Journal of Loss Prevention in the Process Industries 26 (2013) 164–171

Contents lists available at SciVerse ScienceDirect

Journal of Loss Prevention in the Process Industries

journal homepage: www.elsevier.com/locate/jlp

A safety barrier-based accident model for offshore drilling blowouts

Luning Xue [a,*], Jianchun Fan [a], Marvin Rausand [b], Laibin Zhang [a]

[a] Department of Safety Engineering, China University of Petroleum, Beijing, 18 Fuxue Road, Changping, Beijing, China
[b] Department of Production and Quality Engineering, Norwegian University of Science and Technology, NO7491 Trondheim, Norway

ARTICLE INFO

Article history:
Received 10 July 2012
Received in revised form
18 October 2012
Accepted 19 October 2012

Keywords:
Offshore drilling
Blowout
Safety barrier
Accident model
Active failures

ABSTRACT

Blowout is one of the most serious accidents in the offshore oil and gas industry. Accident records show that most of the offshore blowouts have occurred in the drilling phase. Efficient measures to prevent, mitigate, and control offshore drilling blowouts are important for the entire offshore oil and gas industry. This article proposes a new barrier-based accident model for drilling blowouts. The model is based on the three-level well control theory, and primary and secondary well control barriers and an extra well monitoring barrier are established between the reservoir and the blowout event. The three barriers are illustrated in a graphical model that is similar to the well-known Swiss cheese model. Five additional barriers are established to mitigate and control the blowout accident, and event tree analysis is used to analyze the possible consequence chains. Based on statistical data and literature reviews, failures of each barrier are presented. These failures can be used as guidance for offshore drilling operators to become aware of the vulnerabilities of the safety barrier system, and to assess the risk related to these barriers. The Macondo accident is used as a case study to show how the new model can be used to understand the development of the events leading to the accident. The model can also be used as an aid to prevent future blowouts or to stop the escalation of events.

1. Introduction

Offshore drilling, especially deepwater drilling, is a high-risk and high-cost operation, and blowout is one the most serious accidents to a drilling rig and its crew. Oil spill caused by offshore blowouts may result in massive damage to the maritime environment and eco-systems. The Macondo blowout, which caused 11 fatalities, a lost drilling rig, and the largest marine oil spill in the history of the petroleum industry, warns operators that the vigilance to blowouts should never be reduced.

Skogdalen, Utne, and Vinnem (2011) propose measures for preventing offshore oil and gas deepwater drilling blowouts in the various life cycle phases of a well. Their goal is to develop safety indicators that can be used to *prevent* offshore drilling blowouts, and possible barriers to mitigate and control blowouts are therefore not examined. Haugen, Seljelid, and Nyheim (2011) present a risk model for blowouts according to the time sequence of the operations. The model provides relevant risk-influencing factors related to blowout risk, but barriers after the blowout event has occurred are not analyzed in their research. Pitblado and Fisher (2011) propose an incident investigation method built on barrier-based risk assessment diagrams (bow-ties), called BSCAT. The well-established *loss causation model* (Bird, Germain, & Clark, 2003) is used to identify the root causes of the incident. By considering the barriers, one-by-one, this method makes the incident investigation rather straightforward. The BSCAT method might also be used to identify root causes of a specific offshore drilling blowout, and to establish an accident model for offshore drilling blowouts. Unfortunately, such a model has not been established.

The objective of this article is to build an accident model for offshore drilling blowouts based on the *Swiss cheese model* (Reason, 1990). The model will explicitly present the accident progression of an offshore drilling blowout and may be used as a "living" model to prevent future blowout accidents or to intervene into a blowout accident to stop the development, and delimit the damage.

The rest of this article is organized as follows: Section 2 introduces the Swiss cheese model and presents its application in offshore process safety. Section 3 introduces the concept and classification of safety barrier, and discusses barriers in a well. The proposed model, which is based on the three-level well control theory and the Swiss cheese model, is presented in Section 4. The Macondo blowout is analyzed by using the proposed model in Section 5. Finally, conclusions are given in Section 6.

* Corresponding author.
E-mail address: weilaizhixing08@163.com (L. Xue).

0950-4230/$ – see front matter © 2012 Elsevier Ltd. All rights reserved.
http://dx.doi.org/10.1016/j.jlp.2012.10.008

2. The Swiss cheese model and its application in offshore process safety

Accident models can be classified into three categories: (a) sequential models (or simple linear system models), (b) epidemiological models (or complex linear system models), and (c) systematic models (Hollnagel, 2004; Lundberg, Rollenhagen, & Hollnagel, 2009). Sequential models are the simplest, and are often in line with our natural understanding of accidents. These models focus on preventing accidents in comparatively simple systems, e.g., for an operator working with a machine. Epidemiological models can be seen as a response to the demand for more powerful and more complex accident models, and are more comprehensive and better suited for analysis of complicated systems. An important feature of epidemiological models is the concept of latent conditions, which remind the accident investigators to analyze deeper into organizational factors to prevent future accidents. Systematic models describe the characteristic performance on a system level, rather than on the level of specific cause-effect mechanisms or even epidemiological factors. A noticeable feature of systemic models is the sharp end–blunt end relationships that extends the scope of accident analysis to regulators and the government level – even morals and social norms will be analyzed.

There are two reasons for choosing the Swiss cheese model as basis of the proposed model in this article:

1. The well control operations can be divided into distinct phases (see Section 3.2) and these operations can be considered as safety barriers in the Swiss cheese model.
2. The proposed model is intended to be used by offshore drilling contractors and operators to identify vulnerabilities in their safety barrier systems, and thereby to prevent, control, and mitigate blowouts. This is analogous to the Swiss cheese model.

Reason (1990) claims that accidents can be seen as the result of interrelations between real time "unsafe acts" of operators and latent conditions. He formulates his views based on the Swiss cheese model in Fig. 1 (Reason, Carthey, & De Leval, 2001). The model is highly pedagogical and has been used by a large number of safety analysts around the world and in many different industries (Reason, Hollnagel, & Paries, 2006).

Kujath, Amyotte, and Khan (2009) propose a special version of the Swiss cheese model for oil and gas process accidents with five categories of barriers.

