Journal of Hazardous Materials, 21 (1989) 105-124
Elsevier Science Publishers B.V., Amsterdam — Printed in The Netherlands

Review

ON THE PROBLEMS AND FUTURE OF SAFETY AND RISK ANALYSIS

J. SUOKAS and R. KAKKO

Technical Research Center of Finland, Occupational Safety Engineering Laboratory, BOX 656, SF-33101 Tampere (Finland)

(Received February 1, 1988; accepted in revised form November 7, 1988)

Summary

A review on the problems with the identification of hazards and assessing the risks is first presented. Special emphasis is given to the critical evaluation of the problems with the gas dispersion modelling. Ideas and attempts for avoiding the existing problems and for improving the cost/benefit relation of safety analysis are then discussed. These include the use of computer support and knowledge engineering, validation of methods and models, analysis of human and organizational factors, and evaluation of the quality of safety analysis. Finally, the European legislation concerning safety analysis is shortly discussed.

1. Introduction

Safety and risk analyses are increasingly employed in the process industry to assure the safety of new installations. This use has mainly been voluntarily, but since the EC-directive 82/501 legislation in several countries has given the authorities the opportunity to require a safety or risk analysis on hazardous installations.

This paper begins with a short overview of the common limitations of safety and risk analysis. Some problems and limitations concerning the identification of accident contributors and the assessment of accident consequences are then discussed in greater detail. Finally, some trends to avoid the problems and deficiencies, and to improve the cost-effectiveness of safety and risk analyses are presented.

2. Common problems of safety and risk analysis

Safety and risk analyses begin with a qualitative phase including the identification of accident contributors and the modelling of accidents. The modelling phase is then continued with the quantification of accident frequencies

0304-3894/89/$03.50

by using component failure and human error data. The investigation may then be carried on with the assessment of consequences and the calculation of risks. In the case of the process industries this means the use of gas release and dispersion models, fire and explosion models, meteorological data, and toxicity data. The risks are then expressed in the form of risk contours or F/N-curves. The investigation resulting in quantitative estimate on the size of risk is called risk analysis. The term safety analysis is sometimes used for the qualitative phase, or for the general concept of the approach. In the following, safety analysis is used as a general term and risk analysis for reasons of clarity only when the quantitative assessment of risks is discussed.

Safety analyses have certain common problems and deficiencies. The main deficiencies mainly concern two things: *1* incompleteness in the identification of accident contributors and the modelling of accidents, and *2* inaccuracy of the quantification of risk in terms of frequency and consequences.

Table 1 shows a summary of the criticism often presented on safety analysis.

The most common criticism has been focused on the uncertainties in component failure rate and human error data employed in the quantification of risks. In the following, a review has been made of the problems and uncertainties of the different steps of safety analysis giving special emphasis to the problems of the consequence assessment.

TABLE 1

Topics of the criticism of safety analysis [1]

Phase of analysis	Deficiencies presented
1 Definition and description of system	Relevant subsystems or activities are excluded The description of the system does not correspond to the real world
2 Hazard identification	Important accident contributors or families of them are excluded or omitted
3 Accident modelling	Important accident type(s) or accident contributors are excluded or omitted
4 Quantification of risks	Uncertainties of component failure rate or human error data Inaccuracies in consequence modelling
5 Documentation of results	Boundaries of and assumptions in analysis are not described Sources of quantitative data are not presented

3. Problems with hazard identification and accident modelling

The identification of hazards and their contributors followed by the modelling of major accident possibilities form the basis for quantitative assessments. Hence, the errors and omissions made at these phases affect the results employed in the risk assessment and decision making.

In the identification of accident contributors, the criticism has mainly been directed towards human factors and the simplifications made in the plant description and modelling. Human activities are seen as difficult to include in the existing methods and practices of carrying out the analyses [2–6]. The references also give some examples on human errors which are difficult to include in hazard identification. A few references also point out the importance and, on the other hand, the difficulty in dealing with organizational and training factors in safety analyses [2,5]. Further common topics for criticism have been deficiencies and simplifications in the modelling of accidents [7,8].

Only a few critical evaluations of individual methods are available. Clemens [9] and Daniels and Holden [10] are examples of mainly heuristic evaluations based on the structure of the methods. Taylor [11,12] and Suokas [1] have also performed empirical evaluations on a few identification methods.

Taylor applied hazard and operability studies (HAZOP) and action error analyses (AEA) to two plants and augmented the results by an analysis of commissioning-checks and problems found during a short operating period. The percentage of hazards identified by HAZOP was found to vary between 22 and 80. The corresponding percentage of AEA varied between 60 and 20 in the two analyses evaluated. For fault tree analyses (FTA) a share of 80% is presented [11,12].

Recently, Suokas [1] evaluated HAZOP by employing three methods; action error analyses (AEA), work safety analyses and accident investigations as references. He found HAZOP to cover 77% of the contributors to a gas release in the two storage systems analyzed. The effect of the factors remaining outside HAZOP increased the assessed frequency of the gas release by 28% in the first case and by 38% in the second case.

An evaluation on four methods, HAZOP, FMEA, AEA and MORT (Management Oversight and Risk Tree) was made by Suokas and Pyy [13]. They defined the search patterns and types of factors to be covered by the methods, and collected incident and accident information in seven process plants and one accident data bank. Next, three groups were formed to evaluate which of the contributors to the incidents and accidents would have been identified if one of the methods had been used in the corresponding process system. HAZOP was found to be the best method identifying 36% of the contributors. However, only 55% of the contributors were expected to be covered by the four methods [13].

4. Problems with the accident frequency assessment

There are three types of evaluations concerning the accuracy of accident frequencies:

1 investigations into the accuracy of the source data, component failures and human errors

2 critical evaluations — analyses of the uncertainties and sensitivities — of a specific investigation

3 benchmark exercises, where several independent analyses have been carried out in the same system.

Snaith [14] has compared the predicted and actual reliability of components and equipment at the National Center of Systems Reliability. He concluded that in more than 60% of the cases, the predicted and observed values are within a factor 2 and in more than 80% they are within a factor 4. In some instances, particularly when the quality of the field data was unknown and the analysis was coarse, he observed greater disagreement with factors of over 10.

