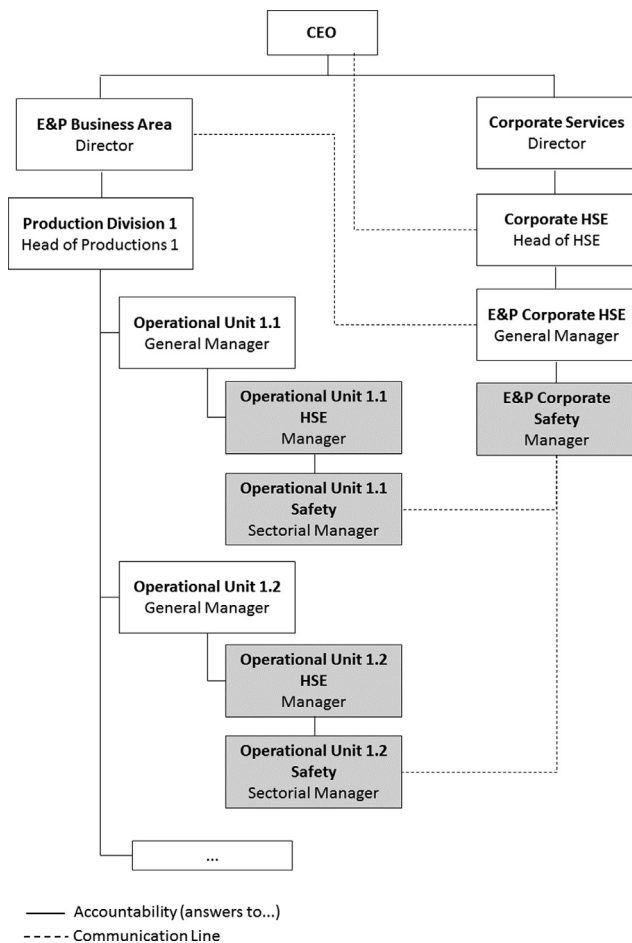


Fig. 8. The case study –the E&P business area and the corporate HSE departments.



— Accountability (answers to...)
 - - - - Communication Line

Fig. 9. Asymmetrical Matrix structure adopted for the safety function – one boss at asset level.

matrix structure was not capable of promoting the safety function centralization aimed by this organizational change.

At the time the safety structure in Fig. 9 was established, a similar organizational restructuring was defined for another corporate function: Human Resources (HR). However, in this case, a total centralization was the aim to be achieved. The final solution adopted by the company was again an asymmetrical matrix, but with a crucial difference in relation to the structure depicted in Fig. 9: instead of answering to an asset leader, the HR manager of each Operational Unit is accountable to a higher-level HR manager located at corporate level. The final HR chart is shown in Fig. 10, where the dotted line portrays a provision of corporate services to the assets.

The type of structure illustrated in Fig. 10 ensures a higher capacity to standardize the practices applied among the operational units, reducing the procedures and systems proliferation typically observed when independent units do not share common functional resources. Therefore, the standardization promoted by this structure could lead to simplifications and these, in turn, to the cost reductions intended by this HR restructuring. But an additional feature of an asymmetrical matrix such as the one depicted in Fig. 10 is the higher function independence from business pressures, which strengthens the functional dimension.

After the Macondo accident, BP has used this type of asymmetrical matrix to create an enhanced and independent Safety & Operational Risk (S&OR) function, to oversee and audit the company’s operations around the world (BP, 2010). In this new structure, the S&OR’s specialists are embedded in the operating units, not only providing services to the assets, but rather exerting a decision-making role,

“with defined intervention rights with respect to technical and operational activities” (BP, 2010, p. 15).

With this S&OR structure, BP has established an independent function intimately involved in the operational activities, reporting at the very top of the corporation (Hopkins, 2012). This could have been a more effective strategy to centralize the safety function within the company selected as a case study.

According to Hopkins (2008),

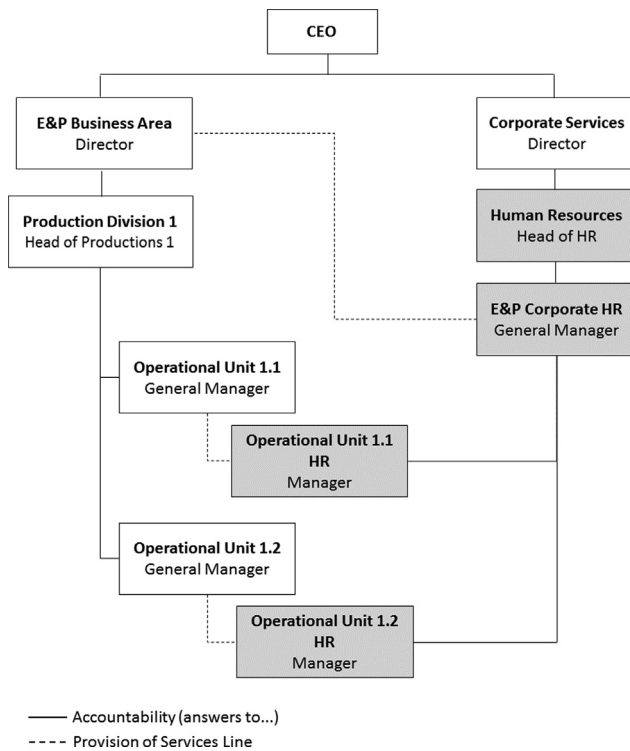


Fig. 10. Asymmetrical matrix structure adopted for the Human Resources (HR) function – one boss at corporate level.

