Available online at www.sciencedirect.com
SCIENCE DIRECT
Journal of Loss Prevention in the Process Industries 19 (2006) 494–506
Journal of Loss Prevention in the process industries
www.elsevier.com/locate/jlp

Safety barriers: Definition, classification, and performance

Snorre Sklet*

Department of Production and Quality Engineering, The Norwegian University of Science and Technology (NTNU), NO-7491 Trondheim, Norway

Received 18 October 2005; received in revised form 6 December 2005; accepted 6 December 2005

Abstract

In spite of the fact that the concept of safety barriers is applied in practice, discussed in the literature, and even required in legislation and standards, no common terminology that is applicable across sectors have been developed of the concept of safety barriers. This paper focuses on safety barriers and addresses the following aspects; definitions and understanding of what is a safety barrier, classification of safety barriers, and attributes of importance for the performance of safety barriers. Safety barriers are physical or non-physical means planned to prevent, control, or mitigate undesired events or accidents. Barrier systems may be classified according to several dimensions, for example as passive or active barrier systems, and as physical, technical, or human/operational barrier systems. Several attributes are necessary to include in order to characterize the performance of safety barriers; functionality/effectiveness, reliability/availability, response time, robustness, and finally a description of the triggering event or condition. For some types of barriers, not all the attributes are relevant or necessary in order to describe the barrier performance.

Keywords: Safety barrier; Defence-in-depth; Barrier performance; Risk analysis

1. Introduction

Safety barriers have been used to protect humans and property from enemies and natural hazards since the origin of human beings. When human-induced hazards were created due to the industrialism, safety barriers were implemented to prevent accidents caused by these hazards. The concept of safety barriers is often related to an accident model called the energy model (see Fig. 1). Gibson (1961) pioneered the development of the energy model, while Haddon (1980) developed the model further as he presented his ten strategies for accident prevention. Safety barriers also play an important role in the Management Oversight & Risk Tree (MORT) concept (Johnson, 1980).

During recent years, an extended perspective on safety barriers has evolved. This is emphasized by Hollnagel (2004) who states that "whereas the barriers used to defend a medieval castle mostly were of a physical nature, the modern principle of defence-in-depth combines different types of barriers—from protection against the release of radioactive materials to event reporting and safety policies". This development is also supported by Fleming and Silady (2002) who states that "the definitions of defence-in-depth have evolved from a rather simple set of strategies to apply multiple lines of defence to a more comprehensive set of cornerstones, strategies, and tactics to protect the public health and safety". The concept of defence-in-depth was developed within the nuclear industry, but is also used in other high risk industries (e.g., the process industry where also the term multiple protection layers is used; CCPS, 1993).

The focus on the use of risk-informed principles and safety barriers in European regulations such as the Seveso II directive (EC, 1996) and the Machinery directive (EC, 1998), national regulations as the Management regulation from the Petroleum Safety Authority Norway (PSA) (PSA, 2001), and standards such as IEC:61508 (1998), IEC:61511 (2002), and ISO:13702 (1999) demonstrates the importance of safety barriers in order to reduce the risk of accidents. PSA has developed requirements to safety barriers, but has not given a clear definition of the concept. Discussions have emerged on what is a safety barrier. Specialists do not fully agree on this issue and it is difficult for the companies

*Tel.: +47 73 59 29 02; fax: +47 73 59 28 96.
E-mail address: snorre.sklet@sintef.no.

0950-4230/$ - see front matter © 2006 Elsevier Ltd. All rights reserved.
doi:10.1016/j.jlp.2005.12.004

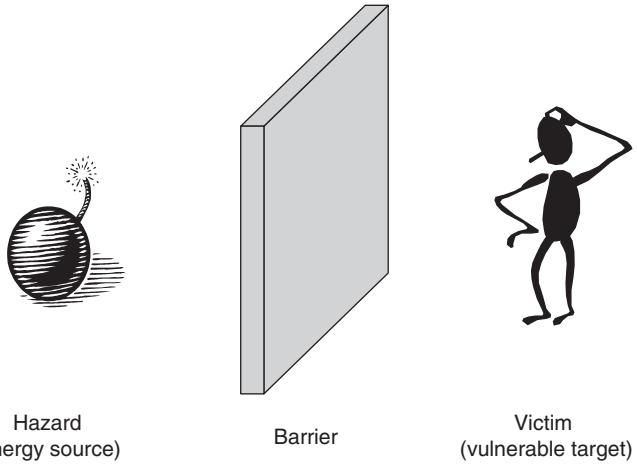


Fig. 1. The energy model (based on Haddon, 1980).

to know how to fulfil the requirements. It is also difficult for the PSA to manage the regulations without a clear definition and delimitation of the concept.

No common definition of the term safety barrier has been found in the literature, although different aspects of the term have been discussed, see, e.g., (CCPS, 2001; Duijm, Andersen, Hale, Goossens, & Hourtolou, 2004; Goossens & Hourtolou, 2003; Harms-Ringdahl, 2003; Hollnagel, 2004; Johnson, 1980; Kecklund, Edland, Wedin, & Svenson, 1996; Neogy, Hanson, Davis, & Fenstermacher, 1996; Rosness, 2005; Sklet & Hauge, 2004; Svenson, 1991), and applied in practice for several decades. Different terms with similar meanings (barrier, defence, protection layer, safety critical element, safety function, etc.) have been used crosswise between industries, sectors, and countries. Safety barriers are categorized in numerous ways by different authors and the performance of the barriers is described in several ways.

The extended use of the term safety barrier (and similar terms) and the lack of a common terminology imply a need for clarifying the terminology both in the Norwegian offshore industry and crosswise between sectors. This need is supported by the following statement from Kaplan (1990); "When words are used sloppily, concepts become fuzzy, thinking is muddled, communication is ambiguous, and decisions and actions are suboptimal, to say the least". To clarify the terms will be useful in order to avoid misconceptions in communication about risk and safety barriers. The results should be of general interest, and furthermore, a clarification of the term will make it easier for the Norwegian offshore industry to fulfil the requirements from the PSA with respect to classification of barriers and analysis of the performance of different types of safety barriers and barrier elements.

The objectives of the paper are: (1) to present a survey of how the concept safety barrier and similar concepts are interpreted and used in various industries and various applications, (2) to provide a clear definition of the concept safety barrier, and associated concepts like barrier function, barrier system, and barrier element, (3) to develop a classification system for safety barriers, (4) to define attributes describing the performance of safety barriers, and (5) to give recommendations on how the concept of safety barrier should be interpreted and used in different contexts.

The paper is based on experience from a literature survey concerning the understanding of safety barriers in different industries, several projects focusing on analysis of safety barriers (e.g., the BORA project (Barrier and Operational Risk Analysis) (Aven, Sklet, & Vinnem, 2005; Sklet, Aven, Hauge, & Vinnem, 2005; Sklet, Vinnem, & Aven, 2005; Vinnem, Aven, Hauge, Seljelid, & Veire, 2004) and a project on behalf of PSA focusing on barriers during well interventions (Sklet, Steiro, & Tjelta, 2005), and a study of how safety barriers are analysed in different accident investigation methods (Sklet, 2004). The literature is identified in literature databases, from references in reviewed literature, and by attending international conferences.

The main focus in this paper is the use of the barrier concept within industrial safety, especially as applied to technical systems in the process and nuclear industry. Even though the main focus is on demands for clarification of the term safety barrier from the Norwegian offshore industry, the discussions are also relevant for other industries (e.g., the process industry) and application areas (e.g., the transport sector). The focus is on the risk of major accidents, i.e., occupational accidents have not been discussed in detail. The attention is directed toward safety issues, but the concepts may also be useful for security issues.

