CHEMICAL ENGINEERING TRANSACTIONS
VOL. 31, 2013
A publication of AIDIC
The Italian Association of Chemical Engineering
Online at: www.aidic.it/cet
Guest Editors: Eddy De Rademaeker, Bruno Fabiano, Simberto Senni Buratti

ISBN 978-88-95608-22-8; **ISSN** 1974-9791
DOI: 10.3303/CET1331048

Modelling of Safety Barriers Including Human and Organisational Factors to Improve Process Safety

Frank Markert*, Nijs J. Duijm[a], Jacob Thommesen

[a]Technical University of Denmark (DTU), Department of Management Engineering, Produktionstorvet 424, Dk-2800 Kongens Lyngby, Denmark
fram@dtu.dk

It is believed that traditional safety management needs to be improved on the aspect of preparedness for coping with expected and unexpected deviations, avoiding an overly optimistic reliance on safety systems. Remembering recent major accidents, such as the Deep Water Horizon, the Texas City explosion, and the Mont Blanc Tunnel Fire, such an approach may have helped to maintain the integrity of the designed provisions against major deviations resulting in these disasters. In order to make this paradigm operational, safety management and in particular risk assessment tools need to be refined.
A valuable approach is the inclusion of human and organisational factors into the simulation of the reliability of the technical system using event trees and fault trees and the concept of safety barriers. This has been demonstrated e.g. in the former European research project ARAMIS (Accidental Risk Assessment Methodology for IndustrieS, see Salvi et al 2006). ARAMIS employs the bow-tie approach to modelling hazardous scenarios, and it suggests the outcome of auditing safety management to be connected to a semi-quantitative assessment of the quality of safety barriers. ARAMIS discriminates a number of different management issues such as competence management, dealing with conflicts, management of maintenance and inspection, and management of procedures. Shortcomings in these management processes effectuate increased probabilities of failure-on-demand (PFD) of the safety barriers, depending on the type of safety barrier (passive, automated, or involving human action). Such models are valuable for many purposes, but are difficult to apply to more complex situations, as the influences are to be set individually for each barrier.
The approach described in this paper is trying to improve the state-of-the–art, and it is based on the understanding that certain human and organisational factors may be seen as a kind of common cause failures that influence the performance of several barriers. Therefore, the model links the performance of a barrier with the necessary set of specific activities to maintain and/or to control that barrier. These specific activities are executed within one of the aforementioned management processes, and the efficiency of the activity will depend on the quality of this management process.

1. Introduction

Any technical system is part of a wider socio-technical system including many mutual impacts. Due to many environmental influences these systems have a tendency to degrade over time. An important factor to the degradation of the technical system (including any control for operation) is its maintenance by the socio-technical system. The latter can be a factor to inhibit or slow down degradation or in the worst case contribute to an accelerated degradation depending on factors as the safety culture of an organisation. Therefore, the influence of human and organisational factors (HOF) on the performance of installations has been subject for a wide range of investigations (Gambetti et al. 2012, Embrey 1992, Colombo, Demichela 2008, Davoudian, Wu & Apostolakis 1994, Øien 2001, Aven, Sklet & Vinnem 2006, Paté-Cornell, Murphy 1996). The research's state-of-the-art has established a strong link between the respective organisations' safety culture and a number of risk influencing factors taking various approaches ranging from qualitative and quantitative to probabilistic ones (e.g.: Hurst et al. 1991, Cacciabue 2000). Leveson (2004) suggested a broader, qualitative approach based on system dynamics theory with the

Please cite this article as: Markert F., Duijm N.J. and Thommesen J., 2013, Modelling of safety barriers including human and organisational factors to improve process safety, Chemical Engineering Transactions, 31, 283-288 DOI: 10.3303/CET1331048

accident model STAMP. The model includes the governmental control towards organisations and by that the societal influences on safety management. The STAMP model is based on former work by Rasmussen (1997) and Rasmussen and Svedung (2000).
Back in 1992, Bley et al. (1992) pointed out that probabilistic safety assessment (PSA) has difficulties assessing human reliability and the impact of organisational factors. This again makes it difficult for decision makers to decide as the lack of explicit HOF's is only shown implicit in the assessments in form of greater uncertainty. There are also basic events rooted in the organisation that may affect the integrity of multiple elements in the system. Thus there is a dependency, through the HOF, between these elements, that traditionally are treated as failing independently from each other. Bley et al. (1992) conclude the article despite these deficiencies: "PSA provides the only integrated way to balance influences from design, construction, and operation in terms of their impacts on safety. It provides the coordinated basis for ordering the importance of human actions and various component failures with respect to their impacts on plant safety. It calls for cooperation among design, manufacturing, and operations to optimize safety while minimizing costs. That promise may appear as a challenge to the traditional independent, serial interfaces of industry. Care, diplomacy, and competence are required of PSA organisations and are essential if the promise is to be realized" (p. 22).
This statement still has a lot of truth even today as e.g. stated by Skogdalen and Vinnem (2011). During time several authors have tried to close the gap with different approaches of integration of PSA and HOF impacts. Embrey (1992) suggested using a probabilistic approach to model the relation between failure and organisational factors, which is in line with the organisational factors chosen in e.g. ARAMIS shown in Table 1.

