ELSEVIER

Journal of Hazardous Materials 130 (2006) 284–292

Journal of Hazardous Materials

www.elsevier.com/locate/jhazmat

# Quantifying the influence of safety management on the reliability of safety barriers

Nijs Jan Duijm [a,*], Louis Goossens [b]

[a] *Risø National Laboratory, Systems Analysis Department, P.O. Box 49, DK-4000 Roskilde, Denmark*
[b] *Delft University of Technology, Faculty of Technology, Policy & Management, Safety Science Group, The Netherlands*

Available online 16 August 2005

**Abstract**

A methodology is described that enables to use safety management audit assessments and safety culture questionnaire results for estimating the reductions in the reliability of safety barriers in major hazard plants. The critical issue is the establishment of weight factors in combination with the anchoring of "good" safety management. A method is proposed to derive weight factors from statistical accident analysis in combination with a statistical analysis of safety management assessments at a representative sample of major hazard industries. A preliminary set of weight factors is presented with some examples of resulting reductions in reliability—this demonstration confirms that the set of weight factors needs further development.


*Keywords:* Safety management; Safety barriers; Probability of failure on demand; Quantified risk assessment

## 1. Introduction

Major hazard industrial sites in the European Union, covered by the so-called "Seveso-II" directive [1] are required to demonstrate the implementation of a "Major Accident Prevention Policy" (MAPP) and a safety management system. The directive and its national implementations provide prescriptions and requirements for the elements that need to be covered by the MAPP and the safety management system. The directive also requires a risk analysis to be performed and documented, demonstrating the possible development of major accidents and the likelihood of these accidents.

Until now, it has been difficult to discount the quality and effectiveness of safety management in the risk level of the industry, let alone to show satisfactorily how this should be accounted for in the risk analysis.

One of the goals of the "ARAMIS" project was to include the safety management efficiency in the risk assessment. The methodology should in principle be suitable to be used both in the context of a quantitative risk assessment (where risk is represented by contours of individual (fatality) risk and/or societal risk) and a qualitative risk assessment (where risk is represented by describing the consequences of a series of representative accidents at distances from the major hazard source). Depending on national implementations of the "Seveso-II" directive, both methods are applied in the European Union. However, it should be realized that safety management focuses on prevention and mitigation of accidents. Therefore, its efficiency can primarily be expressed by how much the *likelihood* of major consequences can be reduced, rather than by the absolute *magnitude* of the worst-case consequences. In other words, even in a qualitative risk assessment, considerations regarding *probability* need to be included.

The approach adopted by ARAMIS follows the structure from the I-RISK project [2]. This approach is based on the assessment of safety indicators by using an audit procedure; in the case of ARAMIS an additional indicator derived from a safety culture evaluation is included. The audit procedure is described in an accompanying paper [3], the safety culture questionnaire is exemplified in Ref. [4].

These indicators are indirect indicators of a company's safety performance as compared to direct indicators that are

* Corresponding author. Tel.: +45 4677 5165; fax: +45 4677 5199.
*E-mail address:* nijs.j.duijm@risoe.dk (N.J. Duijm).

0304-3894/$ – see front matter © 2005 Elsevier B.V. All rights reserved.
doi:10.1016/j.jhazmat.2005.07.014

based on the observation of (number of) actual incidents or unintended events. Replacing any monitoring of direct indicators by the present assessment approach is not suggested in here, but indirect indicators are considered to be precursor conditions for the unintended events, and direct indicators may not, neither qualitatively nor quantitatively, be extrapolated with respect to the prevention of major accidents. Quantification of safety management assessments to estimate a risk level of a given site is one goal, but it can also be a tool to prioritise the development of the safety management system and to focus on those safety management factors that, for a given site, have the largest impact on the likelihood of causing major accidents.

## 2. Previous work

There have been several attempts to link an assessment of the quality of safety management to the expected frequency of unwanted events, especially of Loss of Containment events. A recent overview of approaches towards indicators of organisational factors in relation to risk level can be found in Ref. [5].[1]

The variation and uncertainty in generic Loss of Containment frequencies is large and several sources presenting generic Loss of Containment frequencies suggest that for a specific case, the analyst applies a qualitative assessment of safety management in order to choose an adequate Loss of Containment frequency out of the available interval of frequencies. Examples are the FRED database [6], where the choice of the failure rate of a pressure vessel within a range of a factor of three may depend on the manufacturing procedures and inspection schemes, and the "Purple Book" [7], where the Loss of Containment frequency of similar equipment may be decreased by a factor of 5 based on the design code or on other provisions that have "indisputable failure-reducing effect".