In another investigation [15] even greater differences between the actual and predicted failure frequencies were found. These comparisons showed a variation from 0.4 to 1680 in the ratio between the actual and predicted occurrences of fault conditions in a process system (i.e. events demanding the operation of a safety system). During nine years, the ratio between the actual and predicted failure rate of some instruments in the safety system varied respectively between 0.04 and 2.23. The main reason for the largest discrepancies was found to be a design error [15].

A few evaluations have been made in the nuclear industry to determine the uncertainty of the source data. In a recent publication Vesely and Rasmuson [16] presented an evaluation of the accuracy of four public risk analyses carried out in the U.S.A. in the nuclear industry. They give a range of 1.3–30 for the error factor (the error factor is the ratio of the upper 95th percentile, or confidence value to the median, or 50th percentile confidence value). The smallest values belong to higher event frequencies (1 or more per reactor year) for which a larger amount of recorded data generally exists. Rarer accident frequencies with mean values in the vicinity of 10^{-7} per reactor per year are presented to yield an error factor within the range of 20–30.

Some results were recently published on a reliability benchmark exercise in the nuclear industry in which ten different teams involving seventeen organizations from nine European countries executed parallel reliability analyses on the same system. In that project, differences in modelling and data were investigated. According to the results, the modelling was a more sensitive phase, representing a ratio of 36 between the highest and lowest probabilities of the TOP event of the different fault trees (the probabilities were calculated afterwards by using joint failure data). When the fault trees were modified and a joint tree was quantified by different teams with the data they considered the

TABLE 2

Evaluation of the accuray of accident frequencies in a few safety analyses [20]

Reference	Accuracy of accident frequency	Type of reference
Amendola [17,18]	Range of mean failure probability as evaluated on the basis of common fault tree and data $8.3 \cdot 10^{-4}$-$3 \cdot 10^{-2}$	Benchmark exercise in several European countries
[21]	Inaccuracy estimated to be from one to two orders of magnitude for accident probabilities and about one order of magnitude for consequence estimates	Rijnmond study
[22]	Probability assessment estimated to be inaccurate by a factor of two or three	Canvey Island study
[23]	Estimate for the inaccuray factor of reference [22] ten or more	Critical analysis of the Canvey Island study
Jäger et al. [24,25]	Range of lower and upper 95% confidence level estimated to be seven orders of magnitude	Pilot study
Vessely and Rasmuson [16]	The error factors of initiating event data range from a factor of 1.3 to a factor of 30	Assessed on the basis of PRAs of nuclear power plants
Daniels and Holden [10]	Reliability assessments of some subsystems often have uncertainty of much less than half an order of magnitude	Assessment presented on the basis of several analyses

best, the corresponding ratio was reduced to 9 [17,18]. Similar results were observed in the reliability benchmark exercise performed by the Nordic countries [19].

Table 2 presents a short summary on some evaluations of the accuracy of the assessed accident frequencies.

5. Problems with the consequence assessment

The models for consequence analyses must be appropriate and consistent both in terms of their accuracy and in their economy of effort. It is particularly important to avoid unnecessary use of very complicated and time-consuming methods when the basic data to be used are of low accuracy. Therefore, in constructing the models, the aim has been to achieve an appropriate practical compromise between the conflicting requirements of accuracy and economy.

TABLE 3

A summary on the main results and problems of the models in consequence assessment [20]

Model type	Results	Deficiencies and restrictions
Outflow models	Estimates discharged amount or rate of the release Basis for - evaporation and gas dispersion analysis - pressure impact of vapour cloud explosion analysis	Models are usually not applicable, if the storage pressure is lower than air pressure
Evaporation models	Estimates amount or rate of evaporated material Basis for - vapour cloud dispersion analysis - pressure impact and vulnerability analysis of vapour cloud explosions	Models are usually not tested in practice Estimation of evaporation of substance mixed with water inaccurate Stability class of weather condition is usually supposed to be neutral
Vapor cloud dispersion models	Estimation concentration as a function of distance and/ or time Basis for - vulnerability analysis	Generally it's supposed that the dispersing gas cloud does not react or absorb during dispersion The topography of complex terrain is difficult to take into account Great variation in the results of heavy gas dispersion models
Pressure impact models of vapour cloud explosions	Estimates maximum pressure, impacts as a function of distance and duration Basis for - vulnerability analysis	Generally it's supposed that the mixture of gas and air is homogeneous The mechanism of explosion is not exactly known Estimation of consequences of explosion is difficult in closely built areas; it's difficult to estimate impact of surrounding building to the dispersion of pressure waves
Heat radiation models	Estimates thermal load as a function of distance and gives information about possible influence on people and environment. Basis for - vulnerability analysis	Generally it is supposed that the pool is circular or rectangular Estimation of the amount of heat radiation in deflagration or BLEVE is difficult The influence of obstacles is not exactly estimated
Vulnerbility models of people and environment	Estimates impacts of toxic/ flammable materials and/or pressure waves on people (or vegetation and animals)	Great variation in existing toxicity data Escape of people difficult to include Variations in the water and soil models

The models of hazardous incidents include:

- discharge rates
- evaporation of liquids
- dispersion
- combustion of vapour clouds, liquids and jets
- toxic gas effects, etc.

Table 3 presents a summary on the main results and problems of the models employed in the different phases of consequence assessment.

An important feature of any of the physical models should be their ability to extrapolate from the results of relatively small-scale experiments to large-scale ones by employing hypothetical accidental releases. All models, to some degree, suffer from errors arising from extrapolation, but those that are the best from this point of view are the ones which have a sound fundamental basis and the minimum of empirical constants [21].

In carrying out a risk assessment for a chemical process plant containing toxic or flammable gases it is necessary not only to calculate the dispersion behavior following a release but also to take into account the several other external factors which may affect the final number of casualties.

In the following, one specific topic — the dispersion of heavy gases — is discussed in more detail. Heavy gas means that a gas cloud may be denser than air intrinsically or because of its coldness [26].

5.1 Heavy gas models

Mathematical models in concentration calculus can be classified as box, 3-D, and intermediate type models.

