Journal of Loss Prevention in the Process Industries 67 (2020) 104260

Contents lists available at ScienceDirect

Journal of Loss Prevention in the Process Industries

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

Safety barriers: Research advances and new thoughts on theory, engineering and management

Yiliu Liu

Department of Mechanical and Industrial Engineering, Norwegian University of Science and Technology, S. P. Andersens 3, Trondheim, 7491, Norway

ARTICLE INFO

Keywords:
Safety barrier
Safety-instrumented system
Barrier theory
Barrier engineering
Barrier management

ABSTRACT

Safety barriers include physical and non-physical means in different industries for preventing the occurrences of hazardous events and mitigating the consequences in case they have occurred. After clarifying the relevant terminologies, this article reviews the literature in the domain of safety barriers in the recent decade, and categorizes these studies into barrier theory, barrier engineering and barrier management. Classifications of barriers, performance measures, modeling approaches and data-driven analysis for safety barriers are reviewed as parts of barrier theories. In the engineering section, the research advances are presented in accordance with design for reliability and safety, test and maintenance strategies, responses to dependent failures, and diagnosis and prognosis of degradations. Then, project and process management, human and organizational factors, and standardization and compliance management of safety barriers are summarized. Based on the review of literature, research perspectives on safety barriers for resilience, digital safety, security of barriers, utilizing data, and dealing with intelligence, are highlighted and potential challenges are mentioned. This study is therefore expected to be beneficial to the researchers of system and safety engineering, with systematically streamlining and innovatively categorizing the recent findings and insights.

1. Introduction

Even though no universal definition is existing, safety barriers are always regarded as those physical or non-physical approaches to protect assets from the damage (Sklet, 2006). In road transportation, where the term of safety barriers comes from, barriers originally refer to those concrete obstacles on bridges and road edges to avoid driving out of way, or central reservations of roads to prevent collisions (Szymanek, 2010). With more industries adopting this term, the scope of safety barriers is becoming wider in more applications. For example, in the oil & gas and process industries, safety barriers can be the shutdown valves in a pipeline, blowout preventers or evacuation ways. In a new Deepwater Artificial Seabed (DAS) system, the online risk monitoring system acts as safety barrier (Zhen et al., 2020). Hayes (2012) has deeply discussed the cases of safety barriers in different applications, such as chemical processes, nuclear plants and aviation industries. When safety barriers are technical systems, they can be called as safety-critical systems. By involving instrumentation, electric, electronic, and programmable electronic technologies, safety barriers are regarded as safety instrumented systems (SISs) (IEC 61508, 2010).

In 2006, Sklet contributed a thorough literature review on the definitions and classifications of safety barriers. Barrier analysis were also reviewed in the article of Shahrokhi and Bernard in 2010. However, in the recent decade, especially after the Deepwater Horizon accident in 2010 due to the failure of blowout preventer, a kind of safety barriers, many new research results have been released in this domain. For example, by searching the exact term of "safety barrier" as the keyword within paper topics, 274 articles can be found (by March 2020) on the *web of science*, 213 of which (77.7%) were published since 2009. Although such a simple survey does not 100% reflect the whole situation of studies on safety barriers because researchers often use other names for barriers, but the high publication ratio in the recent 10 years clearly indicates the increasing research interests. A number of papers occurred on the journals with more focuses on specific industries, including *Journal of Loss Prevention in the Process Industries, Nuclear Engineering and Design*, *Process Safety Progress*, and *Process Safety and Environmental Protection*. Journals for methodology and general approaches of safety science and engineering, such as *Reliability Engineering & System Safety* and *Safety Science*, are also important dissemination channels. Several recently published works have reviewed various aspects of safety barriers, such as the dependability analysis of safety-critical systems (Kaur et al., 2018), and the evaluation approaches of SISs (Gabriel et al.,

E-mail address: yiliu.liu@ntnu.no.

https://doi.org/10.1016/j.jlp.2020.104260
Received 23 March 2020; Accepted 30 July 2020
Available online 4 August 2020

2018). However, a systematic review on more researches under the bigger umbrella of safety barriers can be beneficial, with providing readers the picture of the inter-connections among different categories of researches and help the academics and practitioners to identify the development trends in this field.

The aims of this paper include presenting the recent ideas of the definitions and categorizations of safety barriers, exploring the distinctions of similar concepts, summarizing the research advances on different topics related with safety barriers, and proposing some research perspectives. The focus of this review article will be in the works published after 2006, but some classical articles are also involved. It should be noted that although many advanced have been achieved in analyzing and improving the material properties of safety barriers, e.g. see Gomez-Mares et al. (2012) and Argenti and Landucci (2014), this article delimits itself within the scope of industrial and systems engineering, and so that skips most of literature whose contributions are in chemistry and material science.

The remainder of this article is organized as following: terminologies of safety barriers will be discussed at first in section 2. Then, we will review the relevant literature with grouping them into barrier theory, barrier engineering, and barrier management in sections 3-5. It must be noticed that the purpose of such categorization is to streamline the reviews of the existing studies, instead of emphasizing the boundaries between different groups, since many research outputs are contributive to more than one area. In section 6, perspectives for future researches will be presented.

2. Terminology and delimitation

The concept of safety barriers is based on the LOPA (layers of protection analysis) method and the energy-barrier accident model, where the identification of possible barriers is the prerequisite of preventing accidents (see CCPS, 2001a; CCPS, 2001b; Pitblado et al., 2015; Chastain-Knight, 2020). Although safety barriers are defined in variety of ways, we here accept the common features in the existing definitions, e.g. by Johnson (2003), Schupp et al. (2004), Miura et al. (2006), Sklet (2006), Basnyat et al. (2007), that safety barriers are measures to prevent or protect against hazardous events. One safety barrier can include several technical, operational and organizational barrier elements, and can perform one or more safety functions, which determine the purpose of the barrier (DNV GL, 2014). A barrier function is defined by a verb and a noun, e.g. release pressure, and this function is always related with the functions of assets that the barrier protects.

A trend in many applications is to use the term of safety barrier to describe all functions, elements, and systems associated with safety (Ersdal, 2017). This is because barriers are not only used to stop energy flow as in the original model, but also are related to other hazards, such as human errors (Rollenhagen, 2011). Another trend is that people use other terms, such as layers of protection, defenses, and risk reducing measures, to describe safety barriers. In this systematic review, we try to clarify the slight distinctions between different terms, and to see what should/should not be regarded as safety barriers.

For the several terms mentioned above, risk-reducing measures can be nonetheless a broader concept, which is not necessarily as a safety barrier. In general, two types of risk-reducing measures are useful for a system, including safety characteristics or inherent/integrated safety design, and (add-on) safety barriers (as presented by Kjellen, 2007). A system can be designed to be inherently safe, e.g. with the structures as simple as possible, and natural separation of vulnerable assets and energy. However, when hazards to a system cannot be completely eliminated with their own design characteristics, safety relies on the added measures (Tugnoli et al., 2013; Khakzad et al., 2017) that are not directly related to the essential function of the system. In the LOPA method, the Center of Chemical Process Safety (CCPS, 2001a; CCPS, 2001b) regards inherent safe design and safety barriers as different layers of protection, and Kjellen (2007) has discussed that safety is realized by optimally combining add-on safety barriers and inherent safety design. In the presenting article, we will mainly review add-on safety barriers as those are only used for a safety function instead of multi-functional or for other functions.

Arguments exist although Harms-Ringdahl (2009) thinks that defense is a wider concept than barrier. According to this researcher, commonly used physical safety barriers belong to hard defenses, while regulation, procedures, and training are soft defenses, but they are excluded from the scope of safety barriers. While in most definitions, like by Sklet (2006), these soft defenses are non-physical safety barriers. In fact, safety barriers and their elements have been categorized (PSA, 2011; Øien et al., 2015; Lauridsen et al., 2016) as physical barriers (such as firewalls), technical barriers (equipment and systems in realizing a barrier function), operational barriers (or activities that must be carried out to realize a barrier function) and organizational barriers (personnel with defined roles). We consider all of them as safety barriers, but it is noted that this review will pay more attention to technical safety barriers, namely safety-critical systems or engineered barrier systems (NEA, 2003; RWM, 2016) called in the nuclear industry. IEC 61508 (2010), ISO 13849 (2015) and some other literatures use the term of safety-related systems, or electrical/electronic/programmable electronic (E/E/PE) safety-related systems in consideration of their involved technologies.

It is also necessary to discriminate safety-critical systems from safety-related systems even though different understandings are unneglectable. In this paper, safety-critical systems are limited as the technical systems with the main function as safety and barrier function. They are introduced into a larger system to protect assets or equipment under control (EUC), but the functionality of a safety-critical system is not affecting the performance of the larger system when no hazardous event has occurred. While safety-related systems are sub-systems of or integrated in a larger system, they can reduce risks and keep the system safe or fail-safe, but performance of the larger system is also dependent on the status of these sub-systems even in cases of no hazardous event. Within the scope of safety-critical systems, we advocate the concept of SISs used in IEC 61511 (2016) but consider them as the safety-critical ones with using instrumentation technology.

The concept of mission-critical systems also has overlaps with that of safety-critical systems. For example, we can regard navigation systems on aircrafts, railway-signaling systems, and brakes on cars as both mission- and safety-critical (see Fowler, 2004). One principle to judge whether a mission-critical system is safety-critical, is whether the failure of the mission will have serious damages on human, environment and other assets. For example in a car, the start-up battery is mission-critical but not safety-critical, while the airbag is not mission-critical but safety-critical.

3. Barrier theories

In this section, we will review the studies on how safety barriers are classified for further analysis, what measures are used to evaluate safety barriers, and how the performance of safety barriers are analyzed with models and data.

