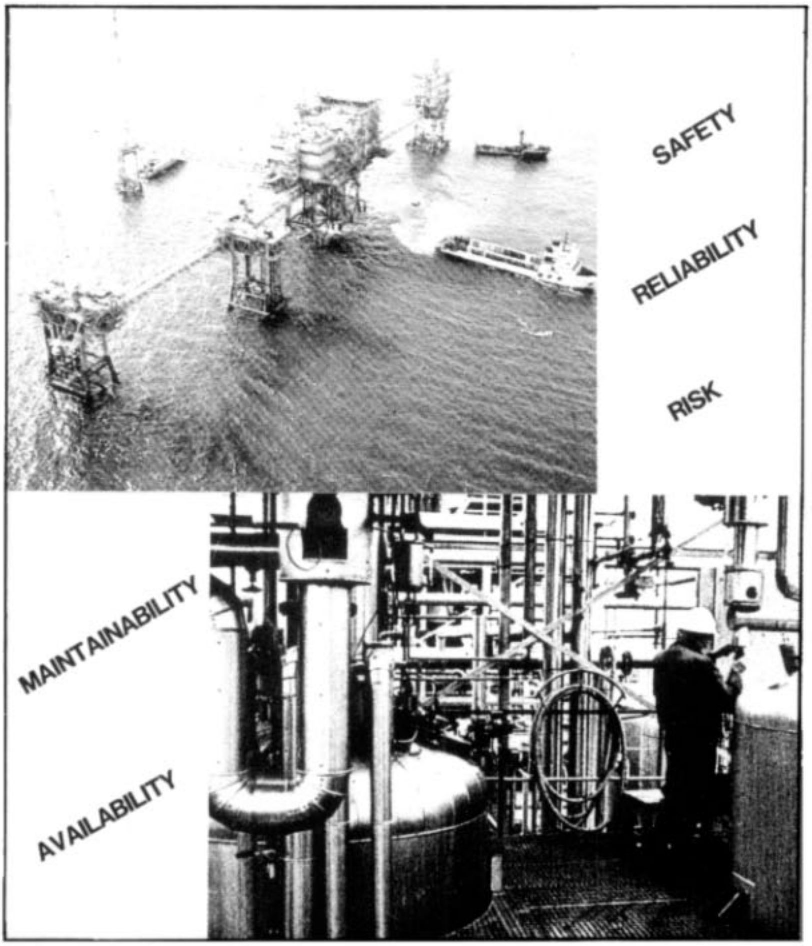
NORD
FEBRUARY 1986

RISK ANALYSIS
USES AND TECHNIQUES
IN THE NON-NUCLEAR FIELD
A NORDIC PERSPECTIVE



nka

Nordic
liaison committee for
atomic energy

nka

Nordisk kontaktorgan for atomenergispørgsmål	Nordiska kontaktorganet för atomenergifrågor	Pohjoismainen atomienergia- yhdyselin	Nordic liaison committee for atomic energy

RISK ANALYSIS
USES AND TECHNIQUES
IN THE NON-NUCLEAR FIELD
A NORDIC PERSPECTIVE

Written by
Kurt E. Petersen
Risø National Laboratory
Denmark

February 1986

Nordic
Liaison Committee for
Atomic Energy

ISBN 87-550-1192-6

ABSTRACT

Techniques for probabilistic risk analysis (PRA) have been analyzed within the Nordic SÄK-1 project with special emphasis on their application in nuclear power plants. The results of the project are reviewed with respect to non-nuclear applications. The review is based on discussions with industry in the Nordic countries. It will focus on evaluation and comparison of available computer codes, the importance of reliability and accident data, and the subsequent application of PRA techniques as an aid in the licensing and regulatory process. Areas, which were not included in the SÄK-1 project but are of great importance in non-nuclear PRA's, are identified.

KEY words

Probabilistic Risk Analysis - Reliability Analysis - Availability Analysis - Nuclear Power Plants - Chemical Plants - Offshore-Platforms - Complex Systems - Computer Codes - Reliability Data - Accident Data - Regulatory work.

This report describes the utilization of the results of the SÄK-1 project, which was part of the safety programme sponsored by NKA, the Nordic Liaison Committee for Atomic Energy, 1981-85. This additional work has been financed by the Nordic Council of Ministers and Risø National Laboratory.

SUMMARY

Risk analysis techniques are increasingly being used at industrial plants to improve safety and reliability and in some specific areas as a part of the documentation for approval by the authorities. These techniques are more and more based on a probabilistic approach taking into account the frequencies for occurrence of failures, incidents, or accidents. This approach is called PRA (probabilistic risk analysis). In the Nordic countries, PRA techniques are coming into use as a tool during the evaluation of the safety of chemical plants, off-shore platforms, nuclear power plants, and other complex industrial systems. The risk analyses are being performed in order to ensure that accidents and losses are prevented and that improvements are made in a cost effective way.