“matrix organizations are not installed; they grow up from various starting points” (Hopkins, 2008, p. 99).

In this case study, the starting point was a decentralized structure divided into Operational Units, on which a safety functional structure has been gradually evolving. Figs. 8 and 9 show this organizational evolution. Only time will tell if a further step in the direction of a higher safety centralization, through the adoption of a structure similar to the BP’s, will be considered. However, the evolution achieved so far is limited to personal safety. And, at this point, we can turn to the role of the Process Safety division illustrated in Fig. 8.

This Process Safety department established within the E&P Business Area performs tasks such as operational safety standardization, advisory and oversight activities related to the upstream production operations. Although the Corporate Safety division has a staff dedicated to process safety, there is only one expert, with an impossible workload, performing technical activities. The other corporate engineers are assigned with mainly administrative tasks related to the control of some safety work processes such as auditing, reporting of incidents required by the regulator, among others. Hence, in the end, the operational safety remains as a decentralized function and decision-making processes occur at business level with little or almost no corporate safety involvement or influence. But what is more critical is that this kind of structure sometimes leads the Operational Units’ staff to “shop around” for the safety expert opinion that best fits the asset’s intentions. Putting it another way, the asset staff ask for advice from experts located at the Process Safety division and, if this technical advice is against the asset’s intentions, they look for a different opinion from the expert serving the Corporate Safety department. With such an organizational dynamic, the safety experts from these divisions are required to rely on direct contact to meet informally and discuss the common issues to which they have been individually presented, in order to avoid divergent opinions that can degrade safety.

Having discussed the main features of the organizational chart, it’s possible to present the examples that provide evidence of the impacts

exerted by this decentralized structure to operational safety.

3.2. The case study – the examples

This section presents three real situations experienced by the company chosen as a case study. In the first example, operations in one of the production facilities were shut down by the Regulator. In the second, an accident that severely injured two operators is discussed. Finally, the third example reveals that relying solely on mindful leadership may not be enough to achieve an organizational state of collective mindfulness that is vital to major accidents prevention.

3.2.1. Variations in operational safety management strategies

In the decentralized organization illustrated in Fig. 8, safety criteria and guidelines are established by the corporate safety departments and deployed in the standards of each Operational Unit. The asset leaders are responsible for developing standards and for adopting practices that are in accordance with the corporate requirements. But how to ensure that the operational safety concepts established at the top of the organization are being correctly interpreted, assessed and evenly applied at process facilities? If the structure allows for decision-making processes made solely at the asset level and does not promote an upward flow of information to the head offices, variations in the operational practices established at the facilities are almost inevitable. As a result, Operational Units can adopt completely different strategies to manage similar safety-related situations.

Consider for instance, two production facilities, P-A and P-B, owned by the different Operational Units illustrated in Fig. 8. P-A is owned by the Operational Unit 1.1, and P-B, by Operational Unit 1.2. Both facilities present a safety system whose function is to deliver a fluid in accordance with the designed flow rate and pressure. However, the facilities present design differences for this safety system, as illustrated in Fig. 11, where block diagrams depict these two cases.

As showed in Fig. 11, at P-A, the safety system was designed with two similar pumps. Both pumps are capable of individually meeting the system requirements. Hence, a single pump is sufficient to meet the system demand (or, in other words, 100% of the design condition), while the second pump works as a backup. When both pumps are in service, the redundant piece of equipment can be started to ensure the proper functioning of this safety barrier if the primary pump fails on demand. And when one pump is out of service for maintenance, the system demand can still be met with the remaining pump. Operations are stopped if both pumps are impaired.

At P-B, the same safety system presents three similar pumps. Two pumps are required to meet the design demand and the third piece of equipment is a system redundancy. This means that each pump is capable of meeting 50% of the design condition. In other words, two pieces of equipment must function for the system to be effective and, in case one of them fails, the third one ensures the system functioning. When one pump is out of service for maintenance, the two remaining pumps can meet the system demand. Operations are stopped if two pumps are impaired.

Both facilities had the redundant pump removed from service due to a corrective maintenance activity, as illustrated in Fig. 12.

The company policy is that any modification that alters the operational risks or the systems reliability shall be considered as a “change”. These “change” situations must be properly managed to ensure that new hazards are not inadvertently introduced to a process and that the risks of existing hazards are not unknowingly increased. This is a safety guideline defined by the Corporate HSE department that is then, deployed in the Operational Units MOC (Management of Change) standards. And the initial step of a MOC process is an analysis to recognize whether the modification constitutes a “change” situation.