5.1.1 Box models

Principal contributors to the development of box models include Van Ulden [27], Germeles and Drake [28], Fay [29], Fay and Ranck [30], Pickness [31], Fryer and Kaiser [32], Cox and Carpenter [33], Eidsvik [34] and Webber [26]. All the models are essentially similar in their account of gravity spreading, but differ to a large extent in accounting for air entrainment [35].

Box models are cheap to run and fairly ready to be used as an everyday's tool. They are rather difficult to be applied to problems involving complex terrain, calm wind conditions and time varying releases [36]. A number of box-models take into account humidity and latent heat of condensation, heat transfer at the ground, difference of speeds between the cloud and the wind (DENZ and EIDSVIK). Some of the models have been written for continuous releases (EIDSVIK, Ooms, CRUNCH [37]). Box models are the most commonly used numerical models for evaluating the consequences of dispersion of denser-than-air gases in safety studies. According to them the cloud remains a cylinder for instantaneous releases and has a rectangular profile in each direction. The computational time used by box models is very short due to the parameterization of the behavior of the cloud with simple functions. The determination of the coefficients of these parameterizations is an important issue. Difficulties arise when the validity of models considering the low number of field experiments is to be determined.

5.1.2 3-D models

These models use basic equations which are fair approximations and are in principle capable of accommodating non-uniform terrain and time varying releases. All existing models rely on a turbulence closure hypothesis whose validity is highly questionable. The solutions are obtained by numerical integration schemes which have not been separately evaluated. It is therefore difficult to make judgments on the validity of the models based on such comparisons with data as have been published. The present limitations on the use of such models are both practical and fundamental. Computer hardware and time requirement for 3-D model simulation of practical dispersion problems are substantial, and the solution of such large systems of partial differential equations is complex and difficult [38].

5.1.3 Intermediate type models

Intermediate type models retain most of the advantages of 3-D codes but largely evade the possible numerical solution problems. It is possible to solve some cases analytically. Their development and running costs fall between the other two types. Because of the comparative neglect of them relative to box and 3-D models, they cannot be said to be familiar working tools at the present. This is likely to change as demands for modelling complex terrain and time varying releases arise, although their application may be restricted to some standard cases. Trends of development in this area, associated with the trials with obstructions performed at Thorney Island, are reported by Rottman et al. [39].

5.2 Model comparison

Figures 1, 2 and 3 represent some results concerning experimental versus typical concentration calculation models. In Fig. 1, the box model DENZ is overpredicting the distance from the release point as a function of time from release. In Fig. 2, the 3-D model MERCURE-GL seems to be dependent on isoconcentrations. DENZ box model gives rather a good approximation for the height of the cloud as a function of time. In Fig. 3, the cloud area is overpredicted by DENZ, while the 3-D model MERCURE-GL gives a good approximation. It should be noted that there always are problems when comparing different models. The models have different hypotheses and limitations which also should be considered in the comparisons.

When the environmental risks are not significant, box model simulations seem to be a well-suited approach. The quality of their results is rather high

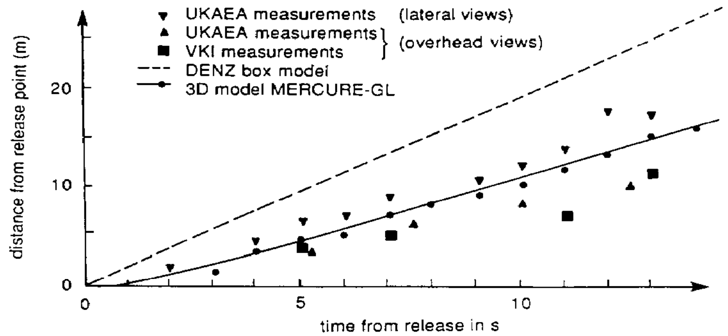

Fig. 1. Cloud centroid position [40].

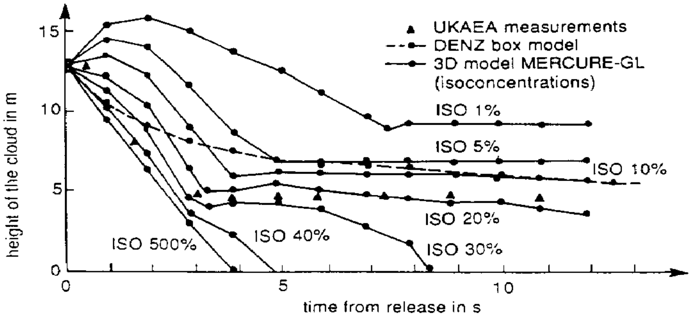

Fig. 2. Cloud height [40].

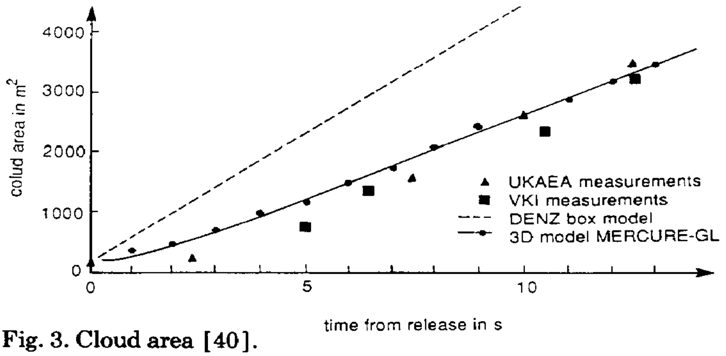

Fig. 3. Cloud area [40].

and their cost is low. However, it must not be ignored that they are more of an approximation than anything else since they possess limitations such as: flat terrain, no obstacles, no buildings, no trees, no low wind speed, and no strong atmospheric stability.

6. Future of safety analyses

6.1 Common trends

Common subjects to be developed in safety analyses at the present are

- computer programs supporting the analyses

- validation of the identification and modelling methods and modelling of gas release and dispersion
- modelling of the effects of fires and explosions
- analysis of human and organizational factors
- evaluation and management of the quality of safety analyses
- effective use of the results.

Legislation concerning safety analyses is being developed in several countries at the same time.