2. Barriers and management factors

The model presented in this paper is based on the ARAMIS (Duijm 2009) and the BORA release (Aven et al. 2006, Sklet et al. 2006) methods that consider a barrier approach to describe systems safety. Both have suggested a modification factor (MF) to modify the probability of failure-on-demand (PFD) of each safety barrier to implement the risk influencing factors defined as a set of management factors (shown in Table 1). They describe procedures to quantify the MF, which are based on scores from e.g. expert judgments, audits and/or literature data. The outcome provides a HOF modified barrier performance (PFD_{HOF} = PFD * MF) for each barrier. It has to be remarked that the items taken from the ARAMIS concept (listed Table 1) express the necessary functions to be fulfilled by management to ensure barrier integrity, rather than HOF's in their traditional meaning. For instance, a typical HOF "time pressure" is not directly included, but implicitly as a result of how well management deals with manpower planning and conflict resolution.
The concept of safety barriers has become an accepted approach in risk assessment, though with varying understandings of the term "safety barrier". This article adheres to a more strict definition of the term, which distinguishes the safety barrier from other safety measures, by applying the safety function concept (Duijm 2009, Harms-Ringdahl 2003): 1) A barrier function is a function planned to prevent, control, or mitigate the propagation of a condition or event into an undesired condition or event. 2) A safety barrier is a series of elements that implement a barrier function, each element consisting of a technical system or a human action.
It is noted that an action of a safety barrier is an unplanned action, in response to an unexpected deviation. Safety measures to control the integrity of the barrier, i.e. to ensure that the barrier is available for action when needed, are planned actions, which can be properly managed (scheduled). Failure in a primary process system will be revealed during normal operation because the main, productive function will fail. In contrast, the integrity of additional safety barriers is invisible during normal operation. Reliability of safety barriers is only revealed by dedicated inspection and testing– safety barriers therefore require extra awareness from management. Inspection and testing include activities to ensure proper human responses, such as interrogating staff during safety audits, emergency drills, and practising operators using table-top exercises or simulators.
When discussing the effect of human and organisational factors on safety, the effect is equally important for the avoidance of failures in the primary processes as for safety barriers, under the recognition that one should be aware of the differences between routine activities (related to the primary process) and activities that are performed seldom (related to safety barrier interventions), and how that affects human performance. Note that the definition of "Safety Critical Elements", as adopted in the legislation for offshore safety (UK Government 2005) covers both safety barriers as defined above, and what we have called "primary process systems" that on failure will cause (major) accidents.

Table 1: Management factors influencing barriers PFD in the ARAMIS (Duijm 2009)

Safety Culture
Manpower planning and availability
Competence and suitability
Commitment, compliance and conflict resolution
Communication and coordination
Procedures, rules, and goals
Hard/software purchase, build, interface, install
Hard/software inspection, maintenance, and replacement

If a barrier fails it may be caused by a complete random failure caused by technical or individual human factors, or by a systemic failure of the management processes to support the barrier. When we speak of "failure of the management processes" we mean that management has failed to ensure the integrity of a barrier according to its design specifications. Examples are degradation of a technical barrier due to lack of inspection (or inspection periods are exceeded), assigning tasks to staff that do not have the necessary competences, not providing necessary training or competence refreshment, assigning too few people to perform a task, management not responding when staff violates safety-related procedures, etc. Such management failures will not necessarily produce a barrier failure, but are latent failures that increase the probability that the barrier actually fails, e.g. an error by an operator due to inadequate competences or time pressure. By distinguishing the organisational processes as shown in Table 1 or any other set of organisational factors, we may in a first approach assume the factors being independent and thus will add up in an OR-gate to give the barrier's overall PFD value, as shown in Figure 1.