3.1. Classification of safety barriers

Besides the aforementioned approach according to operational types (physical, technical, operational and organizational), one of the most acknowledged classification of safety barriers is based on the bow-tie model widely used in risk analysis. As shown in Fig. 1, barriers, like B1 and B2, between threats and the hazardous event are proactive barriers, frequency-reducing barriers or preventive barriers, which are used to prevent the occurrence of the hazardous event or at least reduce the occurring probability/frequency of the event; while the barriers, like B7 and B8, between the hazardous event and consequences, are reactive barriers, consequence-reducing barriers or mitigating barriers, for alleviating the consequences of the event (Sklet, 2006; Rausand, 2014). In

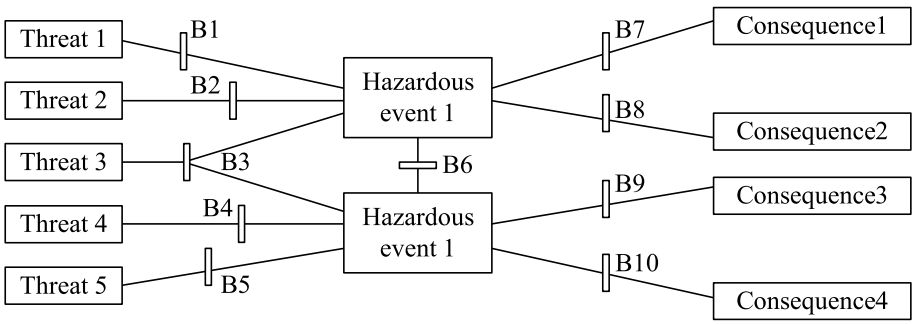

Fig. 1. An extended Bow-Tie model.

the SHIPP methodology proposed by Rathnayakaa et al. (2011), safety barriers in the process industries (especially to release) include: (1) human factor barrier, (2) management and organizational barrier, (3) release prevention barrier, (4) dispersion prevention barrier, (5) ignition prevention barrier, (6) escalation prevention barrier, and (7) damage control emergency management barrier. It can be found that types (1)–(3) are often proactive barriers, and types (4)–(7) are reactive ones.

Safety barriers are also often classified according to the operational modes. Generally, safety barriers are divided into passive- and active-barriers (Rausand, 2014; Lugauer et al., 2016a), where safety function is always available as an inherent property of the former ones (e.g. road bump), and the safety function is performed by the latter ones only in response to certain events (e.g. air bag). In the classification matrix proposed by Sobral and Soares (2019), two dimensions are considered, including both operational types (physical and non-physical) and modes. Active barriers are called as positive barriers in some studies (Kang et al., 2016). Most SISs are active barriers, and their operational modes are further categorized as low-demand mode, and high-demand and continuous mode (IEC 61508, 2010; IEC 61511, 2016), based on the frequency of the events which need the response of SISs. In these standards, sensors or transmitters are one of the three sub-systems (sensor, logic solver and actuator) of a SIS, but some literature (Kang et al., 2016) group them separately as detection barriers. In the classification of CCPS (2001), the third group beyond passive- and active-barriers is procedural and emergency measures.

Some recent studies on classifications reflect the trend of researches on safety barriers. Pitblado et al. (2016) find that safety barriers include static barriers with assumed constant performance achieved by predetermined inspections and maintenances, and dynamic barriers with performance degradations. Safety barriers are not only used for suppressing immediate failures with a direct influence on the accident causation (immediate barriers), but also are introduced for latent failures that are defects or flaws in the system indirectly allowing accident scenarios to develop (temporal barriers).

In addition, considering dependent- and interdependent-failures in a complex system, safety barriers against these failures need to be studied. Chen et al. (2015) have proposed five correlations among failure mechanisms: competition, inhibit, trigger, acceleration, and accumulation, at least the latter three of which are kind of cascading failures in a system. Corresponding safety barriers are necessary to avoid system bankrupt due to a single component failure. Xie et al. (2018a, 2018b) have distinguished safety barriers against individual failures, common cause failures (as B3 in Fig. 1 to prevent the development from a common threat to the hazardous events 1 and 2), and cascading failures (as B6 in Fig. 1 to prevent the cascade from the hazardous event 1 to 2).

3.2. Performance measures of safety barriers

Assessment of the performance of safety barriers is a key issue to identify the final consequences of natural disasters and catastrophic and technological accidents (Misuri et al., 2020). Performance measures or indicators reflect how well safety barriers perform their barrier functions. Measures can be general, or can be for specific barriers, e.g. proactive barriers. Johansen and Rausand (2015) have highlighted different requirements on barrier performance, including: specificity, functionality, reliability, response time, capacity, durability, robustness, audit-ability, and independence. In a more recent empirical study, Prashanth et al. (2017) have identified 17 types of variables relevant with the performance of safety barriers, but some of them may be not measures, e.g. triggering events, and some are overlapping or can be grouped, e.g. availability and integrity. In this paper, we present performance measures that are not design parameters but can be influenced by decision-makings in barrier design and operations, so that they illustrate whether the engineering and management efforts for barriers are meaningful and reasonable.

Effectiveness is a widely accepted measure of safety barriers, as the ability of a safety barrier prevents accidents or achieves proper safety functions (Kang et al., 2016; Moreno et al., 2018). The term of efficiency or sufficiency has the similar implications in some other literatures (see Hollnagel, 2008; Shahrokhi and Bernard, 2010). Khakzad et al. (2017) define effectiveness from the perspective of reactive barrier as a measure related with the mitigation degree of damage. In ISO 13702 (2015), the capacity of barrier to manage the major accident hazards is considered as a performance measure. Landucci et al. (2015) have used hazard intensity reduction factor (IN/OUT) for reflecting the effectiveness of safety barriers. In analyzing the effectiveness of fire & gas systems (FGSs), ISA 84.00.07 (2010) has taken geographic and scenario coverages into account.

In many cases, effectiveness is linked with the response time of a safety barrier to events, and the time to failure of the barrier or withstanding time of the barrier after a hazardous event occurs. For example, Landucci et al. (2015) consider time to (on-site and final) mitigation as the measure of non-physical barriers, and time to failure as the measure of physically passive barriers. The same authors (Landucci et al., 2016) have compared the times to failure in case of effective barrier activation and in case of absent mitigation, for measuring the performance of barriers.

Availability or *unavailability* is also widely used, especially for those active barriers. Availability means the ability of a barrier to perform its required function or to be effective at a certain time. Availability and effectiveness of safety barriers sometimes are evaluated in one metric (Landucci et al., 2016; Bucelli et al., 2018). Different from the time to failure during response that is used in effectiveness evaluation, availability is always measuring whether a barrier can have a response when it is needed, although both of the two measures are time-dependent and can be stochastic.

IEC standards (such as IEC 61508, 2010; IEC 61511, 2016) define the average availability, or probability of a SIS to satisfactorily perform its required SIF within a period of time as safety integrity and use discrete four levels specifying the safety integrity requirements. Safety integrity level 4 (SIL 4) has the strictest requirement. ISO 13702 (2015) implements the terminology of integrity for all safety barriers, not limited in

SISs, and indicates that several operational parameters, such as demand rates, test frequencies, deterioration of system components, environmental impairment etc. are influential factors. Kang et al. (2016) regard integrity as degree of confidence on the functioning of a barrier.

When determining SIL with quantitative approaches, IEC standards (IEC 61508, 2010; IEC 61511, 2016) and a lot of literature (e.g. Liu and Rausand, 2011, 2013; Innal et al., 2016a) have adopted probability of failure on demand (PFD) and average frequency of failures (PFH, from the old name of 'probability of having a dangerous failure per hour') for the SISs in low-demand and high- and continuous-demand modes respectively. IEC 61508 (2010) uses a practical approach to group the operational modes where the demand rate to activate a SIS is less than 1 year as the low-demand, while Liu (2014a) has identified that the discrimination of the two operational modes is related with the frequency of proof tests that are used to reveal hidden failures of SISs. Demand rate or the probability of occurrences of hazardous events can influence the adaptability of PFD (Liu and Rausand, 2011, 2013; Liu, 2014a), and some common measures, such as hazardous event frequency (HEF) by Jin et al. (2011), probability of a hazardous situation (PHS) by Sobral and Soares (2019) have been proposed for SISs in any operational mode.

The availability of a SIS when the underlying variables or assumptions are altered is called *robustness* (Hollnagel, 2008; Hauge et al., 2011; Prashanth et al., 2017). According to Rausand (2011), a barrier is robust when it is able to withstand extreme events and is not to be disabled by the activation of other barriers. Robustness can be reflected by the change of availability or effectiveness of a barrier when the operational conditions are different. Robustness is combined with load resistance as survivability, the ability of barriers to function under loads and accident scenarios, in the report of Hauge and Øien (2018).

3.3. Modeling approaches for safety barriers

Accidental models, such as energy-barrier model, bow-tie diagram, the Swiss cheese model (see e.g. Reason et al., 2006) are the basis of understanding the functions of safety barriers. Barriers can be regarded as stoppages of the development path of an accident. Proactive barriers are upstream of accidental event nodes, while reactive barriers are downstream of those events (de Dianous and Fiéviez, 2006; Sobral and Soares, 2019). Deterministic or probabilistic performance requirements for safety barriers can be established in accordance with their locations in the model (Johansen and Rausand, 2015). For further and quantitative analysis, these illustrative models should be integrated with other methods, e.g. event tree. Xue et al. (2013) have adopted the event tree method based on the Swiss cheese model to analyze the sequential failures of several barriers for offshore drilling blowouts. Kang et al. (2016) evaluate effectiveness of different barriers within an event tree model, Tsunemi et al. (2019) consider the impact of failure probability of safety barriers through event tree analysis for different accident scenarios of a hydrogen refueling station, while Landucci et al. (2016, 2017) develop gates for describing barrier performance in an event tree and put the values of availability and effectiveness of barriers in the event tree analysis associated to cascading events.

Probabilistic models, with random variables and probability distributions, are the basis of most quantitative studies for safety barriers. Probabilistic models are working together with schematic models, such as fault tree (FT) and reliability block diagram (RBD), which have been widely used for several decades in reliability and availability analysis of technical systems, including those with barrier functions. For example, Guo and Yang (2007) have used reliability block diagram to provide a clear and feasible way of calculation of the average PFD (PFD_{avg}) in the long term and explain the concept of mean down times of channels and voted groups in IEC 61508. Kaczor et al. (2016) provide a comparative analysis of the safety integrity level with the application of the Monte Carlo simulation and RBD methods. The quantification of PFD and spurious trip rates of SISs by Torres-Echeverria (2009) is based on the fault tree method. However, it should be noted that neither FT nor RBD is naturally effective in dealing with dependence of nodes, just as what Rausand (2014) has indicated: It is possible to use FT to calculate instantaneous unavailability of a redundant SIS, but PFD_{avg} cannot be directly estimated with occurrence probabilities of the basic events in a FT. Innal et al. (2014) have reviewed the main modeling approaches for safety barriers and compared their effectiveness with simple cases. The authors have the same concerns on FT when calculating PFD_{avg}.

State transition models, the Markov method and Petri net (PN), are used to reflect the operations of active safety barriers, and then to analyze their integrity. The Markov method is recommended by IEC 61508 (2010) due to its flexibility and has been adopted by many researchers (e.g. Guo and Yang, 2008; Liu and Rausand, 2011, 2013; Cai et al., 2012a, 2012b; Verlinden et al., 2012; Mechri et al., 2015; Zeng and Zio, 2018). He et al. (2016) have combined RBD and the Markov method to construct a model for analyzing SISs in nuclear plants. The standard Markov chain is suitable for a stochastic process where the occurrence time of random events or state transitions follow the exponential distribution. When deterministic delays exist between transitions, the multi-phase Markov chain will be the alternative solution (see Innal et al., 2016a). The Markov method is more effective for a small system with more complex behaviors, and when there are many states, the approach will lead to intractable calculations.