1. Release prevention
2. Ignition prevention
3. Escalation prevention
4. Harm prevention
5. Loss prevention

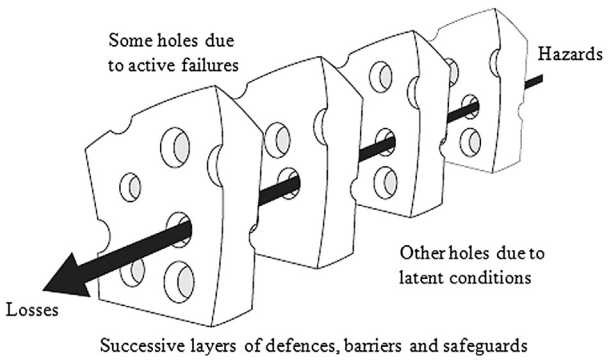


Fig. 1. Swiss cheese model adapted from Reason et al. (2001).

Their accident model starts by reducing the likelihood of hydrocarbon release and applies successive safety barriers to minimize the escalation of events. Each safety barrier is further branched to highlight applicable safety barrier sub-elements. The accident model of Kujath et al. (2009) is extended by Rathnayaka, Khan, and Amyotte (2011), who add a safety analysis procedure that demonstrates how their process accident model is integrated into process system safety. The analysis procedure is called *system hazard identification, prediction, and prevention* (SHIPP). Their extended process accident model is shown in Fig. 2 and has five main safety barriers in a sequence together with two additional barriers that influence these five barriers, a management and organizational barrier and a human factor barrier.

The oil company Shell has adopted the TRIPOD methodology (Hudson et al., 1991, 1994) for safety management. In TRIPOD, accidents occur when unsafe acts and triggering events outdo the available defenses. Underlying causes behind the immediate failures are regarded as important in TRIPOD and are latent failures that are present for a long time. TRIPOD is also derived from the Swiss cheese model.

The Swiss cheese model is a conceptual framework and is a heuristic explanatory means for communicating how accidents can occur in complex systems. It conveys the fact that no single failure, human or technical, is sufficient to cause an accident. On the contrary, an accident involves the coexistence of several contributing factors arising from different levels of the system (Reason et al., 2006). The Swiss cheese model presents a simple, but effective way to model a specific accident. To build the Swiss cheese model for a specific accident, the analyst needs to identify the barriers, and then their failures. Barrier (or defense) is the basic element in this model. In the next section, the safety barrier concept is introduced.

3. Safety barrier

3.1. Definition and classification

A *safety barrier* is implemented to protect people, the environment, and assets from hazards or dangers. Different terms with similar meanings (barrier, defense, protection layer, safety critical element, etc.) have been used in various industries, sectors, and countries.

To formally define the concept of safety barrier, we first need to define the term safety barrier function, which is "what" is needed to assure, increase and/or promote safety (De Dianous & Fievez, 2006). Rausand (2011) divides safety barrier functions into proactive and reactive functions according to if their service time is before or after a specific undesired event. Barriers that are intended to function before an undesired event are proactive, while barriers that are intended to function after the event are reactive. In the ARAMIS project, safety barrier functions are divided into "to avoid", "to prevent", "to control", and "to limit, reduce, or mitigate" (De Dianous & Fievez, 2006). Based on experience from a literature survey concerning the understanding of safety barriers in different industries, Sklet (2006) defines safety barrier function as:

> *A barrier function is a function planned to prevent, control, or mitigate undesired events or accidents.*

Prevent means reduction of the likelihood of an undesired event, control means limiting the extent and/or duration of the event to prevent escalation, and mitigate means reduction of the effects of the undesired event.

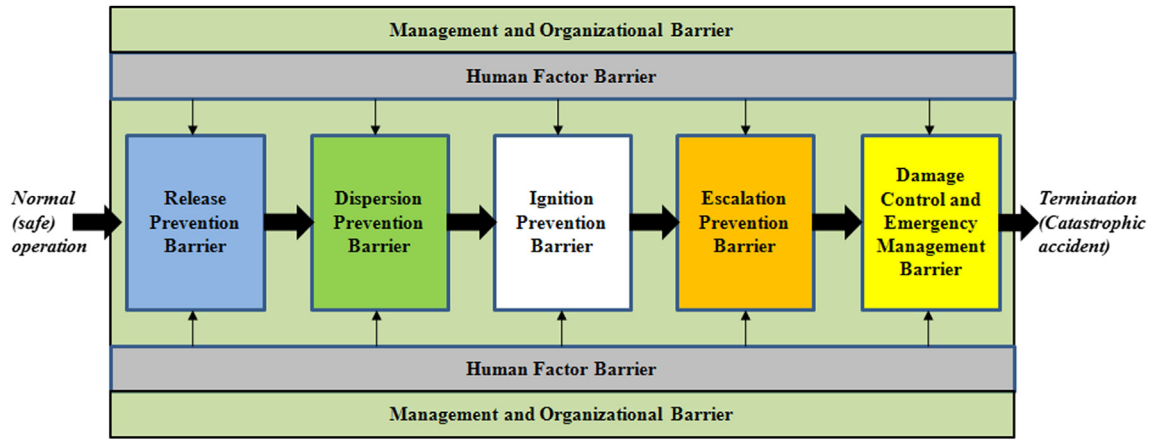


Fig. 2. Process accident model adapted from Rathnayaka et al. (2011).

Correspondingly, Sklet (2006) defines safety barrier as:

A safety barrier is a physical and/or non-physical means planned to prevent, control, or mitigate undesired events or accidents.

He also recommends a way to classify barrier systems as shown in Fig. 3. Sklet's definition and classification of safety barrier are adopted in this article.

3.2. Barriers in a well

In oil/gas wells, the safety barriers are called *well barriers*. NORSOK D-010 (NORSOK, 2004) defines a well barrier as an envelope of one or several dependent barrier elements preventing fluids or gases from flowing unintentionally from the formation, into another formation or to the surface. Well barriers are divided into *primary* well barriers and *secondary* well barriers. Two well barriers must be available during all well activities and operations where a pressure differential exists that may cause uncontrolled outflow from the borehole/well to the external environment. The two-barrier principle is followed both in the UK and the U.S. Gulf of Mexico even if this is not stated explicitly in the regulations (Holand, 1997).

Except for the two-barrier principle, another important issue is the *three-level well control theory*. According to blowout development stages and well control activities, well control operation can be divided into three phases. These three phases include primary well control, secondary well control, and tertiary well control (WCTMWG, 2008).

