Energy flow /barrier analysis, a novel view

Mahmoud Shahrokhi, Alain Bernard

IRCCyN laboratory - Ecole Centrale de Nantes
1, rue de la Noë BP 92101 F - 44321 - NANTES Cedex 03 (France)

Abstract

In this paper, the principal concepts of the energy flow/barrier analysis are used to define an accident as a series of events including failure of the control and protective barriers, which results exposure of a target to a hazardous agent. "Barrier structure" is introduced, as a combination of serial and parallel barriers, to calculate the severity of risks of accidents. It is defined for each hazards and targets, separately, to identify the different accident processes. The accidents risk are estimated by using the barriers reliability and efficiency. This approach can be used to identify the different accidents scenarios and to recognize the more critical barriers.

Keywords : Risk, Barrier, Energy analysis, Industrial production systems

1. Introduction

In this paper, the energy flow/barrier concepts are studied and a novel approach is introduced to recognize different accident processes and to identify the more critical barriers. Based of the energy flow/barrier concepts an accident is defined as a series of events including failure of the control and protective barriers, which results exposure of a target to a harmful agent. A barrier modelling method, "barrier structure", is introduced, which is applicable for evaluating the probability and the severity of the risk of the accidents by using the reliability and efficiency of the barriers, as the known parameters.

2. Energy flow/barrier analysis

Energy Analysis is a straightforward method, which is performed by evaluation of hazards associated with identified energies and making proposals for improvements (Harms-Ringdahla 2003). The advantage of energy analysis is that it is dependant on information at a relatively coarse level and may be performed at an early project phase (Kjellén and Sklet 1995).

Barrier analysis provides a structured way to consider the events related to a safety system failure (Livingston et al. 2001), and helps to identify the system weak points which have an insufficient level of risk control (De Dianous and Fiévez 2006). It is used to select, optimise, and verify the barriers (Kjellén and Sklet 1995), and to determine how these barriers or controls may be failed (USDE 1992) by considering the technical or human dysfunctions (Polet 2002).

3. Related works

The theories utilised in energy flow/barrier analysis were originally based on the successive works of Hienrich's domino theory back in the 1930s, Haddon in 1966 and Gibson in 1961 (Livingston et al. 2001). The accident process is modelled as transferring energy from one domino to another, and to prevent the accident; the energy transfer must be prevented by removing one of the intermediate dominoes or by erecting a barrier between them ((Livingston et al. 2001, Trost and Nertney 1995).

The 'classical' barrier concept presumes a hazard and a target, which is protected by the barrier. In this context, distance is also considered a barrier (Guldenmund et al. 2006).

Using this definition, Hasan [these hassan] simply explains that barriers ("safety measures") are used to avoid the exposure of operator to the dangerous phenomena.

In accordance with the further requirements, this concept stretched comprising also the measures that prevent some sorts of the "loss of the control" (Guldenmund et al. 2006), resurrect the target, or mitigate the accident consequences (Polet 2002, Zhang et al. 2004).

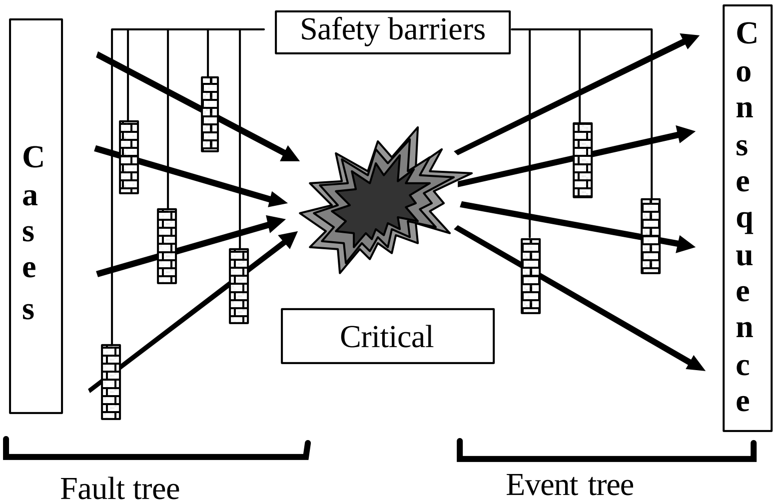

Fig. 1: Prevention and mitigation safety functions presented in the Bow-tie model