PN is another option with more flexibility and stronger expressiveness. PNs are more effective to model different scenarios, some of which may not be revealed in the preliminary analysis. de Souza et al. (2017) convert a bow-tie diagram into a PN to analyze the role of active barrier in stopping accident scenarios. Liu (2014b) and Liu and Rausand (2016) have adopted PN and RBD-driven PN respectively, to study the effects of different test strategies on SIS availability. PNs have been used in different industries for design and assessment of technical safety barriers, such as oil & gas (Wu et al., 2018a, 2018b), nuclear (Kumar et al., 2019; Singh and Singh, 2019), manufacturing (de Souza et al., 2017) and aviation (Skorupski, 2015). Based on the understanding of different modeling approaches, Meng et al. (2018) have proposed a versatile set of modeling patterns for SISs to capture the common behaviors, to make modeling works more simplified and more efficient.

Bayesian network (BN) is also helpful for modeling safety barriers, although it is not emphasized in IEC 61508 (2010). Cai and his co-authors (2012b, 2012c, 2013 and 2015) have used BN and dynamic BN in risk, reliability and performance assessment of technical safety barriers in oil & gas industry, especially for subsea blowout preventers. Khakzad and Reniers (2015a, 2017) have used BN to evaluate the effect of a barrier in stopping fire propagation, Simon et al. (2019) have introduced dynamic BN to assess the integrity of a SIS with considering test duration, Ding et al. (2020) establish a model of Bow-Tie and BN to relationships among accident causes, safety barriers, and possible consequences, as well evaluate importance of barriers.

In terms of modeling safety barriers in a larger system, Khakzad and Reniers (2015b), Khakzad et al. (2017) have applied the graph theory in analyzing failure propagation. In their studies with cases of process plants, EUCs or assets being protected are denoted as nodes, passive safety barriers are reflected by marking the node in protection, and the effectiveness of active safety barriers are modeled by the weight of edges between nodes.

3.4. Data driven analysis of safety barriers

With higher availability and affordability of sensors, data acquisition systems and advanced computers, data driven analysis is being more accepted by the researchers focusing on safety barriers. In this context, data driven analysis refers to the quantitative analysis of identifying the correlations of different variables based on amounts of data. For the model-based approaches aforementioned, the values of meaningful parameters, e.g. failure rate, need to be estimated based on data. In some guidance and data handbooks, such as OREDA0 (2015), the maximum

likelihood estimation (MLE) is the generic and suggested method, where the failure rate of a type of SISs is often calculated by the total number of failures divided by the aggregated time in service.

There have been some practices of data drive methods in the domain of safety barriers. Wang et al. (2016a,b) have developed a method to utilize SIS experience information stored in common databases for SIL allocation. Zhu and Liyanage (2018) have used recorded condition data for 15 years to estimate the failure rate of ESD systems as safety barriers, and to help the decision-making on test intervals. Xie et al. (2019) have used the approaches like principal component analysis to handle data from six oil and gas facilities involving 12,788 equipment to identify the underlying influencing factors of failure rates of SISs.

In the parameter estimation of the model-based approaches, uncertainty in data as input parameters of models can result in misleading evaluation of the performance of SISs (Wang et al., 2004; Tang et a, 2017). An uncertainty distribution is always given for the main parameters (Jin et al., 2012). Monte Carlo simulation is the widely used method for reflecting uncertainty propagation, and Innal et al. (2016b) have combined Monte Carlo analysis and the fuzzy set approach for treating data uncertainty of SISs. Ramzali et al. (2015) also employ the fuzzy method together with event tree for safety barrier analysis since the available data is limited. Francese et al. (2014) use the interval-valued information supplied by a team of experts to deal with data uncertainty of SISs, and Freeman and Summers (2016), Freeman (2018) have proposed the approach of variance contribution analysis to evaluate the uncertainty in the PFD calculations, where the variation of PFD is determined by the parameter sensitivity weighted contributions.

4. Barrier engineering

In this study, we regard those efforts on how to identify, analyze, design, operate and maintain safety barriers in the category of barrier engineering. The works in barrier engineering are based on the HAZOP studies and/or methods such as LOPA (Johansen and Rausand, 2015), and other approaches mentioned in the last section. In general, the focus of barrier engineering is on improving the integrity of barriers.

Barrier engineering is conducted in different industries. Paltrinieri and his co-authors (2009 and 2012) have studied safety barriers in road and rail LNG transportation. Sun et al. (2017) have investigated the safety barriers engineering in coal mining. Winge and Albrechtsen (2018) have discussed the effects of safety barriers in the construction industry. Moreno et al. (2018) recently identify safety barriers in biogas production by revealing the reference critical events and cause-consequence chains. Lugauer et al. (2016b) have developed a statistical method for the estimation of protection times of laser safety barriers in production systems. In this paper, we will review these engineering efforts from four aspects.

4.1. Design for reliability and safety

Technical safety barriers are always designed complying with the related standards and regulations. IEC 61508 (2010) has given a general guideline on the design of E/E/PE safety-related systems, and some industrial standards, e.g. IEC 61511 (2016) in the process industry, and EN 50126 (2017) in the railway industry, also guide the design in their sectors. Macii et al. (2015) present a whole design process of a modular and flexible SIS following EN 51026 to avoid two types of hazards occurring on rolling stocks. Khalil (2019) proposes new statistical formulations to design efficient reliability demonstration test plans of SIS subject to requirement of IEC 61508.

Redundancy is the main approach from the perspective of architecture to improve reliability of a technical barrier system. Both hardware and software can be designed in a redundant way to improve system reliability. When all the redundant items are actively performing the specific function, such kind of architecture is called as active redundancy. While if only one or several perform the function, and the others wait to be in operation only when the active items fail, the architecture is called as standby redundancy (Rausand, 2014). Torres-Echeverria et al. (2011) have discussed PFD values of different configurations of *K*-out-of-*N* structures, where the functioning of *K* in the *N* parallel components can ensure the system functioning. However, as what we will discuss in subsection 4.2, dependent failures can weaken the usefulness of redundancy in the improvement of reliability. Heterogeneous items have been used in the design of redundancy structures of safety barriers (Ma et al., 2017a).

One the other hand, simplicity and minimalism are also recommended in the design of systems with barrier functions, because more installations can bring higher complexity that sometimes is more dangerous. Summers (2018) has suggested to reduce the use of automation features that tend to increase failure mechanisms, for example, the devices using a justification process.

The design of safety barrier needs to consider lifecycle cost while the safety requirement has been satisfied (Torres-Echeverria et al., 2009; Szymanek, 2010; Kang et al., 2016; Julsereewong and Thepmanee, 2017). As Kjellen (2007) has mentioned, significant expenditures will be involved in implementing an adequate barrier philosophy in design, and the maintenances of barrier systems, training of personnel, and spurious trips also increase operational costs and decreased revenues. Each barrier should undergo a cost-effective evaluation since the maximization of profits is always the main target of companies in practices. Therefore, among the approaches proposed by Janssens et al. (2015) and Mancuso et al. (2016) for barrier selection, the decision is constrained both by the residual risk and by the predefined budget/investment cost. Similarly, Paltrinieri et al. (2012) have conducted cost-effective analysis for passive barriers of fire in road LNG transportation.

When the barrier functions are realized by a complex system or multiple safety barriers are installed in a large system, the arrangement/layout and functionality of barriers and their combined effects should be studied to guarantee EUC safe. Jahanian and Lucas (2015) have developed a set of guidelines for SIS design with a focus on component arrangement. de Lira-Flores et al. (2019) have integrated design of SIS with process equipment and facility layout. Bain et al. (2015) and Pitblado et al. (2016) define barrier importance as the impact on EUC risk, based on the current PFDs of barriers, and utilize it as an indicator to guide the installation of barriers. Zhu et al. (2015) have optimize the allocation of safety measures including barriers, by maximizing the sum of risk reductions of all relevant measures under limited budgets. Khakzad and Reniers (2017) have proposed a BN-based methodology for cost-effective allocation of safety barriers in chemical plants to mitigate both internal and external risks while considering land use.

4.2. Optimal tests and maintenances with high availability

Currently, diagnostic tests are automatedly performed on many SISs in their operational phase, but only a ratio of faults can be found immediately since these technical barriers are often subject to several failure mechanisms. Regular proof tests (reliability demonstration tests in some literature) are still the main approach to ensure SIS high availability and EUC safety (IEC 61508, 2010; IEC 61511, 2016), by revealing those undetected faults and then restoring the system to an as good as new condition if necessary. A full-trip proof test shall include several tasks, such as examining alarm functions, measuring response time for a specific SIF, and operating all input devices (Rausand, 2014). Preventive maintenances and corrective maintenances in case of failure found are needed. Sometimes, such a full-trip proof test is costly or even can damage the SIS, the interval of tests and preventive maintenances should be optimized (Han et al., 2019; Zhang et al., 2020), and partial tests (e.g. visual inspections, partial stroke testing) are helpful to detect specific faults and leave the others latent (Brissaud et al., 2010).

Test policies have been proved to be influential on the availability of technical safety barriers. According to the basic formulation of PFD_{avg} of a single component SIS, (see Rausand, 2014), where λ is failure rate and

τ is proof test interval, more frequent proof tests can increase availability of the SIS. Longhi et al. (2015) understand the conduction of tests on SISs as the activities with adding costs, raising risks of failures and spurious activations, so that they propose a method based on FTA and genetic algorithm to optimize test strategies for these systems. Chebila and Innal (2015) have considered the effects of partial stroke testing (PST) in their calculation for PFD_{avg} and PFH. Wu et al. (2018b) have analyzed the performance of subsea blind shear ram preventers as safety barriers with both PSTs and proof tests. In addition, Rausand (2014), Mechri et al. (2015) and Jigar et al. (2016) have mentioned the issues of imperfect proof tests, where not all faults are revealed as expected.

Test strategies can be more complex for redundant systems. Simultaneous-, sequential- and staggered-tests can be conducted on different channels of a SIS, meaning that the tests on those channels can be at the same time, one-by-one in no time or with some delays. Liu (2014) has found that the optimal staggered time for a SIS with two heterogenous components is the half of the test interval. When one of redundant channels are found failed, the follow-up testing strategies and repairs are also influencing the availability of a SIS, so that the maintenance crews should select an appropriate testing approach to ensure safety while minimizing costs (see the discussion for standby configuration by Hellmich and Berg, 2015 and that for parallel configuration by Liu and Rausand, 2016). Kahlil (2019) has discussed the trade-off between test duration and number of units on test and has developed statistical formulations to design optimum proof test plans.