However, observations from major accidents such as from Bhopal (Leveson 2004) show that degradation of safety management may happen simultaneously throughout the whole organisation. Company-wide degradation of management processes are often related due to a general lack of focus, interest, policy, etc. at a high level in the organisation. In Figure 2 we have called this "Faults in Company Policy and Management Leadership", but it may require a much broader definition. The degradation leads to latent deficiencies in safety management processes and (thus) the outcomes of these processes. This applies finally to the safety-barrier's performance. Figure 2 shows how systemic faults in specific management functions and outcomes are conditional on (at least) one common cause. Note that deficiencies in process or outcome of safety management functions also include random causes, which are not shown in Figure 2. By combining Figure 2 with Figure 1 (i.e. the right-hand outputs of Figure 2 - combined with random failures - are to be inserted as inputs at the left-hand side of Figure 1 for any specific barrier) for different barriers sharing the same management processes, it becomes apparent that a system failure, that requires the simultaneous failure of several barriers, no longer can be considered as a series of independent failures, but that system failure also depends on common cause systemic faults. For instance, two successive barriers may both fail due to time pressure created by inadequate manpower planning. The conditional relations in Figure 2 express that the right-hand failure is conditioned on, but not necessarily a consequence of, the left-hand "parent" failure. This behaviour can also be (and is usually) expressed by Bayesian Belief Networks (BBN). Here the old-fashioned fault tree approach was chosen, extended with the notion of conditional probability, to avoid the need to develop the extensive conditional probability tables that follow with the use of BBN's. For this reason we also limit ourselves to two states: A condition is faulty, i.e. it can cause a barrier to fail, or it is not faulty, i.e. it will not contribute to the failure of the barrier.

While the combination of Figures 1 and 2 thus illustrates a high level common cause failure (where a failure in company policy may lead to systemic failures in several safety management functions), the example below will focus on a lower level common cause failure, where a failure in one safety management function undermines several barriers.

3. Elicitation

The problem of parameter estimation is an important aspect of a quantified modelling of human and organisational factors in risk analysis. These problems relate to *weighting* (how important is a management factor compared to random and other management factors) and to *anchoring* (given some level of management performance, how will it affect the barrier). Normally these factors are assessed using some form of expert elicitation. The challenge is to make this elicitation as simple as possible, keeping close to observable and easily perceptible notions and terms, so that the "experts" can be ordinary staff familiar with the organisation, rather than experts knowledgeable about the risk analysis process. In this paper, a barrier failure is assumed to be caused by a combination of random failures and systemic

failures of management processes. The distinction between random and systemic failures is suggested to be elicited by asking some questions on the management process and safety barrier performance, which will be described below.

Table 2: Example of apportionment of failures

Measure causing barrier failure	Fraction failures	of Ranking	Absolute probability
(Total Barrier)	100 %		0.1
Random failures	50%	1	0.053
Instruction of Operators	30%	2	0.03
Operating procedures	15%	3	0.015
User interface	5%	4	0.005

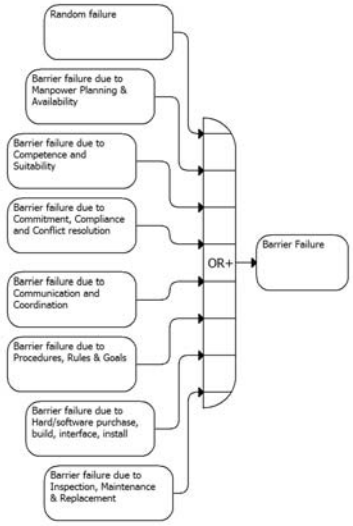

Figure 1. Barrier failure seen as resulting from a random cause or due to deficiency in outcomes of specific safety management functions.

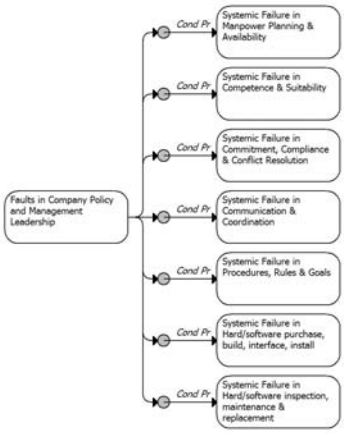

Figure 2. Deficiency in safety management functions may have a common cause in top management. "Cond Pr" - conditional probability.

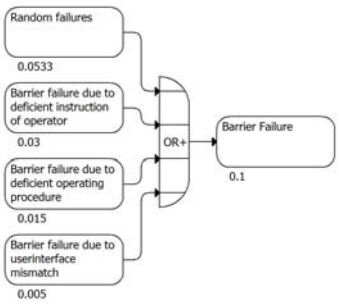

Figure 3. Structure of apportionment of failures in the quantified barrier model. Numbers below boxes indicate probabilities as in Table 2.