6.2 Computer support

Computer support has been developed to speed up analyses and to reduce the resources needed. The first applications have concerned the calculation of accident frequencies (e.g. RELVEC [41,42]) and gas dispersion. Generally the

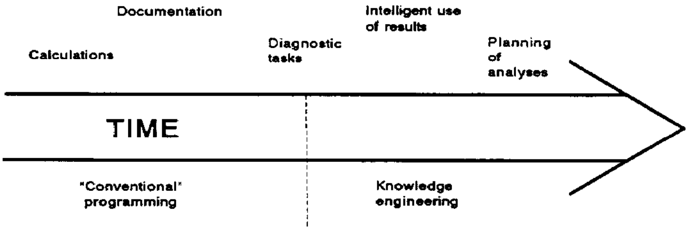

Fig. 4. The development of computer aid to safety and risk analyses. The earlier computer programs were based on "conventional" programming. The new challenges can be met with knowledge engineering [50].

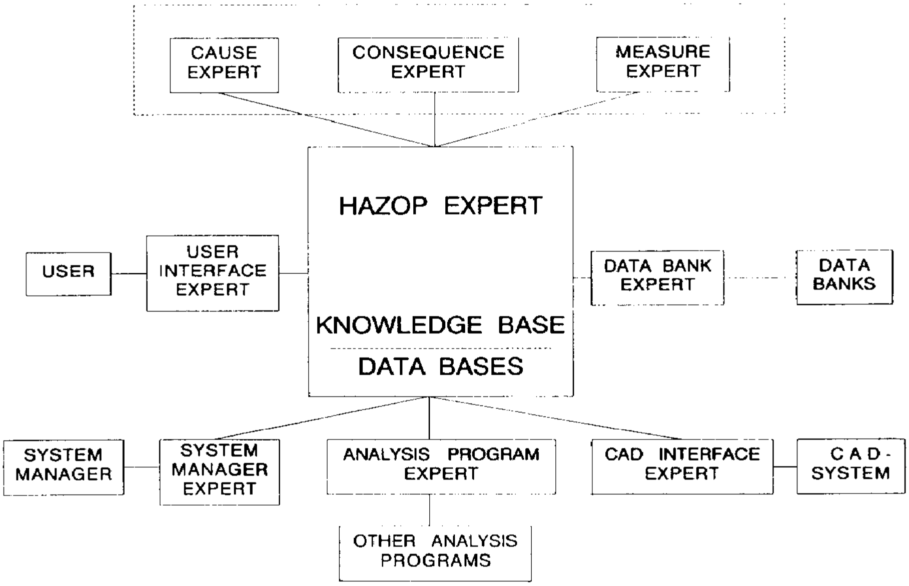

Fig. 5. The structure of HAZOPEX [48].

programs have been developed for supporting the documentation of analyses. For example, CAFOS [43] has been developed for this purpose. Risk Assessment Tool developed by Health and Safety Executive [44] and the SAFETI-package [45] are examples of quite extensive software packages developed for risk assessment.

Some new computer programs, such as RIKKE [46] and CAFTS [47], also support the reasoning and diagnosis needed in an analyses. This task, however, is difficult to perform with "conventional" programming. The most promising approach for modelling human reasoning seems to be the knowledge engineering which has rapidly advanced in recent years.

Figure 4 shows the development of computer support and future trends. The latest approach is to use knowledge engineering in order to model the human reasoning used in hazard identification and accident modelling. The HAZOPEX expert system supporting hazard and operability studies of process systems is an example of this development. The HAZOPEX expert system gets pipe and instrumentation diagram as the input, and includes a knowledge base to be used in the search for causes and consequencess of deviations [48–50]. Figure 5 shows the structure of HAZOPEX. Similar development for expert systems supporting the construction of fault trees has recently been presented by Poucet et al. [51] and Barbet [52].

6.3 Validation of methods and models

The results obtained by a safety analysis depend on the analysis team and on the methods and models employed. Comparisons where analysis teams have carried out parallel analyses on the same plant – often called benchmark exercises – have mainly been done in the field of nuclear industry. These have concerned the primary cooling system and common mode failures [18,19,53].

A similar investigation was planned for chemical industry by the Joint Research Center a short time ago. Some smaller comparisons in process industry had earlier been made in Italy [54] and in Finland [1].

Controlled comparisons between experienced research teams are an important approach when common guidelines for safety analyses are searched and higher reliability in the results of an analysis is sought. Complementary comparisons are also needed in case accident information is used as reference. This twofold approach shows which of the real accident contributors can be covered by safety analyses.

6.4 Source term and dispersion modelling

6.4.1 Source term

In the near future, experiments will probably be concentrated on particular aspects of real releases, such as the nature of the source term. The nature of a loss-of-containment accident can influence the results of the subsequent dispersion calculation. Moreover, the releases of superheated liquefied gas can lead to considerable aerosol generation which may subsequently affect the concentration field of a dispersing cloud.

Now that well validated codes for predicting the spreading and time dependency of the vaporization of liquid spills [55] are available, the problems in this area concern: *1* validation and improvement of techniques for predicting two-phase discharges from pipe networks, and *2* development and validation of techniques in view of the possible significance of aerosol in dispersing clouds for predicting the source term dispersion calculation and the quantity of material that may be present as aerosol [56].

6.4.2 Dispersion modelling

Although current box models are adequate for assisting decision making on problems that can be framed in a deterministic way, and useful for probabilistic assessments, there is, in the latter case some scope for worthwhile reduction in uncertainty due to the development of more sophisticated models with the following technical capabilities: *1* improved top entrainment and advection prescriptions that are also valid at low wind speeds, *2* improved treatment of passive dispersion and transition to passivity and definition of meteorological conditions, *3* heat and mass transfer at the advection surface, *4* time-varying sources and transient releases, *5* aerosol effects, *6* obstacle effects, *7* spatial and temporal variation of mean concentrations and estimates of statistical variability and peak concentration, and *8* chemical reactions [56].

6.5 Fire and explosion effect modelling

During the last few years vapour cloud fires and explosions have become a subject of major concern. The effects, loss of life and damage to property, have proved to be very severe. The authorities responsible for safety have an urgent need for methods and models to assess the possible damage from accidental fires and explosions so as to be able to estimate the risk of certain installations or activities such as handling, storing and transporting combustible gases and liquids.

Further experiments are needed to investigate the influence of various parameters, such as: obstacles, degree of confinement, mixture reactivity and ignition location [57]. The extension of heavy gas dispersion into risk assessment for flammable gases is more complex than is generally realized, and requires greater emphasis on a more thoroughly reasoned model to interpret the effects in a more realistic manner.