A more formal approach was explored by MANAGER, developed by DNV [8–11]. The results of a questionnaire-based audit give a single score or "modifying factor" (MF) for the company on a scale from good–average–bad (where average relates to industry's average performance) with corresponding numerical values 0.1–1–100. The general failure rates are multiplied with the modifying factor for a specific plant. The numerical range was justified by the uncertainties in failure rate data from the COVO-study [12]. In practice, the variation between modified failure rates for "good" and "bad" companies appears to be half an order of magnitude lower and one order of magnitude higher as compared to the averaged, generic failure rates, respectively.

The Dutch authorities developed a tool for assessing accidental releases to the environment, "Proteus" [13].[2] This tool includes a questionnaire (based on a previous tool "VERIS") addressing five management aspects (safety management in general, competence of the personnel, work procedures, emergency management and technical standards of the installation). The likelihood of events during release scenarios is adjusted within the uncertainty interval of generic Loss of Containment frequencies and failure rates, depending on the type of event (mechanical failure, human error or mitigative action). This approach assumes implicitly that the range of Loss of Containment frequencies and failure rates as those reported in, e.g., FRED [6] and COVO [12] originates from differences in the safety management at the sites where the information was collected. It is, however, doubtful that this can be assumed for rare events like catastrophic failure of tanks, where there are no multiple events at a single site within a reasonable time span.

In the framework of developing the PRIMA tool, the differences in accident rates and Loss of Containment events were investigated [14] using data from earlier studies [15,16]. This investigation suggests that there exists a variation of two orders of magnitude (the study reports values between 40 and 100) between "very best" and "very worst" performance with respect to Loss of Containment events.

The PRIMA methodology [14] uses an audit that provides discrete ratings on eight key audit areas, which originate from this analysis of accident causation:

- hazard review of design;
- human factors review of maintenance;
- checking and supervision of maintenance tasks;
- routine inspection and maintenance;
- human factors review of operations;
- checking/supervision of construction and installation;
- hazard review of operations;
- checking/supervision of operations.

The ratings $x(i)$ are rated $-1$, 0 or 1 for "poor", "average" and "good" performances, respectively. Each key audit area has an assigned weight, $a(i)$, that differs for vessels, pipework and hoses and the modifying factor, MF, for the generic failure rate becomes:

$$\log(\mathrm{MF}) = \sum_{i=1}^{8} a(i)x(i) \tag{1}$$

As the sum over all $a(i)$ is close to 1, this means that a maximum variation of $\pm 1$ order of magnitude is obtained between the "average" rated companies and the "worst" or "best" ones.

The MANAGER and PRIMA methodologies address a single generic Loss of Containment failure rate. In contrast, the I-RISK methodology tried to develop a more transparent way of modelling management influences on the technical system [2]. Therefore, it links management factors, expressed as "delivery systems" to a number of parameters that characterise the events in the many fault trees that are generated during the quantified risk assessment (QRA). The idea is that management provides (delivers) the conditions for maintaining the integrity (both of human behaviour and hardware

[1] Only available in Norwegian.
[2] Only available in Dutch.

elements) of the safety-critical systems. The methodology addresses general elements that are common for all delivery systems (the process of maintaining safety policy and organisation and the process of risk analysis and designing the risk control and monitoring system) and eight specific elements:

- availability of personnel;
- commitment of personnel;
- competence of personnel;
- conflict resolution;
- interface and modifications;
- internal communication and coordination;
- procedures and plans;
- spares.

Even though I-RISK reduced the number of links by introducing "common mode" activities that control several of the fault tree events at the same time, the resources for performing the assessment, analysis and audit are large and beyond practical application. Likewise, there is not established a satisfactory quantitative link between the audit assessment and the event parameters.

The ARAMIS approach builds on the I-RISK methodology, but tries to make the approach practical by changing the link from delivery system to fault tree event to a link from delivery system to types of safety barriers, where the different types reflect the characteristics of the events in the fault tree (or barrier diagram). The delivery systems in ARAMIS are slightly different from I-RISK. The delivery systems and the safety barrier typology are described in the accompanying paper [3].

There are other approaches to relating safety management to risk level, mainly developed for other domains (nuclear, transport and spacecraft). We only name here the work process analysis model (WPAM) [17,18] that focuses on uncovering dependencies between events assumed to be independent in a technical assessment. By including the dependency of the events, the final frequency of the top event is automatically modified (to a higher frequency).

## 3. Quantification procedure in ARAMIS

The input to the quantification process of management influences on the safety level in ARAMIS comes from two assessments. One input is the result from the audit assessment by means of seven ratings $S_1$–$S_7$ for the following safety management delivery systems:

1. manpower planning and availability;
2. competence and suitability;
3. commitment, compliance and conflict resolution;
4. communication and coordination;
5. procedures, rules and goals;
6. hard/software purchase, build, interface, install;
7. hard/software inspect, maintain, replace.

This as well as the distinction between 11 types of safety barriers[3] is described in the accompanying paper [3]. The other input exists of the collective score from the safety culture assessment $S_0$ (see Ref. [4]). These ratings $S$ are expressed as a percentage, where 100% corresponds to optimal performance.

