ELSEVIER

Journal of Hazardous Materials 130 (2006) 234–241

Journal of Hazardous Materials

www.elsevier.com/locate/jhazmat

The development of an audit technique to assess the quality of safety barrier management

Frank Guldenmund [a,*], Andrew Hale [a], Louis Goossens [a], Jeroen Betten [a], Nijs Jan Duijm [b]

[a] *Safety Science Group, Delft University of Technology, Netherlands*
[b] *Risø National Laboratory, Denmark*

Available online 18 August 2005

Abstract

This paper describes the development of a management model to control barriers devised to prevent major hazard scenarios. Additionally, an audit technique is explained that assesses the quality of such a management system. The final purpose of the audit technique is to quantify those aspects of the management system that have a direct impact on the reliability and effectiveness of the barriers and, hence, the probability of the scenarios involved.

First, an outline of the management model is given and its elements are explained. Then, the development of the audit technique is described. Because the audit technique uses actual major hazard scenarios and barriers within these as its focus, the technique achieves a concreteness and clarity that many other techniques often lack. However, this strength is also its limitation, since the full safety management system is not covered with the technique. Finally, some preliminary experiences obtained from several test sites are compiled and discussed.

Keywords: Safety management; Audit technique; Risk analysis; Safety barriers

1. Introduction

The safety management audit described in this paper has been developed within the context of the ARAMIS-project [1], which is fully explained elsewhere in this special issue. Although primarily aimed at companies that fall under the European Seveso-regime, the audit is not necessarily restricted to such companies. While major hazard scenarios are its prime input, the underlying management system controlling these is considered sufficiently generic to cover most issues of safety management.

The ARAMIS audit builds on experiences gained with the I-Risk Management Audit (IRMA audit technique) [2,3] that was developed within an prior European project I-RISK [4]. The main improvement appears to be a more concrete focus on barriers rather than the base events of fault trees, like time to repair or error rate. Nevertheless, the establishment of a valid link between the quantitative world of fault and event trees (technical model) and the qualitative world of barrier reliability and its management control (management model) remains a challenge.

The purpose of this paper is to describe the audit in more detail. First, the model underlying the audit will be outlined followed by a description of the barrier concept. Barriers are conceived here in a somewhat different way, which will be discussed below. Thereafter, the development of the audit manual will be described and some initial experiences obtained with the audit will be sketchily reported. The paper closes with an evaluation of the audit technique and a glimpse of future developments.

2. Underlying models

2.1. Management model

As indicated above, the ARAMIS audit takes as its primary input major hazard scenarios that have been developed[1] for a

* Corresponding author.
E-mail address: f.w.guldenmund@tbm.tudelft.nl (F. Guldenmund).

[1] The way that these scenarios are developed and the lists of barriers are produced is described elsewhere in this issue.

0304-3894/$ – see front matter © 2005 Elsevier B.V. All rights reserved.
doi:10.1016/j.jhazmat.2005.07.011

particular Seveso plant (or installation) and the barrier solutions devised to prevent these scenarios from materializing. The evident purpose of the safety management of a (Seveso) company is to ensure that the barriers are operating as specified or required and the audit aims to assess whether this is actually the case. For this purpose the audit concentrates on systems the company has in place to choose barrier solutions and select barriers, the life cycle of barriers and on systems to learn from and improve the current approaches to barrier selection and management.

As has been pointed out, barriers are selected based on scenarios, which are developed from so-called bow ties. Combining a fault tree and an event tree at their top events and turning this on its side, results in a figure that resembles a 'bow tie'. Scenarios then are formulated by describing escalation paths through this bow tie, starting at initial events on the fault tree side ('threats') and ending at unwanted ones on the event tree side of the figure ('consequences'). The use of bow ties for this purpose has become quite common in the last few years and, consequently, the development of scenario based auditing techniques has become opportune.

To define scenarios and devise barrier solutions for these, the company must have a risk identification system in place and working. The outputs of this system are barrier solutions, which initiate the barrier life cycle. Barriers have to be designed or ordered according to particular specifications, have to be built or delivered, installed and adjusted for use. Importantly, when barrier solutions are deliberated and functions are defined, certain trade-offs should be considered. For instance, should the barrier be a passive hardware solution like a wall or a layer of paint or should it be active like a pressure relief valve or an interlock, and what should be the desired or required involvement of people in its operation? Hence, when the barrier life cycle starts, two other life cycles start with it, namely a life cycle related to the development of procedures and another one aimed at the competence of people working with the barrier (see Ref. [5] for comparable reasoning). Additionally, this competence can be defined at the skill, rule and knowledge based level.