Once a list of safety measures for a specific barrier is compiled, it may be asked how important each of the safety measures is for this barrier, i.e.: What fraction of the failures of the barrier can be attributed to a failure of the safety measure? Such a list may look as shown in Table 2 and Figure 3. The "random failures" are understood as the failures not related to a specific measure. In this case the probability for random failures is calculated to satisfy that the barrier fails by one or more of the underlying causes

(measures or random failures). Instead of asking about fractions, one can also, to simplify the elicitation, ask for a ranking (Table 2) and afterwards apply consistent rules to transfer ranking into fractions. In Figure 4, we illustrate our ideas by showing the probabilistic dependency of two barriers on one of the underlying management processes, viz. “Insufficient delivery of procedures”. This may lead (but not necessarily so, hence the conditional probability) to a faulty procedure (which also can fail by a random factor). By that the faulty procedure is treated as a latent failure, which may lead (but not necessarily so) to an actual barrier failure. Both barriers may fail when the different procedures for the two barriers are both deficient due to weaknesses in the same management process. A deterministic approach with the same failure rates for the barrier failure causes (i.e. when everything to the left of the right-most conditional probabilities is taken out of the probabilistic analysis) would lead to a system failure probability of 0.005. Including the dependence of both barriers on the management process “delivery of procedures” increases the probability of system failure to 0.005244 (Figure 4). This effect will become more pronounced when the joint dependency on the other management processes (Figure 3) is included as well. Based on a model as in Figure 4 we can formulate questions for the next step of the elicitation. First we can assess the likelihood that a faulty procedure actually leads to a barrier failure, i.e. the right-most conditional probabilities in Figure 4. The next step in elicitation is an assessment of the systemic relations. This can be done by asking: “How likely will it be that, if the barrier fails due to some management process failure, e.g. an operating procedure fault, another, similar barrier will fail due to a similar fault, i.e. a fault in that other barrier’s operating procedure?” The question tries to estimate the conditional probability P(F2|F1), where Fi is “Bi(arrier) failure due to faulty procedure” in Figure 4. In a first approximation the probabilities P dependent or conditionally dependent on the management factor fault M (Insufficient delivery of procedures) can be expressed by:

$$P(F_1 \cap F_2) = P(F_1|F_2)\cdot P(F_2) = P(F_2|F_1)\cdot P(F_1) \approx P(M)\cdot P(F_1|M)\cdot P(F_2|M) \quad (1)$$

where, by nature of the similarity, the conditional probability $P(F_1|M)$ should be close to $P(F_2|M)$. Note that $P(F_i|M)$ is the product of the two consecutive conditional probabilities shown in Figure 4 (i.e. with values 0.08 and 0.04 for Barrier 1 and Barrier 2, respectively). How the probability of systemic failure is divided between the probability of failure P(M) of the high level process “Insufficient delivery of procedures” and the conditional probabilities P(F|M) depends on an optimization that fits best to the elicitations for the different barriers in the system.

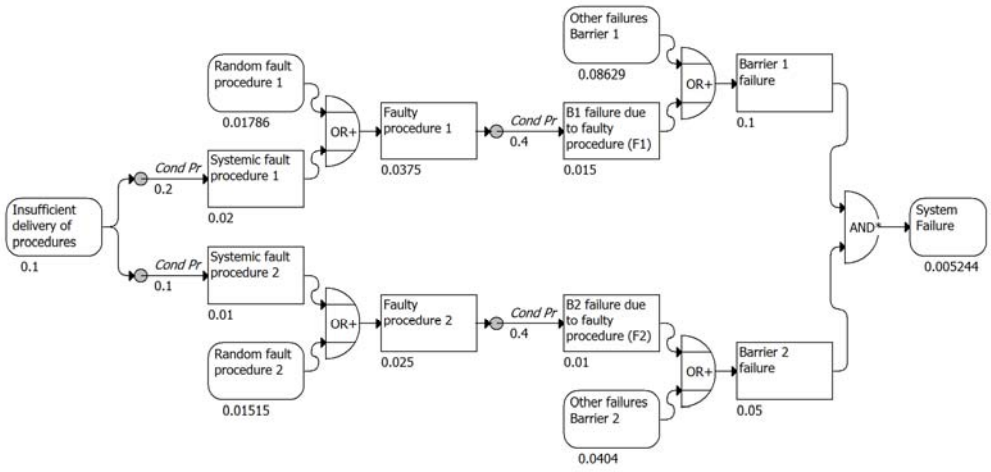

Figure 4 Model for the assignment of conditional probabilities using two similar barriers. Only one management function is shown. Data are included to reproduce the failure rates from Table 2 for barrier 1.