PRA methodology provides a comprehensive framework which leads to a well documented analysis of a plant and its functions. The results of a PRA can be used to evaluate the safety of a plant, to identify weak points, to evaluate proposed changes and to select between alternatives. The PRA techniques are useful tools for the authorities as well as for the operators of plants. The numerical results from such evaluations provide a means for referencing existing functions to a common scale allowing comparisons which otherwise would remain nontractable and subjective. It must be emphasized that the numerical results should be used with proper regard to the current limitations. Despite the uncertainties the results are still valid, as the results usually are given as ratios or other relative measures, which means that the results are not so sensitive to uncertainties.

In a Nordic project, NKA/SÄK-1, some of the existing PRA techniques were compared while other techniques were further developed. The work was essentially limited to functional modelling and subsequent probabilistic evaluation of accident sequences at nuclear power plants (the so called level 1 PRA). The results of this work are presented in the report titled, "PRA Uses and Techniques - A Nordic Perspective", (1).

The present report describes the uses of these techniques in other, non-nuclear, applications. The work has been carried out in close contact with industry, consultants and authorities within the Nordic countries.

Concerning level 1 PRA, the functional modelling and subsequent probabilistic evaluation, the results of the project are valid and very useful also in non-nuclear application. One very important method for identification of failures, the HAZOP (Hazards and Operability Studies) method, has not been carefully studied and compared to other alternative methods within NKA/SÄK-1. This method is extensively used in identification of weak points at chemical plants, where processes are generally more complex than those found in nuclear plants.

Currently level 2 and level 3 PRA's are growingly emphasized in evaluations of the safety at chemical, off-shore and other complex industrial plants. Level 2 and level 3 risk analysis constitutes the evaluation of the accident consequences. Level 2 PRA is limited to the consequences within the plant while level 3 PRA describes the consequences to the public situated in the surroundings of the plant. Methods and techniques for such assessments are very important, since the impact of an accident on the plant, its operational staff and the environment needs to be calculated, due to authorities' requirements and the possibility of economical losses. The latter subjects were not discussed within the project.

Although some important subjects were not considered within the NKA/SÄK-1 project the results are useful in other applications, since the project report gives a concentrated description of the state of the art of a large number of techniques used in level 1 PRA, which are available for non-nuclear applications as well.

The results in the NKA/SÄK-1 report must be supplemented by results from other work concerning the methods and techniques unique for non-nuclear applications. In this respect the report constitutes a necessary but not complete description of the elements of a probabilistic risk analysis.

SAMMENFATNING

Risikoanalyse anvendes i stigende grad ved industrielle anlæg med henblik på at forbedre sikkerhed og pålidelighed, og på visse områder som en del af dokumentationen ved godkendelse hos myndighederne. Metoderne bygger i stigende grad på sandsynlighedsbaserede overvejelser, hvor hyppigheden for fejl, uheld og ulykker medinddrages. Denne type analyser kaldes PRA (sandsynlighedsbaseret risikovurdering = Probabilistic Risk Analysis). Indenfor de nordiske lande anvendes PRA-teknikken som et redskab i forbindelse med vurderingen af kemiske anlæg, offshore platforme, nukleare anlæg og andre komplekse industrielle systemer. Risikoanalyser udføres for at sikre, at ulykker og tab forebygges, og at forbedringer udføres på en økonomisk måde.

PRA-metodikken udgør en omfattende ramme, som sikrer en veldokumenteret analyse af et anlæg og dets funktioner. Resultaterne af en PRA kan anvendes ved vurdering af sikkerheden ved et anlæg, ved identifikation af svage punkter, ved vurdering af foreslåede anlægsændringer, og ved valg mellem alternativer. PRA-teknikkerne er nyttige redskaber for myndigheder såvel som for anlægsindehavere. De numeriske resultater fra sådanne vurderinger muliggør sammenligninger med eksisterende anlæg i en fælles skala - sammenligninger, som ellers ville forblive besværlige og subjektive. Det må understreges, at de numeriske resultater må anvendes med skyldig hensyntagen til eksisterende begrænsninger. På trods af usikkerheder vil resultaterne være gyldige, da disse sædvanligvis gives som relative mål, og dette betyder, at resultaterne ikke er så følsomme overfor usikkerheder.