Following the MOC procedures, the operational staff at facility P-A analyzed the situation illustrated in Fig. 12 and considered that the unavailability of the redundant pump would temporarily impact the

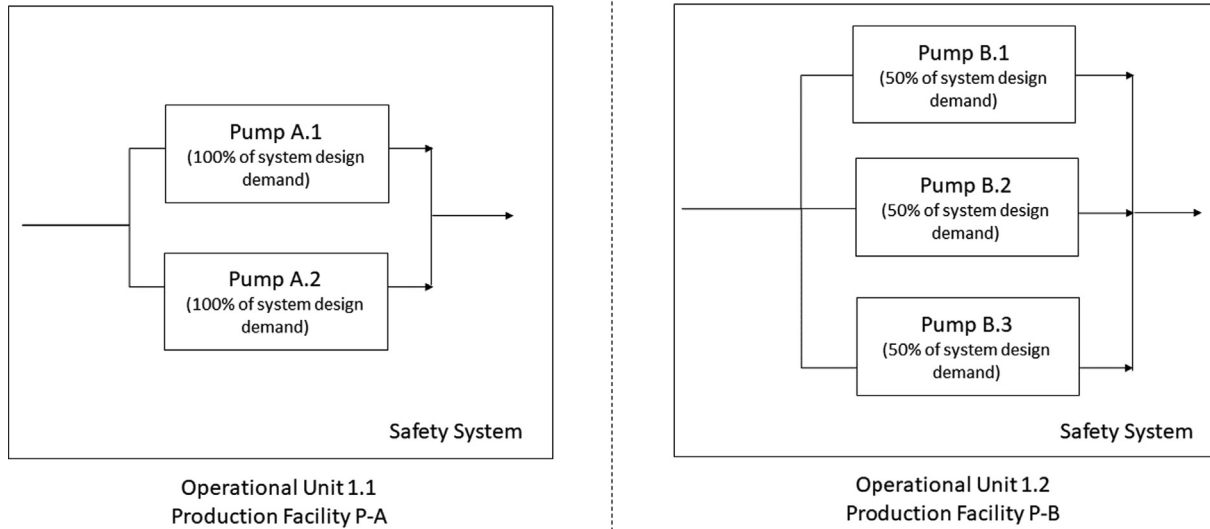


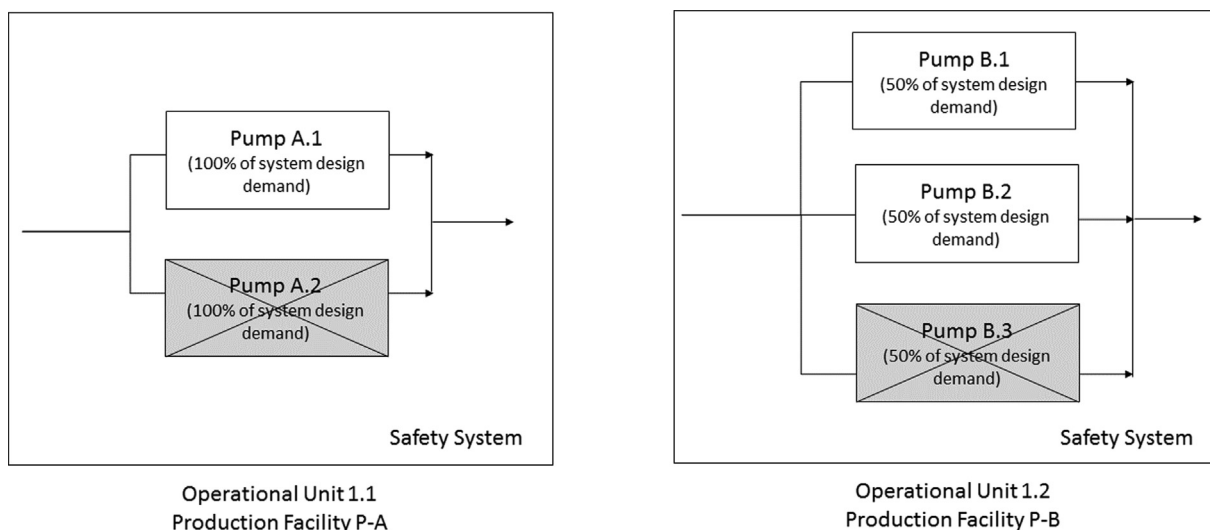
Fig. 11. The safety system design differences.

overall safety system reliability, affecting the operational risks. Based on this assumption, this situation was considered as a “change”. A risk analysis was then performed, and additional measures were established to allow the mitigation of any increased risks during this temporary “change”. These compensating measures included the high cost acquisition of a temporary external system to independently supply the fluid and provide protection in case the remaining pump failed on demand.

However, at facility P-B, the operational staff considered that the safety system would not be affected by the unavailability of the redundant pump. As the two remaining pumps could meet the system demand, the situation depicted in Fig. 12 was not identified as a “change”. Hence, no risk analysis was performed and the decision to continue the operations without any additional risk reduction measure was approved at the Operational Unit level.