The suggested direct coupling of the rating of safety management and safety culture to the barrier's reliability is a simplification of reality, but introduced because it is even harder to quantify the "real" links in between, as indicated in Fig. 1: In reality, deficiencies in the process of safety management will increase the likelihood of deficiencies in the output of safety management (follow-up on training, maintenance planning). This in turn will increase the likelihood of deficiencies in conditions for safe operation (competence and maintenance) and finally increase the probability of failure on demand (PFD), the most obvious measure of barrier reliability. The most important short-cut is that the present methodology presumes that deficiencies in the process of safety management are directly linked to deficiencies in the performance of the safety barriers, while the actual causal relationship is such that the deficiencies in the output of safety management drive the probability of failures of the barriers (see Fig. 1).

The safety barrier-oriented approach throughout the ARAMIS methodology, see the accompanying paper [19], aims at applications both in a *qualitative* (or deterministic) and a *quantitative* risk assessment tradition. Therefore, the approach of international standard IEC 61511 [20] is applied, where the reliability of instrumented safety barriers or layers of protection is expressed by a safety integrity level (SIL). The relation between SIL and the probability of failure on demand is as follows:

$$\text{SIL} = 1\text{: } 10^{-1} < \text{PFD} \leq 10^{-2};$$
$$\text{SIL} = 2\text{: } 10^{-2} < \text{PFD} \leq 10^{-3};$$
$$\text{SIL} = 3\text{: } 10^{-3} < \text{PFD} \leq 10^{-4};$$
$$\text{SIL} = 4\text{: } 10^{-4} < \text{PFD} \leq 10^{-5}.$$

So, SIL-values refer to intervals of PFD rather than point values: this representation of "uncertainty" or "fuzziness" is attractive, especially for qualitative risk assessment approaches. It should be noted, that the SIL classification not only relates to intervals of PFD, but also to qualitative requirements on the (independence of) management of the instrumented systems. For non-instrumented systems (typically human action and behaviour), one often expresses SIL in terms of "Level of Confidence". In the remainder of this paper we will refer to the reliability of any layer of protection by using Level of Confidence (LC), because we focus on

[3] These types are: (1) permanent passive barriers for process control, (2) for process safety, (3) temporary passive barriers, (4) permanent active barriers, (5) activated barriers with hardware on demand, (6) activated barriers with automated devices, (7) activated barriers manually handled, (8) activated barriers with human action based on passive warning, (9) activated barriers assisted by software, (10) activated barriers based on procedures and (11) activated barriers in emergency situations.

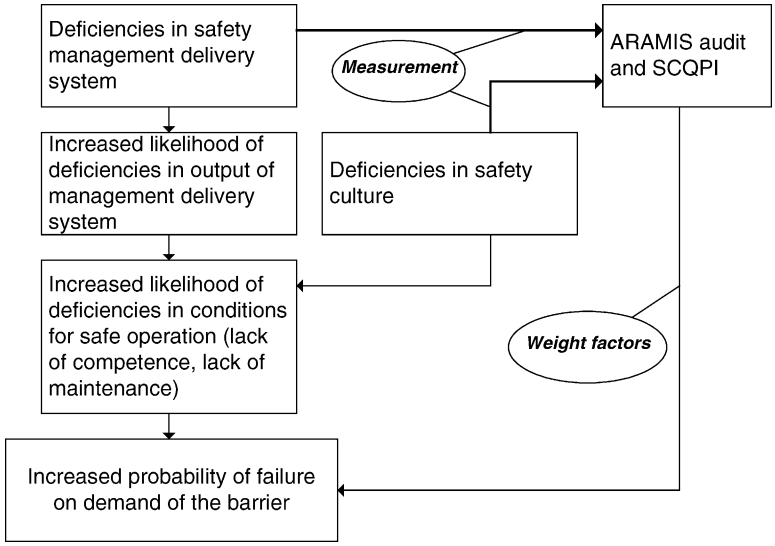


Fig. 1. Assumed relationships between safety management quality, safety culture (SCQPI) and probability of failure on demand (PFD) of safety barriers.

the effect of management on PFD and not on the qualitative requirements.

The design (also referred to as *nominal* or *optimal*) LC should be allocated to the actually implemented barriers. The design LC is based on historical or experimental failure data in combination with specifications, e.g., inspection intervals. The ARAMIS philosophy is that one cannot claim a better reliability for a safety barrier than its design value. In other words, good safety management cannot improve barrier reliability, but bad safety management can very well deteriorate it. This philosophy deviates from the approaches in PRIMA and MANAGER, where the anchor point of the assessment is the average safety management performance of industry. As such it introduces some difficulties, such as how to anchor "optimal" safety management, where "optimal" means sufficiently good to guarantee the design LC over the lifetime of the barrier, and that reliability data obtained from operational experience not (necessarily) represent the design LC of the barrier. But the advantage of this philosophy is that it includes a more objective description of the anchor point, and it is in principle not sensitive to the (hopefully positive) development of the average safety management performance of industry.