When all three life cycles have developed up to the point of use of the barrier, an additional five safety management issues become pertinent. For instance, when procedures for a barrier have been developed, they should be adequately adhered to. In the ARAMIS audit, the management system concerned with commitment and conflict resolution has been defined for this purpose. Another management system is involved in the planning of work and allocating competent people to it (availability), whilst a system for inspection and maintenance monitors the barriers in operation. Also, when several people are involved in the use or maintenance of barriers, communication systems have to be in place, to ensure appropriate interaction. Finally, experiences gained during operation or maintenance or due to incidents, accidents or other new insights, should be used for changing and improving the whole safety management system. This learning process copes with one aspect of change. In addition, the company

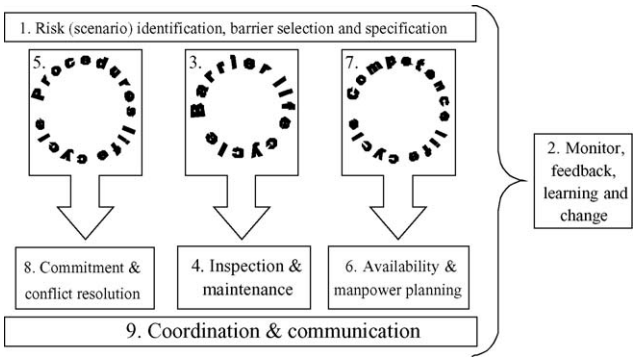

Fig. 1. Overview of barrier management delivery systems.

may decide to change its technology, process or management systems, to improve productivity or other company objectives, to profit from good practice elsewhere or to develop new markets. All of these system changes may require new or modified barriers or adjustments to management systems. These change processes require careful management, which partially repeats the processes of risk analysis and barrier selection described earlier. They are all considered part of the learning system.

The nine systems summed up above define the safety management system that is assessed in the ARAMIS audit. Together these systems deliver the controls and resources for proper barrier functioning and which should prevent (major hazard) scenarios from happening. Therefore, these management systems are appropriately called in the ARAMIS audit 'delivery systems'. In Fig. 1, these delivery systems and their relationships are shown.

Delivery systems can also be envisioned as being concerned with hardware barriers or behavioural (elements of) barriers. In that case the life cycle of barriers, including inspection and maintenance, would be considered the hardware side of barriers, whereas the behavioural side would be supported by the delivery systems procedures, manpower planning, competence, commitment and communication. These delivery systems all presume some human involvement in barrier operation. This distinction between hardware and behavioural barriers and their related management delivery systems is made in the ARAMIS audit as well.

A. Hardware related systems:
   1. risk (scenario) identification, barrier selection and specification;
   2. monitoring, feedback, learning and change management;
   3. design specification, purchase, construction, installation, interface design/layout and spares;
   4. inspection, testing, performance monitoring, maintenance and repair;

B. Behaviour related systems:
   5. procedures, plans, rules and goals;
   6. availability, manpower planning;
   7. competence, suitability;

8. commitment, conflict resolution;
9. coordination, communication.

A main objective of the management model has been that it is both comprehensive and parsimonious. Therefore, aspects of management that are often considered separately in other safety management systems are here subsumed under one or more delivery systems, or combinations thereof. For instance, the notion of supervision is addressed in the delivery system for commitment (8) but is also of concern in the delivery systems for competence (7) and learning (2).

2.2. Barrier concept

The barrier concept first appeared in the work of Haddon [6,7], is prominently present in the MORT tree [8] but has been elaborated lately in particular by Hollnagel [9,10]. The 'classical' barrier concept presumes a hazard (a dangerous source of energy) and a target (a vulnerable object, like humans, animals or the environment), which is protected by the barrier. Obviously, this barrier is physical in nature; otherwise, it cannot protect the target. Distance is also considered a barrier in this context, and when the energy level is high, the critical distance must be large.