At this point, one can argue that the situation at P-A was more critical than that at P-B and that is why completely different

management strategies have been adopted. After all, considering that the redundant piece of equipment is out of service in both cases, a pump failure on demand at P-A would lead this facility to a situation of no fluid being delivered for process protection while at P-B, some fluid could still be supplied by the remaining pump. However, the comparison between the two situations in Fig. 12 is not so straightforward. The safety system at P-B is not capable of fulfilling its function with only one pump. The amount of fluid would not be supplied with the designed flow rate, rendering the protective system ineffective. Additionally, a comparative analysis to define which case is more critical would require reliability calculations to estimate the probability of failure on demand of each case, which is out of this paper's scope. The point here is that, despite the design differences between P-A and P-B, both facilities had to decide if operating without the redundant piece of equipment could impact the risks. If the P-B staff have posed the right question (“are the risks higher in this situation?”), they would have




 Pump out of service

Fig. 12. Unavailability of a redundant operational safety equipment.

realized that additional risk reduction measures might be required when the redundant pump was out of service, especially if one considers the potential catastrophic consequences associated with a failure on demand of this safety barrier. However, the question posed was limited to identifying if the situation should be considered as a “change”. To answer that, forms were filled by the P-B staff with a tick-box mentality. And, since the situation was not considered as a “change”, the risks were not analyzed, revealing a kind of inverted rationale, in which the documentation took precedence over the reality of the risks.

As the Operational Units are autonomous, the decision to continue the operations for almost two months without the redundant piece of equipment and with no additional measure was made at asset level with no involvement of the E&P Corporate Safety department or even the E&P Process Safety division highlighted in Fig. 8. The two completely different management strategies adopted by these Operational Units were identified during inspections performed by the Regulator in both facilities. As a result, operations at P-B were shut down by the Regulator until the impaired pump was restored to normal conditions or a MOC process was performed by the Operational Unit 1.2 to assess the risks and properly manage the situation illustrated in Fig. 12.

The questions that really matter at the initial stage of a MOC process are whether the existent operational risks are getting higher or if new hazards are being introduced by the modification. A positive answer means that the modification is a “change”. Posing the right questions is therefore fundamental to assess and properly manage situations that impact the operational risks. But knowing what questions must be posed is a kind of expertise that asset teams may lack, as shown by this example. That is why it is so important that the organizational structure provides a more centralized approach for the safety function, ensuring that specialists who have this technical expertise are involved in the decision-making processes that impact operational safety at asset level.

In the example herein discussed, it is reasonable to conclude that the decentralized structure in Fig. 8 allowed for variations in the way a safety-related concept was interpreted, assessed and managed by the Operational Units. And this increases the chances that the practices adopted at some facilities might be substandard. Although inspection and auditing activities can identify these improper practices, there is no guarantee that they will be uncovered and corrected before it is too late.

3.2.2. Waivers to technical requirements

In the organization illustrated in Fig. 13, developing and maintaining internal technical standards for the facilities is a responsibility assigned to a department within the Engineering division. Each standard is developed by a group of senior experts, gathering the theoretical knowledge and the practical experience of these specialists. However, the business area's leaders are responsible for adopting and applying the requirements established within these engineering standards. In case of non-compliance with a requirement, technical and managerial arguments shall support the decision of not following the standard and this decision shall be approved by the asset manager, as illustrated in Fig. 13.

As Fig. 13 makes clear, the structure does not provide a process that is independent from business lines to support the waiver decision making. Putting it another way, senior technical experts within the Engineering functional division establish the standards, but they do not control the waivers to the technical requirements. The waiver decision-making process occur at asset level, where an analysis is performed to assess the risks and define compensating measures to ensure that the final situation is “safe”. However, the asset team, in charge for this assessment process, may lack the expertise, as well as the independence required for an effective operational risks evaluation. As a result, flawed rationales can lead to bad decisions.

Consider for instance some onshore drilling facilities operating for the Regional Production Asset illustrated in Fig. 13. These facilities were contracted to perform different well intervention activities. In one

of these interventions, the facility receives a stream comprised of water, oil, gas and debris from the wellbore and routes it to a vessel for gas separation, as illustrated in Fig. 14.

As depicted in Fig. 14, the vessel effluent gas stream is disposed of in a flare system, while the outlet liquid stream is directed to the next stage of the process. However, this gas separation initial stage was required only when the gas/oil ratio was above the threshold value established in a company technical standard. The standard was developed within the Engineering division depicted in Fig. 13. According to this internal standard, when this intervention was performed in oil wells with a lower gas/oil ratio, the gas separator and, consequently, the flaring system, were not required and could remain disassembled within the operations support base. Based on this standard's item, a limited number of flaring systems was defined within the contract supply scope and the asset staff had to prioritize the use of this limited resource to the interventions handling higher gas content fluids.

However, the technical standard was reviewed, and the gas separation stage was made mandatory, regardless of the gas/oil ratio value. With this new requirement, all onshore drilling facilities should have been equipped with a gas separator vessel and a flaring system to perform this type of intervention. But instead of reviewing the contract scope to ensure compliance with this technical requirement, a decision was made in the Regional Production Asset to perform a PHA (Preliminary Hazard Analysis²) to assess the risks of operating without flaring the gas. The intervention to be analyzed would be performed in a well with a gas/oil ratio above the threshold value, a situation that would not comply even with the previous revision of the standard. It is worth noting that operating the gas separator vessel without flaring the separated gas stream was a significant change to the process. This kind of process arrangement was not considered in any of the standard's revisions. With this change, the vessel effluent gas stream would end up being discharged directly to the atmosphere.