I det nordiske projekt, NKA/SÄK-1, blev visse af de eksisterende PRA-metoder sammenlignet, medens andre metoder blev videreudviklet. Arbejdet var i det væsentlige begrænset til modellering af anlægsfunktioner og efterfølgende sandsynlighedsbaseret analyse af ulykkessekvenser ved nukleare anlæg (såkaldte niveau 1 PRA). Resultaterne af arbejdet er præsenteret i rapporten "PRA Uses and Techniques - A Nordic Perspective", (1).

Den foreliggende rapport beskriver anvendelserne af disse resultater i andre, ikke-nukleare, anvendelser. Arbejdet er blevet udført i tæt kontakt med industri, konsulenter og myndigheder i de nordiske lande.

Vedrørende niveau 1 PRA, modellering af anlægsfunktion og efterfølgende sandsynlighedsbaseret analyse af ulykkessekvenser, gælder, at resultaterne fra projektet er gyldige og anvendelige også ved ikke-nukleare anlæg. En vigtig metode til identifikation af fejl, HAZOP (Hazards and Operability Studies), er dog ikke blevet nærmere studeret og sammenlignet med andre alternative metoder i NKA/SÄK-1. Denne metode anvendes i stor udstrækning ved identifikation af svage punkter ved kemiske anlæg, hvor processerne generelt er mere komplekse end i nukleare anlæg.

I øjeblikket lægges hovedvægten i stigende grad på niveau 2 og niveau 3 PRA ved vurderinger af sikkerheden ved kemiske, offshore og andre komplekse industrielle anlæg. Niveau 2 og niveau 3 risikoanalyser omfatter vurderinger af konsekvenserne af en ulykke. Niveau 2 PRA er begrænset til konsekvenserne indenfor anlægget, mens niveau 3 PRA beskriver konsekvenserne for beboerne i omgivelserne af anlægget. Metoder og teknikker for sådanne analyser er meget vigtige, da følgerne af et uheld for anlægget, dets personale og omgivelserne må beregnes på grund af myndighedernes krav og mulighederne for økonomiske tab. De sidst beskrevne emner blev ikke diskuteret i projektet.

Visse vigtige emner ikke blev betragtet i NKA/SÄK-1 projektet. Dets resultater er dog nyttige i andre anvendelser, da projektrapporten giver en koncentreret beskrivelse af status for et stort antal metoder, der kan anvendes ved niveau 1 PRA. Disse metoder er ligeledes anvendelige ved ikke-nukleare anlæg.

Resultaterne i NKA/SÄK-1 rapporten må suppleres med resultater fra andet arbejde vedrørende metoder og teknikker, der er særlige for ikkenukleare anvendelser. På den måde udgør rapporten en nødvendig, men ikke fuldstændig, beskrivelse af elementerne i en probabilistisk risikoanalyse.

LIST OF CONTENTS

1. INTRODUCTION

Probabilistic Risk Analysis (PRA) has been widely used in regulatory work within the nuclear field both in the US and in the Nordic countries. Risø has reviewed the results obtained within the Nordic project NKA/SÄK-1, Probabilistic Risk Assessment and Licensing, sponsored by the Nordic Liaison Committee for Atomic Energy, with respect to non-nuclear applications.

The NKA/SÄK-1 project was aimed at

- verification of methods
- improvement of data bases
- guidelines for use of PRA in regulatory work.

The main contents of the work will be described emphasizing the milestones and the main results of the project. A comprehensive description of the project is given in the project report "PRA Uses and Techniques - A Nordic Perspective", (1).

As a continuation of this work the results were discussed with industry, consultants and authorities in the Nordic countries with respect to non-nuclear applications. Some general experiences obtained by Risø and others performing risk analyses of off-shore, chemical, or other complex industrial systems are collected emphasizing the applicability of the findings of the project.

It was found that the majority of the results of the project are valid also for non-nuclear applications. Further, areas outside the scope of the project were discussed and a need for future research in these areas identified.

Chapter 3 discusses some important differences and similarities between nuclear and non-nuclear plants. In chapter 4 some general observations concerning the application of PRA techniques by the industry and the authorities are given. In chapter 5 the usefulness of the NKA/SÄK-1 results in non-nuclear applications are discussed including important recommandations and references to the report (1).

2. SUMMARY OF THE NKA SÄK-1 PROJECT

The NKA/SÄK-1 project, Probabilistic Risk Assessment and Licensing, was performed in the period 1981-84 with the aim to study risk analysis methods and their application in regulatory work of nuclear power plants. The project has been carried out within the research program of the Nordic Liaison Committee for Atomic Energy (NKA).

The work was performed by

- Technical Research Centre of Finland (VTT), Finland
- Risø National Laboratory, Denmark
- Institute for Energy Technology (IFE), Norway
- Studsvik Energy Technology, Sweden
- ASEA ATOM, Sweden.