4. Discussion and conclusions

We have outlined a methodology to include the effect of deficiencies in management processes as common causes for the failure of safety barriers. Inclusion of such common causes leads to prediction of a higher probability of system failure compared to an approach where these deficiencies are included by deterministic adjustment of the individual barriers’ failure rates, as e.g. in the ARAMIS methodology. The methodology allows also the inclusion of common causes for management deficiencies at a higher level, such as company policies and leadership. Each deficiency or failure at some organisational level can thus

be considered as having systemic causes and non-systemic (independent, random) causes. The methodology is similar to earlier approaches using Influence diagrams or Bayesian Belief Networks (e.g. Galan et al. (2007)). However, we restrict ourselves to a binary approach at each level, discriminating only failure and success which means either or not fulfilling functional requirements. We expect that the clarity with respect to both the meaning of failure but also the simpler logical relations (as compared to complex probability matrices in a BNN) makes it easier to collect the necessary data in the method by expert elicitation, i.e. the assessment of the single conditional probabilities, the random single contributions, and the systemic effects. Finally we pursue to develop a framework for abstract safety management functions, e.g. by using the ARAMIS set of functions, that would make the framework applicable to organisations in general, without the need to develop distinct models for each organisation. Application on a specific organisation would mean a mapping for the abstract functions to the real organisation. We hope thereby also that the systemic effects and conditional probabilities throughout the framework can be chosen more generically, while audits can be used to adjust the random causes (especially at top level) to the specific organisation's safety management performance.

References

Aven, T., Sklet, S. & Vinnem, J.E. 2006, Barrier and operational risk analysis of hydrocarbon releases (BORA-Release): Part I. Method description, Journal of hazardous materials, 137, 681-691.

Bley, D., Kaplan, S. & Johnson, D. 1992, the strengths and limitations of PSA: where we stand, Reliability Engineering and System Safety, 38, 3-26.

Cacciabue, P.C. 2000, Human factors impact on risk analysis of complex systems, Journal of hazardous materials, 71, 101-116.

Colombo, S. & Demichela, M. 2008, The systematic integration of human factors into safety analyses: An integrated engineering approach, Reliability Engineering and System Safety, 93, 1911-1921.

Davoudian, K., Wu, J.S. & Apostolakis, G. 1994, The work process analysis model (WPAM), Reliability Engineering and System Safety, 45, 107-125.

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

Embrey, D.E. 1992, Incorporating management and organisational factors into probabilistic safety assessment, Reliability Engineering and System Safety, 38, 199-208.

Galán, S.F., Mosleh, A. & Izquierdo, J.M. 2007, Incorporating organizational factors into probabilistic safety assessment of nuclear power plants through canonical probabilistic models, Reliability Engineering and System Safety, 92, 1131-1138.

Gambetti, F., Casalli, A., Chisari, V. 2012, The Human Factor in Process Safety Management, Chemical Engineering Transactions, 26, 279

Harms-Ringdahl, L. 2003, Assessing safety functions - results from a case study at an industrial workplace, Safety Science, 41, 701-720.

Hurst, N.W., Bellamy, L.J., Geyer, T.A.W. & Astley, J.A. 1991, A classification scheme for pipework failures to include human and sociotechnical errors and their contribution to pipework failure frequencies, Journal of Hazardous Materials, 26, 159-186.

Leveson, N. 2004, A new accident model for engineering safer systems, Safety Science, 42, 237-270.

Øien, K. 2001, A framework for the establishment of organizational risk indicators, Reliability Engineering and System Safety, 74, 147-167.

Paté-Cornell, E.M. & Murphy, D.M. 1996, Human and management factors in probabilistic risk analysis: the SAM approach and observations from recent applications, Reliability Engineering & System Safety, 53, 115-126.

Rasmussen, J. 1997, Risk management in a dynamic society: a modelling problem, Safety Science, 27, 183-213.

Rasmussen, J. & Svedung, I. 2000, Proactive risk management in a dynamic society, Swedish Rescue Services Agency, Karlstad, Sweden.

Salvi, O., Duijm, N.J. (eds.), 2006, Special Issue Outcomes of the ARAMIS Project, Journal of Hazardous Materials, 130,

Sklet, S., Vinnem, J.E. & Aven, T. 2006, Barrier and operational risk analysis of hydrocarbon releases (BORA-Release). Part II: Results from a case study, Journal of hazardous materials, 137, 692-708.

Skogdalen, J.E. & Vinnem, J.E. 2011, Quantitative risk analysis offshore human and organizational factors, Reliability Engineering and System Safety, 96, 468-479.

UK Government 2005, The Offshore Installations (safety Case) Regulations 2005 No 3117.