The decision to discharge hydrocarbons to the atmosphere requires careful attention to ensure that disposal can be accomplished without creating a potential hazard such as the formation of flammable mixtures at ground level or on elevated structures, among other problems (API, 2014). An engineering analysis is then required to assess these hazards and relevant aspects must be considered, such as the physical state and properties of the released material, the velocity and the temperature of the exit gas, the facility layout, the meteorological conditions, the location of the emission point, potential ignition sources, among other issues. However, in the example herein discussed, no engineering analysis was performed. Only a PHA was carried out by an asset team that recommended to monitor the flammable gas concentration within the facility area with portable detectors and to interrupt operations if gas concentration achieved a value close to the flammability limit. In other words, only one mitigation protection layer, based on the human response to an alarm, was provided to ensure a “safe” operation. The higher risks associated with this less-than-specification situation were considered as acceptable and the waiver was approved.

Teams carrying out risk analyses may experience different psychological phenomena, such as confirmation bias. This is an unconscious process that refers to the

“tendency to test one's beliefs or conjectures by seeking evidence that might confirm or verify them and to ignore evidence that might disconfirm or refute them” (Colman, 2015).

With this kind of bias, the group tends to make selective use of information to suggest that the risks of an accidental scenario are

² PHA (Preliminary Hazard Analysis) is a simple, inductive method of analysis whose objective is to identify the hazards and hazardous situations and events that can cause harm for a given activity, facility or system (IEC/ISO 31010, 2009). It is used to review process areas where energy can be released in an uncontrolled manner (CCPS, 2008).

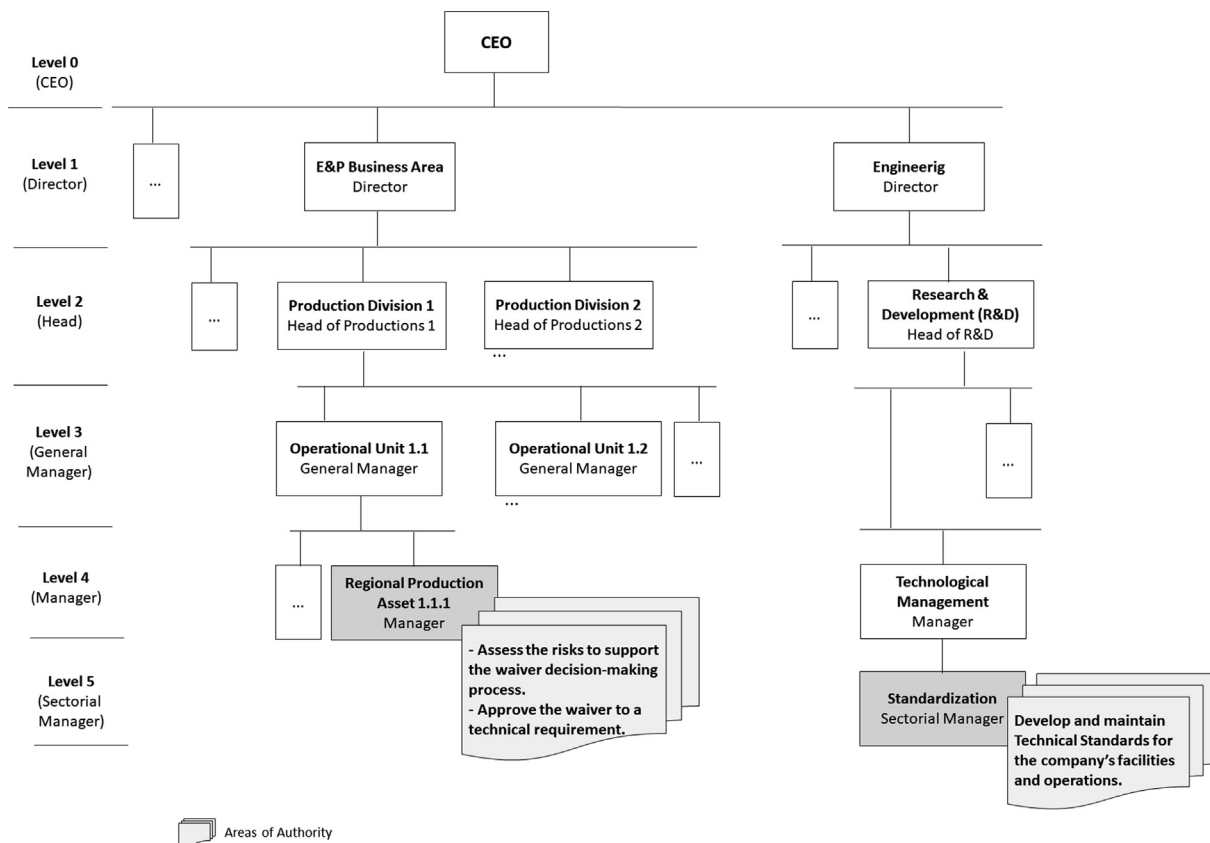


Fig. 13. Waiver decision-making process at asset level.