However, in the context of fault and event trees and the notion of 'defence in depth', the barrier concept has been stretched comprising also barriers that in themselves cannot protect the target from the hazard, but are part of a whole set of measures that together represent the classical barrier concept of the MORT tree. Hence, between the hazard and the target many 'barriers' are put that together should prevent the hazard from damaging the target, i.e. 'defence in depth'. In such a series, many barriers are not so much concerned with actual hazards but with occurrences or events that might lead to some sort of loss of control and, in the long run, the unwanted release of a hazardous energy source. Barriers therefore have different functions, based on their location in the fault tree (or event tree).

This barrier concept is incorporated into the management model described above. A barrier function is developed in a risk analysis and then specified, based on its position in the fault or event tree, i.e. in relation to the event it should prevent. The main consideration then will be if the barrier should have any behavioural involvement, and if so, what the nature of this involvement will be.

This highlights the fact that there is a need to distinguish between what is meant by a barrier and the influence management has on its effective operation. For instance, in some approaches 'training' is considered a barrier, whereas in the current conception 'training' (i.e. competence) is something that is provided by management to ensure correct functioning of some barriers. Similar reasoning applies to the other 'behavioural' delivery systems – e.g. 'procedures', 'commitment', 'availability' – these all being behavioural elements of barriers that should be provided and maintained by management. Hence, these systems do not appear as separate barriers in the bow tie but rather are defined as the means management has to influence their effectiveness. Evidently, the approach elaborated here somewhat deviates from other developments of fault and event trees where such barriers commonly are defined. Moreover, the idea of 'barriers for barriers' (see Schupp et al. [11]) also will not be applied here. Rather the aim is to link management quality to barrier effectiveness in a practical and comprehensible way.

Because several scenarios are considered in the ARAMIS audit and, therefore, many barriers are involved, a classification system has been developed to reduce the amount of barriers to a limited number of categories that supposedly have common management influences for all members of one category but different across categories. This classification system is based on three barrier characteristics: the main barrier tasks – detect, diagnose and act – the cognitive effort to carry out these tasks – skill (s), rule (r) or knowledge (k) based – and whether the barrier has a control (positioned in fault tree or left-hand side of bow tie) or safety function (positioned in both fault and event trees). This would actually result in $3 \times 3 \times 2 = 18$ types, but the distinction between some types is so small that their categories have been merged. The 11 resulting types are provided in Table 1.

Table 1 shows how different combinations (first column) result in different types of barrier, which require different types of management. For passive hardware the emphasis is on design and installation. For active hardware the involvement of workers becomes important in the functioning of barriers and aspects like inspection and maintenance, competence (at either skill, rule or knowledge based level) and commitment are highly relevant.

2.3. Recursivity

One other important aspect of the approach towards barriers and their management outlined above is the notion of recursivity. That is, some delivery systems function as Russian dolls or using a common Dutch expression, according to the 'Droste effect'.[2] For instance, the delivery of competence as an element of proper barrier functioning also implies the delivery of competence to those who deliver such competence. Similarly, inspection and maintenance, being also a delivery system, again requires competence, procedures and commitment to be of sufficient quality and so on. This essential characteristic should be kept in mind when envisioning the management model or using the ARAMIS audit. Fig. 2 provides another overview of the delivery systems to illustrate this characteristic. For the sake of clarity not all arrows have been drawn in the figure.

[2] The 'Droste effect' refers to an image which contains the same image ad infinitum. Such an image has been used on a tin of a famous Dutch chocolate brand. On it a nurse brings in the chocolate on a tray with the tin on it, which has the nurse on it bring in the chocolate on a tray, etc.