1. *Primary well control* means using the drilling fluid column to control the reservoir pressure during normal drilling or drilling through the high-pressure hydrocarbon zone. The target of the primary well control is to maintain the well integrity in the drilling cycle.
2. *Secondary well control* is the process of rebuilding the pressure balance through shut-in and circulating operations when the well integrity is broken and a kick or blowout occurs. Secondary well control is the key of the whole well control practice.
3. *Tertiary well control* is the technologies of recovering control of the wellhead after the blowout.

Compared to the two-barrier principle, the three-level well control theory is more comprehensive, and it contains human/operational barriers mentioned in Sklet's safety barrier classification. In addition, some failures of secondary barrier elements in the two-barrier principle can damage the integrity of the primary barrier, such as casing leaks and downhole plug failures that can cause lost circulation (API, 2006). Holand's primary barrier failures that cause drilling blowout (Holand, 1997) also include failures of secondary

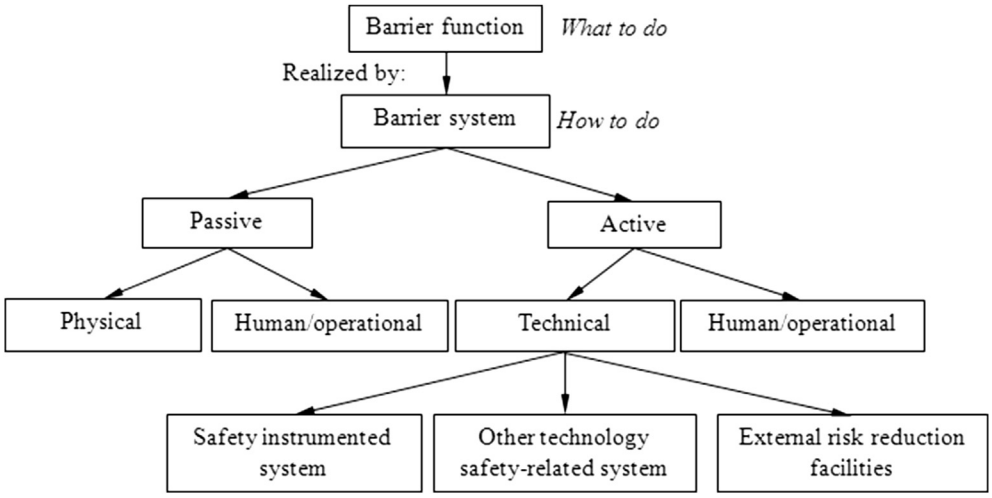


Fig. 3. Classification of safety barriers adapted from Sklet (2006).

barriers. Therefore, the three-level well control theory will be the basis of the proposed model, and barriers in a well will include primary and secondary well control barriers that are different from the primary and secondary barriers in NORSOK D-010.

Primary well control barriers include physical barriers and active human/operational barriers. Physical barriers comprise the fluid column (including cement slurry) and relevant physical barriers to keep its integrity, such as casing and drilling string. Human/operational barriers are operator procedures that contribute to the primary well control activity. The essential function of a primary well control barrier is to prevent a well kick. The secondary well control barrier contains physical barriers on the wellhead, active barriers like the blowout preventer (BOP), inside blowout prevention instruments, diverter, and active human/operational barriers directing well control response after well kick is "signaled".

4. Proposed model

4.1. Safety barriers in the model

Based on the three-level well control theory and the safety barrier functions proposed by Sklet (2006), a new accident model for offshore drilling blowouts is presented in Fig. 4. Table 1 describes the consequences in Fig. 4. For a more thorough explanation of the consequences and the abnormal events in this model, the reader is referred to Rathnayaka et al. (2011). The model in Fig. 4 integrates the Swiss cheese model and event tree analysis. It may also be seen as an integration of the Swiss cheese model and the bow-tie method (e.g., see Rausand, 2011). To illustrate the sequence and the functions of the primary well barrier, the secondary well barrier, and the special well monitoring barrier between them, fault tree analysis in the bow-tie method is replaced by a graphical model that is similar to the Swiss cheese model. The possible scenarios after a blowout has occurred are developed by event tree analysis.

As shown in Fig. 4, a well kick will occur when the primary well control barrier has failed. If the well kick is not diverted, or stopped by shutting the well timely, it will develop into a blowout. The primary and secondary well control barriers are barriers to prevent blowout. Well monitoring is defined as a special barrier and placed between these two barriers. It is illustrated as a slice with dashed borders because successful well monitoring cannot stop the well kick by itself. In drilling well control operations, well monitoring is essential to keep the primary well control barrier intact, or restore a failed one. Meanwhile, once a well kick is "signaled", the normal operations will be suspended, and the secondary well control barrier activated to maintain the well integrity (Goins & Sheffield, 1983). Therefore, well monitoring can be seen as a "back guard" of the primary well control barrier, and as a "vanguard" of the secondary well control barrier. Successful well monitoring is essential to prevent a blowout. The standard well kick warning signs in offshore drilling include (IADC, 2002):

- Flow rate increase
- Pit volume increase
- Rate of penetration increase
- Reduced pump pressure
- High gas units
- Sudden torque increase
- Change in mud chlorides
- While tripping, hole not taking the proper amount of fluid
- Well flow with pump shutdown
- Increasing rate of flow on return flow during connections

The drill crew should monitor all the signals mentioned above and special signals specified to be monitored. If any one of them cannot be monitored accurately, or ignored, the well monitoring is said to be failed.

Once a blowout occurs, there are five categories of barriers to control or mitigate the blowout event. The ignition prevention barrier includes physical barriers (e.g., hot surface shielding), technical barriers (e.g., fire and gas system), and human/operational barriers (e.g., work permit procedures). The ignition prevention barrier has failed when there is a fire or explosion after the blowout. The escalation prevention barrier includes passive barriers (e.g., firewalls and blast walls) and technical barriers (e.g., firefighting system, and emergency disconnection system). The escalation prevention barrier has failed if there is a continuous fire or a series of explosions once the blowout has been ignited. The emergency response barrier includes physical barriers (e.g., personnel protection equipment), passive human/operational barriers (e.g., muster road), technical barriers (e.g., energy buffering or diversion system), and active human/operational barriers (e.g., emergency response plan). The emergency response barrier is said to be successful if no one lost his life, and no permanent major disability. Blowout control or oil spill control is the process of *reestablishing* or *establishing* physical barriers, technical barriers to control blowout or oil spill based on well planned active human/operational barriers. The blowout control barriers are said to be successful if there is no need to activate the oil spill control barrier. The oil spill control barrier is successful if the effect to marine ecosystem can be limited and localized. As shown in Fig. 4, due to high population density on the rig, high energy and potential toxicity of the hydrocarbon flow, and potential damage to marine ecology system, a blowout can develop into an accident, a catastrophic accident, or a disaster even if only one or two barriers after the blowout fail.