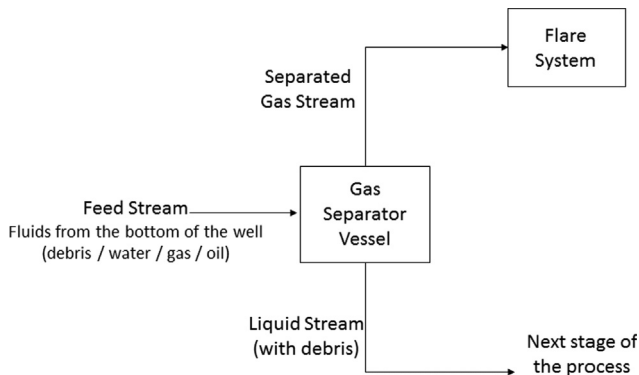


Fig. 14. The gas separation stage.

acceptable, discarding or failing to consider evidences that suggests the contrary (Hopkins, 2012). Within a team lacking the required technical expertise and subjected to business pressures, this kind of psychological phenomenon may lead to flawed rationales that support inadequate risk judgements. And these improper risk evaluations have been systematically used to support the waiver decision-making processes.

It was not the first time that operating without the flaring system was approved to process a high gas/oil ratio fluid. In a two months period, three similar waivers have been approved, which reveals that this kind of deviation had become “normalized” within this production asset. Unfortunately, in the example herein presented, a flammable vapor cloud was formed within the facility area and ignited two hours after the commencement of the operations, leading to a fire that severely injured two operators. The gas continuous monitoring, which was the only risk reduction measure recommended by the PHA team, was not performed on that day, revealing the poor risk perception of the asset operational staff.

Poor risk perception and lack of expertise to properly identify the hazards are merely starting points to explain this accident. A more thorough analysis reveals how the decentralized organizational structure illustrated in Fig. 13 was not able to provide an independent engineering evaluation process to support the waiver decision-making. The experts that developed the standard and could correctly interpret its technical requirements were never consulted. In the end, the structure combined, in the Regional Production Asset division, all authority and responsibility for production, costs, schedule, safety and waiver to technical requirements. And this, in turn, undermined operational safety.

3.2.3. Relying on mindful leaders

Disasters in complex socio-technical systems are always preceded by early warning signs that something might be amiss. However, as stated by Hopkins (2008), these pieces of information usually

“fail to make their way upwards to the leaders with the capacity and inclination to take effective actions” (Hopkins, 2008, p. 114).

Concerned with potential weaknesses and problems that might exist within their organizations, mindful leaders use every means available to identify these warning signs. These leaders welcome the bad news and usually challenge the reports that just show that everything is complying with the rules.

In this example, mindful leaders at the top of the E&P Business Area developed a way through which significant safety issues related to the maintenance campaigns at offshore production facilities were identified and directly reported to them. They were concerned about potential accidents that could occur due to the adoption of substandard practices during this critical period of the facilities. Exhibiting the kind of chronic unease that characterizes mindful leaders, the E&P Director and the Head of Production Division 1 illustrated in Fig. 8 asked the E&P Corporate HSE General Manager to carry out a study to identify any

substandard maintenance practice and recommend improvements to the procedures adopted during these campaigns. These leaders have not requested an overall assessment to confirm that everything was complying with the best industrial practices. Rather, they asked the E&P Corporate HSE division to identify the weaknesses and the most relevant safety-related issues experienced by the facilities within these periods. In short, they wanted the bad news and appointed others to investigate and work “*as their eyes and ears*”, a kind of attitude suggested by Hopkins when describing mindful leaders (Hopkins, 2008, p. 115). The scope of the work included two Operational Units and the goals of the study were thoroughly explained to the respective general managers, as well as the asset HSE and safety managers. Hence, everyone started from the assumption that significant safety problems likely existed. With this mindset, the corporate safety expert assigned to lead this study was able to raise and discuss the problems without anybody feeling undermined by the duly identified issues.

A more practical example of the study outcomes will be presented below, confirming that mindful leadership is essential to reduce the risks of major accidents. But this successful story also raises the question of how to extend this kind of individual mindful behavior and attitude to the organization as a whole. Putting it another way, how to achieve a sort of collective mindfulness? We will turn to this point at the end of this section to discuss the role of the organizational structure in achieving this goal. All the discussions will be based on the following example, where a substandard practice adopted during the maintenance campaigns was revealed by this study and immediately suspended by the high-level leaders.

At the start of a shutdown for plant maintenance, there is always a concern about potential costly schedule interruptions due to the difficulties in removing the bolts of flanged joints that have been in service. In order to stay on schedule and avoid increases in plant downtime, the Operational Units decided to apply a hot bolting removal procedure as a pre-shutdown activity. “Hot bolting” is the sequential removal and replacement of bolts fitted to live pressurized flanges. With this procedure, the bolts are removed one at a time, cleaned, lubricated and re-installed while under reduced operating pressure. However, since the activity is conducted on a live plant, it is a potentially hazardous procedure. Due to increased bolting stresses and relaxation of gasket compressions, it increases the risks of fluid leakage and gasket segment blowout (ASME, 2015), with potential for personal and process incidents.