Table 1
Barrier typology

Barrier	Examples	Detect	Diagnose/activate	Act
1. Permanent–passive, MORT control	Pipe/hose wall, anti-corrosion paint, tank support, floating tank lid, viewing port in vessel	None	None	Hardware
2. Permanent–passive, MORT barrier	Bund, dyke, drainage sump, railing, fence, blast wall, lightning conductor, bursting disc	None	None	Hardware
3. Temporary–passive, put in place (and removed) by person	Barriers round repair work, blind flange over open pipe, helmet/gloves/safety shoes/goggles, inhibitor in mixture	None	None (human must put them in place)	Hardware
4. Permanent–active	Active corrosion protection, heating/cooling system, ventilation, explosion venting, inerting system	None	None (may need activation by operator for certain process phases)	Hardware
5. Activated–hardware on demand, MORT barrier or control	Pressure relief valve, interlock with "hard" logic, sprinkler installation, p/t/level control	Hardware	Hardware	Hardware
6. Activated–automated	Programmable automated device, control system or shutdown system	Hardware	Software	Hardware
7. Activated–manual, human action triggered by active hardware detection(s)	Manual shutdown or adjustment in response to instrument reading or alarm, evacuation donning breathing apparatus or calling fire brigade on alarm, action triggered by remote camera, drain valve, close/open (correct) valve	Hardware	Human (s/r/k)	Human/remote control
8. Activated–warned, human action based on passive warning	Donning personal protection equipment in danger area, refraining from smoking, keeping within white lines, opening labelled pipe, keeping out of prohibited areas	Hardware	Human (r)	Human
9. Activated–assisted, software presents diagnosis to the operator	Using an expert system	Hardware	Software–human (r/k)	Human/remote control
10. Activated–procedural, observation of local conditions not using instruments	(Correctly) follow start up/shutdown/batch process procedure, adjust setting of hardware, warn others to act or evacuate, (un)couple tanker from storage, empty & purge line before opening, drive tanker, lay down water curtain	Human	Human (s/r)	Human/remote control
11. Activated–emergency, ad hoc observation of deviation + improvisation of response	Response to unexpected emergency, improvised jury-rig during maintenance, fight fire	Human	Human (k)	Human/remote control

3. ARAMIS audit

3.1. Audit support

The ARAMIS audit support consists of the following components:

1. an audit manual;
2. audit protocols;
3. a support tool.

The audit manual explains the general reasoning behind the audit and its scope. It provides an outline of the audit procedure including an audit strategy, team composition, lists of people to interview and of documents to review. The most important element of this part of the audit though is the mapping procedure, which describes the translation that has to be made of the company's specific safety management system to the normative system of the ARAMIS audit. This is quite an important task because through this mapping process the people who will be involved in the audit are to be determined and also what will be required of them. The manual concludes with a description of the way audit findings should be scored. At the moment the audit does not have clear-cut assessment rules, only very global ones (see below). In addition, templates are provided for the primary feedback to the company on the last day of the audit.

The audit manual has separate protocols for the assessment of the nine delivery systems defined above. These protocols are accompanied by diagrams depicting the general outline of a delivery system. All delivery systems (and henceforth also all diagrams) are designed according to the well-known Plan-Do-Check-Adjust cycle (PDCA cycle) of the quality gurus (see, e.g. Ref. [12]). These cycles have been adapted to the specific needs of a particular delivery system. For instance the delivery system design/purchase/construct hardware barrier has as its steps:

1. specify barriers, equipment, tools, spares including human factor (HF) considerations;

2a. choose to *buy* barrier:
   a. make inventory and selection of suppliers;
   b. select and order equipment, materials;