4.2. Failures of safety barriers

In the Swiss cheese model, some "holes" in the barriers are due to active failures, while other "holes" are due to latent conditions. Latent conditions are typically connected to the organizational factors influencing the safety of a system. The fault trees in Fig. 5 present the barrier failures in the proposed model, and include active failures and organizational failures, shown as dashed textboxes. The identification of active failures are based on a careful review of literature, standards, and guidelines (e.g., Adams & Kuhlman, 1993; API, 2006; CNPC, 2006; CSIC-SY, 2005a; CSIC-SY, 2005b; Danenberger, 1993; Holand, 1997; Holand & Skalle, 2001; IADC, 2002; Rathnayaka et al., 2011), and discussions with personnel from the Development Research Department of China National Offshore Oil Corporation (CNOOC) Research Center. Organizational factors are identified based on a review of literature on organizational factors that may influence offshore oil and gas process industry (e.g., Attwood, Khan, & Veitch, 2006; Aven, Sklet, & Vinnem, 2006; Gordon, 1998; IADC, 2010; Schönbeck, Rausand, & Rouvroye, 2010; Sklet et al., 2010; Øien, 2001), and summarizing lessons learned from the Macondo blowout (Commission, 2011a; Commission, 2011b; DHSG, 2010; DHSG, 2011; Skogdalen et al., 2011; Skogdalen, Khorsandi, & Vinnem, 2012). The logic relationships between the top events and relevant failures are achieved through OR gates in fault trees (Rausand & Høyland, 2004), meaning that every failure will cause a "hole" in the relevant barrier.

The way the energy flow passes through the last four barriers when the barriers have failed, is different from the traditional Swiss cheese model. The more holes in the barrier, the higher the damage or harm.

This characteristic is obvious for escalation prevention barrier through its possible failures shown in Fig. 5. The rig personnel may be in different locations performing different operations. All the methods in Fig. 5 to mitigate casualties should therefore be available

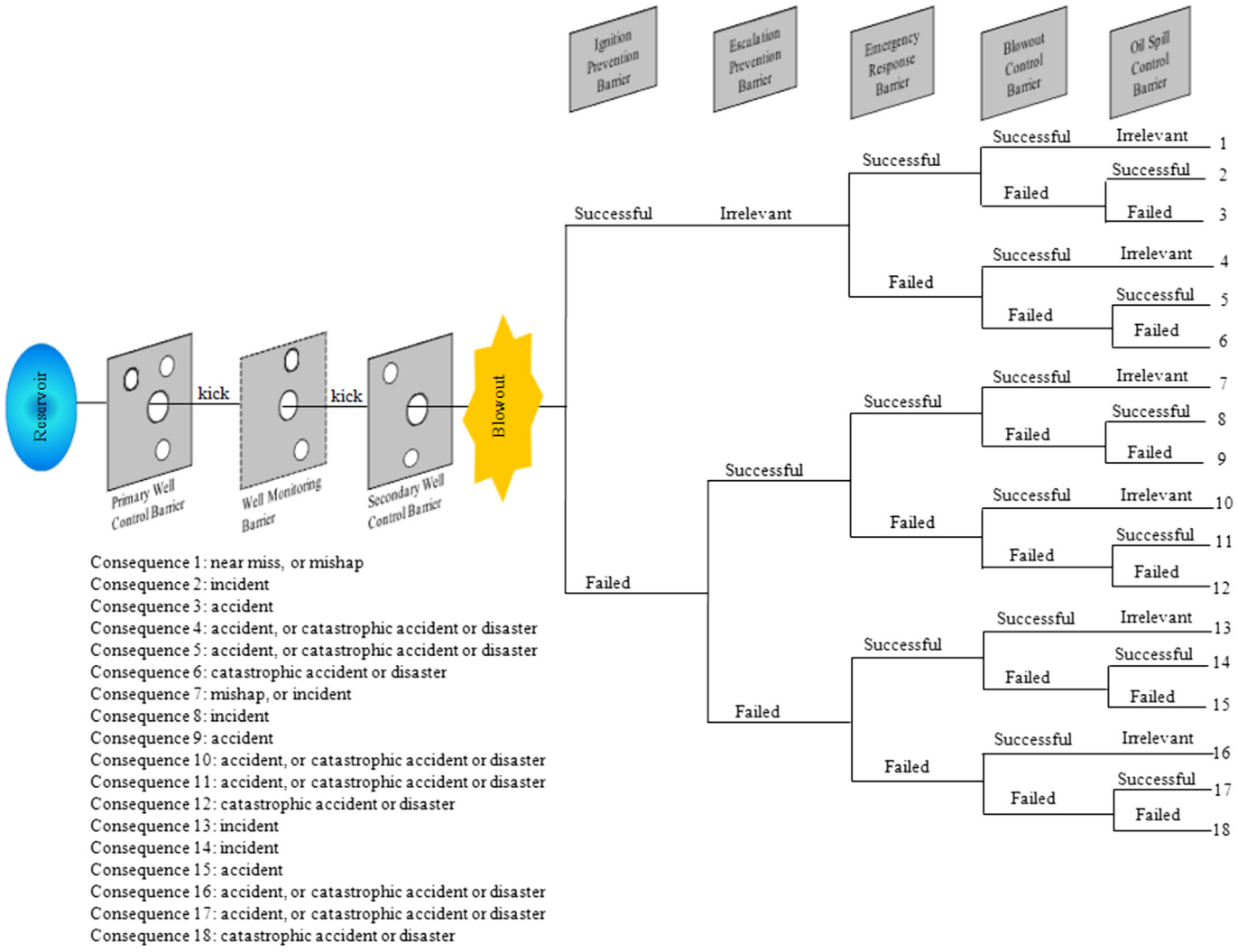


Fig. 4. Offshore drilling blowout accident model.

in an emergency, and each failure may increase the number of casualties. For the blowout control barrier, only one blowout control method can be tried at the same time. Therefore, the more failures that occurs, the longer the blowout continues, with more hydrocarbons released and more damage. If one of the four methods to control the oil spill is successful, the oil spill control barrier may be claimed to be successful. In practical operations, however, only one method is available in each particular situation. Many states in the USA have, for example, preapproved the use of dispersants outside three nautical miles from shore and/or in water depths greater than 10 m (Chapman, Purnell, Law, & Kirby, 2007). In some countries, particularly those with recurring rough seas, which can make mechanical response problematic, oil dispersal may be the single available method (Lessard & DeMarco, 2000). Therefore, the four different oil spill control methods in Fig. 5 may not all be available in a specific accident. Oil collection is the optimal method to control the oil spill.