The American Society of Mechanical Engineers (ASME) provides a standard (ASME, 2015) with requirements and guidance to perform this activity. According to this standard, an engineering and risk analysis shall be carried out to establish that the operation can be performed safely. An extensive list of issues to be considered in this analysis is presented, together with other prescriptive requirements. Using this standard (ASME, 2015) as a reference, the E&P Inspection and Maintenance division illustrated in Fig. 8 developed an internal procedure which was followed by the Operational Units to perform the hot bolting removal activity. However, the internal procedure failed to address relevant requirements established within the ASME standard (ASME, 2015). Besides that, the experts required to perform the engineering and risk analysis were not clearly defined, increasing the potential for failures when planning this hazardous activity. These deficiencies were presented by the corporate expert in charge for the study, in a meeting attended by the asset leaders. The recommendation was to immediately suspend this activity, until the internal procedure was completely reviewed to address all the identified issues. Additionally, it was recommended to assess industry available technologies and tools that could be applied to enhance safety in this work practice, complementing the internal procedure with further requirements that were not provided by the referred international standard. But, due to the impacts that the immediate suspension of the procedure would cause in the schedule of the ongoing maintenance campaigns, the issue had to be pushed up the hierarchy for a final decision. The expert in charge for

the study was then able to directly present the situation to the Head of Production Division 1 and finally, to the E&P Director. Both understood the high risks associated with the procedure and the recommendation to immediately suspend this practice was approved, despite the high costly impacts to the ongoing maintenance campaigns schedules. In so doing, these leaders also sent an important message to the organization, clearly informing that safety was the top priority.

While the E&P high-level leaders have proved to be mindful decision makers, the fact that such a deficient procedure was approved at the E&P and applied, without a questioning attitude, within the Operational Units, challenge us to think deeply about the reasons that could explain this lack of collective mindfulness. To understand this organizational behavior, it is worth returning to the structure illustrated in Fig. 8. Firstly, we will focus on the Support to Operations division. Besides the Inspection and Maintenance department, this division has many other technical departments, such as Marine Engineering, Automation, among others. Each department has its own standards. But the structure does not provide a safety function, separated from the business line and with the required authority to intervene with these technical areas, ensuring an independent check at this level of the organization. Although the experts located at the Process Safety division interface with these technical areas and provide safety advice, their position in the chart limits their oversight role. In short, the current structure fails to provide an independent check-and-balance function to identify and monitor signals of potential dangers within the practices and standards adopted by these technical areas.

Now, we can focus on the Operational Units and on the lack of a questioning attitude by the asset safety divisions regarding the hot bolting removal procedure. At this point, it is worth returning to the structure illustrated in Fig. 9, that depicts the position of the asset HSE and safety managers in the organizational chart. They are directly subordinated to the Operational Unit General Manager, who is accountable for the asset production and schedules. As previously discussed, in this kind of asymmetrical matrix structure, the safety function lacks the independence from business pressures. Besides that, the control of rewards exerted by the asset boss can lead these safety managers to experience some psychological incentives such as the need for boss approval, among others human motives already discussed in Section 2. Within this social context, the tension between safety and production goals may end up not being effectively managed and a right balance may not be achieved. Higher risks are accepted for short periods so as not to affect long-term production goals. When critical safety issues are identified, no one wants to come to the conclusion that the associated risks are within the red, that is, intolerable region. Instead of falling at this extreme of the risk spectrum, the risks are assessed as moderate and inappropriately judged as acceptable. With an inadequate risk judgment, unsafe practices may be adopted and, over time, become the normal way of performing the activities, without any further questioning.

With the above discussion as a backdrop, it is possible to conclude that, although mindful leadership is essential to reduce the risks of major accidents and to communicate the values and attitudes that are expected from the members of an organization, the organizational structure is paramount to achieve a collective mindfulness. Among other characteristics, mindful organizations exhibit a constant pre-occupation with failures and are reluctant to simplify interpretations (Weick et al., 1999) that can lead to an improper risk judgement. Diverse checks and balances are promoted, and production pressures are perceived as an obstacle to the maintenance of a broad operational awareness (Weick et al., 1999). Individuals at all levels of the organization present a questioning attitude that avoids complacency. In short, these organizations seek for failures and weaknesses, think about these issues and act on them. But how to achieve this organizational state with a decentralized structure that does not provide independent checks and balances and where the safety function is directly subordinated to line managers in charge for schedules and costs? This

example makes clear that a different structure would be required and that, relying solely on mindful leadership is not enough to achieve a collective mindfulness within the organization.

4. Conclusions

The aim of this paper (Part 1) was to identify typical structural characteristics that can be detrimental to operational safety. The examples discussed in the previous section clearly revealed how a decentralized structure contributed to poor risk decisions, which in turn led to negative consequences. In the first example, operations in a production facility were shut down by the Regulator. In the second, a fire severely injured two operators. In both cases, inadequate risk management decisions were taken solely at business unit level with no involvement from corporate safety specialists. Finally, in the third example, a deficient procedure for hot bolting removal operations was vetoed by high-level business unit leaders immediately after a corporate risk expert had brought the substandard practice to their attention. As a result, the ongoing maintenance campaigns schedules of some production facilities were high costly impacted. The deficient procedure was adopted by the asset teams without a questioning attitude and, if it were not for these mindful leaders, who had asked for the corporate involvement, this inadequate standard could still be in force.