As a consequence of using LC as the dimension for expressing reliability, the a priori simplest model of expressing variation in the operational value of LC of a barrier (or safety barrier component[4]) of type $k$ was thought to be a linear variation between the design value for optimal safety management and zero for "absent" safety management:

$$\mathrm{LC}_{\mathrm{operational},k} = \left(1 - \sum_{i=0}^{7}(1 - S_i)B_{i,k}\right)\mathrm{LC}_{\mathrm{design},k} \qquad (2)$$

Here, $S_i$ represents the final rating for the delivery corresponding to structural element $i$ including audit and safety culture assessments, $B_{i,k}$ represents an array of weight factors linking the importance of the delivery system $i$ to the barrier type[5] $k$ in question, with $B_{i,k} \geq 0$ for all $k$ and $i$.

One can question the appropriateness of this way of incorporating management influences on barrier reliability. Existing approaches (MANAGER and PRIMA) apply a linear variation in the PFD, while the formula above describes an exponential variation in the PFD. Change in human error probability under influence of performing shaping factors in the models HEART and NARA [21] is expressed by a linear variation in the error probability. Also, for technical systems, the expressions to derive the PFD from failure rate data show that the PFD varies linearly with the time between inspections, which is a factor expected to be closely related to management performance. Still, one can argue that reliable, and therefore, more complex systems or actions may be more sensitive to management influences, and therefore, are reduced more strongly in PFD than barrier systems with lower design reliability. This argument coincides with the broader definition of safety integrity level to include qualitative requirements, i.e., a deficiency in safety management is likely to result in a (linear) reduction in the fulfilment of these requirements. Therefore, we continue to use the expression above, though this should be an issue for further consideration.

## 4. Weight factors for safety management influence

The essential problem in expressing the influence of safety management on safety barrier reliability is the determination of the set of influence weights $B_{i,k}$. One approach is to

[4] The probability of failure on demand of a barrier is approximately (rare event approximation) the sum of the probabilities of failure on demand of the serial barrier components.

[5] ARAMIS distinguishes 11 types of barriers, see footnote 3.

use expert elicitation. In the I-RISK project, expert elicitations were done for maintenance [22]. In the present project, questionnaires were distributed to selected experts in order to obtain their ranking of influences of the aforementioned seven management factors (delivery systems) for all 11 types of safety barriers, that for practical reasons were reduced to four categories:

1. *Hardware barrier category*: this category includes the barrier types 1, 2, 4 (permanent barriers), 5 and 6 (active hardware barriers);
2. *Temporary barriers*: including types 3 (temporary passive barriers) and 8 (barriers based on warnings, e.g., donning personal protection equipment);
3. *Behavioural skill and rule based barriers*: types 7, 9 and 10;
4. *Behavioural knowledge based barriers*: type 11.

The experts' ranking of influence can be transferred to a list of relative weight factors. The problem is that it is not a priori known, whether the management influences explain the total reliability completely or not. There are three possible conditions; these conditions correspond with the value of the sum of the weight factors:

If $\sum_{i=0}^{7} B_{i,k} = 1$, all reliability is explained by the (included) management factors. This unique situation will be rare.
If $\sum_{i=0}^{7} B_{i,k} < 1$, there is residual reliability, i.e., even in case of very bad safety management, still LC > 0 and PFD < 1. These barriers can be considered resilient to management failures; passive hardware barriers are probably most resilient.
If $\sum_{i=0}^{7} B_{i,k} > 1$, there are some factors that can reduce the LC to zero (PFD = 1) even before all ratings reach the minimum values. Although one can show that specific barriers will not work at all under some conditions (e.g., safety helmets if there is a general attitude not to don personal protective equipment), we should remind, that in the present approach we adjust the reliability of types of barriers, not of single, specific barriers.

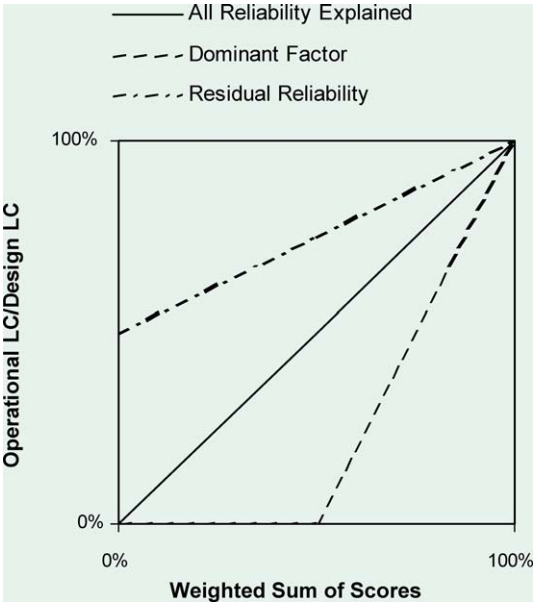


Fig. 2. Variation of the value for the operational LC depending on the conditions for the weight factors.