When multiple barriers exist in a larger facility, tests and maintenances should be planned optimally based on quantitative barrier importance analysis (Pitblado et al., 2016). Barriers with higher importance barriers should be assigned higher priority to achieve safety at lower cost and risk. With the same purpose, Miura et al. (2006) have calculated the reasonable number of active barriers for each sequenced operation, and Tugnoli et al. (2013) have optimized the application of passive safety barriers with the case of fireproofing.

4.3. Responses to dependent failures

Although independence is extremely important to ensure that safety barriers are effective, they are rarely fully independent (Johansen and Rausand, 2015). Both common cause failures (CCFs) and cascading failures (domino failures) are threats to barriers. Especially when cascading failures are studied, it is necessary to clarify that dependent failures include the failures of EUCs need to be stopped by barriers and the failures within barriers.

CCFs are the failures as the result of one or more events, causing failures of two or more separate channels in a multiple channel system (IEC 61511, 2016), which are the dominant contributor to unavailability of redundant structures. Lundteigen and Rausand (2007) has reviewed the analyzing approaches of CCFs in the oil & gas industry. IEC 62340 (2007) has summarized the approaches against CCFs of EUCs in the nuclear industry, and most of them are inherently safe design precaution, but precaution against dependencies from external data or messages can be realized with some barriers.

IEC 61508 (2010) recommends β-factor model in the analysis of CCFs within barriers, where β is the conditional probability of a CCF on all channels when a failure has occurred. In the PDS method proposed by SINTEF (Hauge et al., 2013), the β-factor model is extended to the cases where CCFs are on several channels but not on the entire system. The values of β is estimated by checklists and operational experiences (IEC 61508, 2010). Rahimi and Rausand (2013) have identified human and organizational factors influencing the value of β in the operational phase. In the newer version of PDS handbook (Hauge et al., 2015), the suggested values of β for several SISs have been greatly increased (for example, for fire detectors, from 5% to 15%).

In fact, many probability models have been applied for analyzing CCFs of safety barriers in the recent decades. For example, Vinnem et al. (2012) and Cai et al. (2016) have used BN and DBN models respectively to study CCFs, Ma et al. (2017b) have adopted the binomial failure rate (BFR) model for CCFs of digital reactor protection system, Jia et al. (2018) have used the Copula method to model the dependent relationships of different parts within a technical safety barrier. Fan et al. (2018) have developed a stochastic hybrid model for CCFs of degrading components, Jin and Rasuand (2014) consider testing strategies in evaluating CCFs, while Alizadeh and Sriramula (2017, 2018) take process demands into account in the CCF analysis for active safety barriers.

On the other hand, several researches have been initiated with safety barriers against cascading failures. When a cascading failure is the propagation from an initially failed node, the barrier function is to stop failure path. For example, the failures triggered by heat radiation and overpressure need to be stopped by active and passive barriers. Meanwhile, if the failures of EUCs are due to the redistribution of workloads after the first failure, the barrier function is to avoid the overload of the functioning EUC. As Tugnoli et al. (2012) have mentioned, when the inherent design is not enough to eliminate cascading failures, engineered safety barriers are relied on.

A framework has been suggested by Cozzani et al. (2013) for selecting the correct methodology to defense cascading failures between EUCs. The models by Janssens et al. (2015), Landucci et al. (2016, 2017), and Khakzad et al. (2017) are usefully evaluating the effects of safety barriers and locating them properly to mitigate cascading failures. Xie et al. (2020) have integrated safety barriers into a reliability block diagram to evaluate the effectiveness of these barriers when they are layout in different ways. However, it should be noted that modeling and analysis of cascading failures among the components within a safety barrier have not been well studied in the current literature.

4.4. Diagnosis and prognosis of degradation

A common assumption in many current studies is that the performance of barriers is stable, namely the barriers are static barriers with the failure rates as constant values, and all proof tests and follow-up maintenance can restore the barriers to the as-good-as-new condition. In practices, safety barriers, especially for those mechanical final elements of SISs, are subject to chronic degradations due to mechanisms of corrosion, wear-out, and fatigue, so that they can be called as dynamic barriers (Pitblado et al., 2016). In addition, external shocks, or demands on safety barriers also result in the deterioration of barriers. PSA (2013) has required to monitor the status of barriers and implement compensating measures for degradation, and Hoem et al. (2016) have proposed to present system status with red, yellow and green lights to present their associated criticality.

Condition-based maintenance (CBM) is an approach to carry out maintenance actions based on the information collected through condition monitoring on systems (Jardine et al., 2006; Shin and Jun 2015). Elusakin and Shafiee (2020) have adopted stochastic PNs to analyze of reliability of subsea blowout preventers, as safety barriers, with condition-based maintenances. CBM is extended to prognosis and health management (PHM), which includes diagnosis for fault detection and identification, prognosis for estimating the time to failure and risks (ISO-13381, 2015), and health management. CBM and PHM have started being utilized in the domain of safety barriers. For example, van Oosterom et al. (2017) consider the optimal maintenance of a safety-critical system with deteriorating sensors, and Zeng and Zio (2018) utilize condition-monitoring data to update the reliability estimation of safety barriers. Kumar et al. (2018) capture time-dependent system requirements along with dynamic behavioral analysis and calculate state transition probabilities of a safety-critical system. Zhang et al. (2018) have summarized some benefits of implementing PHM on safety barriers, such as warning of failures, optimized maintenances, logistics support and cost reduction. The same authors model the degradation of SIS final element as a stochastic process, consider the effects of demands on degradation (Zhang et al., 2019), and propose a method for an optimal maintenance strategy by choosing a PM or

corrective maintenance (CM), as well deciding what degree of mitigation of degradation is enough in case of a PM (Zhang et al., 2020). It should be noted that although CBM approaches on other systems can be adopted to safety barriers, some characteristics of barriers, including diverse operational modes, complex voting configurations, hidden failures and specific measures, need to be taken into consideration.

5. Barrier management

In the 7 groups of performance factors of safety barriers proposed by Prashanth et al. (2017), 4 groups: performance-, confidence-, trust- and limit-factors, are related with engineering design and maintenances, while the other 3 groups: perception-, dependability- and robustness-factors, are relevant with management. In our view, management is important because: 1) safety barriers can be a combination of hardware, software, and human or organizational ones (Pitbablo et al., 2016); 2) safety barriers need to interact with other components in a large system (NRC, 2007; Xie et al., 2018a, 2018b); and 3) the design and implementation of barriers is a systematic work (Kjellen, 2007). As what Pitblado et al. (2016) have highlighted, the effectiveness of safety barriers decreases not only due to the physical degradation, but due to management issues, e.g. updates of safety documentation.

In the definition of PSA (2013), barrier management refers to the coordinated activities to establish and maintain safety barriers so that they always maintain their function. Barrier management is an integrated part of risk and safety management (PSA, 2011), where barrier analysis is conducted after the identification of hazards and frequency and consequence analysis. When barriers are installed, the risk analysis should be iterated to examine the possible effects of barriers. In the safety management framework developed by Li and Guldenmund (2018), barriers are the input of management efforts, while safety performance is the output. Barrier management includes managements on processes, systems, solutions and measures (PSA, 2011). DNV GL (2014) has highlighted that barrier management interacts with several other aspects related to management of safety, environment, and asset, e.g. safety culture, operational risk management, and organizational learning. In this article, barrier management is reviewed from three aspects.

5.1. Project and process management

It is not unreasonable to regard the activities of analysis, specification, installation, operation and maintenance of barriers as parts of a project or a process. The purpose of such a project is to handle risks by preventing an undesirable incident from occurring or by limiting the consequences given that such an incident occurs (PSA, 2011). Kjellen (2007) has categorized the tasks of barrier management according to temporal sequence, as establishment and implementation of barrier management, management in operation, monitoring, and risk management. PSA (2011) divides barrier management into 6 steps with iterations and feedbacks: establishing the context, risk assessment, risk treatment, communication and consultation, establishment of barrier strategies and performance standards, and monitoring and review. In the guidance of barrier management by Hauge and Øien (2016), major accident hazard analysis is followed by barrier analysis, which includes three steps: barrier function analysis, barrier element analysis, and requirement/PIF/verification analysis. Then, barrier strategy and performance standards can be developed. In addition, Pitblado et al. (2016) have proposed the concept of dynamic barrier management with the tasks of inspection, information analysis, preventive maintenance, audit, process control, and near-miss or incident records.

The project ARAMIS (Markert et al., 2013) has identified several issues in the process of barrier management, including competence management, dealing with conflicts, management of maintenance and inspection, and management of procedures. In general, good barrier management needs a comprehensive and common understanding on how barriers are designed, verified, monitored and maintained. Verification is a significant step in the project management for barriers, for confirming whether the barrier elements will be, are, and remain suitable, or are adequately specified and constructed, and are being maintained in adequate condition to meet the requirements (PSA, 2011). In the ARAMIS (Accidental Risk Assessment Methodology for IndustrieS) project (Guldenmund et al., 2006), verification tasks for hardware/technical barriers and human/organizational barriers are specified respectively.

5.2. Human and organizational management

In this subsection, what we would like to summarize is not the human and organizational barriers themselves, but how humans and organizational factors, as well as the relevant management activities interact with the barrier functions of technical systems. In fact, some barrier systems are constituted by hardware, software and humans. For example, some shutdown operations are finished manually based on alarms from temperature or pressure transmitters. Duijm (2009) has revealed several human and organizational factors affecting barrier availability, including safety culture, manpower planning and availability, competence and suitability, commitment, compliance and conflict resolution, communication and coordination, and procedures, rules, and organizational goals.

Safety barrier functions can be enhanced with human and organizational factors. McLeod (2017) indicates that even though humans cannot be relied on as a full barrier, they can support the availability or performance of technical barriers. Meanwhile, human factors/errors are also threating to barrier management in some cases. McLeod (2017) has highlighted some reasons: 1) human thought and performance are highly influenced by the situation and experience; 2) some technical issues can affect the ways people behave and interact with technology; 3) people are subject to find the easier but risky way of doing things, and; 4) it is difficult to assume that people are always rational.