6.6 Human factors and management

A few methods have been developed for the analyses of human activities. Well-known methods are THERP [58] and action error analyses [59,60].

These methods are, however, unsuitable for the analyses of human diagnosis and decision making.

The diagnosing of a production disturbance includes several factors which require new methods in order to be properly included in an analysis. It is obvious that the assessment of a successful operation is not enough. Moreover, potential hazardous human contributions and the circumstances of their occurrence should be predicted. This implies wider concepts for describing types and contributors of human errors. Interesting proposals have been presented, for example, by Rasmussen et al. [61], Norman [62] and Reason [63,64].

Decision making is closely related to the diagnosis of a production disturbance and it is based on the information retained from the production system, and the policy and principles of the management. These factors are often left outside the hazard identification and accident modelling. MORT-method has been developed for the analysis of information and management factors, but, perhaps because of the complexity of the method, is not so often used [1,65].

Nevertheless, the research done in human and management factors has been rather small-scale when compared with the large effort put into the reliability analysis of technical systems. In order to improve the quality of safety analyses more comprehensive research work is needed as for human factors and management.

6.7 Evaluation and management of quality

There are different approaches for the evaluation of the quality of safety analyses. Parallel analyses and comparisons with test and incident information were described above. The major problem with a parallel safety analysis is the large effort needed to perform it.

One way to reduce the resources needed in safety analyses and to maintain a standard quality is to develop computer aids as described earlier in 6.2.

Incident information would be a useful reference in the quality evaluation if good incident descriptions were available. The development of the accident data banks, such as FACTS [66] and MHIDAS [67], improve the access of accident information. And yet, the problem with the quality of the data [1] remains. An attempt to improve the quality of accident reports falling into the Seveso-directive has recently been made [68]. However, further attempts should be made to develop a systematic analysis and collection of accident information and critical production disturbances in order to achieve better incident data and data banks. Production disturbances often include some contributors to accidents giving an opportunity to expand the amount of valuable information.

The quality of safety analyses can also be evaluated indirectly by inspecting the process behind the analyses. That resembles similar approaches used in quality control for evaluating the quality management of a potential vendor. The Technical Research Center and SINTEF are developing criteria to be set and questions to be asked in the indirect evaluation of quality [20]. The results of this Nordic project can also be relied on in discussions between the authorities and industry to define more precisely the content of a safety analysis of a specific activity. This is also one way to integrate the quality management as a part of the planning and execution of safety analyses.

6.8 Legislation

Major accidents, such as Flixborough (1974), Seveso (1976), Bhopal (1984), Mexico (1984) and Sandoz (1986), have raised the interest among the authorities and the public to make use of safety analysis mandatory in certain potentially hazardous installations. Norway was one of the first countries to require probabilistic safety analysis on off-shore installations [69]. The frequency of 10^{-4}/year for certain catastrophic events was made the acceptability limit. The same requirement has also been applied in Denmark.

In 1982, the joint EC-recommendation Seveso-directive was accepted which recommended for example the use of safety analysis in the context of potentially hazardous process/storage installations. The national legislation enables the authorities at least in six EC-countries today to require safety analysis [70]. Most of the requirements concern qualitative analyses of the system. Such is the case for example in West Germany [71–73] and in Denmark [74,75]. A lately proposed environmental program in the Netherlands is the first attempt to require a quantitative risk analysis and to present quantitative acceptability limits for individual and group risks (Fig. 6).

In the United Kingdom, the NIHSS Regulations [77] concern the identification of hazardous sites, and CIMAH [78] and Health and Safety at Work Act concern the assessment and control of the risks. The CIMAH regulations require the preparation of the safety case. A safety case includes, among other

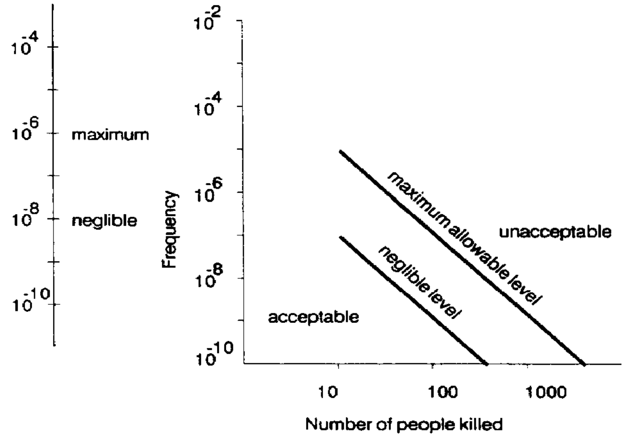

Fig. 6. The limits for risk acceptance in the Netherlands [76]. The left axis relates to individual risk per year.

things, the identification of the type of consequences and relative likelihood of potential major accidents [79}. HSE has a statutory role to judge the adequacy of the investigation of hazards and risks, and can in the case of significant consequences or risks require systematic quantitative risk analysis.

The regulations above have mainly been developed to protect people who live in the neighborhood of a process plant or a large storage system. In the Netherlands, the occupational safety authorities have also required a qualitative safety analysis on certain potentially hazardous process installations [80].

In Finland, the occupational safety legislation was recently renewed. According to the new law, it is the employer and the designer that are responsible for the investigation of the safety of a new production system or machine [81]. The explanatory memorandum states that in the case of a complex and particularly hazardous system the investigation can require the use of systematic safety analysis. Corresponding ideas on safety analysis and consequence assessment are also presented by the committee preparing new laws for chemical industry [82].

7. Conclusions

Safety analysis has spread from its original fields of military technology, aviation, space technology, and nuclear industry rapidly into the field of traditional industry. Its pioneers in the Nordic countries have been chemical industry, pulp and paper industry, energy production, off-shore technology and the transportation of hazardous materials [83].

Some important problems still remain unsolved in safety analyses. They lie in the quality of an analysis and the resources and time needed for the analysis. The quality problems mainly concern the level of the identification and modelling of hazards and their contributors, the accuracy of accident frequency assessment, the accuracy of gas release and dispersion modelling, and the assessment of the effects.