The three examples herein discussed demonstrated that a more centralized and independent design to the operational safety function is fundamental to reduce the risks of major accidents. A more centralized approach to risk management can avoid variations in the standards and practices adopted at asset level; provide effective checks and balances; promote a common understanding of what constitutes acceptable risks and facilitate the development of a state of collective mindfulness within the organization. But all this raises the question of what types of design features could be adopted to handle safety in a more centralized and independent approach even within a decentralized company organized into business units. In a separate paper (Part 2) following on from these discussions, the authors aim to answer this question.

The influence of organizational structures on the way major accident risks are managed can no longer be overlooked. High hazard industries need to comprehend what lies behind their work processes; the backdrop that determine the “way things are done within the organization” (CCPS, 2007), that is, its culture. In hindsight, it is easy to explain a major accident in terms of a defective safety culture. What is not easy is to recognize ahead of time, the organizational factors that create and reinforce cultural traits that progressively undermine safety. The examples herein discussed demonstrated the dangers of a decentralized structure, expanding the comprehension of this organizational factor

and improving the ability to recognize the design influence on operational safety.

References

- API (American Petroleum Institute), 2014. Pressure-relieving and Depressuring Systems. API Standard 521. API Publishing Services, Washington DC, US.
- API (American Petroleum Institute), 2016. Process Safety Performance Indicators for the Refining and Petrochemical Industries. API Recommended Practice 754, 2nd ed. API Publishing Services, Washington DC, US.
- ASME (American Society of Mechanical Engineers), 2015. Article 3.11 – Hot and Half Bolting Removal Procedures in ASME PCC-2-2015 (Repair of Pressure Equipment and Piping). New York, US.
- BP (British Petroleum), 2007. The Report of the BP US Refineries Independent Safety Review Panel. <http://sunnyday.mit.edu/Baker-panel-report.pdf> (accessed 4 June 2018).
- BP (British Petroleum), 2010. Annual Report and Form 20-F 2010. <https://www.bp.com/content/dam/bp/pdf/investors/bp-annual-report-and-form-20f-2010.pdf> (accessed 26 March 2018).
- CAIB (Columbia Accident Investigation Board), 2003. Final Report on Columbia Space Shuttle Accident. -Volume 1. Government Printing Office, Washington, DC, US.
- CCPS (Center for Chemical Process Safety), 2007. Guidelines for Risk-Based Process Safety. John Wiley & Sons, New Jersey, US.
- CCPS (Center for Chemical Process Safety), 2008. Guidelines for Hazard Evaluation Procedures, 3rd ed. John Wiley & Sons, New Jersey, US.
- Colman, A.M., 2015. Dictionary of Psychology, 4th ed. Oxford University Press, Oxford, UK.
- Duncan, R., 1979. What is the Right Organization Structure? Decision Tree Analysis Provides the Answer. Organizational Dynamics, Winter, pp. 59–80.
- Galbraith, J.R., 2009. Designing Matrix Organizations That Actually Work – How IBM, Procter & Gamble, and Others Design for Success. Jossey-Bass – A Wiley Company, San Francisco US.
- Hopkins, A., 2008. Failure to learn: the BP Texas City Refinery Disaster. CCH Australia Ltd, Sydney, Australia.
- Hopkins, A., 2012. Disastrous decisions: the human and organisational causes of the Gulf of Mexico blowout. CCH Australia Ltd, Sydney, Australia.
- Hopkins, A., Maslen, S., 2015. Risky rewards – how company bonuses affect safety. Ashgate, UK.
- IEC (International Electrotechnical Commission)/ISO (International Organization for Standardization), 2009. Risk Management – Risk Assessment Techniques. IEC/ISO 31010. CENELEC, Brussels.
- IAEA (International Atomic Energy Agency), 2013. Human and Organizational Factors in Nuclear Safety in the Light of the Accident at the Fukushima Daiichi Nuclear Power Plant, Vienna, Austria.
- IAEA (International Atomic Energy Agency), 2016. IAEA Safety Glossary – Terminology Used in Nuclear Safety and Radiation Protection – 2016 Revision, Vienna, Austria.
- IOGP (International Association of Oil & Gas Producers), 2011. Process Safety – Recommended Practice on Key Performance Indicators. Report No. 456. London, UK.
- NDJ (National Diet of Japan), 2012. The Official Report of the Fukushima Nuclear Accident Independent Investigation Commission, Tokyo, Japan.
- TEPCO (Tokyo Electric Power Company), 2013. Fukushima Nuclear Accident Summary & Nuclear Safety Reform Plan. http://www.tepco.co.jp/en/press/corp-com/release/betu13_e/images/130329e0802.pdf (accessed 28 May 2019).
- Weick, K.E., Sutcliffe, K.M., Obstfeld, D., 1999. Organising for high reliability: processes of collective mindfulness. Res. Organ. Behaviour 1, 81–123.