The concept of safety barriers is briefly introduced in this section together with the purpose of the paper. The next section discusses what a safety barrier is and gives an overview of some definitions applicable for explanation of the concept of safety barriers. Section three gives an overview of some schemes for classification of barrier functions and barrier systems. Several measures of barrier performance are presented and discussed in section four. Comments, a brief discussion, and recommendations are included in each section. Finally, some conclusions concerning the concept of safety barriers end the paper.

2. What is a safety barrier?

2.1. Features of safety barriers

The term safety barrier and similar terms like defence (in-depth), layer of protection, safety (critical) function, safety critical element, and safety system are applied in regulations, standards, and the scientific literature. A literature review (e.g., CCPS, 2001; Duijm et al., 2004; Goossens & Hourtolou, 2003; Harms-Ringdahl, 2003; Hollnagel, 2004; Johnson, 1980; Kecklund et al., 1996; Neogy et al., 1996; Rosness, 2005; SfS, 2004; Sklet & Hauge, 2004; Svenson, 1991) shows that there is no

universal and commonly accepted definition of these terms in the literature. In the Oxford English Dictionary (OED, 2005) a barrier is defined as a "fence of material obstruction of any kind erected (or serving) to bar the advance of persons or things, or to prevent access to a place".

The concept of defence-in-depth constitutes the basis for the discussion of safety barriers. IAEA (1999) describes the defence-in-depth principle in the following way: "To compensate for potential human and mechanical failures, a defence in depth concept is implemented, centred on several levels of protection including successive barriers preventing the release of radioactive material to the environment. The concept includes protection of the barriers by averting damage to the plant and to the barriers themselves. It includes further measures to protect the public and the environment from harm in case these barriers are not fully effective". As mentioned above, the term safety barrier is often used in a broader meaning as a collective term for different means used to realize the concept of defence-in-depth.

A safety barrier is related to a hazard, an energy source or an event sequence. This is supported by the requirement stated by PSA (2001); "it shall be known what barriers have been established and which function they are intended to fulfil". This means that a barrier should be well defined or formalised and be related to a specific hazard.

Hollnagel (1999) states that in daily language the term barrier is largely synonymous with the notion of a barrier function. To be linguistically stringent, we should use the term barrier function instead of only barrier. It is common to distinguish between barrier functions and barrier systems (see, e.g., Andersen et al., 2004; ISO:13702, 1999; Kecklund et al., 1996; Svenson, 1991). According to Svenson (1991), a barrier function represents a function (and not, e.g., an object) which can arrest the accident evolution so that the next event in the chain is never realized, while a barrier system is maintaining the barrier function. A barrier system may consist of several barrier elements, and the elements may be of different types (e.g., technical, operational, human, and software). The different definitions of barriers seem to cover all phases of an accident sequence and include prevention, control, and mitigation.

2.2. Recommendations

Based on the synthesis of some common features of the terms, the following definitions of the terms safety barrier, barrier function, and barrier system are proposed as basis for further discussion and analysis of safety barriers.

- *Safety barriers are physical and/or non-physical means planned to prevent, control, or mitigate undesired events or accidents*

The means may range from a single technical unit or human action, to a complex socio-technical system. Planned implies that at least one of the purposes of the means is to reduce the risk. In line with ISO:13702, prevention means reduction of the likelihood of a hazardous event, control means limiting the extent and/or duration of a hazardous event to prevent escalation, while mitigation means reduction of the effects of a hazardous event. Undesired events are, e.g., technical failures, human errors, external events, or a combination of these occurrences that may realize potential hazards. Accidents are undesired and unplanned events that lead to loss of human lives, personal injuries, environmental damage, and/or material damage.

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

Barrier functions describe the purpose of safety barriers or what the safety barriers shall do in order to prevent, control, or mitigate undesired events or accidents. If a barrier function is performed successfully, it should have a direct and significant effect on the occurrence and/or consequences of an undesired event or accident. A function that has at most an indirect effect is not classified as a barrier function, but as a risk influencing factor/function. A barrier function should preferably be defined by a verb and a noun, e.g., "close flow" and "stop engine". The verbs avoid, prevent, control, and protect are suggested in the ARAMIS (Accidental Risk Assessment Methodology for Industries in the Context of the Seveso II Directive) project (Andersen et al., 2004) to describe generic barrier functions. Sometimes it may be necessary to include a modifier describing the object of the function.

- *A barrier system is a system that has been designed and implemented to perform one or more barrier functions*

A barrier system describes how a barrier function is realized or executed. If the barrier system is functioning, the barrier function is performed. A barrier system may have several barrier functions. In some cases, there may be several barrier systems that carry out a barrier function. A barrier element is a component or a subsystem of a barrier system that by itself is not sufficient, to perform a barrier function. A barrier subsystem may comprise several redundant barrier elements. In this case, a specific barrier element does not need to be functioning for the system to perform the barrier function. This is the case for redundant gas detectors connected in a k-out-of-n configuration. The barrier system may consist of different types of system elements, e.g., physical and technical elements (hardware, software), operational activities executed by humans, or a combination thereof.

2.3. Comments

Even though the proposed definitions may be slightly different from other definitions of safety barriers proposed

(DoE, 1997; Hollnagel, 2004; ISO:17776, 2000; Rosness, 2005; SfS, 2004) and protection layer proposed by CCPS (2001) and IEC:61508/11, the interpretations of the proposed definitions are in accordance with these definitions. However, CCPS and IEC:61508 stress the independence between different protection layers as part of their definitions. Barriers are restricted to flow of energy in MORT (Johnson, 1980) where barriers are defined as "the physical and procedural measures to direct energy in wanted channels and control unwanted release". In the ARAMIS-project (Duijm et al., 2004), the safety barriers are limited to focus on release of hazardous agents and the following definition is applied; "A safety barrier is a system element that prevents, limits, or mitigates the release of a hazardous agent". Another equivalent term to safety barrier is the commonly used term defence that Reason (1997) defines as "various means by which the goals of ensuring the safety of people and assets can be achieved". Reason describes defence-in-depth as "successive layers of protection". Within the concept of MTO-analysis (Human, Techology, and Organizations) applied in accident investigations, a safety barrier is defined as "any operational, organisational, or technical solution or system that minimizes the probability of events to occur, and limit the consequences of such events" (Bento, 2003). It seems that almost all types of organizational risk influencing factors are included as barriers in the MTO-diagrams presented in the investigation reports.

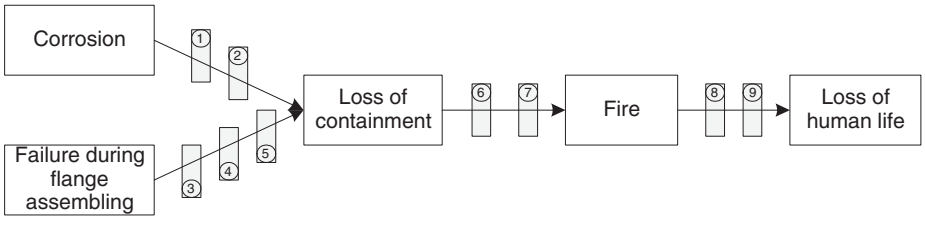
The definition of a barrier function is similar to several definitions of the term safety function. For example, as presented by Harms-Ringdahl (2000) who states that "a safety function is a technical, organisational or combined function, which can reduce the probability and/or consequences of a set of hazards in a specific system", and IEC:61511 that defines safety function as "a function […] which is intended to achieve or maintain a safe state for the process, in respect of a specific hazardous event". A system may have several functions, and the barrier function may be one of them (Rausand & Høyland, 2004). For example, the essential function of a pipe on an oil platform is to transport hydrocarbons from system A to system B, whereas the barrier function to prevent release of hydrocarbons to the atmosphere is an auxiliary function. Sometimes a failure of the auxiliary function may be as least as critical as a failure of the essential function.