Computer support and the use of knowledge engineering are areas of intensive development. In future, better computer support is probably achieved also in the qualitative tasks of an analysis. Further validation studies in the identification methods and in the field of gas release and dispersion modelling are needed in order to achieve a better reliance as regards the results. International benchmark studies play an important role in this.

The problems concerning the evaluation of the quality of an analysis are becoming more apparent when more analyses for licensing purposes are further carried out for the authorities. To evaluate the content of an analysis is, however, difficult and time-consuming. One approach could be the evaluation of the process behind the analysis. This resembles the evaluation of the quality management of a vendor in the field of quality control.

The development described earlier aims to improve the quality of safety analysis and to achieve a better integration in system design. This development is making the analyses faster and improving the cost-effectiveness of the analyses. In future, safety analysis will become one of the routine tools to be used in process design and to obtain licenses for new installations.

References

1 J. Suokas, On the reliability and validity of safety analyses. Espoo, Technical Research Center of Finland, Publications 25, 1985, 60 pp.+ app. 8 pp.

2 E. Bjordal, Is risk analysis obsolete? 3rd Int. Symp. on Loss Prevention and Safety Promotion in Process Industries. Basle, 15-19 Sept., 1980. Preprints. Swiss Society of Chemical Engineers, Basle, 1980, pp. 440-447.

3 R.A. Cox, Improving risk assessment methods for process plant, J. Hazardous Mater., 6 (1982) 249-260.

4 P. Jäger, The question of quality of risk analyses for chemical plants. Discussing the results for a sulphuric acid plant. 4th Int. Symp. on Loss Prevention and Safety Promotion in the Process Industries. Harrogate, 12-16 Sept., 1983. IChemE Symposium Series No. 80, Pergamon Press, Oxford, 1983, pp. B9-B19.

5 T.A. Kletz, Hazard analyses - The manager and the expert, Reliability Eng., 2 (1981) 35-43.

6 V. Piltz, What is wrong with risk analyses? 3rd Int. Symp. on Loss Prevention and Safety Promotion in Process Industries. Basle, 15-19 Sept., 1980. Preprints. Swiss Society of Chemical Engineers, Basle, 1980, pp. 448-454.

7 T.A. Kletz, The man in the middle. 3rd Int. Symp. on Loss Prevention and Safety Promotion in Process Industries. Basle, 15-19 Sept., 1980. Preprints. Swiss Society of Chemical Engineers, Basle, 1980, pp. 205-219.

8 F.P. Lees, Quantitative assessment and reliability engineering of major hazard plants in the context of hazard control. Symp. on the assessment of major hazards. Manchester, 14-16 April, 1981. IChemE Symposium Series No. 71, The Institution of Chemical Engineers, London, 1982, pp. 225-243.

9 P.L. Clemens, A. compendium of hazard identification and evaluation techniques for system safety application, Hazard Prev., 18 (1982) 11-18.

10 J.T. Daniels and P.L. Holden, Quantification of risk. 4th Int. Symp. on Loss Prevention and Safety Promotion in the Process Industries. Harrogate, 12-16 Sept., 1983. IChemE Symposium Series No. 80, Pergamon, Oxford, 1983, pp. G33-G45.

11 J.R. Taylor, Completeness and discrimination of hazard analyses. Risø National Laboratory, Roskilde, Risø-M-2306, 1981, 19 pp.

12 J.R. Taylor, Evaluation of costs, completeness and benefits for risk analyses procedures. Risø National Laboratory, Roskilde, report N-14-82, 1982, 38 pp.

13 J. Suokas and P. Pyy, Evaluation of the validity of four hazard identification methods with event descriptions. Technical Research Center of Finland, Espoo, Research Reports 516, 1988, 66 pp.+app. 8 pp.

14 E.R. Snaith, The correlation between the predicted and the observed reliabilities of components, equipment and systems, NCSR R18, (Report of the National Center of Systems Reliability, Warrington, U.K., 1981).

15 A. Taylor, Comparison of actual and predicted reliabilities in a chemical plant. IChemE Symposium Series No. 66, The Institution of Chemical Engineers, London, 1981, pp. 105-116.

16 W.E.Vesely and D.M. Rasmuson, Uncertainties in nuclear probabilistic risk analyses, Risk Anal., 4 (1985) 313-322.

17 A. Amendola, Results of the reliability benchmark exercise and the future CEC-JRC programme. Int. ANS/ENS Topical Meeting on Probabilistic Safety Methods and Applications. Preprints, San Francisco, CA, 24-28, Feb., 1985, 10 pp.

18 A. Amendola (Ed.), Systems Reliability Benchmark Exercise. Final Report. Joint Research Center, Ispra, EUR 10696/1 EN, 1986, 175 pp.

19 S. Dinsmore (Ed.), PRA Uses and Techniques. A Nordic Perspective. Oslo, Nordic Liaison Committee for Atomic Energy, 1985, 121 pp.

20 V. Rouhiainen, Turvallisuusanalyysin laadun arviointi (Evaluation of the quality of safety and risk analyses), Technical Research Center of Finland, Research Reports 517, 1988, 84 pp. (in Finnish).

21 Risk Analyses of Six Potentially Hazardous Industrial Objects in The Rijnmond Area. A Pilot Study. D. Reidel Publishing Company, Dordrecht, 1982, 793 pp.

22 Canvey, An Investigation of Potential Hazards from Operations in The Canvey Island/Thurrock Area. Health and Safety Executive, HMSO, London, 1978, 192 pp.

23 An analyses of the Canvey report. Oyez Intelligence Reports, Cremer and Warner, London, 1980, 55 pp.

24 P. Jäger, L. Kropp, L. Orenstat, H. Schenk and H. Thon, Analyse möglicher Störfälle in industriellen Anlagen im Hinblick auf die Luftreinhaltung, Durchfuhrung am Beispiel einer Schwefelsäureanlage (Analysis of possible disturbances in industrial plants aiming to air protection, examining as example a sulphuric acid plant). Köln, TÜV Rheinland, Forschungsbericht 77-10403352, 1983, 254 pp.+app. 80 pp. (in German).