Hollnagel (1999) and De Dianous and Fiévez (2006) distinct passive, active, and procedural barriers. Polet (2002), Zhang et al. (2004) and Hollnagel (1999) dassify barriers as material, functional, symbolic, and immaterial.

In an organisational view, Hollnagel (1999) describes another classification for barriers namely physical, technical, and human factors/organisational barriers. In a similar regard Guldenmund et al. (2006) regroups the different elements of the hardware and behaviour barriers.

Hollnagel (1999) distincts the protector, and the preventive barriers. It defines barrier as the "equipment, constructions, or rules that can stop the development of an accident". Using the same idea, De Dianous and Fiévez (2006) categorise the preventive and mitigate barrier effects, illustrated as the bow-tie diagram (see figure1). In this model the frequency of occurrence of the events is calculated, by taking into account, the reliability of the safety functions.

According to TPSAN (2005), control barriers limit the hazards, and defence barriers protect the targets.
This same suggestion is proposed by De Dianous and Fiévez (2006), which states that potential consequence of the dangerous phenomena depends on the severity of the accident and the vulnerability of the target.
De Dianous and Fiévez (2006) introduce barrier necessary requirements, including: (1) the effectiveness (2) the response time, and (3) the level of confidence (reliability).

4. Methodology

According to Hollnagel (1999), an accident can be described as a set of failed barriers, which results transfer energy to the target. A barrier failure is the termination of the ability of a barrier to perform its required function (Rausand 2005a). Considering these definitions, as illustrated in figure 2, for occurring an accident, barriers should be breached by energy and/or by targets. For simplicity these processes can be modelled as the progress of energy and target toward each other, through the barriers. In this case contact of the energy with the target is occurred in an intermediate point.
The effects of barriers according to the energy view and target view are different. In the energy view, by breaking the barriers, generally the amount of the energy and therefore

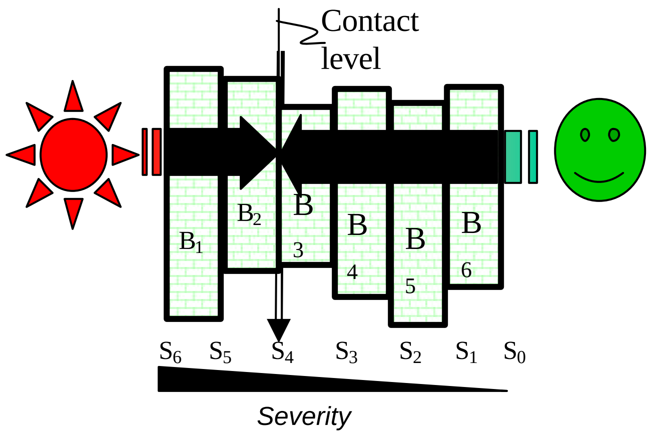

Fig. 2: Accident process model as failure of the barriers

its potential for damaging is reduced however in the target view, when it breach a barrier, target is less protected, and therefore the probability and the severity of potential damage increase. This means that the effect of breaching a barrier, on the risk, is depend of how, and by which agent, it is breached. For example there is difference between a cases that an operator take off his safety casket voluntary, before impact of an dangerous object with his head, and the case that dangerous object break his casket by its energy. In both cases this barrier is breached, however in the first case operator expose his head directly to the dangerous energy, therefore the risk of accident increase, and in the second case, impacted energy is reduced before contact with the operator head, and we can hope that the damage will be limited.
Other aspect is that in the discussed model, barriers are considered in a serial structure, this means that barriers are substitution of each other, however, to model practical cases more complicated structures are required. As a schematic example in the figure 3, four kinds of the barriers are illustrated: (1) two wall, (2) a door, (3) a lock, and a (4) danger

sign. The danger sign is serial with all of the other barriers (it is supposed that it is