Most of the authors cover both physical and non-physical barriers as part of their definitions, but two exceptions are Holand (1997) and IAEA (1999). Holand defines a well barrier as a physical item only, while IAEA distinguishes between physical barriers and other types of protection where both types are incorporated in the concept of defence-in-depth.

There are distinctions between the different definitions regarding to which extent barriers should influence the energy flow or event sequence. On one hand, ISO:17776 (2000) states that a barrier should "reduce the probability" or "reduce the consequences". On the other hand, Holand (1997) says that a barrier should "prevent the flow" and CCPS (2001) says that a protection layer should be "capable of preventing a scenario from proceeding to the undesired consequences". This topic is related to the effectiveness of the barrier and is further discussed in Section 4 about barrier performance.

Another aspect of the definition is whether such a broad definition undermines the concept of barrier as some claim that almost everything may be considered as a barrier. Therefore, it is important to distinguish between the barrier itself that may prevent, control, or mitigate the event sequence or accident scenario directly (as illustrated in Fig. 2), and the risk influencing factors that influence the barrier performance. Examples on risk influencing factors are competence of a third party checker and testing of gas detectors. Thus, it is important to specify the barrier function in order to clarify at which level different barriers influence the accident scenario. This may be illustrated by the following example; the containment (e.g., a pipe) should prevent release of hydrocarbon to the atmosphere, while inspection is executed to reveal corrosion such that risk reducing measures may be implemented to prevent that corrosion results in a leak.

At least two different accident models or perspectives may be the basis for the concept of safety barriers; the *energy model* and the *process model*. The basic principle in the energy model is to separate hazards (energy sources) from victims (vulnerable targets) by safety barriers (Haddon, 1980). Process models divide the accident



1. Condition monitoring to reveal corrosion
2. Inspection to reveal corrosion
3. Self control of work to reveal failure
4. 3rd party control of work to reveal failure
5. Leak test to reveal failure
6. Process shutdown to reduce size of release
7. Disconnection of ignition sources to prevent ignition
8. Deluge activation to extinguish fire
9. Escape ways for evacuation

Fig. 2. Illustration of barriers influencing a process accident.

sequences in different phases and help us to understand how a system gradually deteriorates from a normal state into a state where an accident occurs (Kjellén, 2000). For process models, factors that prevent transitions between phases in the accident sequence (or process) may be regarded as safety barriers. While the energy model focuses primarily on how to avoid injuries or losses due to release of energy, process models are more focused on event sequences or work processes.

3. Classification of safety barriers

3.1. Classification of barrier functions

When barrier functions are related to a process model or phases in an accident sequence, it is common to classify the barrier functions as *prevention*, *control*, and *mitigation* (IEC:61508, IEC:61511, ISO:13702). This classification is similar to the categorization of barrier functions used in MORT (Johnson, 1980), where the terms prevention, control, and minimization are used. Hollnagel (2004) describes only two main functions for safety barriers; prevention and protection. Barriers intended to work before a specific initiating event takes place serve as a means of prevention. They are supposed to ensure that the accident does not happen, or at least to slow down the developments that may result in an accident. Barriers intended to work after a specific initiating event has taken place, serve as means of protection, and are supposed to shield the environment and the people in it, as well as the system itself, from the consequences of the accident.

The ARAMIS-project (Andersen et al., 2004) classifies safety functions into four main categories described by the action verbs to *avoid*, to *prevent*, to *control*, and to *protect*. These verbs are described by Duijm et al. (2003), and the avoid function aims at suppressing all the potential causes of an event by changing the design of the equipment or the type of product used, e.g., the use of a non-flammable product is a way to avoid fire. The prevent function aims at reducing the probability of an event by suppressing part of its potential causes or by reducing their intensity, e.g., to prevent corrosion, a better steel grade can be used. It is probably not sufficient to avoid it, but it may reduce its probability. The control function aims at limiting the deviation from a normal situation to an unacceptable one. A pressure relief system and a computerized supervision system perform a control function. Once an event has occurred, it is necessary to protect the environment from its consequences.

Another viewpoint is used by Vatn (2001) while discussing safety critical functions within the Norwegian railway industry. He differentiates between *primary*, *secondary*, and *tertiary safety critical* functions. Primary safety critical functions are related to technical systems for the rolling material, the rail network, and the traffic control. Secondary safety critical functions are activities performed in order to maintain the primary safety critical functions. Tertiary safety critical functions are safety management systems, maintenance management systems, etc. Wahlström and Gunsell (1998) distinguish between *primary* and *secondary barriers*, and as Vatn, they relate the term secondary barriers to control/surveillance of the primary barriers. A similar approach is presented by Schupp (2004), where primary barriers are associated with primary hazards, and secondary barriers with functional hazards. Primary hazards are hazards that are directly harmful to humans, the environment, or the economy, while functional hazards are hazardous to functions of the process (or plant) system. A functional hazard may indirectly become hazardous to humans, for instance, corrosion is a common functional hazard. Corrosion may cause the containment system to fail, thus releasing a primary hazard.

Leveson (1995) focuses on barriers related to software systems and distinguishes between three types of barrier functions, *lockout*, *lockin*, and *interlock*. A lockout "prevents a dangerous event from occurring or prevents someone or something from entering a dangerous area or state", a lockin is "something that maintains a condition or preserves a system state", while an interlock serves "to enforce correct sequencing or to isolate two events in time".

In Fig. 3 the different barrier functions are related to phases in the Occupational Accident Research Unit (OARU) process model (Kjellén & larsson, 1981). The accident sequence is divided into three phases, the initial phase, the concluding phase, and the injury phase. The generic safety functions prevent, control, and mitigate are related to the transitions between the different phases in the OARU-model. To prevent means to prevent transition

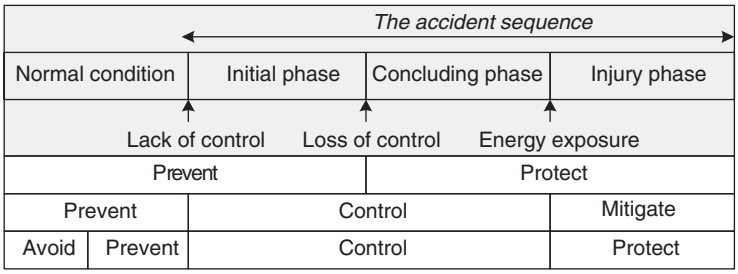


Fig. 3. Generic safety functions related to a process model.

from normal condition to a state of lack of control. To control means to prevent transition from lack of control to loss of control, while to mitigate means to prevent that the targets start to absorb energy.

According to the classification described by Hollnagel (2004) in prevention and protection, both control and mitigation go into protection. As a comment to this classification, Sklet and Hauge (2003) emphasize that there are two types of preventive barriers that both have to function before the initiating event occurs; preventive functions that are introduced to reduce the probability of an initiating event, and preventive functions that are introduced to reduce the probability of escalation (e.g., measures for reducing the probability of ignition, as area classification and restrictions on hot work). However, whether safety functions are classified as preventing or protecting, depends on the definition of the initiating event. This topic may be illustrated by the following example; the process shutdown function "protection against overpressure" is preventing related to the initiating event "release", but protecting (or controlling) related to the initiating event "overpressure".