The above-mentioned conditions are visualised in Fig. 2.

## 5. The use of accident causation statistics for establishing management influence

The derivation of weighting factors for PRIMA [14,16] is based on accident causation. The factors $a(i)$ in formula (1) are identical to the percentage of (exclusive) causes in the set of accidents analysed. This means that for an "average" company with all ratings $x(i)$ equal to 0, the expected cause distribution for a Loss of Containment is assumed to be equal to the distribution in the studied sample. The rationale for using these percentages as weight factors is that bad performance on one factor will increase, in absolute terms, the number of accidents due to this factor and vice versa, good performance cannot reduce the number of accidents to more than those that are caused by this factor.

In principle, statistical accident–cause analysis provides an estimate of the conditional probabilities $P(B_i|A)$, where $A$ is the event of an accident or failure on demand and $B_i$ the different causes. When those $B_i$ correspond to management factors, we are actually interested in the probability $P(A|B_i)$, i.e., the likelihood of a failure under the knowledge that a deficiency in management factor $B_i$ is a contributing factor to the failure, and $P(A|\neg B_i)$, the likelihood of a failure under the knowledge that there is no deficiency in this management factor. The latter situation corresponds with the optimal or design situation in the ARAMIS philosophy, so we are actually interested in the ratio $\frac{P(A|B_i)}{P(A|\neg B_i)}$, which would be the modifying factor for management factor $B_i$.

According to Bayes' theorem:

$$P(A|B_i) = \frac{P(B_i|A)P(A)}{P(B_i)} \tag{3}$$

where $P(A)$ is the generic failure rate as derived from an "average" industrial sample that includes examples of "good" and "bad" management, and $P(B_i)$ the likelihood that there is a deficiency in management factor $B_i$ which could be a contributing factor to a failure, to be obtained from the same sample or, if this is not possible, from a sample of companies that is representative for the sample that provided the failure rate $P(A)$. From (3) we derive the modification factor $\mathrm{MF}_i$:

$$\mathrm{MF}_i = \frac{P(A|B_i)}{P(A|\neg B_i)} = \frac{P(B_i|A)}{1 - P(B_i|A)} \frac{1 - P(B_i)}{P(B_i)} \tag{4}$$

As can be seen from (3) and (4), the modification factor not only depends on the observed frequency of failures where the management factor actually was a contributing factor, but also

how often there is a deficiency in the management factor with the potential to contribute to a failure, but without the failure happening. Formula (4) offers an opportunity to include data from statistical accident analysis to obtain weight factors for the safety management factors, but this needs additional statistical information about the actual status of safety management in a sample of industrial sites, e.g., by performing a series of audits. The studies that led to PRIMA actually included these audit activities [14,16].

In case we assume that occurrences of deficiencies in safety management factors are independent of each other (which is a severe assumption—bad management will probably be apparent in different management factors), the modification factors can be multiplied with each other for the different factors. In case there are (known) correlations between the occurrence of different deficiencies, the situation can best be analysed using a Bayesian Belief Network.

## 6. A set of preliminary weight factors for the ARAMIS approach

In the absence of results from the expert elicitation, weight factors where derived from existing data. For the expert elicitation, the original 11 barrier types were grouped together into four categories.[6]

For the behavioural barriers, use has been made of the overlap between the relevant management factors of ARAMIS and the error producing conditions as recognised by the NARA database [21]. The correspondence between the items is shown in Table 1. The transition to the weight factors based on adjustment of LC values according to formula (2) has been done by taking characteristic values of human error probabilities for skill and rule based actions, and knowledge based actions, respectively. These values have been used for the two respective barrier categories. For the temporary barriers, the skill and rule based weight factors have been halved.

For hardware barriers, no such data are directly available, so use has been made of the approach by using formula (4). This requires results from a statistical accident or incident analysis. There are several published studies, but as both taxonomy, reporting procedures for accident notification, etc. are quite different, the results are hardly comparable. Table 2 shows a comparison of a recent analysis using the US EPA RPM*Info database [23], and the data from the pipework failure analysis prior to the development of PRIMA [15]. A recent analysis from the European Union's MARS database uses a different taxonomy, where maintenance and construction/purchase/design issues cannot be distinguished [24]. The problem is evident: if the aforementioned approach is used, there needs to be close agreement between the management factors for which one wants to derive the modifying factors and the classifications used during the accident analysis. For that reason, we restrict ourselves to using the pipework failure study, because the PRIMA audit methodology follows the same modelling framework. From ref. [14] we have information on results from audits of six representative plants. We assume that a rating of "−1" corresponds to a deficiency in the corresponding management factor (audit area). The results for the factors that have our interest are listed in Table 3. By combining these results with the fraction of accidents caused by these factors (Table 2, last column) we obtain the modifying factors for the failure rate of hardware barriers, as included in Table 1 (fifth column). These modifying factors are transferred to weight factors to be used by the ARAMIS methodology, assuming a barrier with LC = 3 and assuming that "deficiency" means an audit score of 40% on the delivery system in question (an audit score of 40% corresponds to the audit judgement "under development, overall improvement needed"). This preliminary exercise shows that even if "design" and "maintenance" are equally often a contributing factor to a failure, "design" is a more serious management factor, because *relative to the number of deficiencies observed* in design, the number of failures is three times higher.