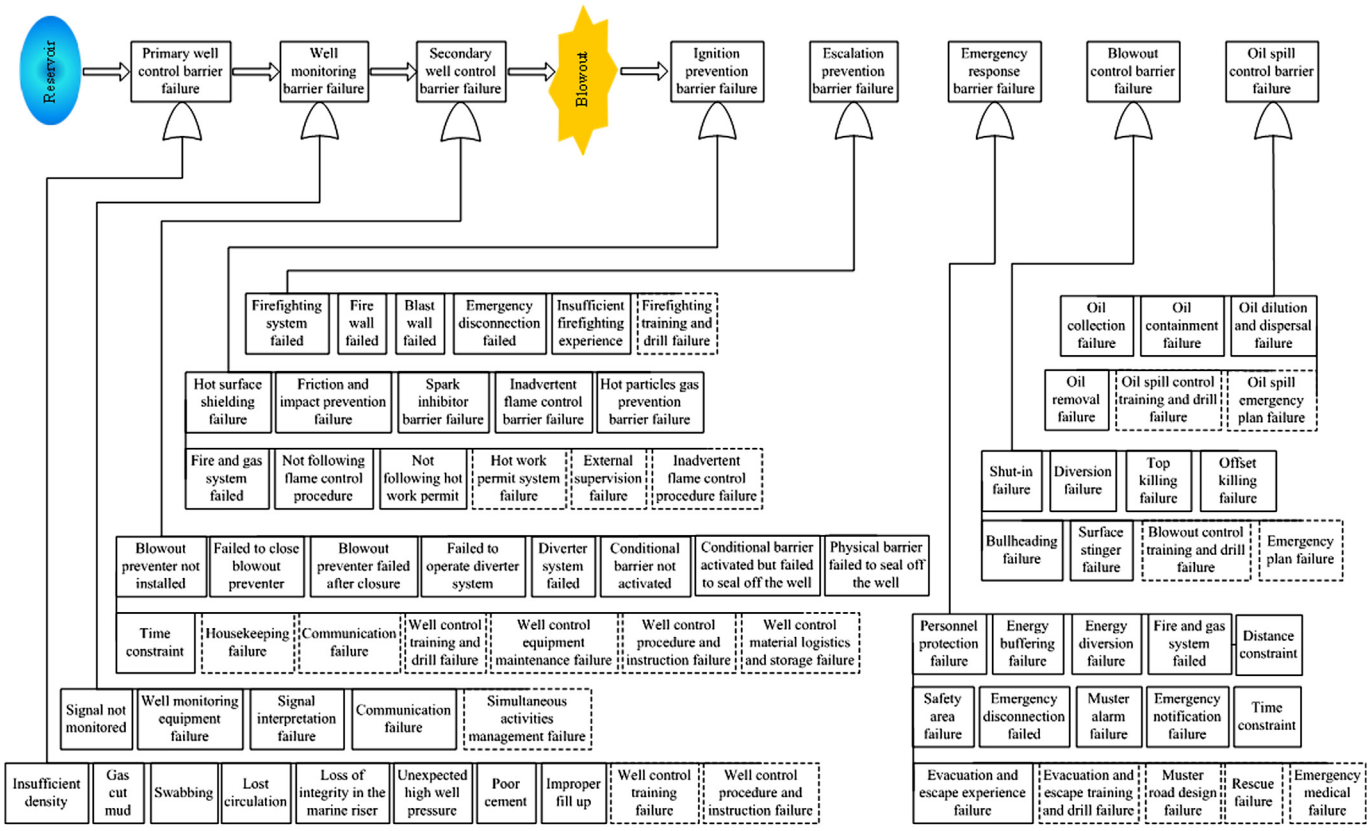
Table 1
Abnormal events from Rathnayaka et al. (2011).

Abnormal events	Description
Near miss	An event that does not result in an actual loss but that has the potential to do so.
Mishap	An event that could cause minor health effects, and/or minor impact to property and the environment.
Incident	An event that could cause considerable harm or loss, or a major health effect or injury, localized damage to assets and environment, or considerable loss of production.
Accident	An event that may cause one or more fatalities, or permanent major disabilities, and/or heavy financial loss. It may also cause major impact to the environment.
Catastrophic accident or disaster	An event that could cause multiple fatalities, extensive damage to property, system and production. It may also cause massive environmental effects.

5. Case study

In this section, the Macondo blowout accident in the U.S. Gulf of Mexico is analyzed by the proposed model. The case study shows that the investigation results are in line with the results obtained from using the model. The model further shows how the accident could have been prevented or mitigated if relevant barriers were kept intact. The highlighted failures in Fig. 6 are the ones that are likely to have occurred in this accident.

On the evening of April 20, 2010, a blowout happened in the Macondo well and ignited immediately, resulting in explosions and fire on Transocean's *Deepwater Horizon* drilling rig. Eleven people lost their lives, and 17 others were injured. The fire continued for



Note: The event sequences after blowout are shown by event tree in Fig. 4.

Fig. 5. Failures of barriers in the proposed model.

36 h until the rig sank. Hydrocarbon continued to flow for 87 days, causing a massive oil spill (BP, 2010).

In the proposed model, the primary well barrier is analyzed first. The Macondo blowout occurred during a negative pressure test before abandonment. Therefore, the pressure of the fluid column was, on purpose, lower than the formation pressure. The event "poor cement" is highlighted as a reason for the primary well barrier failure because the annular cement was the only barrier resisting the reservoir pressure during the negative pressure test, and it did not isolate the hydrocarbon zones (Commission, 2011a).