The classification suggested in the ARAMIS-project (Duijm et al., 2003) is more detailed than the tri-partition (prevention, control, mitigation). Compared to tri-partition (see also Fig. 3), both the functions avoid and prevent used in ARAMIS correspond to the function prevention in Fig. 3. The function control in ARAMIS corresponds to control in Fig. 3, while the term protect used by ARAMIS corresponds to mitigation.

3.2. Classification of barrier systems

A commonly used categorization is to distinguish between *physical* and *non-physical* barriers as used in MORT (Johnson, 1980), in ISO:17776 (2000), and by DoE (1997). Also PSA (2002) states that barriers may be physical or non-physical, or a combination thereof. Reason (1997) uses the terms *hard* and *soft defences*. Wahlström and Gunsell (1998) make a similar classification, and differentiate between *physical*, *technical*, and *administrative* barriers. Physical barriers are incorporated in the design of a construction, technical barriers are initiated if a hazard is realized, while administrative barriers are incorporated in administrative systems and procedures.

Svenson (1991) classifies barrier systems as physical, *technical*, or *human factors-organizational* systems, while Neogy et al. (1996) classify barriers as *physical*, procedural or administrative, or *human action*. In a study of the refuelling process in a nuclear power plant, Kecklund et al. (1996) classify barrier functions as technical, human, or human/organizational. The technical barrier functions are performed by a technical barrier system, and correspondingly, human barrier functions are performed by human barrier function systems. Human/organisational barrier functions can be seen as planned into the process but in the end executed by humans with the support of an organisation designing the refuelling work process. DoE (1997) has a similar perspective as Kecklund et al. and distinguishes between physical and management barriers. DoE claims that management barriers exist at three levels within the organisation, the activity level, the facility level, and the institutional level.

Management barriers may be seen as a kind of *organisational control*, and Hopwood (1974) describes three types of organisational controls; *administrative*, *social*, and *self-control*. Johnson and Gill (1993) define administrative control as "those mechanisms, techniques, and processes that have been consciously and purposefully designed in order to try to control the organisational behaviour(s) of other individuals, groups and organisations". Administrative controls may involve control of the process or the output. By contrast, where socialization is not the result of a planned strategy, but, instead, arises spontaneously out of the everyday social interaction among members, we are referring to the informed area of social control. Self-control is defined as "the control people exert over their own behaviour". In order for this to happen, the norms embodied in administrative or social control must be "either directly or indirectly […] internalized by the members of the enterprise and operate as personal controls over attitudes and behaviour". Due to advances in technology, Reason, Parker, and Lawton (1998) add another control mechanism, *technical controls*, that include engineered safety features.

Reason (1997) claims that administrative controls form a major part of any hazardous system's defences and are of two main kinds (based on Johnson & Gill, 1993); (a) *external controls* made up of rules, regulations, and procedures that closely prescribe what actions may be performed and how they should be carried out, and (b) *internal controls* derived from the knowledge and principles acquired through training and experience. External controls are written down, while internal controls seldom are written down.

In IEC:61511, risk reduction measures are categorized as: (1) *safety instrumented systems* (SIS),[1] (2) *other technology safety-related systems*, and (3) *external risk reduction facilities*. A SIS is composed of any combination of sensor(s), logic solver(s), and final element(s). Other technology safety-related systems are safety-related systems based on a technology other than electrical, electronic, or programmable electronic, for example, a relief valve. External risk reduction facilities are measures to reduce or mitigate the risk that is separate and distinct from the SIS or other technology safety-related systems, e.g., drain systems and firewalls.

A comparison of some terms used to classify barrier systems according to the main division line between "physical" ("left side") or "non-physical" ("right side") is shown in Table 1. As seen from the table the notations

[1]The term E/E/PE safety related systems (electrical/electronic/programmable electronic system) is used in IEC 61508.

Table 1
Different classifications of barriers as physical or non-physical

Terms				References
Physical		Non-physical		(Johnson, 1980; ISO:17776, 2000; DoE, 1997; PSA, 2002)
Hard defence		Soft defence		(Reason, 1997)
Physical	Technical	Administrative		(Wahlström & Gunsell, 1998)
Physical	Technical	Human factors/organizational		(Svenson, 1991)
Technical		Procedural/administrative	Human actions	(Neogy et al., 1996)
Technical		Human/organizational	Human	(Kecklund et al., 1996)
Technical		Organizational	Operational	(Bento, 2003)
Physical		Management		(DoE, 1997)
Hardware		Behavioural		(Hale, 2003)

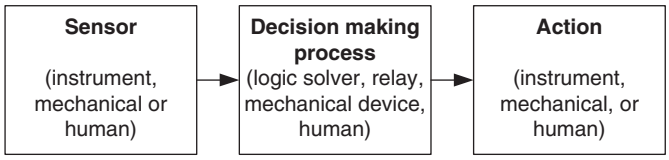


Fig. 4. Basic elements of active independent protection layer (CCPS, 2001).

physical or technical are both used to describe the "left side", only Svenson (1991), and Wahlström and Gunsell (1998) distinguish between these two terms. On the non-physical side, different terms as soft defence, administrative, organisational, human, operational, and management are used. A barrier may consist of physical as well as non-physical elements.

Several authors distinguish between *passive* and *active* barriers (see, e.g., CCPS, 2001; Hale, 2003; Kjellén, 2000). CCPS (2001) distinguishes between passive and active independent protection layers where a passive protection layer is not required to take an action in order for it to achieve its function in reducing risk, while active protection layers are required to move from one state to another in response to a change in a measurable process property (e.g., temperature or pressure), or a signal from another source (such as a push-button or a switch). An active protection layer generally comprises a sensor of some type, a decision-making process, and an action (see Fig. 4). Also Kjellén (2000) differentiates between passive and active safety barriers, and states that passive barriers are embedded in the design of the workplace and are independent of the operational control system. Active barriers are, however, dependant on actions by the operators or on a technical control system to function as intended.

Similarly, Hale et al. (2004) distinguish between four parts of a barrier function that all have to be fulfilled. They claim that this division can form the basis of a matrix for classifying different forms of a barrier for fulfilling a given safety function. The four parts are; definition or specification of the barrier, detection mechanism, activation mechanism, and response mechanism. Barriers are divided into passive, active, or procedural (or human action barriers) in an ARAMIS-memo (Goossens & Hourtolou, 2003). Hale (2003) presents a somewhat more refined classification of barriers with the categories: (a) passive hardware barriers, (b) active hardware barriers, (c) passive behavioural barriers, (d) active behavioural barriers, and (e) mixed barriers, where both hardware and behaviour are involved.

3.3. Other lines of classification

Hollnagel (2004) has developed a classification of barriers based on their nature, and describes four groups of barriers; *material or physical barriers, functional barriers, symbolic barriers*, and *incorporeal barriers* (called immaterial in another memo). Material or physical barriers are barriers that physically prevent an action from being carried out or an event from taking place (e.g., buildings, walls, and railings). Functional barriers work by impeding the action to be carried out, for instance by establishing an interlock, either logical or temporal. Symbolic barriers require an act of interpretation in order to achieve its purpose, hence an "intelligent" agent of some kind that can react or respond to the barrier (e.g., signs and signals). Whereas a functional barrier works by establishing an actual pre-condition that must be met by the system, or the user, before further actions can be carried out, a symbolic barrier indicates a limitation on performance that may be disregarded or neglected. Incorporeal barriers mean that the barrier is not physically present or represented in the situation, but that it depends on the knowledge of the user in order to achieve its purpose (typically rules and guidelines).