Therefore, human and organizational factors need to be coordinated to deliver the high reliability organization (HRO), so as to well perform the barrier function of technical systems (see Markert et al., 2013). Pitblado and Nelson (2013) have combined traditional barrier models with safety objective methods, to include human and organizational aspects in barrier management. Li et al. (2017) have developed a systematic approach for identifying management factors influencing the referred safety barriers. Performance influence (PIF) factors have been proposed (PSA, 2013; Hauge and Øien, 2016; Lauridsen et al., 2016) as the significant conditions for ability of barrier functions to perform as intended, to be a framework to coordinate technical, human and organizational barrier elements. It is important to monitor these factors in barrier management. Grattan (2018) has recommended several tools for validating barriers from the perspective of human factors perspective, such as safety critical task analysis, human reliability assessments, and those based on behavioral economics.

5.3. Standardization and compliance management

One of the purposes of barrier management is to streamline the works related to the realization of barrier functions, with international and national standards as the main tool. Recognized standards include generic standards and industry standards. For example, IEC 61508 (2010) - and IEC 31000 series for risk management are generic ones, applicable to almost all the industries. While the following standards developed in the recent decades are guiding the practitioners in different sectors:

- IEC 61511 (2016): Safety instrumented systems for the process industry sector;

- IEC 62061 (2005): Safety of machinery - Functional safety of safety-related electrical, electronic and programmable electronic control systems;
- ISO 19353 (2019): Machine Safety - Preventive Fire Protection and Protection
- ISO 16530 (2017): Petroleum and natural gas industries — Well integrity;
- AS/NZS 3845.1 (2015): Road safety barrier systems and devices - Road safety barrier systems;
- EN 50126 (2017): Railway applications - The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS)

In addition, some standards have been developed for specific equipment with barrier functions, for example:

- EN 62682 (2015): Management of alarms systems for the process industries;
- ISO 13577-4 (2014): Industrial furnace and associated processing equipment - Safety - Part 4: Protective systems
- ISO 28781 (2010) Petroleum and natural gas industries — Drilling and production equipment —Subsurface barrier valves and related equipment

It should be noted that an appropriate procedure of adopting standards (see ISO 12100, 2012) is to start from referencing the standards for specific equipment or specific risks (Type C standards), and then adopt industry standards (Type B standards) if Type C ones are unavailable. Type B standards include Type B1 standards for particular safety aspects and Type B2 standards for safety barriers. Generic standards (Type A standards) are for all applications when Types B and C are not ready.

6. Research perspectives in the domain of safety barriers

Systems in the era of Industry 4.0 are becoming more complex, by integrating physical systems with computerized elements in the cyber layer. Considering such systems with inter-dependability and functional redundancies, it is naturally wanted to be unaffected or little affected by single failures or hazardous events. New researches on safety barriers are needed to address the challenges from new complexities and to protect EUCs with computational, communicational and physical elements.

6.1. Enhancing barriers for resilience

Failure, or performance degradation in a broader context, of a complex system is always the consequence of some event or behavior. It is necessary to understand how the system or EUC ensures proactively that things are under control and reacts when things are out of control. It is for this reason that the system should be made resilient. Although resilience has been defined in many ways (e.g. see Francis and Bekera, 2014; Cai et al., 2018), it at least can consist of extensibility and recoverability. The extensibility is the answer to the question how the system stretches to handle failures, hazardous events or just surprises in general (Woods, 2015). While recoverability is the ability to initialize and allocate various resources in short time to recover the system from the disruption. Barriers can play more than one role in changing the profile of EUC resilience, by preventing the failure, mitigating the consequence, and gentling the EUC performance degradation curve through withstanding the disruption. In a large system, if one barrier is failed, other barriers should be implemented to stop the failure propagation and recover the system performance to a relatively higher level.

6.2. Realizing digital and cyber safety

Security issues in digital and cyber worlds have been discussed everywhere nowadays, but safety issues are same important, and they are different from security issues. Digital and cyber safety can be realized relying on not only the defenses to the intended attacks, but also the measures to mitigate those unintended events, especially when the EUC has a cyber layer closely connected with the physical layer. Some researchers have proposed protection measure for specific systems, such as smart grid (Kundur et al., 2011), and smart building cyber-physical systems (CPSs) (Wu, 2015). However, very few of the current researches have considered the performance of protection measures for CPSs as a whole or analyzed the universal safety barrier functions against interdependency failures, e.g. common cause and cascading ones, in these systems. Bolbot et al. (2019) have listed barrier management as an approach of safety assurance of cyber-physical systems, but the authors have no further discussion on the applications and procedures.

Meanwhile, it is unneglectable that SISs as distributed control systems face cyber security threats. According to Kanamaru (2017), new international standards, IEC TR 63069 and IEC 63074, are being developed to bridge functional safety and cyber security of SIS/SCS. In system design, two consideration ways are being discussed: safety is designed prior to security, and safety and security are analyzed in parallel. Sliwiniski (2018) also has suggested SIL verification with regard of the security assurance levels (SAL).

6.3. Adapting barrier approaches for security

On the other hand, the methodologies, models, and engineering approaches existing for safety barriers can be used to enhance the role of these things in ensuring EUC security. Barriers should be designed, installed, operated and managed in a way where intended attacks can be stopped, and their influences can be alleviated. There are many studies in the areas of computer science, telecommunication and cybernetics for developing protection measures against cyber-attacks, but researchers of safety engineering can be more active with applying their knowledge of probability theory, risk analysis and engineering improvement.

6.4. Utilizing data, no matter how much

Big data has been a buzzword in both academics and industries, but the available data for assessment of highly reliable systems, such as SISs, is often sparse or insufficiently detailed (Selvik and Abrahamsen, 2017). Pitblado et al. (2016) have also highlighted three problems commonly encountered in barrier management, including: lack of data for some barriers, poor understanding of available data, and over analysis of data. Considering PIFs in barrier management are related to many aspects in a company, the approach based on PIF is only effective when all the necessary data is collected and well processed. Difficulties in technical and administrative aspects are unavoidable. For example, it is a real challenge for barrier engineer to obtain and analyze the staff training records from the human resource department.

Even though some studies have been conducted as mentioned in section 3.4, new tools of big data analytics are needed to interpret data and reveal more facts behind data, given that amount of data is available. The application of the approaches based on machine learning for safety barriers is expected. Safety engineers and researchers need to have closer collaborations with experts of database techniques, query language programmers, and other data scientists.

6.5. Dealing with intelligence

The terms like intelligence and smartness have not always been together with safety or safety barriers. With the general design rules, safety barriers should be designed as simple as possible, without intelligent elements as possible. However, the involvement of new techniques and the introduction of intelligent equipment seem unstoppable. Mkhida et al. (2014) have discussed the challenges in the integration of

intelligent sensors within safety barriers. The justification for using these instruments in safety applications is not fully proved and the dependability evaluation of such systems is not trivial. Agrawal et al. (2018) have also indicated different issues and challenges faced during the reliability assessment of safety-critical intelligent systems. Researches are therefore required on understanding the effects of intelligence on the performance of safety barriers, and the new methods in designing, operating, maintaining and managing intelligent barriers.

7. Summaries

In this article, we have delimited the concept of safety barrier based on the existing studies and reviewed the research advances in the categories of barrier theory, barrier engineering and barrier management. The main purpose of such categorization is to make the reviews clearly, but it is unnecessary to strictly discriminate the researches in different groups. In most cases, models and algorithms, engineering approaches and management frameworks are integrated to deliver effectiveness and high availability of safety barriers.

Some research perspectives have been proposed at the end. The general idea is that researchers, analysts and engineers related to safety barriers should have more collaborations with those experts in information techniques and data science, to address the challenges accompanying with technical development. Inter- and multi-disciplinary studies are expected and even a must.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Appendix A. Supplementary data

Supplementary data to this article can be found online at https://doi.org/10.1016/j.jlp.2020.104260.

References

Agrawal, R., Verma, A., Gayen, T., 2018. Reliability assessment of safety critical intelligent systems: issues and challenges. In: Silhavy, R., Silhavy, P., Prokopova, Z. (Eds.), Cybernetics Approaches in Intelligent Systems. Springer, Cham.

Alizadeh, S., Sriramula, S., 2017. Reliability modelling of redundant safety systems without automatic diagnostics incorporating common cause failures and process demand. ISA (Instrum. Soc. Am.) Trans. 71, 599–614.

Alizadeh, S., Sriramula, S., 2018. Impact of common cause failure on reliability performance of redundant safety related systems subject to process demand. Reliab. Eng. Syst. Saf. 172, 129–150.

Argenti, F., Landucci, G., 2014. Experimental and numerical methodology for the analysis of fireproofing materials. J. Loss Prev. Process. Ind. 28, 60–71.

As/Nzs 3845, 2015. 1. Road Safety Barrier Systems and Devices - Road Safety Barrier Systems. AS/NZS 3845.1. Road Safety Barrier Systems and Devices - Road Safety Barrier Systems.

Bain, B., Worthington, D., Spitzenberger, C.A., 2015. Falck Modeling the Progression of an Offshore Hydrocarbon Release Accident. whitepaper, DNV GL.

Basnyat, S., Palanquea, P., Schupp, B., Wright, P., 2007. Formal socio-technical barrier modelling for safety-critical interactive systems design. Saf. Sci. 45 (5), 545–565.

Bolbot, V., Theotokatos, G., Bujorianu, L.M., Boulougouris, E., Vassalos, D., 2019. Vulnerabilities and safety assurance methods in Cyber-Physical- Systems: a comprehensive review. Reliab. Eng. Syst. Saf. 182, 179–193.

Brissaud, F., Barros, A., Bérenguer, C., 2010. Probability of Failure of Safety-Critical Systems Subject to Partial Tests. Reliability and Maintainability Symposium. RAMS 2010, San Jose, CA.

Bucelli, M., Landucci, G., Haugen, S., Paltrinieri, N., Cozzani, V., 2018. Assessment of safety barriers for the prevention of cascading events in oil and gas offshore installations operating in harsh environment. Ocean Eng. 158, 171–185.

Cai, B.P., Liu, Y.H., Liu, Z.K., Tian, X.J., Li, H., Ren, C.K., 2012a. Reliability analysis of subsea blowout preventer control systems subjected to multiple error shocks. J. Loss Prev. Process. Ind. 25 (6), 1044–1054.

Cai, B.P., Liu, Y.H., Liu, Z.K., Tian, X., Zhang, Y., Liu, J., 2012b. Performance evaluation of subsea blowout preventer systems with common-cause failures. J. Petrol. Sci. Eng. 90, 18–25.

Cai, B.P., Liu, Y.H., Liu, Z.K., Tian, X., Dong, X., Yu, S., 2012c. Using Bayesian networks in reliability evaluation for subsea blowout preventer control system. Reliab. Eng. Syst. Saf. 108, 32–41.