## 7. Example

During the ARAMIS project, a number of case studies were performed in order to test the approaches. The results are summarised in Fig. 3. To demonstrate the effect of quantification, the reduction in reliability (LC) of a barrier from each of the four categories is calculated, using the minimum, average and maximum values of the ratings found during the case studies. One should note, that the audit is barrier-oriented, which means that there can be different ratings for different identified, representative barriers on specific site,

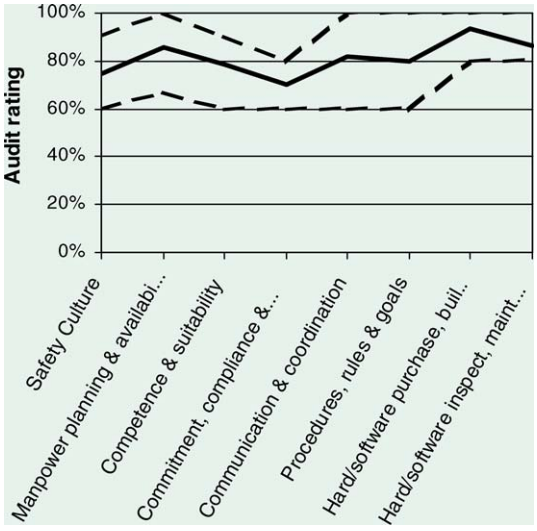


Fig. 3. Summary of the results from the ARAMIS case studies, showing the minimum, averaged and maximum ratings of the management factors.

[6] See above, the categories are: (1) hardware barriers, (2) temporary barriers, (3) behavioural skill and rule based barriers and (4) behavioural knowledge based barriers.

Table 1
Preliminary weight factors for the ARAMIS methodology

| ARAMIS delivery system/ management factors | NARA EPC ID/NARA EPC description | NARA EPC affect | PRIMA audit area | Modifying factor (see text) | ARAMIS weight factor $B_{i,k}$ Barrier types | | | |
|---|---|---|---|---|---|---|---|---|
| | | | | | 1, 2, 4, 5, 6 (hardware) (%) | 3, 8 (temporary) (%) | 7, 9, 10 (behaviour *R*/*S*) (%) | 11 (behaviour *K*) (%) |
| 0 Safety culture | 19 Low workforce morale or adverse organisational environment | 2 | | | 0 | 8 | 15 | 25 |
| 1 Manpower planning and availability | 3 Time pressure | 11 | | | 0 | 29 | 58 | 87 |
| 2 Competence and suitability | 2 Unfamiliarity, i.e., a potentially important situation which only occurs infrequently or is novel | 20 | | | 0 | 36 | 72 | 100 |
| 3 Commitment, compliance and conflict resolution | 14 A conflict between immediate and longterm objectives | 2.5 | | | 0 | 10 | 20 | 33 |
| 4 Communication and coordination | 6 Difficulties caused by poor shift hand-over practices and/or team coordination problems or friction between team members | 10 | | | 0 | 25 | 50 | 83 |
| 5 Procedures, rules and goals | 12 Shortfalls in the quality of information conveyed by procedures | 3 | | | 0 | 9 | 18 | 40 |
| 6 Hard/software purchase, build, interface, install | | | *Design* + hazard study, *construction* + task checking | 6 | 43 | 22 | 0 | 0 |
| 7 Hard/software inspect, maintain, replace | | | *Maintenance* + task checking and routine checking | 2 | 17 | 8 | 0 | 0 |

Table 2
Comparison of two different statistical accident–cause analyses

| Analysis of RPM*Info [23] | Fraction contributing factor (%) | Analysis of pipework failures [15] | Fraction underlying cause (%) |
|---|---|---|---|
| Maintenance (equipment failure) | 9 | Maintenance | 38.7 |
| Process design failure (equipment failure) | 4 | Design | 26.7 |
| Unsuitable equipment (equipment failure) | 4 | Construction<br>Manufacture | 10.3<br>2.4 |

The data from the RPM*Info database only includes the accidents where equipment failure was the direct cause.