In the description of the Safety Modelling Language (SML), Schupp (2004) specifies one dimension of barriers called *inherent* versus *add-on*. An inherent barrier is a barrier that is created by changing a parameter of a design, for example, using a thicker vessel wall to withstand internal pressure, using stainless steel or a smaller inventory. Add-on barriers are systems or components that are added just because of safety considerations, e.g., pressure valves, interlocks, and sprinkler devices.

Trost and Nertney (1995) describe the following types of barriers within MORT; equipment design, physical

barriers, warning devices, procedures/work processes, knowledge and skill, and supervision. Another aspect emphasized in a MORT analysis (Johnson, 1980), is the *location* of the barriers. The location is divided in four categories; on the energy source, between the energy source and worker, on persons/objects, or separation through time and space. This corresponds to the classification developed by Haddon (1980) of risk reducing measures as strategies related to the energy source, strategies related to barriers or strategies related to the vulnerable target. Further, the MORT-concept differentiates between *control* and *safety* barriers (Trost & Nertney, 1995). Control barriers are related to control of wanted energy flows, while safety barriers are related to control of unwanted energy flows. An equivalent differentiation is made by DoE (1997).

A distinction between *global* and *local* safety functions is made by The Norwegian Oil Industry Association (OLF, 2001). Global safety functions, i.e., fire and explosion hazard safety functions, are functions that typically provide protection for one or several fire cells. Examples comprise emergency shutdown (EDS), isolation of ignition sources and emergency blowdown. Local safety functions, i.e., process equipment safety functions, are functions confined to protection of a specific process equipment unit. A typical example will be protection against high liquid level in a separator through the process shutdown system (PSD). Further, Bodsberg (1994) distinguishes between *process control* function and *control of the conditions* of the equipment. The purpose of the process control function is to prevent that a stable process deviates into a state of lack of control (i.e., high pressure), while, for instance, condition monitoring will measure directly the condition of the plant equipment and may provide advance warning on possible process equipment failures.

Goossens and Hourtolou (2003) distinguish between *permanent* and *activated* barriers, where permanent barriers are functioning permanently independent of the state of the process, while activated barriers need a sequence of detection—diagnosis—action. This classification is similar to the distinction between on-line and off-line functions described by Rausand and Høyland (2004).

Hollnagel (2004) uses the terms *permanent* and *temporary* barriers to explain another aspect of barriers. Permanent barriers are usually part of the design base, although they also may be introduced later, for instance, as a response to an accident. Temporary barriers are restrictions that apply for a limited period of time only, typically referring to a change in external conditions. In the same way, Holand (1997) emphasizes two main types of barriers related to well operations, *static* barriers and *dynamic* barriers. A static barrier is a barrier that is available over a "long" period of time, while a dynamic barrier is a barrier that varies over time, and will apply for drilling, workover, and completion operations.

Within the human reliability analysis (HRA) domain, the term *recovery* of human errors is used. In THERP (Technique for Human Error Rate Prediction; Swain & Guttmann, 1983), a recovery factor is any element of a nuclear power plant system that acts to prevent deviant conditions from producing unwanted effects. Kirwan (1994) describes four types of recovery; *internal recovery, external recovery, independent human recovery*, and *system recovery*. Internal recovery means that the operator, having committed an error or failed to carry out an act, realises this immediately, or later, and corrects the situation. External recovery means that the operator, having committed an error or having failed to do something that is required, is prompted by a signal from the environment (e.g., an alarm, an error message, some other non-usual system-event). Independent human recovery means that another operator monitors the first operator, detects the error and either corrects it or brings it to the attention to the first operator, who then corrects it. System recovery means that the system itself recovers from the human error. This implies a degree of error tolerance, or of error detection and automatic recovery.

3.4. Recommendations and comments

A recommended way to classify barrier systems is shown in Fig. 5. However, note that active barrier systems often are based on a combination of technical and human/operational elements (e.g., see (Corneliussen & Sklet, 2003) for a discussion of human/operational and technical elements in an ESD-system). Even though different words are applied, the classification in the fourth level in Fig. 5 is similar to the classification suggested by Hale (2003), and the classification of active, technical barriers is in accordance with IEC:61511.

As regards the time aspect, some barrier systems are on-line (continuously functioning), while some are off-line (need to be activated). Further, some barriers are permanent while some are temporary. Permanent barriers are implemented as an integrated part of the whole operational life cycle, while temporary barriers only are used in a specified time period, often during specific activities or conditions.

The physical, passive barriers (e.g., containment, fences, and firewalls) are usually functioning continuously as they do not need to be activated. They may also be temporary, e.g., a temporary obstruction fencing a working area during an activity. The passive, human operational barriers (e.g., safety distances in accordance with Haddon's principle separation in time and space) may be functioning continuously, or be implemented as part of high-risk activities.

Active, human/operational barriers may be in a continuous mode or activated on demand. Often, these barriers are an integrated part of a work process (e.g., self-control of work and third party control of work) in order to reveal potential failures, e.g. introduced by humans.

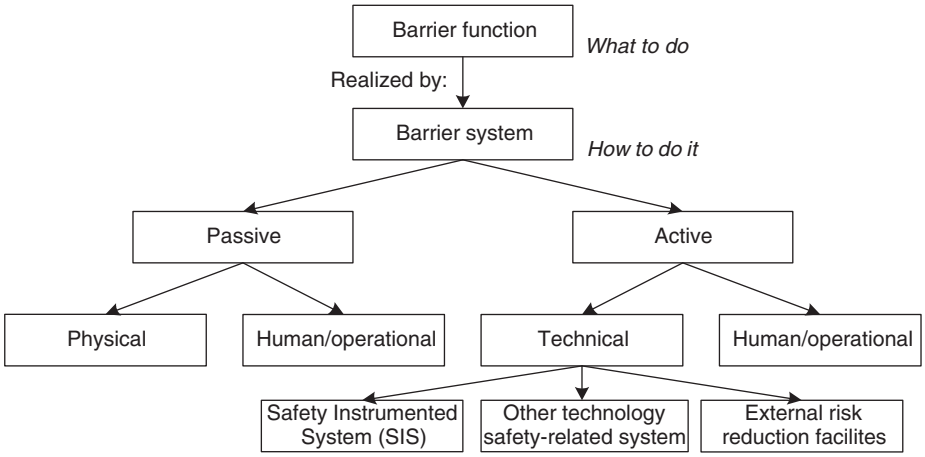


Fig. 5. Classification of safety barriers.

Safety barriers may also be classified on several other ways. The classification illustrated in Fig. 5 may not always be best suitable for the purpose of the classification. Then, some other lines of classification described in Section 3 can be used.

4. Performance of safety barriers

4.1. Performance criteria

To identify failed, missing, or functioning barriers is an important part of a MTO-analysis (Rollenhagen, 1997), and DoE (1999) addresses the following topics regarding analysis of barriers in an accident investigation:

- Barriers that were in place and how they performed.
- Barriers that were in place but not used.
- Barriers that were not in place but were required.

The assessment of barrier performance is manageable in accident investigations where a specific event sequence already has occurred (Sklet, 2004). The situation is somewhat different in proactive risk analyses. There are several accident scenarios to analyse, and the analyses of expected barrier performance are a vital part of the risk analyses. As mentioned in Section 1, there are distinctions regarding to which extent barriers should influence the energy flow or event sequence, from "reduce the probability", to "prevent the flow". This discussion may be related to the discussion about the performance of the barriers, and the subject is further delineated in this section.