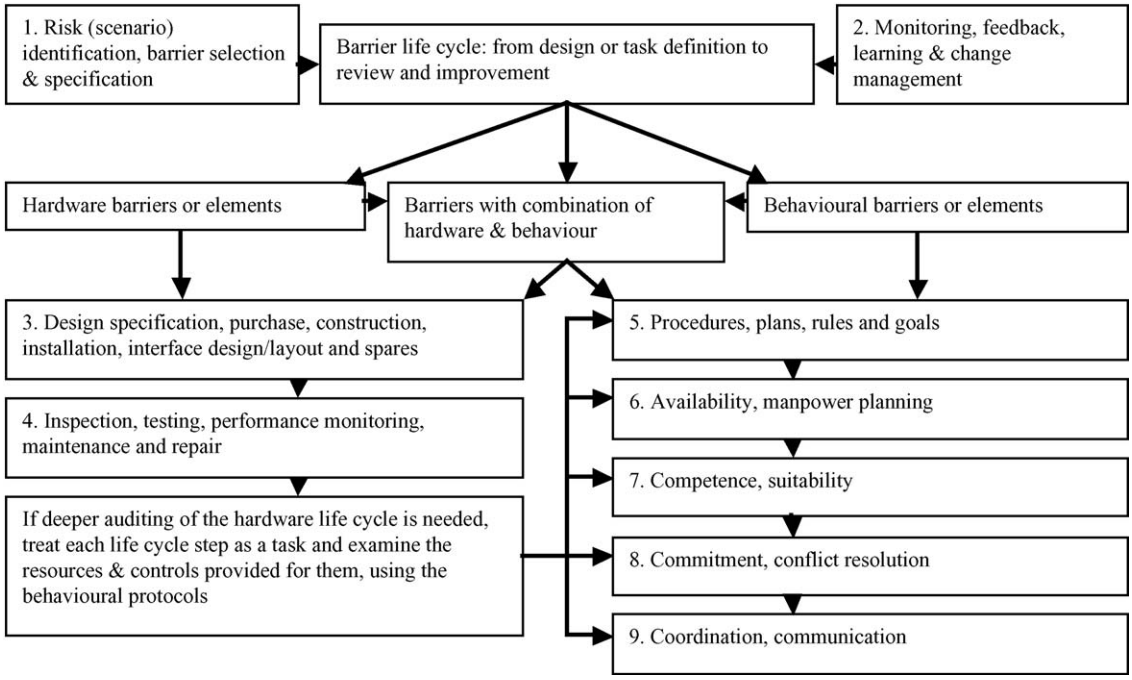

Fig. 2. The relationship between hardware barriers and their behavioural elements.

c. receive, check and store orders and purchases;
d. check requisition and issue;

2b. or *fabricate* barrier:
a. plan resources for fabrication;
b. fabricate, including HF;

3. install and adjust, including HF;
4. register performance, evaluate and learn.

Although each delivery system roughly follows the path above, they all differ in the amount of steps they need to achieve – i.e. 'deliver' – their result. The number of steps in each of the delivery systems is as follows: risk analysis and barrier selection (8), learning and change management (10), design, purchase or construct hardware (9), inspection, maintenance, etc. of hardware (7), procedures and rules (9), availability/manpower planning (9), competence and suitability (10), commitment and motivation (6) and communication and coordination (4).

Assessments are made based on the amount of deviation or compliance the company demonstrates to these normative models. That is, the audit considers whether the company takes systematic and effective actions for each step, based on well-considered plans and appropriate techniques. The assessment is based on a combination of good plans and good execution of them, as posed by descriptions and documentation. These steps are scored using a five-point rating scale, with an accompanying colouring scheme:

5- fully implemented, improvement not (really) needed (dark green);
4- largely implemented, minor improvements needed (light green);
3- some aspects present, significant improvements needed (orange);
2- under development, overall improvement needed (light red);
1- absent, development must yet be started (dark red).[3]

The colours are used in the diagrams depicting the steps within a delivery system provided for the initial feedback to the company.

In addition to this paper manual a software support tool, programmed in Microsoft® Excel, has been developed that includes all of the above, but provides search, selection and print possibilities within the audit manual. Through this tool customized interview protocols can be assembled and printed for use during the audit. In the audit tool, all steps within all delivery systems can be scored separately and these scores then are shown on a separate worksheet in an overall view using the three colours green, orange and red, described above. Also, hyperlinks are established to the diagrams of the delivery systems in their respective protocols.

3.2. Audit process

The ARAMIS audit follows the traditional steps of an audit—i.e. first contact with plant management, audit contract, site-familiarisation, audit, feedback, draft report and final report. However, because of the particular focus of the audit on scenarios and barriers an investigation aimed at defining scenarios for a particular plant or installation and identifying the barrier functions that have been installed

[3] For the quantifications fractions are used, i.e. 1 = 0.2, 2 = 0.4, 3 = 0.6, etc.

should be carried out well in advance of the on-site audit. Based on these results, the audit team agrees on a manageable number of scenarios (generally, two or more) and a representative sample of barriers (usually with a maximum of 20–30) to be used as focal points during the audit. The choice of scenarios and the sample of barriers are both determined by the purpose of the audit and through guidelines provided with the audit and described below.