Cai, B.P., Liu, Y.H., Liu, Z.K., Tian, X., Zhang, Y., Ji, R., 2013. Application of Bayesian networks in quantitative risk assessment of subsea blowout preventer operations. Risk Anal. 33 (7), 1293–1311.

Cai, B.P., Liu, Y.H., Ma, Y., Liu, Z.K., Zhou, Y., Sun, J., 2015. Real-time reliability evaluation methodology based on dynamic Bayesian networks: a case study of a subsea pipe ram BOP system. ISA Trans. 58, 595–604.

Cai, B.P., Liu, Y., Feng, Q., 2016. A multiphase dynamic Bayesian networks methodology for the determination of safety integrity levels. Reliab. Eng. Syst. Saf. 150, 105–115.

CCPS-Center of Chemical Process Safety, 2001a. Guidelines for Engineering Design for Process Safety. American Institute of Chemical Engineers, New York, NY.

CCPS-Center of Chemical Process Safety, 2001b. Layer of Protection Analysis: Simplified Process Risk Assessment. American Institute of Chemical Engineers, New York, NY.

Chastain-Knight, D., 2020. Confirming the safety instrumented system layer of protection. Process Saf. Prog. 39 (1), e12079.

Chebila, M., Innal, F., 2015. Generalized analytical expressions for safety instrumented systems' performance measures: PFDavg and PFH. J. Loss Prev. Process. Ind. 34, 167–176.

Chen, Y., Yang, L., Ye, C., Kang, R., 2015. Failure mechanism dependence and reliability evaluation of non-repairable system. Reliab. Eng. Syst. Saf. 138, 273–283.

de Dianous, V., Fiévez, 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. J. Hazard Mater. 130, 220–233.

de Lira-Flores, J.A., Lopez-Molina, A., Gutierrez-Antonio, C., Vazquez-Roman, R., 2019. Optimal plant layout considering the safety instrumented system design for hazardous equipment. Process Saf. Environ. Protect. 124, 97–120.

de Souza, J.A.L., Fo, D.J.S., Squillante, R.J., Junqueira, F., Miyagi, P.E., Silva, J.R., 2017. Safety active barriers considering different scenarios of faults in modern production systems. In: IFIP Advances in Information and Communication Technology. Springer International Publishing, pp. 154–164.

Ding, L., Ji, J., Khan, F., Li, X.H., Wan, S.A., 2020. Quantitative fire risk assessment of cotton storage and a criticality analysis of risk control strategies. Fire Mater. 44 (2), 165–179.

DNV, G.L., 2014. Good Practices: Barrier Management in Operation for the Rig Industry. Technical report. DNV GL.

Duijm, N., 2009. Safety-barrier diagrams as a safety management tool Reliability Engineering. & System Safety 94, 332–341.

Elusakin, T., Shafiee, M., 2020. Reliability analysis of subsea blowout preventers with condition-based maintenance using stochastic Petri nets. J. Loss Prev. Process. Ind. 63, 104026.

EN 50126, 2017. Railway applications - the specification and demonstration of reliability, availability, maintainability and safety (RAMS). CENELEC - European Committee for Electrotechnical Standardization.

EN 62682, 2015. Management of alarms systems for the process industries. CENELEC - European Committee for Electrotechnical Standardization.

Ersdal, G., 2017. Safety barriers in structural and marine engineering. In: The 36th International Conference on Ocean, Offshore and Arctic Engineering. Trondheim, Norway.

Fan, M.F., Zeng, Z.G., Zio, E., Kang, R., Chen, Y., 2018. A stochastic hybrid systems model of common-cause failures of degrading components. Reliab. Eng. Syst. Saf. 172, 159–170.

Fowler, K., 2004. Mission-critical and safety-critical development. IEEE Instrum. Meas. Mag. DEC, 52–59.

Francese, M., Galante, G.M., La Fata, C.M., Passannanti, G., 2014. Handling Epistemic Uncertainty in the Fault Tree Analysis Using Interval-Valued Expert Information. European Safety and Reliability Conference (ESREL), Wroclaw, Poland.

Francis, R., Bekera, B., 2014. A metric and frameworks for resilience analysis of engineered and infrastructure systems. Reliab. Eng. Syst. Saf 121, 90–103.

Freeman, R.R., 2018. General method for uncertainty evaluation of safety integrity level calculations – part 2 analytical methods. Process Saf. Prog. 37 (2), 153–160.

Freeman, R.R., Summers, A., 2016. Evaluation of uncertainty in safety integrity level calculations. Process Saf. Prog. 35 (4), 341–348.

Gabriel, A., Ozansoy, C., Shi, J., 2018. Developments in SIL determination and calculation. Reliab. Eng. Syst. Saf. 177, 148–161.

Gomez-Mares, M., Tugnoli, A., Landucci, G., Cozzani, V., 2012. Performance assessment of passive fire protection materials. Ind. Eng. Chem. Res. 51, 7679–7689.

Grattan, D.J., 2018. Improving barrier effectiveness using human factors methods. J. Loss Prev. Process. Ind. 55, 400–410.

Guldenmund, F., Hale, A., Goossens, L., Betten, J., Duijm, N.J., 2006. The development of an audit technique to assess the quality of safety barrier management. J. Hazard Mater. 130 (3), 234–241.

Guo, H.T., Yang, X.H., 2007. A simple reliability block diagram method for safety integrity verification. Reliab. Eng. Syst. Saf. 92, 1267–1274.

Guo, H.T., Yang, X.H., 2008. Automatic creation of Markov models for reliability assessment of safety instrumented systems. Reliab. Eng. Syst. Saf. 93 (6), 829–837.

Han, Y., Zhen, X.W., Huang, Y., Vinnem, J.E., 2019. Integrated methodology for determination of preventive maintenance interval of safety barriers on offshore installations. Process Saf. Environ. Protect. 132, 313–324.

Harms-Ringdahl, L., 2009. Analysis of safety functions and barriers in accidents. Saf. Sci. 47 (3), 353–363.

Hauge, S., Øien, K., 2016. Guidance for Barrier Management in the Petroleum Industry. Technical report. SINTEF.

Hauge, S., Krakenes, T., Håbrekke, S., Johansen, G., Merz, M., Onshus, T., 2011. Barriers to Prevent and Limit Acute Releases to Sea. Technical report. SINTEF.