According to PSA (2002), performance of barriers, may, inter alia, refer to *capacity*, *reliability*, *availability*, *efficiency*, *ability to withstand loads*, *integrity*, and *robustness*. Further, PSA writes in a letter to the oil companies (PSA/RNNS, 2002) that the performance of safety barriers are composed of three components; *functionality/efficiency* (i.e., the effect the barriers has on the event sequence if it functions according to the design intent), *availability/reliability* (i.e., the ability to function on demand), and *robustness* (i.e., the ability to function during accident sequences or under influence of given accident loads).

Neogy et al. (1996) use the terms *reliability* and *effectiveness* in order to describe how successful barriers are in providing protection. They state that the reliability of barriers is related to the ability to resist failures, while the effectiveness of a barrier is related to how suitable or how comprehensive the barrier is in protecting against a particular hazard.

Table 2 shows a summary presented by Hollnagel (2004) of a discussion of requirements of barrier quality made by Taylor (1988).

In another paper, Hollnagel (1995) presents a set of pragmatic criteria that address various aspects of barrier quality:

- *Efficiency or adequacy*: how efficient the barrier is expected to be in achieving its purpose.
- *Resources required*: the resources needed to implement and maintain the barrier rather than the resources needed to use it.
- *Robustness (reliability)*: how reliable and resistant the barrier is, i.e., how well it can withstand the variability of the environment.
- *Delay in implementation*: the time from conception to implementation of a barrier.
- *Applicability to safety critical tasks*: Safety critical tasks play a special role in socio-technical systems. On the one hand they are the occasions where specific barriers may be mostly needed; on the other hand they are usually subject to a number of restrictions from either management or regulatory bodies.
- *Availability*: whether the barrier can fulfil its purpose when it is needed.
- *Evaluation*: to determine whether a barrier works as expected and to ensure that it is available when needed. The evaluation can be considered with regard to how easy it is to carry out and in terms of whether suitable methods are available.

Table 2
Requirements to barrier quality (Hollnagel, 2004; Taylor, 1988)

Quality/criterion	Specific requirement
Adequacy	Able to prevent all accidents within the design basis. Meet requirements set by appropriate standards and norms. Capacity must not be exceeded by changes to the primary system. If a barrier is inadequate, additional barriers must be established.
Availability, reliability	All necessary signals must be detectable when barrier activation is required. Active barriers must be fail-safe, and either self-testing or tested regularly. Passive barriers must be inspected routinely.
Robustness	Able to withstand extreme events, such as fire, flooding, etc. The barrier shall not be disabled by the activation of another barrier. Two barriers shall not be affected by a (single) common cause.
Specificity	The effects of activating the barrier must not lead to other accidents. The barrier shall not destroy that which it protects.

- *Dependence of humans*: the extent to which a barrier depends on humans in order to achieve its purpose.

Within the ARAMIS-project (Andersen et al., 2004), evaluation of safety barriers is performed according to three criteria in order to achieve a predetermined risk reduction objective:

- *Effectiveness*
- *Response time*
- *Level of confidence*

Effectiveness of a safety barrier is the ability of a safety barrier to perform a safety function for a duration, in a non-degraded mode and in specified conditions. The effectiveness is either a percentage or a probability of the performance of the defined safety function. If the effectiveness is expressed as a percentage, it may vary during the operating time of the safety barrier. For example, a valve that is not able to close completely on a safety demand will not have an effectiveness of 100%. Response time is the duration between the straining of the safety barrier and the complete achievement (which is equal to the effectiveness) of the safety function performed by the safety barrier. Level of confidence of a safety barrier is the probability of failure on demand to perform properly a required safety function according to a given effectiveness and response time under all the stated conditions within a stated period of time. This notion is similar to the notion of Safety Integrity Level (SIL) defined in IEC:61511 for SIS, but applies here to all types of safety barriers. The ''design'' level of confidence means that the barrier is supposed to be as efficient as when it was installed, while the ''operational'' level of confidence includes the influence of the safety management system. The value could be lower than the ''design'' one if some problems are identified during the audit of the safety management system.

Rollenhagen (1997, 2003) emphasizes that the following dimensions should be focused concerning the strength of barrier systems; *validity* (the ability to handle the deviations, threats, etc., meant to deal with), *reliability* (the ability to fulfil specific properties on demand), *completeness* (whether it is necessary to implement more barriers), and *maintainability* (a measure of how easy it is to maintain the barrier system).

4.2. Recommendations and comments

Based on experience from several projects and a synthesis of the reviewed literature, it is recommended to address the following attributes to characterize the performance of safety barriers:

- *Functionality/effectiveness*
- *Reliability/availability*
- *Response time*
- *Robustness*
- *Triggering event or condition*

For some types of barriers, not all the attributes are relevant or necessary in order to describe the barrier performance.

- *The barrier functionality/effectiveness is the ability to perform a specified function under given technical, environmental, and operational conditions*

The barrier functionality deals with the effect the barrier has on the event or accident sequence. The specified function should be stated as a functional requirement (deterministic requirement). A functional requirement is a specification of the performance criteria related to a function (Rausand & Høyland, 2004). The ''possible'' degree of fulfilment may be expressed in a probabilistic way as the probability of successful execution of the specified function or the percentage of successful execution. For example, if the function is to pump water, a functional requirement may be that the output of water must be

between 100 and 1101/min. Functional requirements for the performance of safety barriers may exist in regulations, standards, design codes, etc., or as risk-informed requirements based on risk assessments using risk acceptance criteria (Hokstad, Vatn, Aven, & Sørum, 2003). The actual functionality of a barrier may be less than the specified functionality due to design constraints, degradation, operational conditions, etc. The functionality of safety barriers corresponds to the safety function requirements demanded by IEC:61511 and the effectiveness of safety barriers as described in the ARAMIS-project (Andersen et al., 2004).

- *The barrier reliability/availability is the ability to perform a function with an actual functionality and response time while needed, or on demand*

The barrier reliability/availability may be expressed as the probability of failure (on demand) to carry out a function. The reliability/availability of safety barriers corresponds to the safety integrity requirements (SIL) demanded by IEC:61511 and the level of confidence as described in the ARAMIS-project. The PDS-method (Hokstad & Corneliussen, 2003) also focuses on various measures of loss of safety or safety unavailability for a safety function (the probability of not to function on demand) and uses the term critical safety unavailability (CSU) to quantify total loss of safety. Requirements to the reliability/availability may be expressed as a SIL-requirement as illustrated in Table 3.

The difference between barrier functionality and barrier reliability/availability may be illustrated by two examples; an ESD-system, and gas detectors. In the former case, the barrier function is to close flow. The functionality of an ESD-valve that closes with no internal leakage may be 100%. An internal leakage through the valve reduces the effectiveness, but the reliability expressed as the probability of valve closure on demand is not influenced by the internal leakage. In the latter case, assume that the barrier function is to detect gas and give a signal. The actual effectiveness is influenced by, e.g., type, numbers, and location of the gas detectors, while the reliability is the probability of signal from the detectors if they are exposed to gas.

- *The response time of a safety barrier is the time from a deviation occurs that should have activated a safety barrier, to the fulfilment of the specified barrier function*

The response time may be defined somewhat different for different types of barrier functions. This may be illustrated by the difference between an ESD-system and a deluge system. The response time for the ESD-system is the time to closure of the ESD-valve where the function "stop flow" is fulfilled, while the response time for a deluge system is the time to delivery of the specified amount of water (and not the time until the fire is extinguished).