The set of barriers is first classified using Table 1 above. Again, depending on both the plant or installation and the purpose of the audit, one, two or more categories can be emphasized in the audit. For the moment, a rather bold assumption is being made that final assessments of barrier *types* generalize to all barrier *tokens* classified under these, i.e. all barriers classified within each category.

For each barrier type, primary delivery systems have been defined that have a substantial bearing on the functioning of a barrier of that type. For instance, barrier type 1 – a permanent control barrier that needs no activation to be effective – is presumed to be significantly influenced only by the quality of management of the original installation, based on the specifications (delivery system for barrier hardware) and by the way it is inspected and maintained (delivery system for inspection and maintenance). This allocation of primary delivery systems is still based on hypothesis and not on process empiricism, which still needs to be carried out. In the ARAMIS project a preliminary expert judgement exercise will provide the first test of which systems affect which barriers.[4]

The audit process itself is rather straightforward. Barrier types and specific barrier tokens are used as concrete examples during the interviews. The life cycle of barriers remains the Leitmotiv but if deeper auditing of any barrier is required, its primary delivery system(s) can be involved to assess whether all life cycle steps are performed up to par. Performing this routine with multiple barrier types and various informed people the auditors gain insight into the workings of the nine delivery systems, differentiated by barrier type if necessary. It should be pointed out, however, that this is only a partial assessment of the full safety management system.

During the audit the 'risk analysis and barrier selection' and 'learning and change management' delivery systems are assessed but they are excluded from the subsequent quantification phase (see next paragraph). The technical risk analysis starts from the actually chosen barriers and so double counting of this effect is not desirable. The learning delivery system does not affect current barrier effectiveness but indicates whether it will get better or deteriorates.

3.3. Quantification

The ARAMIS audit is part of a chain of methods that together arrive at an estimation of the possible impact a particular installation, plant or site will have on its surroundings if one of the major hazard scenarios were to transpire, given its current barrier solutions, its current safety management and various other local conditions.

Although the quantification of the audit results has not been a main concern in the development of the audit, it is an objective of the ARAMIS project to have a numerical indication of the quality of management of barriers, the so called *M*-index. For rather pragmatic reasons, it had been decided that this should be only one number, with which any given barrier would be judged.

Within the chemical industry it has become common practice to assign a so-called SIL-value, which stands for safety integrity level and which is part of the international IEC 61508 standard. It is an expression of a barrier's assumed reliability on a three-point scale. The number actually reflects the exponent x in the formula 10^{-x} rounded-off to the lowest integer. So a SIL-value of 3 corresponds to a probability of failure on demand between 10^{-4} and 10^{-3}. The *M*-index resulting from the ARAMIS audit can be used to modify the SIL-values of any barrier in any scenario under investigation.

The procedure for calculating the *M*-index is still rather experimental, in that it is not based on empirical evidence on management influences or experience. First of all, a decision has been made that the delivery systems 'risk analysis and barrier selection' and 'learning and change management' should be excluded from the quantification phase (see above). The remaining seven delivery systems however do contribute to current barrier effectiveness.

These delivery systems first had to be brought back to one single number, instead of a separate rating per step. Therefore, several persons with a certain degree of expertise (some members from the ARAMIS consortium and 13 delegates from a master's course in safety) judged all steps within these delivery systems for their influence on barrier effectiveness. This resulted in a split between delivery systems having equally weighted steps and systems having unequally weighted steps. For the equally weighted delivery systems, a geometrical mean is calculated to arrive at their overall numerical rating (please note that all steps have been rated on a five-point scale). For the unequally weighted ones, however, a different reasoning applies. An average is first taken, but when steps within a particular delivery system are judged more important than others, the final mean rating of such a system cannot be higher than the lowest scoring important step. Or put in other words, the quality of less important steps cannot compensate for the lesser quality of important steps.

Hence, for one group of delivery systems all steps are assumed to contribute equally to the quality of the delivery system:

a. manpower planning;
b. communication;
c. purchase/install hardware.

[4] The participants in the research acted as 'experts' for this trial. Later research will need to use genuine experts to arrive at better judgments.

Whereas for another group of delivery systems a few steps are assumed to contribute more dominantly to the quality of the delivery system:

a. procedures (step 5: communicate, train, execute rules and step 8: evaluate rule effectiveness);
b. competence (step 2: define suitability and competence needed for behaviour);
c. commitment (step 3: assess and modify behavioural antecedents and consequences);
d. inspection and maintenance (step 1: define maintenance concepts and plans and step 6: execute maintenance and repair).