The second barrier to be considered is the well monitoring barrier. The event "signal not monitored" is highlighted because the well monitoring system on *Deepwater Horizon* did not have adequate coverage, as there was no camera installed to monitor the returns sent overboard and no sensor to indicate whether the valve sending returns overboard was open or closed. In the negative pressure test, the highly viscous spacer might have clogged the open kill line and some of the sensors were not particularly accurate, which highlights the "well monitoring equipment failure" in Fig. 6. The "signal interpretation failure" is highlighted because, during the negative test and displacement, despite noticing the anomalies and taking time to discuss them, the rig crew did not recognize that a kick was under way. The organizational factor "simultaneous activities management failure" is also highlighted because the crew on *Deepwater Horizon* engaged in a number of concurrent activities that could have interfered with the well monitoring activity (Commission, 2011a).

The secondary well barrier is analyzed next. The events "well control training and drill failure" and "well control procedure and instruction failure" are highlighted as the two reasons why the personnel did not close the shear ram preventer when they noticed the well kick. Insufficient training on how to respond to low-frequency, high-risk events explains why the rig crew only initiated the "normal and appropriate" responses to a typical kick – activating the annular preventer and the variable bore rams (Commission, 2011a). Transocean's well control handbook did not offer any specific guidance on the use of the blind shear ram. In fact, these two failures also made the personnel decide to divert the well flow to the mud gas separator, not overboard.

The ignition prevention barrier is analyzed next. The precise cause of ignition may never be known (Commission, 2011a). The "fire and gas system failure" is highlighted because this is the most likely reason why the first ignition occurred in engine room #3, which was testified by two Transocean crew members on the rig. Although the fire and gas system's visual and audible alarms on *Deepwater Horizon* were automatically triggered upon gas detection, there were no automated actions to close the fire dampers or shutdown the engine room ventilation fans.

The next barrier to analyze is the escalation prevention barrier. There is little information about the escalation barrier on the rig, so the exact failures of this barrier are unknown. The "emergency disconnection failure" is highlighted because, although the personnel pushed the button for the emergency disconnection system, the blind shear ram or the remainder of the emergency disconnect system failed to be activated. This left the rig attached to the riser. Gas continued to flow up the riser, fueling the fires on the rig (Commission, 2011a).

The emergency response barrier is analyzed next. The "muster alarm failure" is highlighted because the general alarm did not sound immediately after the blowout and first explosion (Skogdalen et al.,

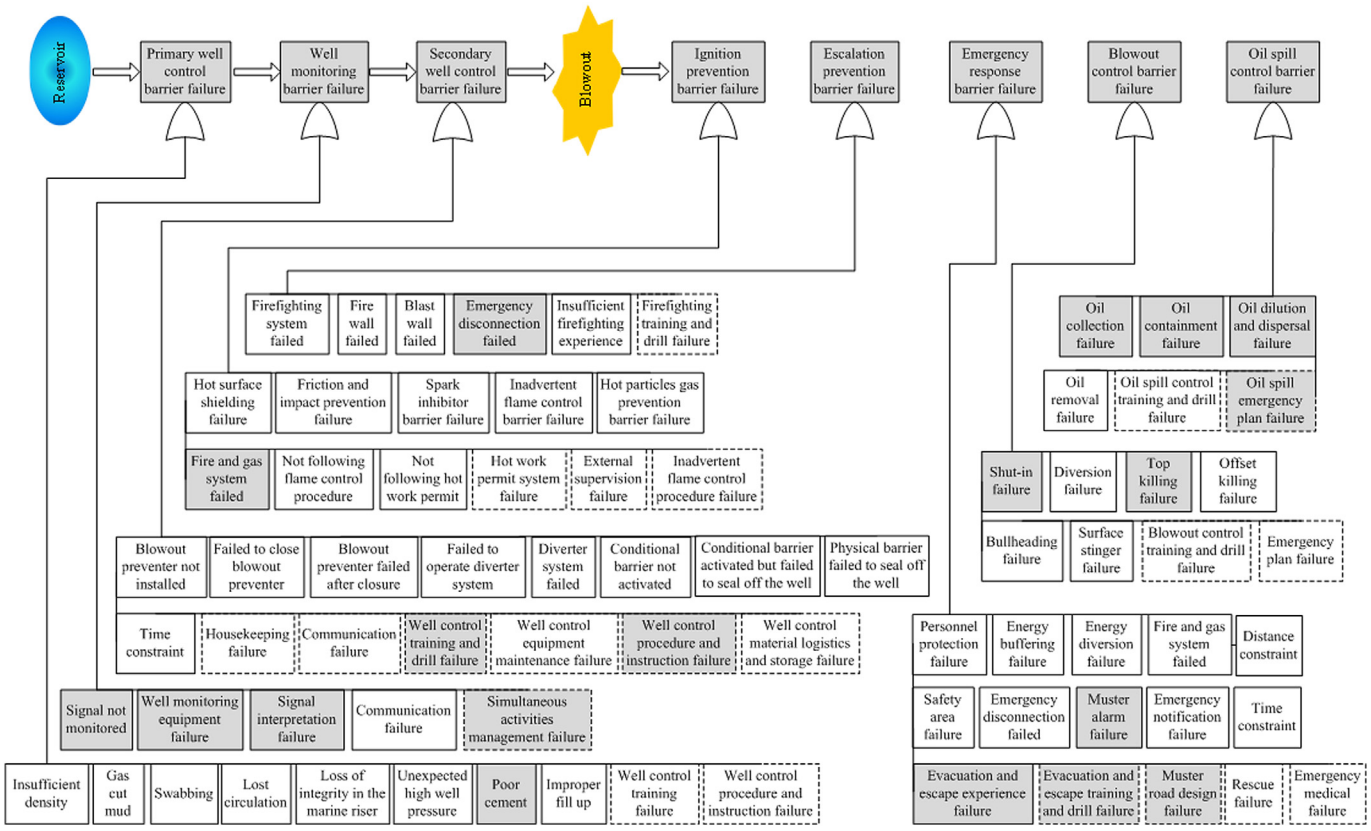


Fig. 6. Failures of barriers in Macondo accident.

2012). The "evacuation and escape experience failure", the "evacuation and escape training and drill failure", and the "muster road design failure" are highlighted as the reasons of the chaotic overwhelming process and blocked escape routes, which made the evacuation and escape difficult and complicated (DHSG, 2011).