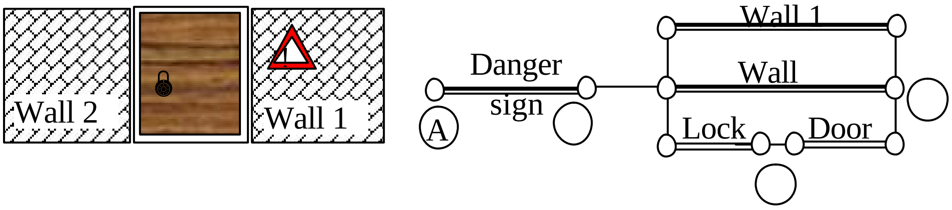

Fig. 3: An example of the serial and parallel barriers

visible everywhere), and the lock is serial with the door. However the walls are not serial with the door and its lock, because it is not obligatory to pass from the walls before or after passing through the door.

The walls are parallel (complement) with each other. A parallel barrier structure will be breached if minimum one of its barriers breaches.

It is supposed that the effectiveness of a barrier is only a function of the impacted HA to it. The inefficiency function of barrier k (f^k) represents the crossed HA from the barrier k, based on the impacted energy to it.

Generally, the barrier sets, including several barriers are used to mitigate the hazardous effects, or to protect the target. A barrier structure, including serial and parallel barriers is introduced to model the accumulation of the barrier effects. In a serial structure, in order to impact HA to the target, it should cross from all barriers.

It is considered that a barrier can be function properly or be failed. For the first case effectiveness of the barrier is considered as a function of impacted energy, and in the second case barrier will have not any effect on the system.

In this case the impacted HA for each barrier, in an serial barrier structure, is the outputted HA from the previous barrier, sequentially, and the successive HA reduction, after applying n serial barriers, is determined by as recursive calculation as:

$$c^k = f^k(c^{k-1})r^k + (1-r^k)c^{k-1}$$

Where c^0 is the impacted HA to the barriers set, and c^k, k=1,..,n is the resulted HA after crossing from barrier k. The Bernoulli random variable r^n demonstrates the truthful functioning of the barrier, with following probability distribution:

$$P(r^k = 1) = R^k$$

R^k is the reliability of the barrier k, for the studied scenario.

In a parallel barrier set, HA may cross through each of the barriers, and the barriers set would fail by failing each of the barriers. The parallel barriers are attached by 'OR' gates. According to the role of the barriers, the designer determines the kind of the 'OR' gates as the 'maximum' or 'bounded sum' functions:

$$c^n = \underset{n}{Max}\left\{f^k(c^0)r^k + (1-r^k)c^0\right\};$$

$$c^n = Min(\sum_n f^k(c^0)r^k + (1-r^k)c^0,\, c^0)$$

The severity of the risk of accidents is a function of the impacted HA to the target, which is calculated as followed:

$$l_j = h_j(c^n)$$

l_j is the severity of accident j, and h_j is a function that map the impacted energy to the estimated accident severity.

When a target beaches the barriers, the severity and the probability of the accidents is changed because target is more vulnerable to the dangers, however, generally, the final vulnerability is path independent. For example when an operator is in danger zone, his vulnerability is not depend of the way that he is passed from it. In the contrast, generally final energy after passing from the barriers is path dependant. It means that final energy is depended not only on the barriers that are breached by energy, but also to the order of the breaching these barriers.

Most of the barriers have effect both on the energy and target, but these effects may be different. A protective wall limits energy in the interior of a zone, and at the same time it limits the access of the target to the dangerous zone. Also there are barriers that have only effect on one of them (energy and target). For example a danger sign only can be considered as a barrier for the target, and has not any effect on the energy source.