Table 3
Observed fraction of deficient management factors observed among six industries [14]

| Audit areas | Fraction observed deficiency (%) |
|---|---|
| *Maintenance* + task checking and routine checking | 25 |
| *Design* + hazard study, *construction* + task checking | 8.3 |

depending on the level of detail during the audit. Of course, one should use the rating that corresponds to the barrier in question. (The results from the safety culture assessment are generic.) The results are presented in Table 4. At first sight, it seems that the weight factors based on the values from the NARA error promoting conditions lead to strong reductions in the reliability of the behaviour-based safety barriers, which does not seem to agree with the general level of the audit assessments.

We can illustrate these results for a pressure relief valve. According to Ref. [25], one can estimate the dangerous failure rate for a pressure relief valve (PRV, unspecified type for this example) to be $2 \times 10^{-6}\,h^{-1}$. With a scheduled inspection interval of 3 months, this corresponds to a PFD of $2.2 \times 10^{-3}$ or a design LC of 2.7 (if we allow real numbers to express LC). When we apply the multiplying factor of 0.88 for the minimum score from Table 4, the operational LC would become 2.3, i.e., the PFD would rise to $4.6 \times 10^{-3}$, twice as high as the design value. If we allow LC to be expressed by whole numbers only, the LC of the PRV would be 2 and remain unchanged.

Table 4
Example of results of calculation of operational LC values, using case-study assessments

| Barrier category | Multiplying factors to determine operational LC values | | |
|---|---|---|---|
| | For minimum score | For averaged score | For maximum score |
| Hardware barrier | 0.88 | 0.95 | 1 (no reduction in reliability) |
| Temporary barriers | 0.49 | 0.75 | 0.94 |
| Behavioural skill and rule based barriers | 0.11 | 0.54 | 0.87 |
| Behavioural knowledge based barriers | 0 (no reliability left) | 0.28 | 0.81 |

## 8. Discussion and conclusions

This paper described the development of the methodology to quantify the assessments of safety management and safety culture.

For sake of simplicity, the project has adopted a methodology that focuses on reductions in the Level of Confidence. The discussions in this paper show that a method based on linear reductions of the probability of failure on demand are perhaps better founded.

The main problem in the quantification is the establishment of weight factors and the anchoring of "good" safety management compared to a design level of the Level of Confidence. Often, use is made of expert elicitation in combination with findings from accident analysis. A method is proposed to exploit the use of statistical accident analysis—it is shown that such a method needs to include a statistical analysis of the occurrence of deficiencies in safety management in the absence of accidents, i.e., two sources of information are needed: the statistics of contributing factors to failure of barriers and statistics of audits and safety culture evaluations from a sufficiently large representative sample of major hazard industries. In both sets the same set of contributing factors should be exploited, and a consistent taxonomy need to be used, a factor that limits the possibility of using available datasets. It is shown that some safety management factors, that appear equally often as a cause in accidents, can have quite different importance in safety management.

The use of the method is demonstrated using a preliminary set of weight factors. From this example, it appears that the set of weight factors need considerable improvement.

There are hesitations for introducing quantified safety management evaluations in the risk assessment. The argument is that management is changing fast, so the risk assessment – and the decisions on, e.g., land-use planning – would not be robust. We like to oppose to this argument for the following reasons:

- Present risk assessments tend to be based on optimal, design values for the safety integrity levels of safety barriers. The inclusion of the safety management evaluation leads to more conservative risk estimates, and as such the results would actually be more robust with respect to future conditions. Neglecting the safety management efficiency means actually neglecting the possible degradation of the

safety barriers under the presumably volatile safety management regimes.

- The *process* of safety management is the (only) element that provides and indication about the expected future state of the safety barriers, i.e., the future risk level. Accepting a risk assessment that includes a safety management evaluation gives the authorities a more explicit reference for plant inspections—and enables the authorities to put explicit requirements on specific items of safety management.

## References


[1] European Council, Council Directive 96/82/EC of 9 December 1996 on the control of major-accident hazards involving dangerous substances, Official J. Eur. Commun., L10 (1997) 13–33.

[2] J.I.H. Oh, W.G.J. Brouwer, L. Bellamy, A.R. Hale, B.J.M. Ale, I.A. Papazoglou, The I-Risk project: development of an integrated technical and management risk control and monitoring methodology for managing and quantifying on-site and off-site risks, in: A. Mosleh, R.A. Bari (Eds.), Probabilistic Safety Assessment and Management, Springer, London, 1998, pp. 2485–2491.

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

[4] N.J. Duijm, H.B. Andersen, B. Cleal, A.R. Hale, F.W. Guldenmund, Development of barrier-oriented audit protocols and safety culture questionnaires: application to Dutch and Danish test sites, in: C.A. Brebbia, T. Bucciarelli, F. Garzia, M. Guarascio (Eds.), Safety and Security Engineering SAFE, WIT Press, Southampton, 2005, pp. 289–298.