- *Barrier robustness is the ability to resist given accident loads and function as specified during accident sequences*

This attribute is relevant for passive as well as active barrier systems, and it may be necessary to assess the robustness for several types of accident scenarios.

- *The triggering event or condition is the event or condition that triggers the activation of a barrier*

It is not itself part of a barrier, however, it is an important attribute in order to fully understand how a barrier may be activated. The barriers that are functioning continuously (e.g., passive barriers and operational restrictions as hot work limits), do not need a trigger to be activated since they are implemented as a result of deterministic requirements or risk assessments (e.g., restrictions on hot work that reduce the ignition probability if a hydrocarbon release occurs).

There are three main types of triggering events and conditions that activate active barriers:

1. Deviations from the normal situation, e.g., process disturbances and hydrocarbon release. These deviations should be revealed by a kind of sensor (either automatically or manually).
2. Execution of specific activities, e.g., activities where barriers are a necessary part of the activity in order to detect possible failures introduced as part of the activity. An example is activities where work permits, self-control of work, and third party control of work are demanded.
3. Scheduled activities, e.g., inspection aimed to reveal corrosion.

Table 3
Safety integrity levels (IEC:61511)

Safety integrity level (SIL)	Demand mode of operation Target average probability of failure on demand	Continuous mode of operation Target frequency of dangerous failures to perform the SIF (per hour)
4	$\geqslant 10^{-5}$ to $<10^{-4}$	$\geqslant 10^{-9}$ to $<10^{-8}$
3	$\geqslant 10^{-4}$ to $<10^{-3}$	$\geqslant 10^{-8}$ to $<10^{-7}$
2	$\geqslant 10^{-3}$ to $<10^{-2}$	$\geqslant 10^{-7}$ to $<10^{-6}$
1	$\geqslant 10^{-2}$ to $<10^{-1}$	$\geqslant 10^{-6}$ to $<10^{-5}$

Implementation of safety barriers may have adverse effects like increased costs, need for maintenance, and introduction of new hazards. These adverse effects should be addressed as part of a total analysis of safety barriers, but they are not further discussed in this paper. Some of these aspects, as loss of production regularity and maintenance, are focused in the PDS-method (Hokstad & Corneliussen, 2003) where a measure for quantifying loss of production regularity is the spurious trip rate.

5. Conclusions

The concept of safety barriers is presented and discussed in the paper. The results are based on experience from several research projects focusing on safety barriers and a review of relevant literature. No common terminology applicable crosswise between sectors and application areas has been found, and a set of definitions is therefore proposed in the paper.

Safety barriers are defined as physical and/or non-physical means planned to prevent, control, or mitigate undesired events or accidents. It is practical to distinguish between the barrier functions and the barrier systems that realize these functions.

Several ways for classification of safety barriers exist. Barrier functions may be classified as preventive, controlling, or mitigating. Barrier systems may be classified in several dimensions, and some main dimensions are; active versus passive, physical/technical versus human/operational, continuously functioning/on-line versus activated/off-line, and permanent versus temporary.

It is recommended to address the following attributes to characterize the performance of safety barriers: (a) functionality/effectiveness, (b) reliability/availability, (c) response time, (d) robustness, and (e) triggering event or condition. For some types of barriers, not all the attributes are relevant or necessary in order to describe the barrier performance.

The paper improves the understanding of the concept of safety barriers. The results are valuable as a basis for identification, description, development of requirements to, and understanding of the effect of the safety barriers within the field of industrial safety. The results with respect to safety barriers in the paper will primarily be useful for the Norwegian oil industry in their effort to fulfil the requirements from PSA. However, the results may also be applied in other industries (e.g., the process industry) and application areas (e.g., the transport sector) in their effort to reduce the risk.

References

Andersen, H., Casal, J., Dandrieux, A., Debray, B., De Dianous, V., Duijm, N. J., et al. (2004). *ARAMIS—user guide*. EC Contract number EVG1-CT-2001-00036.

Aven, T., Sklet, S., & Vinnem, J. E. (2005). Barrier and operational risk analysis of hydrocarbon releases (BORA-Release); Part I. Method description. *Journal of Hazardous Materials*, submitted for publication.

Bento, J.-P. (2003). *Review from an MTO-perspective of five investigation reports from BP (Draft)*. Norway: Stavanger.

Bodsberg, L. (1994). *Reliability quantification of control and safety systems: the PDS-II method*. Trondheim: SINTEF Safety and Reliability.

CCPS. (1993). *Guidelines for safe automation of chemical processes*. New York: Center for Chemical Process Safety of the American Institute of Chemical Engineers.

CCPS. (2001). *Layer of protection analysis simplified process risk assessment*. New York: Center for Chemical Process Safety of the American Institute of Chemical Engineers.

Corneliussen, K., & Sklet, S. (2003). Challenges related to surveillance of safety functions. In *ESREL 2003*. Maastricht, The Netherlands: Balkema.

DoE. (1997). *Implementation guide for use with DOE Order 225.1A, accident Investigation, DOE G 225.1A-1, Rev. 1*. Washington, DC: US Department of Energy (DOE).

DoE. (1999). *Conducting accident investigations DOE workbook, revision 2*. Washington, DC: US Department of Energy.

Duijm, N. J., Andersen, H. B., Hale, A., Goossens, L., & Hourtolou, D. (2004). Evaluating and managing safety barriers in major hazard plants. In *PSAM 7—ESREL '04*, Berlin, Germany.

Duijm, N. J., Madsen, M. D., Andersen, H. B., Hale, A., Goossens, L., Londiche, H., et al. (2003). Assessing the effect of safety management efficiency on industrial risk. In *ESREL 2003*. Maastricht: Balkema.

EC (1996). Council Directive 96/82/EC of 9 December 1996 on the control of major-accident hazards involving dangerous substances (Seveso II-directive).

EC (1998). Directive 98/37/EC of the European Parliament and of the Council of 22 June 1998 on the approximation of the laws of the Member States relating to machinery as amended by Directive 98/79/EC (The Machinery Directive).

Fleming, K. N., & Silady, F. A. (2002). A risk informed defense-in-depth framework for existing and advanced reactors. *Reliability Engineering & System Safety*, *78*(3), 205–225.

Gibson, J. (1961). The contribution of experimental psychology to the formulation of the problem of safety. In *Behavioural Approaches to Accident Research*. New York: Association for the Aid of Crippled Children.

Goossens, L., & Hourtolou, D. (2003). *What is a barrier*? ARAMIS-working document.

Haddon, W. J. (1980). The basic strategies for reducing damage from hazards of all kinds. *Hazard Prevention*, September–October (pp. 8–12).

Hale, A. (2003). Note on barriers and delivery systems. In *PRISM conference*, Athens.

Hale, A., Goossens, L., Ale, B., Bellamy, L., Post, J., Oh, J., et al. (2004). Managing safety barriers and controls at the workplace. In *PSAM 7-ESREL '04*, Berlin.

Harms-Ringdahl, L. (2000). Assessment of safety function at an industrial workplace—A case study. In *ESREL 2000*. Edinburgh: Balkema.

Harms-Ringdahl, L. (2003). Assessing safety functions—Results from a case study at an industrial workplace. *Safety Science*, *41*(8), 701–720.

Hokstad, P., & Corneliussen, K. (2003). *Reliability prediction method for safety instrumented systems: PDS method handbook*. Trondheim: SINTEF Industrial Management Safety and Reliability.