The next barrier to analyze is the blowout control barrier. The "shut-in failure" is highlighted because the well failed to be shut by the emergency shutdown systems, activating the blowout preventer shear ram by automatic mode function and remotely operated vehicle. The "top killing failure" is also highlighted because the attempt of killing the well by injecting heavy mud into the BOP also failed (BP, 2010; DHSG, 2011).

Finally, the oil spill control barrier is analyzed. It is classified as failed due to the national significance of the oil spill. As shown in Fig. 6, three active failures and an "oil spill emergency plan failure" are highlighted. For the "oil collection failure", at least two approaches for oil collection were tried. The first was collecting oil by a containment dome, which failed due to hydrate formation. The other was through a "top hat", which failed due to insufficient capacity of the two oil collection vessels (Commission, 2011b). The event "oil containment failure" is highlighted because much of the containment boom deployed along the Gulf coast was proved ineffective in the oil spill cleanup efforts (Grier, 2010). For the "oil dilution and dispersal failure", the two dispersants that BP used to break up the oil spill were not rated as effective or as safe for marine life as at least 12 other government-approved dispersants on the market (Guarino, 2010). BP's response plan was outdated and amateurish seen in relation to the actual oil spill (Commission, 2011b), which highlights "oil spill emergency plan failure".

In the Macondo blowout accident, all barriers in the proposed model failed and led to consequence 18 in Fig. 4, catastrophic accident. If the primary well control barrier had been intact, the well kick would not occur. If the well monitoring barrier were kept integrated, the displacement would be suspended, and the well kick would have no chance to develop further into a blowout. If the secondary well control barrier were intact, the blowout might be stopped by closing the shear ram immediately. After the blowout, if the ignition prevention barrier were successful, the explosions could be avoided, and it would be very likely that the emergency disconnect system could be activated successfully (Commission, 2011a). As the emergency disconnect system could disconnect the rig from the riser and shut-in the well, escalation prevention and blowout control barriers might not have failed. Therefore, the "energy flow" could change path to 1 or 4 in Fig. 4, which means that the oil spill disaster could have been avoided. The ignition prevention failure and the escalation prevention failure also made emergency response almost impossible to be successful. In practice, there are some dependencies between the barriers in the model. These dependencies may be due to different safety functions integrated in the same safety barrier element, or complicated cascading effects (Khan & Abbasi, 2001). Analysis of these dependencies is outside the scope of this article. The simplest and safest way to prevent blowout accident is certainly keeping all the safety barriers intact.

6. Conclusions and discussion

This article has proposed a new accident model for offshore drilling blowouts, based on the Swiss cheese model and the three-level well control theory. In addition to the traditional primary and secondary well control barriers, well monitoring is introduced as an independent and special barrier between the two mentioned barriers. Successful well monitoring is crucial to remedy the incomplete primary well barrier, or activate the secondary well

barrier timely to prevent blowout. After the blowout, five safety barriers to mitigate or control the possible damage/harm to the drilling rig, the drilling crew, and the marine ecology system are established. The potential scenarios are identified and examined by event tree analysis.

Identification of active barrier failures in the proposed model is based on statistical data, discussions with experienced personnel, and careful review of available specifications and recommendations. These failures, especially the ones based on statistical data or accident reports, are still conceptual because the records or reports are always not sufficiently detailed. To find pertinent preventive measures of these failures, the operator who uses this model to prevent, mitigate, and control the blowout should analyze these failures in detail. The organizational factors presented in the model are quite simple. Failures of these factors will directly and individually cause relevant barriers failures. The organizational factors and their influences on the barriers still need more research.

The case study shows that the conclusions from the investigations into the Macondo blowout fit well with the proposed model. It reveals some dependencies between safety barriers in the model. These dependencies may make the real scenarios more complicated, where two or more barriers may fail simultaneously or within a very short time interval. Common cause failures of the safety system, including common cause failures of the two well control barriers, are not analyzed in the proposed model. Systematic and quantitative analysis of these failures is of major importance to enhance the reliability of the safety barrier system. This is an important topic for future research.

Acknowledgment

The authors would like to acknowledge the help of Hui Jin from Norwegian University of Science and Technology during preparing this paper. The authors also want to acknowledge personnel from Development Research Department in China National Offshore Oil Corporation (CNOOC) Research Center for their precious advice about active failures of barriers in the proposed model.

The research work is sponsored by National Science and Technology Major Project *Risk Analysis and Control Technology for Drilling and Completion Operations in Liwan 3-1 and Its Peripheral Gas Fields* during 12th five-year plan of China.

References

Adams, N. J., & Kuhlman, L. G. (1993). *Contingency planning for offshore blowouts*. Paper # 7120. SPE.

API. (2006). *Recommended practice for well control operations, Recommended practice 59* (2nd ed).

Attwood, D., Khan, F., & Veitch, B. (2006). Occupational accident models—where have we been and where are we going? *Journal of Loss Prevention in the Process Industries, 19*(6), 664–682.

Aven, T., Sklet, S., & Vinnem, J. E. (2006). Barrier and operational risk analysis of hydrocarbon releases (BORA-Release) Part I. Method description. *Journal of Hazardous Materials, 137*(2), 692–708.

Bird, F. E., Germain, G. L., & Clark, M. D. (2003). *Practical loss control leader* (3rd ed.). Georgia: Det Norske Veritas (USA), Inc.

BP. (2010). *Deepwater horizon accident investigation report*.

Chapman, H., Purnell, K., Law, R. J., & Kirby, M. F. (2007). The use of chemical dispersants to combat oil spills at sea: a review of practice and research needs in Europe. *Marine Pollution Bulletin, 54*(7), 827–838.

CNPC (China National Petroleum Corporation). (2006). *Blowout accidents in China national petroleum Corporation*. Beijing, China: Petroleum Industry Press (in Chinese).

Commission. (2011a). *Chief Counsel's Report 2011. National Commission on the BP Deepwater Horizon Oil Spill and Offshore Drilling*.

Commission. (2011b). *Report to the President. National Commission on the BP Deepwater Horizon Oil Spill and Offshore Drilling*.

CSIC-SY. (2005a). *SY/T 6426-2005: Specification for well control technology of drilling* (in Chinese).