The 11 barrier types then are weighted by and summed over the seven delivery systems according to the following formula:

$$M = 1 - \sum_{i=1}^{7}(1 - D_i)B_{i,k}$$

where D_i corresponds to the seven delivery systems and $B_{i,k}$ is a matrix consisting of barrier types ($k = 1, 2, \ldots, 11$) distinguished by delivery system influence ($i = 1, 2, \ldots, 7$). The final outcome of this formula lies somewhere between 1 and 0. When this outcome is multiplied then with any barrier's SIL-value the result is rounded-off to the nearest integer in the triplet $\langle 1, 2, 3 \rangle$.

4. Case studies

The full ARAMIS method has been applied at test sites in several European countries (Denmark, France, Netherlands, Slovenia and Slovakia). With regard to the audit a 1-day training session was arranged to familiarise the auditors with the approach and audit protocols for the nine delivery systems. Audit experience within the ARAMIS group ranged from none to some. The protocols were too abstract for the inexperienced auditors, and therefore, sample questions were added to the protocols that covered the most salient issues. After the training session the audit tool was also developed, to support the auditors and to provide them with a means to print out customized questionnaires.

Being primarily a research project, it was recommended to execute the ARAMIS audit with at least two auditors *and* an observer, to monitor the audit process and to make notes of things that worked well or went wrong. It is not clear whether all audit teams were composed as such but the feedback to the developers of the audit was limited.

As the final results of all audits are not available at the writing of this paper, no detailed overview can be given. The feedback that has been provided has been incorporated in the discussion below.

5. Discussion

Considering the growing interest in what is called nowadays scenario based auditing the development of an audit technique that supports this approach is necessary. The audit technique described in this paper takes (major hazard) scenarios and barriers solutions as its starting point and works its way through the management systems supporting these. The audit assessments result in a final number called the *M*-index, which can be used to adjust SIL-values of barriers in scenarios under scrutiny.

First of all, research such as this would benefit significantly from a multitrait–multimethod approach [13,14], in which the relationships between convergent and divergent measurements are compared. Such an approach would indicate how the audit would relate to other measurements and performance indicators. However, because of the non-experimental design of this study no strict rules can be followed. Companies often have to be seduced into the research setting and expect something – sometimes even more than *something* – in return. Researchers are often eager to satisfy just this demand and do not allow themselves the liberty of scientific discovery.

From a scientific point of view, the issues of validity and reliability of the audit assessments are most important. With regard to the face validity of the audit the following can be put forward. No serious gaps between the nine delivery systems of the ARAMIS audit and company specific safety management systems (SMSs) were found. Some companies did have sub-systems that concerned themselves with, for instance, safety at home or traffic safety, which is not covered in the ARAMIS audit. What seems to be lacking though, is an indication of relative importance of the delivery systems. At the moment all systems are equally important.

How a particular SMS is broken down into meaningful parts and how many of these are truly needed, remains a difficult issue to tackle (content validity). For instance, most large companies have a sub-system called auditing, which is covered in the 'learning and change management' of the ARAMIS audit. Nevertheless, the model put forward in this paper remains open for scrutiny and falsification.

The question whether the audit protocols and diagrams sufficiently cover the actual management processes and therefore provide a 'true' assessment of the delivery systems (construct and criterion validity) cannot be answered. Often, auditors talked about the delivery systems as a whole, using the (graphic) diagrams rather than exploring them step-by-step. This is yet another difficult issue of how to arrive at valid and reliable auditing results. Obviously, when adhering to strict protocols the reliability will be heightened (i.e. random error will be less). However, the measurements might still be systematically wrong, diminishing their validity. At the moment, inexperienced auditors do need more support to find their way through the delivery systems and associated protocols whereas more experienced auditors will probably default to their familiar systems in case of confusion. Both

situations do threaten the validity and reliability of the assessment.

The quantification part of the audit is still very experimental. Nevertheless, this step forces the auditors to make detailed assessments first and then aggregate these to the level of delivery systems. These global assessments are initially fed back to the company for response, which often results in useful comments. This whole chain of steps assures that the audit team does not jump to premature conclusions having no validity whatsoever.