Hauge, S., Kråknes, T., Håbrekke, S., Jin, H., 2013. Reliability Prediction Method for Safety Instrumented System, PDS Method Handbook. SINTEF.
Hauge, S., Hoem, Å.S., Hokstad, P., Håbrekke, S., Lundteigen, M.A., 2015. Common Cause Failures in Safety Instrumented Systems: Beta-Factors and Equipment Specific Checklists Based on Operational Experience. Technical report. SINTEF.
Hayes, J., 2012. Use of safety barriers in operational safety decision making. Saf. Sci. 50, 424–432.
He, W.T., Wang, X.Y., Qiu, K., Zhu, J., Huang, W.J., 2016. Architecture design and safety research of a double-triple-channel redundant and fault-tolerant system. J. Loss Prev. Process. Ind. 44, 495–502.
Hellmich, M., Berg, H.P., 2015. Markov analysis of redundant standby safety systems under periodic surveillance testing. Reliab. Eng. Syst. Saf. 133, 48–58.
Hoem, Å.S., Øien, K., Hauge, S., Bodsberg, L., 2016. Aggregation and presentation of safety barrier status information Risk. In: The 26th European Safety and Reliability Conference. Glasgow, Scotland.
Hollnagel, E., 2008. Risk+barrier=safety? Safety Science 46 (2), 221–229.
IEC 61508, 2010. Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems. International Electrotechnical Commission, Geneva, Switzerland.
IEC 61511, 2016. Functional Safety - Safety Instrumented Systems for the Process Industry Sector. International Electrotechnical Commission, Geneva, Switzerland.
IEC 62061, 2005. Safety of Machinery - Functional Safety of Safety-Related Electrical, Electronic and Programmable Electronic Control Systems. International Electrotechnical Commission, Geneva, Switzerland.
IEC 62340, 2007. Nuclear Power Plants - Instrumentation and Control Systems Important to Safety - Requirements for Coping with Common Cause Failure (CCF). International Electrotechnical Commission, Geneva, Switzerland.
Innal, F., Cacheux, P.J., Collas, S., Dutuit, Y., Folleau, C., Signoret, J.-P., Thomas, P., 2014. Probability and frequency calculations related to protection layers revisited. J. Loss Prev. Process. Ind. 31, 56–69.
Innal, F., Lundteigen, M.A., Liu, Y.L., Barros, A., 2016a. PFDavg generalized formulas for SIS subject to partial and full periodic tests based on multi-phase Markov models. Reliab. Eng. Syst. Saf. 150, 160–170.
Innal, F., Chebila, M., Dutuit, Y., 2016b. Uncertainty handling in safety instrumented systems according to IEC 61508 and new proposal based on coupling Monte Carlo analysis and fuzzy sets. J. Loss Prev. Process. Ind. 44, 503–514.
ISA 84.00.07, 2010. Guidance on the evaluation of fire, combustible gas and toxic gas system effectiveness. International Society of Automation.
ISO 12100, 2012. Safety of Machinery - General Principles for Design - Risk Assessment and Risk Reduction. International Standard Organization, Geneva, Switzerland.
ISO 13577-4, 2014. Industrial Furnace and Associated Processing Equipment - Safety - Part 4: Protective Systems. International Standard Organization, Geneva, Switzerland.
ISO 13702, 2015. Petroleum and Natural Gas Industries – Control and Mitigation of Fires and Explosions on Offshore Production Installations – Requirements and Guidelines. International Standard Organization, Geneva, Switzerland.
ISO 13849, 2015. Safety of Machinery - Safety-Related Parts of Control Systems - Part 1: General Principles for Design. International Standard Organization, Geneva, Switzerland.
ISO 16530, 2017. Petroleum and Natural Gas Industries — Well Integrity. International Standard Organization, Geneva, Switzerland.
ISO 19353, 2015. Machine Safety - Preventive Fire Protection and Protection. International Standard Organization, Geneva, Switzerland.
ISO 28781, 2010. Petroleum and Natural Gas Industries — Drilling and Production Equipment —Subsurface Barrier Valves and Related Equipment. International Standard Organization, Geneva, Switzerland.
Jahanian, H., Lucas, A., 2015. The role of component arrangement in complex safety instrumented systems—a case study. Process Saf. Environ. Protect. 94, 113–130.
Janssens, J., Talarico, L., Reniers, G., Sörensen, K., 2015. A decision model to allocate protective safety barriers and mitigate domino effects. Reliab. Eng. Syst. Saf. 143, 44–52.
Jardine, A.K., Lin, D., Banjevic, D., 2006. A review on machinery diagnostics and prognostics implementing condition-based maintenance. Mech. Syst. Signal Process. 20 (7), 1483–1510.
Jia, X.J., Xing, L.D., Li, G., 2018. Copula-based reliability and safety analysis of safety-critical systems with dependent failures. Qual. Reliab. Eng. Int. 34, 928–938.
Jigar, A.A., Liu, Y.L., Lundteigen, M.A., 2016. Spurious activation analysis of safety-instrumented systems. Reliab. Eng. Syst. Saf. 156, 15–23.
Jin, H., Lundteigen, M.A., Rausand, M., 2011. Reliability performance of safety instrumented systems: a common approach for both low- and high-demand mode of operation. Reliab. Eng. Syst. Saf. 96 (3), 365–373.
Jin, H., Lundteigen, M.A., Rausand, M., 2012. Uncertainty assessment of reliability estimates for safety-instrumented systems. Proc. Inst. Mech. Eng. O J. Risk Reliab. 226 (6), 646–655.
Johansen, I.L., Rausand, M., 2015. Barrier management in the offshore oil and gas industry. J. Loss Prev. Process. Ind. 34, 49–55.
Johnson, C.W., 2003. Failure in Safety-Critical Systems: A Handbook of Accident and Incident Reporting. University of Glasgow Press, Glasgow, Scotland.
Julsereewong, A., Thepmanee, T., 2017. Safety instrumented system design in consideration of cost-benefit analysis: a case study of tail gas treating process. In: Proceedings of the 17th International Conference on Control Automation and Systems, pp. 637–642.
Kaczor, G., Młynarski, S., Szkoda, M., 2016. Verification of safety integrity level with the application of Monte Carlo simulation and reliability block diagrams. J. Loss Prev. Process. Ind. 41, 31–39.
Kanamaru, H., 2017. Bridging functional safety and cyber security of SIS/SCS. In: The 56th Annual Conference of the Society-Of-Instrument-And-Control-Engineers-Of-Japan (SICE). Kanazawa, Japan.
Kang, J., Zhang, J., Gao, J., 2016. Analysis of the safety barrier function: accidents caused by the failure of safety barriers and quantitative evaluation of their performance. J. Loss Prev. Process. Ind. 43, 361–371.
Kaur, R.K., Pandey, B., Singh, L.K., 2018. Dependability analysis of safety critical systems: issues and challenges. Ann. Nucl. Energy 120, 127–154.
Khakzad, N., Reniers, G., 2015a. Risk-based design of process plants with regard to domino effects and land use planning. J. Hazard Mater. 299, 289–297.
Khakzad, N., Reniers, G., 2015b. Using graph theory to analyze the vulnerability of process plants in the context of cascading effects. Reliab. Eng. Syst. Saf. 143, 63–73.
Khakzad, N., Reniers, G., 2017. Cost-effective allocation of safety measures in chemical plants w.r.t. land-use planning. Saf. Sci. 97, 2–9.
Khakzad, N., Landucci, G., Reniers, G., 2017. Application of graph theory to cost-effective fire protection of chemical plants during domino effects. Risk Anal. 37 (9), 1652–1667.
Khalil, Y.F., 2019. New statistical formulations for determination of qualification test plans of safety instrumented systems (SIS) subject to low/high operational demands. Reliab. Eng. Syst. Saf. 189, 196–209.
Kjellen, U., 2007. Safety in the design of offshore platforms: integrated safety versus safety as an add-on characteristic. Saf. Sci. 45, 107–127.
Kumar, V., Singh, L.K., Singh, P., Singh, K.V., Maurya, A.K., Tripathi, A.K., 2018. Parameter estimation for quantitative dependability analysis of safety-critical and control systems of NPP. IEEE Trans. Nucl. Sci. 65 (5), 1080–1090.
Kumar, P., Singh, L.K., Kumar, C., 2019. An optimized technique for reliability analysis of safety-critical systems: a case study of nuclear power plant. Qual. Reliab. Eng. Int. 35 (1), 461–469.
Kundur, D., Feng, X., Mashayekh, S., Liu, S., Zourntos, T., Butler-Purry, K.L., 2011. Towards modelling the impact of cyber attacks on a smart grid. Int. J. Secur. Network. 6 (1), 2–13.
Landucci, G., Argenti, F., Tugnoli, A., Cozzani, V., 2015. Quantitative assessment of safety barrier performance in the prevention of domino scenarios triggered by fire. Reliab. Eng. Syst. Saf. 143, 30–43.
Landucci, G., Argenti, F., Spadoni, G., Cozzani, V., 2016. Domino effect frequency assessment: the role of safety barriers. J. Loss Prev. Process. Ind. 44, 706–717.
Landucci, G., Bucelli, M., Paltrinieri, N., Cozzani, V., 2017. Domino Effect Triggered by Fire: Performance Assessment of Safety Barriers in Harsh Environmental Conditions, vol. 27. HAZARDS, Birmingham, UK.
Lauridsen, O., Lootz, E., Husebo, T., Ersdal, G., 2016. Barrier management and the interaction between technical, operational and organisational barrier elements. In: SPE International Conference and Exhibition on Health, Safety, Security, Environment, and Social Responsibility, Stavanger, Norway.
Li, Y.L., Guldenmund, F.W., 2018. Safety management systems: a broad overview of the literature. Saf. Sci. 103, 94–123.
Liu, Y.L., 2014a. Optimal staggered testing strategies for heterogeneously redundant safety systems. Reliab. Eng. Syst. Saf. 126, 65–71.
Liu, Y.L., 2014b. Discrimination of low- and high-demand modes of safety-instrumented systems based on probability of failure on demand adaptability. Proc. Inst. Mech. Eng. O J. Risk Reliab. 228 (4), 409–418.
Liu, Y.L., Rausand, M., 2011. Reliability assessment of safety instrumented systems subject to different demand modes. J. Loss Prev. Process. Ind. 24, 49–56.
Liu, Y.L., Rausand, M., 2013. Reliability effects of test strategies on safety-instrumented systems in different demand modes. Reliab. Eng. Syst. Saf. 119, 235–243.
Liu, Y.L., Rausand, M., 2016. Proof-testing strategies induced by dangerous detected failures of safety-instrumented systems. Reliab. Eng. Syst. Saf. 145, 366–372.
Longhi, A.E.B., Pessoa, A.A., Garcia, P.A.D., 2015. Multiobjective optimization of strategies for operation and testing of low-demand safety instrumented systems using a genetic algorithm and fault trees. Reliab. Eng. Syst. Saf. 142, 525–538.
Lugauer, F.P., Stiehl, T.H., Zaeh, M.F., 2016a. Functional safety of hybrid laser safety systems – how can a combination between passive and active components prevent accidents? Physics Procedia 83, 1196–1205.
Lugauer, F.P., Wimmer, F., Zaeh, M.F., 2016b. Describing statistical deviations of protection times of laser safety barriers. MM Science Journal NOV, 1445–1450.
Ma, Y., Li, M.S., Yin, Z.Y., Lian, M.J., 2017a. Design of safety PLC execution unit based on redundancy structure of heterogeneous dual-processor. In: Proceeding of the 10th International Conference on Intelligent Computation Technology and Automation, pp. 364–368.
Ma, Z.G., Yoshikawa, H., Yang, M., 2017b. Reliability model of the digital reactor protection system considering the repair time and common cause failure. J. Nucl. Sci. Technol. 54 (5), 539–551.
Macii, D., Dalpez, S., Passerone, R., Corrà, M., Avancini, M., Benciolini, L., 2015. A safety instrumented system for rolling stocks: methodology, design process and safety analysis. Measurement 67, 164–176.
Mancuso, A., Compare, M., Salo, A., Zio, E., 2016. Bayesian approach for safety barrier portfolio optimization. In: The 26th European Safety and Reliability Conference. Glasgow, Scotland.
Markert, F., Duijma, N.J., Thommesen, J., 2013. Modelling of safety barriers including human and organisational factors to improve process safety. Chem. Eng. Process 31, 283–288.
McLeod, R.W., 2017. Human factors in barrier management: hard truths and challenges. Process Saf. Environ. Protect. 110, 31–42.
Mechri, W., Simon, C., BenOthman, K., 2015. Switching Markov chains for a holistic modeling of SIS unavailability. Reliab. Eng. Syst. Saf. 133, 212–222.
Meng, H.X., Kloul, L., Rauzy, A., 2018. Modeling patterns for reliability assessment of safety instrumented systems. Reliab. Eng. Syst. Saf. 180, 111–123.