25 P. Jäger, L. Kropp, L. Orenstat, H. Schenk and H. Thon, Addendum zur Analyse möglicher Störfälle in industriellen Anlagen im Hinblick auf die Luftreinhaltung, Durchfuhrung am Beispiel einer Schwefelsäureanlage (Analysis of possible disturbances in industrial plants aiming to air protection, examining as example a sulphuric acid plant). Köln, TÜV Rheinland, Forschungsbericht, 1984, 44 pp. (in German).

26 D.M. Webber, The Physics of Heavy Gas Cloud Dispersal. UKAEA, Safety and Reliability Directorate, Warrington, U.K., SRD R 243, 1983, 25 pp.

27 A.P. van Ulden, On The Spreading of A Heavy Gas Released Near The Ground. 1st Int. Symp. on Loss Prevention and Safety Promotion in the Process Industries. The Hague/Delft 28-30 May, The Netherlands. Elsevier, Amsterdam, 1974, pp. 211-219.

28 A.E. Germeles and E.M. Drake, Gravity Spreading and Atmospheric Dispersion of LNG Vapor Clouds. 4th Int. Symp. on Transport of Hazardous Cargoes by Sea and Inland Waterways, Jacksonville, FL, 1975.

29 J.A. Fay, Gravitational spread and dilution of heavy vapour clouds. 2nd Int. Symp. on Stratified Flows, Trondheim, 1980.

30 J.A. Fay and D. Ranck, Scale effects in liquified fuel vapour dispersion. M.I.T. Report DOE/EP-0032 UC-11, 1981.

31 R.G. Picknett, Field experiment on the behaviour of dense clouds. Porton Down, Report Ptn. IL/1154/78/1, 1978.

32 L.S. Fryer and G.D. Kaiser, DENZ - A computer program for the calculation of the dispersion of dense toxic or explosive gases in the atmosphere. UKAEA, Safety and Reliability Directorate. Warrington, U.K., SRD R 152, 1979, 43 pp.

33 R.A. Cox and R.J. Carpenter, Further developments of a dense vapour cloud dispersion model for hazard analyses. Symposium on Heavy Gas Dispersion, Frankfurt, 1979.

34 K.J. Eidsvik, A model for heavy gas dispersion in the atmosphere, Atom. Environ., 14 (1980) 769-777.

35 P.K. Raj, Summary of Heavy Gas Spills Modelling Research. Proceedings of the heavy gas (LNG/LPG) Workshop. Jan. 29-30, 1985. Concord Scientific Corporation, Toronto, 1985, pp. 51-75.

36 J. McQuaid, Overview of Current State of Knowledge on Heavy Gas Dispersion and Outstanding Problems/Issues. Proceedings of other heavy gas (LNG/LPG) workshop. Toronto, Jan. 29-30. Concord Scientific corp., Toronto, 1985, pp. 5-28.

37 S.F. Jagger, Development of CRUNCH: A Dispersion Model for Continuous Releases of a Denser-than-Air Vapour into the Atmosphere, UKAEA Report, SRD R229, 1983.

38 J.A. Havens, Session Chairman's Remarks. Proceedings of the heavy gas (LNG/LPG) Workshop. Toronto, Jan. 29-30, 1985. Concord Scientific Corporation, Toronto, 1985, pp. 29-31.

39 J.W. Rottman, J.C.R. Hunt and A. Mercer, The Initial and gravity-spreading phases of heavy gas dispersion: Comparison of models with phase I data, in: J. McQuaid (Ed.), Heavy Gas Dispersion Trials at Thorney Island (reproduced from J. Hazardous Mater., Vol. 11) Elsevier, Amsterdam, 1985, 261-279.

40 Y. Riou and A. Saab, A Three Dimensional Numerical Model for The Dispersion of Heavy Gases over Complex Terrain. EDF-DER Report HE/32-85.12, 1985.

41 RELVEC Manual, Vol. 1: Modelling. Technical Research Center of Finland, Helsinki, 1986, 69 pp.

42 RELVEC Manual, Vol. 2: User's Guide. Technical Research Center of Finland, Helsinki, 1986, 86 pp.

43 D.A. Lihou, Computer-aided operability studies for loss control. 3rd Int. Symp. on Loss Prevention and Safety Promotion in the Process Industries. Basle 15-19 Sept. 1980, pp. 448-454.

44 R.P. Pape and C. Nussey, A basic approach for the analyses of risks from major toxic hazards. The Assessment and Control of Major Hazards. Manchester, 22-24 April, 1985. London, The Institute of Chemical Engineers. IChemE Symposium Series No. 93, pp. 367-388.

45 The SAFETI package; Report on a computer based system for risk assessment of chemical plant using a simplified classical method, Vol. 1, overall description. London, Technica Ltd., 1984, several pages.

46 P. Haastrup, I.V. Olsen, J.R. Taylor, A. Damborg and N.K. Vestergaard RIKKE Users Manual. Risø National Laboratory. Roskilde, Denmark, Risø-M-2480, 1985, 133 pp.

47 A. Poucet, Computer aided fault tree synthesis. Ispra, Joint Research Center, Report EUR 8707 EN, 1983, 34 pp.

48 J. Suokas, P. Heino and I. Karvonen, The development of an expert system to support HAZOP analyses. Birmingham, 14-16 April, 1987. Reliability '87, Birmingham, 11 pp.

49 I. Karvonen, J. Suokas and P. Heino, HAZOPEX – Expert system supporting safety analyses, SRE- Symposium, Helsingör, 5-7 Oct., 1987, 13 pp.

50 J. Suokas, P. Heino and I. Karvonen, Some experiences and developments in computer aided safety analyses, SINTOM seminar on datorhjälpmedel för tillförlighetsanalys, Visby, 27-29 April, 1987. 19 pp. (in English).

51 A. Poucet, S. Contini, N.K. Vestergaard and K. Petersen, An expert system approach to systems safety and reliability analyses, 2nd European Workshop on Fault Diagnostics, Reliability and Related Knowledge-based Approaches. Manchester 6-8 April, 1987, 8 pp.

52 J.F. Barbet, M. Melis and M. Oliviero, Computerized safety and reliability assessment: From computer codes development to expert system techniques application. Int. Symp. on Risk Analyses in Environmental Impact Assessment, Milan, 26-27 Nov., 1987, pp. III/53-62.