Hokstad, P., Vatn, J., Aven, T., & Sørum, M. (2003). Use of risk acceptance criteria in Norwegian offshore industry: dilemmas and challenges. In *ESREL 2003*. Maastricht: Balkema Publishers.

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

Hollnagel, E. (1995). The art of efficient man–machine interaction: Improving the coupling between man and machine. In J.-M. Hoc, P. C. Cacciabue, & E. Hollnagel (Eds.), *Cognition & Human–Computer Cooperation*. Hillsdale, NJ: Lawrence Erlbaum Associates Inc.

Hollnagel, E. (1999). *Memo—Accident analysis and barrier functions*. Halden: IFE.

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

Hopwood, A. G. (1974). *Accounting and human behaviour*. London: Haymarket Publishing.

IAEA. (1999). *Basic safety principles for nuclear power plants: 75-INSAG-3, rev.1*. Vienna: The International Atomic Energy Agency.

IEC:61508. (1998). *Part 1–7 Functional safety of electrical/electronic/programmable electronic safety-related systems*. Geneva: International Electrotechnical Commission.

IEC:61511. (2002). *Functional safety—Safety instrumented systems for the process industry sector*. Geneva: International Electrotechnical Commission.

ISO:13702. (1999). *Petroleum and natural gas industries—Control and mitigation of fires and explosions on offshore production installations—Requirements and guidelines*. Geneva: International Organization for Standardization.

ISO:17776. (2000). *Petroleum and natural gas industries—Offshore production installations—Guidelines on tools and techniques for hazard identification and risk assessment*. Geneva: International Organization for Standardization.

Johnson, P., & Gill, J. (1993). *Management and organizational behaviour*. London: Paul Chapman Publishing Ltd.

Johnson, W. G. (1980). *MORT safety assurance systems*. New York: Marcel Dekker.

Kaplan, S. (1990). Bayes is for eagles. *IEEE Transactions on Reliability*, *53*, 457–481.

Kecklund, L. J., Edland, A., Wedin, P., & Svenson, O. (1996). Safety barrier function analysis in a process industry: A nuclear power application. *International Journal of Industrial Ergonomics*, *17*(3), 275–284.

Kirwan, B. (1994). *A guide to practical human reliability assessment*. London: Taylor & Francis.

Kjellén, U. (2000). *Prevention of accidents through experience feedback*. London: Taylor & Francis.

Kjellén, U., & larsson, T. (1981). Investigating accidents and reducing risks—A dynamic approach. *Journal of occupational accidents*, *3*, 129–140.

Leveson, N. (1995). *SafeWare: System safety and computers*. Reading, MA: Addison-Wesley.

Neogy, P., Hanson, A. L., Davis, P. R., & Fenstermacher, T. E. (1996). *Hazard and Barrier analysis guidance document, Rev. 0*. US Department of Energy (DoE), EH-33 Office of Operating Experience Analysis and Feedback.

OED. (2005). *Oxford English dictionary online*. Oxford: Oxford University Press.

OLF. (2001). *Recommended guidelines for the application of IEC 61508 and IEC 61511 in the petroleum activities on the Norwegian Continental Shelf*. Stavanger, Norway: The Norwegian Oil Industry Association.

PSA. (2001). *Regulations relating to management in the petroleum activities (The Management Regulations). 3 September 2001*. Norway, Stavanger: Petroleum Safety Authority.

PSA. (2002). *Guidelines to regulations relating to management in the petroleum activities (The management regulations)*. Norway, Stavanger: Petroleum Safety Authority.

PSA/RNNS. (2002). *The development in the risk level on the Norwegian Continental Shelf—Requirements for registration of the performance of safety barriers. Letter to the oil companies (in Norwegian). Rev 9. 17.06.2002*. Norway, Stavanger: Petroleum Safety Authority.

Rausand, M., & Høyland, A. (2004). *System reliability theory: Models, statistical methods, and applications*. Hoboken, NJ: Wiley-Interscience.

Reason, J. (1997). *Managing the risks of organizational accidents*. Aldershot: Ashgate.

Reason, J., Parker, D., & Lawton, R. (1998). Organizational controls and safety: The varieties of rule-related behaviour. *Journal of Occupational and Organizational Psychology*, *71*, 289–304.

Rollenhagen, C. (1997). *MTO—An introduction; The relationship between humans, technology, and organisation (In Swedish; MTO—en introduktion; Sambanden människa, teknik och organisation)*. Lund: Utbildningshuset.

Rollenhagen, C. (2003). *To investigate accidents, theory and practice (In Swedish; Att utreda olycksfall, Teori och praktik)*. Lund: Studentlitteratur.

Rosness, R. (2005). *Ten thumbs and zero accidents? About fault tolerance and accidents*. Kjeller: Institute for Energy Technology (in Norwegian).

Schupp, B. (2004). *The safety modeling language. ADVISES tutorial in human error analysis, barriers and the safety modelling language*. Germany: Paderborn.

SfS. (2004). *Barriers—Out of the fog, towards increased safety (in Norwegian—Barrierer—ut av tåkehavet, mot bedre sikkerhet)*. Stavanger, Norway: Together for Safety, OLF.

Sklet, S. (2004). Comparison of some selected methods for accident investigation. *Journal of Hazardous Materials*, *11*(1–3), 29–37.

Sklet, S., Aven, T., Hauge, S., & Vinnem, J. E. (2005). Incorporating human and organizational factors in risk analysis for offshore installations. In *ESREL 2005*, Gdynia.

Sklet, S., & Hauge, S. (2003). *SINTEF-Memo discussion of the term safety barrier*. Trondheim: SINTEF (in Norwegian).

Sklet, S., & Hauge, S. (2004). Reflections on the concept of safety barriers. In *PSAM7—ESREL 2004*, Berlin.

Sklet, S., Steiro, T., & Tjelta, O. (2005). Qualitative analysis of human. Technical and operational barrier elements during well interventions. In *ESREL 2005*, Tri City, Poland.

Sklet, S., Vinnem, J. E., & Aven, T. (2005). Barrier and operational risk analysis of hydrocarbon releases (BORA-Release); Part II. Results from a case study. *Journal of Hazardous Materials*, submitted for publication.

Svenson, O. (1991). The accident evolution and barrier function (AEB) model applied to incident analysis in the processing industries. *Risk Analysis*, *11*(3), 499–507.

Swain, A. D., & Guttmann, H. E. (1983). *Handbook of human reliability analysis with emphasis on nuclear power plant applications: Final report NUREG CR-1278, SAND80-200.* Sandia National Laboratories Statistics Computing and Human Factors Division, Albuquerque.

Taylor, R. J. (1988). *Methods for assessment of weapon safety (In Danish; Analysemetoder til vurdering af våbensikkerhed)*. Glumsø, DK: Institute for Technical Systems Analysis.

Trost, W. A., & Nertney, R. J. (1995). *Barrier analysis*. Idaho Falls, US: SCIENTECH Inc., SCIE-DOE-01-TRAC-29-95.

Vatn, J. (2001). *SINTEF internal memo regarding safety critical functions in the railway system in Norway. Rev. 3*. Trondheim: SINTEF.

Vinnem, J. E., Aven, T., Hauge, S., Seljelid, J., & Veire, G. (2004). Integrated barrier analysis in operational risk assessment in offshore petroleum operations. In PSAM7—ESREL '04. Berlin: Springer.

Wahlström, B., & Gunsell, L. (1998). *Reactor safety; a description and assessment of the Nordic safety work (In Swedish; Reaktorsäkerhet; En beskrivning och en värdering av säkerhetsarbetet i Norden)*. Risö forskningscenter: NKS-sekretariatet.