Misuri, A., Landucci, G., Cozzani, V., 2020. Assessment of safety barrier performance in Natech scenarios. Reliab. Eng. Syst. Saf. 193, 106597.
Miura, K., Morooka, C.K., Mendes, J.R.P., Guilherme, I.R., 2006. Characterization of operational safety in offshore oil wells. J. Petrol. Sci. Eng. 51, 111–126.
Mkhida, A., Thiriet, J.M., Aubry, J.F., 2014. Integration of intelligent sensors in safety instrumented systems (SIS). Process Saf. Environ. Protect. 92 (2), 142–149.
Moreno, V.C., Guglielmi, D., Cozzani, V., 2018. Identification of critical safety barriers in biogas facilities. Reliab. Eng. Syst. Saf. 169, 81–94.
NEA-Nuclear Energy Agency, 2003. Engineered Barrier Systems (EBS) in the Context of the Entire Safety Case. OECD, Paris, France.
NRC-National Research Council, 2007. Assessment of the Performance of Engineered Waste Containment Barriers. The National Academies Press, Washington, DC.
Øien, K., Hauge, S., Tørseth, F., Tinmannsvik, R.K., 2015. Towards a holistic approach for barrier management in the petroleum industry. Technical report. SINTEF.
OREDA0, 2015. Offshore & Onshore Reliability Data Handbook, sixth ed. OREDA Participants.
Paltrinieri, N., Landucci, G., Molag, M., Bonvicini, S., Spadoni, G., Cozzani, V., 2009. Risk reduction in road and rail LPG transportation by passive fire protection. J. Hazard Mater. 167, 332–344.
Paltrinieri, N., Bonvicini, S., Spadoni, G., Cozzani, V., 2012. Cost-benefit analysis of passive fire protections in road LPG transportation. Risk Anal. 32, 200–219.
Pitblado, R., Nelson, W.R., 2013. Advanced safety barrier management with inclusion of human and organizational aspects. Chem. Eng. Process 31, 331–336.
Pitblado, R., Potts, T., Fisher, M., Greenfield, S., 2015. A method for barrier-based incident investigation. Process Saf. Prog. 34 (4), 328–334.
Pitblado, R., Fisher, M., Nelson, B., Fløtaker, H., Molazemi, K.A., 2016. Stokke. Concepts for dynamic barrier management. J. Loss Prev. Process. Ind. 43, 741–746.
Prashanth, I., Fernandez, G.J., Sunder, R.G., Boardman, B., 2017. Factors influencing safety barrier performance for onshore gas drilling operations. J. Loss Prev. Process. Ind. 49, 291–298.
PSA-Petroleum Safety Authority, 2011. Regulations Relating to Management and the Duty to Provide Information in the Petroleum Activities and at Certain Onshore Facilities. Petroleum Safety Authority Norway.
Rahimi, M., Rausand, M., 2013. Monitoring human and organizational factors influencing common-cause failures of safety-instrumented system during the operational phase. Reliab. Eng. Syst. Saf. 120, 10–17.
Ramzali, N., Lavasani, M.R.M., Ghodousi, J., 2015. Safety barriers analysis of offshore drilling system by employing Fuzzy event tree analysis. Saf. Sci. 78, 49–59.
Rathnayakaa, S., Khan, F., Amyotte, P., 2011. SHIPP methodology: predictive accident modeling approach. Part II. Validation with case study. Process Saf. Environ. Protect. 89 (2), 75–88.
Rausand, M., 2011. Risk Assessment: Theory, Methods and Applications. John Wiley & Sons, Hoboken, NJ.
Rausand, M., 2014. Reliability of Safety-Critical Systems: Theory and Applications. John Wiley & Sons, Hoboken, NJ.
Reason, J., Hollnagel, E., Paries, J., 2006. Revisiting the "Swiss cheese" model of accidents. EUROCONTROL Experimental Center.
Rollenhagen, C., 2011. Event investigations at nuclear power plants in Sweden: reflections about a method and some associated practices. Saf. Sci. 49 (1), 21–26.
RWM-Radioactive Waste Management, 2016. Geological disposal: engineered barrier system status report, nuclear decommissioning authority: didcot, UK.
Schupp, B., Smith, S., Wright, P., Goossens, L., 2004. Integrating human factors in the design of safety-critical systems – a barrier based approach. In: Johnson, W., Palanque, P. (Eds.), Human Error, Safety and Systems Development (HESSD 2004), vol. 152, pp. 285–300.
Selvik, J.T., Abrahamsen, E.B., 2017. How to classify failures when collecting data for safety-instrumented systems in the oil and gas industry. J. Risk Res. 20 (7), 952–962.
Shahrokhi, M., Bernard, A., 2010. A development in energy flow/barrier analysis. Saf. Sci. 48 (5), 598–606.
Shin, J.H., Jun, H.B., 2015. On condition based maintenance policy. Journal of Computational Design and Engineering 2 (2), 119–127.
Simon, C., Mechri, W., Capizzi, G., 2019. Assessment of safety integrity level by simulation of dynamic Bayesian networks considering test duration. J. Loss Prev. Process. Ind. 57, 101–113.
Singh, P., Singh, L.K., 2019. Design of safety critical and control systems of nuclear power plants using Petri nets. Nuclear Engineering and Technology 51 (5), 1289–1296.
Sklet, S., 2006. Safety barriers: definition, classification, and performance. J. Loss Prev. Process. Ind. 19 (5), 494–506.
Skorupski, J., 2015. The risk of an air accident as a result of a serious incident of the hybrid type. Reliab. Eng. Syst. Saf. 140, 37–52.
Sliwiniski, M., 2018. Safety integrity level verification for safety-related functions with security aspects. Process Saf. Environ. Protect. 118, 79–92.
Sobral, J., Soares, C.G., 2019. Assessment of the adequacy of safety barriers to hazards. Saf. Sci. 114, 40–48.
Summers, A., 2018. Spring meeting of the American-Institute-of-Chemical-Engineers (AIChE)/13th global congress on process safety. Inherently safer automation 37 (1), 31–36.
Sun, F., Xu, W., Wang, G.J., Sun, B., 2017. A technique to control major hazards of the coal gasification process developed from critical events and safety barriers. Process Saf. Prog. 36 (4), 382–391.
Szymanek, A., 2010. Defence-in-Depth" strategy in transport risk management. In: Proceedings of TST 2010, CCIS, vol. 104. Springer-Verlag, Berlin Heidelberg, pp. 51–58.
Tang, Z.C., Zuo, M.J., Xia, Y.J., 2017. Effect of truncated input parameter distribution on the integrity of safety instrumented systems under epistemic uncertainty. IEEE Trans. Reliab. 66 (3), 745–750.
Torres-Echeverria, A.C., Martorell, S., Thompson, H.A., 2009. Design optimization of a safety-instrumented system based on RAMS+C addressing IEC 61508 requirements and diverse redundancy. Reliab. Eng. Syst. Saf. 94 (2), 162–179.
Torres-Echeverria, A.C., Martorell, S., Thompson, H.A., 2011. Modeling safety instrumented systems with MooN voting architectures addressing system reconfiguration for testing. Reliab. Eng. Syst. Saf. 96 (5), 545–563.
Tsunemi, K., Kihara, T., Kato, E., Kawamoto, A., Saburi, T., 2019. Quantitative risk assessment of the interior of a hydrogen refueling station considering safety barrier systems. Int. J. Hydrogen Energy 44 (41), 23522–23531.
Tugnoli, A., Cozzani, V., Di Padova, A., Barbaresi, T., Tallone, F., 2012. Mitigation of fire damage and escalation by fireproofing: a risk-based strategy. Reliab. Eng. Syst. Saf. 105, 25–35.
Tugnoli, A., Landucci, G., Villa, V., Argenti, F., Cozzani, V., 2013. The performance of inorganic passive fire protections: an experimental and modelling study. Chemical Engineering Transactions 32, 427–432.
van Oosterom, C., Maillart, L.M., Kharoufeh, J.P., 2017. Optimal maintenance policies for a safety-critical system and its deteriorating sensor. Nav. Res. Logist. 64 (5), 399–417.
Verlinden, S., Deconinck, G., Coupe, B., 2012. Hybrid reliability model for nuclear reactor safety system. Reliab. Eng. Syst. Saf. 101, 35–47.
Vinnem, J.E., Bye, R., Gran, B.A., Kongsvik, T., Nyheim, O.M., Okstad, E.H., Seljelid, J., Vatn, J., 2012. Risk modelling of maintenance work on major process equipment on offshore petroleum installations. J. Loss Prev. Process. Ind. 25 (2), 274–292.
Wang, Y., West, H.H., Mannan, M.S., 2004. The impact of data uncertainty in determining safety integrity level. Process Saf. Environ. Protect. 82 (B6), 393–397.
Wang, F., Yang, O., Zhang, R., Shi, L., 2016a. Method for assigning safety integrity level (SIL) during design of safety instrumented systems (SIS) from database. J. Loss Prev. Process. Ind. 44, 212–222.
Wang, T.R., Pedroni, N., Zio, E., 2016b. Identification of protective actions to reduce the vulnerability of safety-critical systems to malevolent acts: a sensitivity-based decision-making approach. Reliab. Eng. Syst. Saf. 147, 9–18.
Winge, S., Albrechtsen, E., 2018. Accident types and barrier failures in the construction industry. Saf. Sci. 105, 158–166.
Woods, D.D., 2015. Four concepts for resilience and the implications for the future of resilience engineering. Reliab. Eng. Syst. Saf. 141, 5–9.
Wu, L.L., 2015. Improving System Reliability for Cyber-Physical Systems. PhD Thesis. Columbia University.
Wu, S.N., Zhang, L.B., Lundteigen, M.A., Liu, Y.L., Zheng, W.P., 2018a. Reliability assessment for final elements of SISs with time dependent failures. J. Loss Prev. Process. Ind. 51, 186–199.
Wu, S.N., Zhang, L.B., Barros, A., Zheng, W.P., Liu, Y.L., 2018b. Performance analysis for subsea blind shear ram preventers subject to testing strategies. Reliab. Eng. Syst. Saf. 169, 281–298.
Xie, L., Lundteigen, M.A., Liu, Y.L., 2018a. Common cause failures and cascading failures in technical systems: similarities, differences and barriers. In: 2018 European Safety and Reliability Conference (ESREL 2018). Trondheim, Norway.
Xie, L., Lundteigen, M.A., Liu, Y.L., 2018b. Safety barriers against common cause failure and cascading failures: a review and pilot analysis. In: 2018 IEEE International Conference on Industrial Engineering and Engineering Management. Bangkok, Thailand.
Xie, L., Lundteigen, M.A., Håbrekke, S., Liu, Y.L., 2019. Operational data-driven prediction for failure rates of equipment in safety-instrumented systems: a case study from the oil and gas industry. J. Loss Prev. Process. Ind. 60, 96–105.
Xie, L., Lundteigen, M.A., Liu, Y.L., 2020. Reliability and barrier assessment of series-parallel systems subject to cascading failures. Proc. Inst. Mech. Eng. O J. Risk Reliab. https://doi.org/10.1177/1748006X19899235.
Xue, L., Fan, J., Rausand, M., Zhang, L., 2013. A safety barrier-based accident model for offshore drilling blowouts. J. Loss Prev. Process. Ind. 26, 164–171.
Zeng, Z., Zio, E., 2018. Dynamic risk assessment based on statistical failure data and condition-monitoring degradation data. IEEE Trans. Reliab. 67 (2), 609–622.
Zhang, A.B., Liu, Y.L., Barros, A., Wang, Y.K., 2018. Prognostic and health management for safety barriers in infrastructures: opportunities and challenges. In: 2018 European Safety and Reliability Conference (ESREL 2018), Trondheim, Norway.
Zhang, A.B., Barros, A., Liu, Y.L., 2019. Performance analysis of redundant safety-instrumented systems subject to degradation and external demands. J. Loss Prev. Process. Ind. 62, 103946.
Zhang, A.B., Zhang, T.L., Barros, A., Liu, Y.L., 2020. Optimization of maintenances following proof tests for the final element of a safety-instrumented system. Reliab. Eng. Syst. Saf. 196, 106779.
Zhen, X.W., Vinnem, J.E., Han, Y., Peng, C.Y., Yang, X., Huang, Y., 2020. New risk control mechanism for innovative deepwater artificial seabed system through online risk monitoring system. Appl. Ocean Res. 95, 102054.
Zhu, P., Liyanage, J.P., 2018. Application of prognostics and health management to low demand systems: use of condition data to help determine function test interval. In: 2018 IEEE International Conference on Industrial Engineering and Engineering Management, Bangkok, Thailand.
Zhu, Y., Khakzad, N., Khan, F., Amyotte, P., 2015. Risk-based optimal safety measure allocation for dust explosions. Saf. Sci. 74, 79–92.