[5] K. Øien, S. Sklet, Bruk av risikoanalyser i driftsfasen, etablering av sikkerhetsindikatorer og modellering av organisatoriske faktorers effekt på risikonivået - en "state-of-the-art" beskrivelse (Use of risk analysis during operation, establishment of safety indicators and modeling of organisational factors' effect on risk level - a "state-of-the-art" description, in Norwegian), Rep. No. STF38 A99416, SINTEF, Trondheim, Norway, 1999.

[6] HSL, Failure Rate en Event Data (FRED), Software Version 1 part 26 (public) release 2, Data Version 2.2, Health and Safety Executive and Health and Safety Laboratory, Sheffield, 2003.

[7] Committee for the Prevention of Disasters, Guidelines for quantitative risk assessment ("Purple Book"), Rep. No. CPR 18E, Sdu Uitgevers, The Hague, Netherlands, 1999.

[8] Technica, The Manager Technique. Management Safety Systems Assessment Guidelines in the Evaluation of Risk, Technica, London, 1988.

[9] R.M. Pitblado, J.C. Williams, D.H. Slater, Quantitative assessment of process safety programs, Plant/Operations Prog. 9 (3) (1990) 169–175.

[10] F.P. Lees, Loss Prevention in the Process Industries—Hazard Identification, Assessment and Control, second ed., Butterworth-Heinemann, Oxford, 1996.

[11] N.W. Hurst, R. Hankin, L.J. Bellamy, M.J. Wright, Auditing—a European perspective, J. Loss. Prev. Process ind. 7 (2) (1994) 197–200.

[12] COVO Steering Committee, Risk Analysis of six potentially hazardous industrial objects in the Rijnmond Area, a pilot study, Central Environmental Control Agency Rijnmond DCMR, Schiedam, Netherlands, 1981.

[13] AVIV, Achtergronddocument Protheus (Background document Protheus, in Dutch) Enschede, Netherlands, 1998.

[14] N.W. Hurst, S. Young, I. Donald, H. Gibson, A. Muyselaar, Measures of safety management performance and attitudes to safety at major hazard sites, J. Loss. Prev. Process Ind. 9 (2) (1996) 161–172.

[15] N.W. Hurst, L.J. Bellamy, T.A.W. Geyer, J.A. Astley, A classification scheme for pipework failures to include human and sociotechnical errors and their contribution to pipework failure frequencies, J. Hazard. Mater. 26 (2) (1991) 159–186.

[16] L.J. Bellamy, T.A.W. Geyer, J.C. Williams, Organisational, Management and Human Factors in Quantified Risk Assessment Report 1, Rep. No. 33/1992, HSE, UK, 1992.

[17] K. Davoudian, J.S. Wu, G. Apostolakis, Incorporating organizational factors into risk assessment through the analysis of work processes, Reliabil. Eng. Syst. Saf. 45 (1–2) (1994) 85–105.

[18] K. Davoudian, J.S. Wu, G. Apostolakis, The work process analysis model (WPAM), Reliabil. Eng. Syst. Saf. 45 (1–2) (1994) 107–125.

[19] C. Delvosalle, C. Fiévez, A. Pipart, B. Debray, ARAMIS Project: A comprehensive methodology for the identification of reference accident scenarios in process industries, J. Hazard. Mater 130 (3) (2006) 200–219.

[20] IEC, International Standard IEC 61511-1, Functional Safety – Safety instrumented systems for the process industry sector – Part 1: Framework, definitions, system, hardware and software requirements, IEC, Geneva, Switzerland, 2003.

[21] B. Kirwan, H. Gibson, R. Kennedy, J. Edmunds, G. Cooksley, I. Umbers, Nuclear action reliability assessment (NARA): a data-based HRA tool, in: C. Spitzer, U. Schmocker, V.N. Dang (Eds.), Probabilistic Safety Assessment and Management PSAM 7—ESREL'04, Springer-Verlag, London, 2004, pp. 1206–1211.

[22] A.R. Hale, M.A.F. Costa, L. Goossens, K. Smit, Relative importance of maintenance management influences on equipment failure and availability in relation to major hazards, in: G.I. Schueller, P. Kafka (Eds.), Safety & Reliability, Balkema, Rotterdam, 1999, pp. 1327–1332.

[23] F. Al-Qurashi, Development of a Relational Chemical Process Safety Database and its Applications to Safety Improvements, Texas A&M University, College Station, Texas, 2000.

[24] N. Kawka, C. Kirchsteiger, Technical note on the contribution of sociotechnical factors to accidents notified to MARS, J. Loss. Prev. Process Ind. 12 (1) (1999) 53–57.

[25] SINTEF Industrial Management, OREDA Offshore Reliability Data Handbook, fourth ed., Det Norske Veritas, Høvik, Norway, 2002.