CSIC-SY. (2005b). *SY/T 5087-2005: Recommended practice for safe drilling operations involving hydrogen sulfide* (in Chinese).

Danenberger, E. P. (1993). *Outer Continental Shelf drilling blowouts, 1971–1991*. Paper # 7248. SPE.

De Dianous, V., & Fievez, C. (2006). ARAMIS project: a more explicit demonstration of risk control through the use of bow–tie diagrams and the evaluation of safety barrier performance. *Journal of Hazardous Materials, 130*(3), 220–233.

DHSG. (2011). *Final report on the investigation of the Macondo well blowout*.

DHSG (Deepwater Horizon Study Group). (2010). *The Macondo blowout, 3rd Progress Report*.

Goins, W. C., & Sheffield, J. R. (1983). *Blowout prevention* (2nd ed.). Houstan, Texas: Gulf Publishing Company.

Gordon, R. P. E. (1998). The contribution of human factors to accidents in the offshore oil industry. *Reliability Engineering & System Safety, 61*(1–2), 95–108.

Grier, P. (2010). *Containment boom effort comes up short in BP oil spill* [cited 03.09.12]. Available from: http://www.csmonitor.com/USA/2010/0611/Containment-boom-effort-comes-up-short-in-BP-oil-spill.

Guarino, M. (2010). *In Gulf oil spill, how helpful – Or damaging – Are dispersants?* [cited 03.09.12]. Available from: http://www.csmonitor.com/USA/2010/0515/In-Gulf-oil-spill-how-helpful-or-damaging-are-dispersants.

Haugen, S., Seljelid, J., & Nyheim, O. M. (2011). *Major accident indicators for monitoring and predicting risk levels*. Paper # 140428, SPE.

Holand, P. (1997). *Offshore blowouts: Causes and control*. Houston, Tex: Gulf Publ. Co.

Holand, P., & Skalle, P. (2001). *Deepwater kicks and BOP performance, unrestricted version*. Trondheim: SINTEF.

Hollnagel, E. (2004). *Barrier and accident prevention*. Hampshire, UK: Ashgate.

Hudson, P. T. W., Groeneweg, J., Reason, J. T., Wagenaar, W. A., Van der Meeren, R. J. W., & Visser, J. P. (1991). *Application of TRIPOD to measure latent errors in north sea gas platforms: Validity of failure state profiles*. Paper # 23293. SPE.

Hudson, P. T. W., Reason, J. T., Wagenaar, W. A., Bentley, P. D., Primrose, M., & Visser, J. P. (1994). *Tripod delta: Proactive approach to enhanced safety*. Paper # 27846. SPE.

IADC. (2002). *Deepwater well control guidelines*. International Association of Drilling Contractors.

IADC. (2010). *Health, safety and environmental case guidelines for mobile offshore drilling units*. International Association of Drilling Contractors.

Khan, F. I., & Abbasi, S. A. (2001). An assessment of the likelihood of occurrence, and the damage potential of domino effect (chain of accidents) in a typical cluster of industries. *Journal of Loss Prevention in the Process Industries, 14*(4), 283–306.

Kujath, M. F., Amyotte, P. R., & Khan, F. I. (2009). A conceptual offshore oil and gas process accident model. *Journal of Loss Prevention in the Process Industries, 23*(2), 323–330.

Lessard, R. R., & DeMarco, G. (2000). The significance of oil spill dispersants. *Spill Science & Technology Bulletin, 6*(1), 59–68.

Lundberg, J., Rollenhagen, C., & Hollnagel, E. (2009). What-you-look-for-is-what-you-find – the consequences of underlying accident models in eight accident investigation manuals. *Safety Science, 47*(10), 1297–1311.

NORSOK. (2004). *NORSOK standard: Well integrity in drilling and well operations, D-010*. Norwegian Technology Centre.

Øien, K. (2001). A framework for the establishment of organizational risk indicators. *Reliability Engineering & System Safety, 74*(2), 147–167.

Pitblado, R., & Fisher, M. (2011). *Novel investigation approach linking management system and barrier failure root causes*. Paper # 22329. SPE.

Rathnayaka, S., Khan, F., & Amyotte, P. (2011). SHIPP methodology: predictive accident modeling approach. Part I: methodology and model description. *Process Safety and Environmental Protection, 89*(2), 75–88.

Rausand, M. (2011). *Risk assessment: Theory, methods, and applications*. Hoboken, NJ: Wiley.

Rausand, M., & Høyland, A. (2004). *System reliability theory: Models, statistical methods, and applications* (2nd ed.). Hoboken, NJ.: Wiley (Chinese Version).

Reason, J. (1990). The contribution of latent human failures to the breakdown of complex systems. *Philosophical Transactions of the Royal Society of London Series B, Biological Sciences, 327*(1241), 475–484.

Reason, J. T., Carthey, J., & De Leval, M. R. (2001). Diagnosing "vulnerable system syndrome": an essential prerequisite to effective risk management. *BMJ Quality & Safety, 10*(Suppl 2), ii21–ii25.

Reason, J., Hollnagel, E., & Paries, J. (2006). *Revisiting the «Swiss cheese» model of accidents*. France: EUROCONTROL Experimental Center.

Schönbeck, M., Rausand, M., & Rouvroye, J. (2010). Human and organisational factors in the operational phase of safety instrumented systems: a new approach. *Safety Science, 48*(3), 310–318.

Sklet, S. (2006). Safety barriers: definition, classification, and performance. *Journal of Loss Prevention in the Process Industries, 19*(5), 494–506.

Sklet, S., Ringstad, A. J., Steen, A. S., Tronstad, L., Haugen, S., Seljelid, J., et al. (2010). *Monitoring of human and organizational factors influencing the risk of major accidents*. Paper # 126530. SPE.

Skogdalen, J. E., Khorsandi, J., & Vinnem, J. E. (2012). Evacuation, escape, and rescue experiences from offshore accidents including the Deepwater Horizon. *Journal of Loss Prevention in the Process Industries, 25*(1), 148–158.

Skogdalen, J. E., Utne, I. B., & Vinnem, J. E. (2011). Developing safety indicators for preventing offshore oil and gas deepwater drilling blowouts. *Safety Science, 49*(8–9), 1187–1199.

WCTMWG (Well Control Training Material Writing Group of Sinopec Group). (2008). *Drilling well control technology*. Shandong, Dongying: Press of University of Petroleum, China (in Chinese).