During the development of the audit some pragmatic decisions had to be made that still need some verification. The issue of whether to use protocols versus diagrams during the interviews is one. However, an auditor should be quite aware of what any step within any delivery system entails before (s)he can make do without the protocols. Obviously, an audit such as the current one is quite demanding and would require auditors that are well trained in its philosophy. Both the standardisation of the approach and the training of auditors in it will heighten the reliability of the audit results.

In addition to the important issues of validity and reliability, there are still other matters open for questioning. For instance, the weighting of the steps within the delivery systems remains to be explored more extensively. Although the reasoning of equally and unequally weighted systems appears to be sound, there is now no empirical evidence for its support. Probably, both an extensive literature survey and expert judgement are needed to supply more answers.

Lastly, the relationship between barrier types and delivery systems is still open for research. What (type of) barrier does benefit from what (type of) management influence? In an attempt to fill in these gaps a new project has been formulated called D-SMART [15] that should provide some answers to these questions. In the mean time, the audit and the accompanying tool will be available upon request for anybody's use and useful comments.

References

[1] O. Salvi, C. Kirchsteiger, C. Delvosalle, N.J. Duijm, J. Casal, L.H.J. Goossens, B. Mazzarotta, K. Lebecki, J.-L. Wybo, G. Duserre, H. Londiche, J. Calzia, ARAMIS. Accidental risk assessment methodology for industries in the framework of Seveso II directive, in: Paper Presented at the Seminar on Progress in European Research on Major Hazards, Chemical Risks Directorate, Belgian Ministry of Labour, Brussels, October 10, 2001.

[2] A.R. Hale, F.W. Guldenmund, L.J. Bellamy, C. Wilson, IRMA: integrated risk management audit for major hazard sites, in: G.I. Schueller, P. Kafka (Eds.), Safety & Reliability, Balkema, Rotterdam, 1999, pp. 1315–1320.

[3] F.W. Guldenmund, A.R. Hale, L.J. Bellamy, The development and application of a tailored audit approach to major chemical hazard sites, Paper Presented at The SEVESO 2000. Risk Management in the European Union of 2000: The Challenge of Implementing Council Directive 96/82/EC "SEVESO II", Athens, November 10–12, 1999, Office for Official Publications of the European Communities, Luxembourg, 2000.

[4] J.I.H. Oh, W.G.J. Brouwer, L.J. 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.

[5] R.J. Nertney, Process operational readiness and operational readiness follow-on, EG&G, Idaho Falls, Idaho, February 1987.

[6] W. Haddon, Energy damage and the ten countermeasure strategies, Hum. Factors 15 (4) (1973) 355–366.

[7] W. Haddon, The basic strategies for reducing damage for hazards of all kinds, Hazard Prev. 16 (11) (1980) 8–12.

[8] W.G. Johnson, MORT—The Management Oversight and Risk Tree, US atomic Energy Commission, Washington, 1973.

[9] E. Hollnagel, Accidents and barriers, Graduate School of Human-Machine Interaction, University of Linköping, Linköping, undated.

[10] E. Hollnagel, Accident Analysis and Barrier Functions, Institute for Energy Technology, Halden, Norway, 1999.

[11] B.A. Schupp, S. Smith, P. Wright, L.H.J. Goossens, Integrating human factors in the design of safety critical systems—a barrier based approach, in: W. Johnson, P. Palanque (Eds.), Human Error, Safety and Systems Development (HESSD 2004), Springer, 2004, pp. 285–300.

[12] R. Deming, Characteristics of an effective management control system in an organisation, Boston, 1968.

[13] D.T. Campbell, D. Fiske, Convergent and discriminant validation by the multitrait-multimethod matrix, Psychol. Bull. 56 (1959) 81–105.

[14] R.P. Bagozzi, Y. Yi, Assessing method variance in multitrait-multimethod matrices: the case of self-reported affect and perceptions at work, J. Appl. Psychol. 75 (1990) 547–560.

[15] J.M. Betten, D-SMART: The Delft Safety Management Auditor Tool, M.Sc. Thesis, Safety Science Group, Delft University of Technology, Delft, 2004.