For considering these aspects, the target view is separated from the energy view by considering the different barrier structure for them.

5. Discussion

It is supposed those barriers are failed independently. Independence implies that the failure of one component will not have any influence on the other components (Rausand 2005b). This assumption is not valid where there are the commune barriers failure causes. In this case the calculation method related to reliability of the barriers should be adopted according to the conditional probability rules.

For simplicity, the barrier effectiveness is considered only as a function of the applied energy, and the effects of other parameters like the environmental conditions, and the variation of barrier effectiveness, and reliability during the time, is ignored, however model remained valid also by considering other parameters.

The effects of impacting more than one HA to barriers are not studied.

Some of barriers may be fail during accident

In some cases amplitude of HA increase after passing from a barrier, by achieving the new dangerous materials for example. In these cases the protective effect of barrier may be considered be a negative value, and this effect also should be considered for the failed barrier.

The mode of the contact is not modelled.

To prove the validity, and applicability of this model, it should be applied through the real cases for the practical analysis.

6. Conclusion

In this paper the essential concepts of the energy flow/barrier analysis are discussed. The various aspects of breaching the barriers by the target and energy are discussed. A barrier modelling approach is introduced by presenting a graphical demonstration method, and a mathematical formulation for evaluating the probability and severity of accidents, for various scenarios.

References

De Dianous V and 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. Journal of Hazardous Materials Vol. 130, Issue 3:220-233

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. Journal of Hazardous Materials Vol. 130, Issue 3:234-241

Harms-Ringdahla L (2003) Assessing safety functions—results from a case study at an industrial workplace. Safety Science 41: 701–720

Hollnagel E (1999) Accident analysis and barrier functions. http://www.it.uu.se/research/project/train/papers/AccidentAnalysis.pdf

Huang D, Chen T, Wang M. J J (2001) A fuzzy set approach for event tree analysis. Fuzzy Sets and Systems 118:153-165

Kjellén U and Sklet S (1995) Integrating analyses of the risk of occupational accidents into the design process Part I: A review of types of acceptance criteria and risk analysis methods. Safety Science 18: 2 15-227

Livingston A D, Jackson G and Priestley K (2001) Root causes analysis: Literature review. HSE Health & Safety Executive http://www.hse.gov.uk/research/crr_pdf/2001/crr01325.pdf

Polet P (2002) Modélisation des Franchissements de Barrières pour l'Analyse des Risques des Systèmes Homme-Machine. Ph.D. thesis presented at Université de Valenciennes et du Hainaut-Cambrésis

Rausand M (2005a) System Analysis Failures and Failure Classification. Department of Production and Quality Engineering Norwegian University of Science and Technology http://www.ntnu.no/ross/srt/slides/failure.pdf

Rausand M (2005b) Systems of Independent Components. Department of Production and Quality Engineering Norwegian University of Science and Technology http://www.ntnu.no/ross/srt/slides/chapt4-1.pdf

The Petroleum Safety Authority Norway (TPSAN) (2005) Excerpt from the SINTEF-report : Investigation methodology: Man technology organization. http://www.ptil.no/NR/rdonlyres/97CAF402-1D94-4F0C-B5D2-BFF226838AEC/0/MTO_engl.pdf

Trost W A and Nertney R J (1995) Barrier Analysis. Technical Research and Analysis Center SCIENTECH, Inc. http://tis-hq.eh.doe.gov/analysis/trac/29/trac29.pdf http://www.hq.nasa.gov/office/codeq/rca/rootcauseppt.pdf

U.S. Department of Energy, Office of Nuclear Safety Policy and Standards (USDE) (1992) Root cause analysis guidance document. http://tis.eh.doe.gov/techstds/standard/nst1004/nst1004.pdf

Zhang Z, Chaali A and Vanderhagen F (2004) A comparative study on prediction of human operator violation using neural networks. International Conference on Systems, Man and Cybernetics October 10-13 2004 The Hague, The Netherlands