53 A. Poucet, A. Amendola and P.C. Cacciabue, CCF-RBE Common cause failure reliability benchmark exercise. Joint Research Center, Ispra, EUR 11054 EN, 1987, 129 pp.

54 S. Messina, N. Piccinini and G. Zappellini, Accident scenarios evaluation: Tools and methodologies. World Conference on Chemical Accidents, Rome, 7-10 July, 1987, CEP Consultants Ltd., Edinburgh, pp. 156-159.

55 D.M. Webber and S.J. Jones, A model of spreading vapor. Proceedings of The Vapour Cloud Modelling Symposium, 2-4 Nov., 1987, Boston Marriott, Cambridge, MA, pp. 226-250.

56 C. Nussey and R.P. Pape, The significance of vapour cloud modelling in the assessment of major toxic hazards. Proceedings of The Vapour Cloud Modelling Symposium, 2-4 Nov., 1987, Boston Marriott, Cambridge, MA, pp. 889-922.

57 A.C. van den Berg, C.J.M. Wingerden, J.P. Zeeuwen and H.J. Pasman, Current research at TNO on vapor cloud explosion modelling. Proceedings of The Vapour Cloud Modelling Symposium, 2–4 Nov., 1987, Boston Marriott, Cambridge, MA, pp. 687–711.

58 A.D. Swain and H.E. Guttman, Handbook of human reliability analyses with emphasis on nuclear power plant applications. Albuquerque, Sandia Laboratories, NUREG/CR-1278, 1980, several pages.

59 J. Suokas, Safety analyses of a liquefied gas storage and loading system. J. Occupational Accidents, 4 (1982) 347–354.

60 J.R. Taylor, A background to risk analyses. Vols. I–IV. Risø National Laboratory, Roskilde, report (unnumbered), 1979, several pp.

61 J. Rasmussen, O.M. Pedersen, A. Carnino, M. Griffon, G. Mancini and P. Gagnolet, Classification system for reporting events involving human malfunction. Risø National Laboratory, Roskilde, Denmark, Risø-M-2240, 54 pp.

62 D.A. Norman, Design rules based on analyses of human error, Commun. ACM. 26(4) (1983), 254–258.

63 J. Reason, A framework for classifying errors, in: J. Rasmussen, K. Duncan and J. Leplat (Eds.), New Technology and Human Error. John Wiley and Sons, Chichester, 1987, pp. 5–14.

64 J. Reason, Generic error-modelling system (gems): A cognitive framework for locating common human error forms, in: J. Rasmussen, K. Duncan and J. Leplat (Eds.), New Technology and Human Error. John Wiley and Sons, Chichester, 1987, pp. 63–83.

65 W.G. Johnson, MORT safety assurance system. National Safety Council and Marcel Dekker, Inc., New York, NY, 1980, 525 pp.

66 P. Bockholts, Collection and application of incident data, 3rd Int. Symp. on Loss Prevention and Safety Promotion in the Process Industries, Harrogate, 12–16 Sept., 1983. Pergamon Press, Oxford, pp. K11–K21.

67 J.J. Clifton and A. Wilkinson, Major hazard incident data service. World Conference on Chemical Accidents, Rome, 7–10 July, 1987, CEP Consultants Ltd., Edingburgh, pp. 64–67.

68 A. Amendola, The reporting of major accidents within the European Community. EuReDatA/3ASI Seminar on Incident Data Bases and Their Use in Risk Analyses, Milan, 9 Oct., 1985, 13 pp.

69 Guidelines for safety evaluation of platform conceptual design. Oslo, Norwegian Petroleum Directorate, 1981, 7 pp.

70 F.L. Kafka, The European chemical industry's view of major hazards legislation. The 1984 European Major Hazards Conf., London, 22–23 May, 1984. Oyez Scientific and Technical Services, Ltd., London, 37 pp.

71 Zwölfte Verordnung zur Durchführung des Bundes-Immissionsschutzgesetzes (Störfall-Verordnung). Bonn, Bundesgesetzblatt 32, 8 pp. (in German).

72 Erste Allgemeine Verwaltungsvorschrift zur Störfall-Verordnung vom 23/4/81 - GMBI, Bonn, 1981, no. 12, 8 pp. (in German).

73 Zweite Allgemeine Verwaltungsvorschrift zur Störfall-Verordnung. Der Bundesminister des Innern, gemeinsames Minsiterialblatt (GMBI), G 3191 A, Ausgabe A, Bonn, 1982, pp. 205–216 (in German).

74 Bekendtgørelse om risikoen för større uheld i förbindelse med en raekke industrielle aktiviteter. Miljöministeriets bekendtgørelse, No. 204, Copenhagen, 1984, 15 pp. (in Danish).

75 Pligter ved risikobetonede aktiviteter (Duties with respect to risk related activities). Danish Labour Inspectorate, Environmental Authority, Guideline 3, Copenhagen, 1985, 65 pp. (in Danish).

76 Environmental program of the Netherlands (partly) 1986–1990. Ministry of Housing, Physical Planning and Environment; Ministry of Agriculture and Fisheries, and Ministry of Transport and Water Management, The Hague, 1985, pp. 50–64 and 153–160.

77 Notification of installations handling hazardous substances regulations. Health and Safety Executive, London, 1982, SI 1982/1357.

78 A Guide to the Control of Industrial Major Accident Hazards Regulations. Health and Safety Executive, London, 1985, HS (R) 21, 98 pp.

79 K. Cassidy, CIMAH safety cases. The Chem. Eng., 43 (1987) 6–7.

80 Operational safety report. Guide for the composition. Directorate General of Labour of the Ministry of Social Affairs, Voorburg (The Netherlands), 1982, CP 3 E, 64 pp.

81 Laki työturvallisuuslain muuttamisesta (A law for changing the occupational safety law). Valtion painatuskeskus, Suomen säädöskokoelma, Helsinki, No. 27–29, 1987, pp. 41–48 (in Finnish).

82 Asetus vaarallisista teollisuuskemikaaleista (The decree on hazardous industrial chemicals). A proposal. Chemical Legislation Committee, Helsinki, 1986, 33 pp. (in Finnish).

83 Sikkerhetsanalyse som beslutningsunderlag. Yrkeslitteratur, Oslo, 1984, 147 pp. (in Norwegian).