The work has been directed by a project group composed of one or two project members from each participating institute and of experts from the Swedish Nuclear Power Inspectorate, Finnish Centre for Radiation Protection and Nuclear Safety, and the Nuclear Safety Board of the Swedish Utilities.

2.1. Main Objectives

The elements of a probabilistic risk analysis include:

1. hazards identification
2. accident sequence modelling
3. system response modelling
4. reliability analysis
5. analysis of physical processes and accidents
6. analysis of consequences within the plant
7. analysis of consequences to the environment

In the nuclear terminology item 1-4 describe a so-called level 1 PRA, item 5-6 a level 2 PRA, and item 7 a level 3 PRA. The scope of the project was limited to level 1 PRA.

The objectives of the project was the following:

- verification of risk analysis methods concerning the completeness of the models and the accuracy of quantitative predictions
- improvements in the data base for the reliability of components
- presentation of guidelines for the application of probabilistic methods in regulatory work including an evaluation of the benefits and limitations.

The tasks of the project are shown in table 1. Task 1 and 4 are studied with the aim of comparison and verification of analysis methods. Task 2 and 3 are related to data base improvements, while task 5 is performed to study PRA as an aid in regulatory work.

Table 1. Tasks within SÅK-1

	Task	Person years	1981	1982	1983	1984
			TIMETABLE			
1	Method development and verification	7	———	———	—— - - -	
2	Data base improvement	5	- - - -	———	———	- - -
3	Sensitivity and uncetainty analyses	2	———	———	———	———
4	Trial studies					
	Benchmark 1	1		——		
	Benchmark 2	3			———	———
5	Implementation of PRA in regulatory work	4	- - - -	- - - -	- - - ———	———
6	Joint activities	2				
	- Project seminars		1st	2nd		3rd
	- Data workshop			x		
	- Dependent failure workshop				x	
	- Licensing workshop					x
	- Expert workshop					x
	Person years total	24				

The main results of the project have been presented at the milestones, internal seminars and workshops.

2.2. Results Concerning Methods

Comparison and verification of the analysis methods have been based mainly on two Benchmark studies concerned with

- reliability analysis of a typical high pressure injection system for a PWR (Pressurized Water Reactor) plant
- modelling and quantification of disturbance sequences resulting in the loss of feedwater in a BWR (Boiling Water Reactor) plant.

The Benchmark studies have for the most part been carried out independently by different institutes. The studies provide insight about the completeness of system function modelling and the uncertainties inherent in the method and data choices. The results of the Benchmark studies are described in (1) and (2).

The aim of Benchmark 1 was to study generation and propagation of reliability parameters. Generic reliability data were collected within each institute. It was found that the reliability data of pipe failures have the largest deviation. An unavailability calculation was performed using the generic data. The results were in good agreement among the different computer codes when the same data set was used. The differences between the codes are small compared with the differences between the different data sets. This strongly emphasizes the need for a careful evaluation of the data available to be used in quantitative analysis. Detailed results of Benchmark 1 are presented in (1) and (3).

The aim of Benchmark 2 was to study system function modelling, identification of failures modes, modelling of event sequences, and quantification of the transients.

During the analysis the documentation of simplifications, truncations, approximations, and other assumptions is strongly emphasized, since such assumptions are made continually. Furthermore, it was possible to analyse completeness in this exercise. Six significant differences were identified, including omissions of hardware or improper modelling. This emphasizes the need of review of PRA's by persons intemately familiar with the system. Once again it became apparent that the modelling phase is the most critical part in reliability analysis.

As a part of the Benchmark 2 study, or initiated by the study, specific work was performed on

- verification and comparison of methods for failure identification
- verification and comparison of methods for event sequence and system reliability modelling

- verification and comparison of computer codes
- idenfification, classification, and quantification of dependent failures
- identification and treatment of some important human errors
- treatment of uncertainties.

The first three items were thoroughly studied and it was found that familiarity with the techniques is the most important factor for ease of model construction and review. The computer codes give similar results for the same data set, so again the familiarity with the codes is essential.

The last three items were not studied in detail. They are subject to a more careful investigation in the new NKA program 1985-88.

2.3. Results Concerning Data

The major part of the work concerning improvement of reliability data was performed in connection with the compilation of the Swedish Data Handbook - T-boken (4). The compilation was based on data contained in the Swedish ATV data base (5), where component reliability information from Swedish and the Finnish TVO power company are collected.

Statistical techniques and computer programs for treatment of component data were developed and compared. Furthermore, specific analyses of pipe failures and closing valves were performed.

2.4. General Conclusions

One task of the project concerns the implementation of PRA methods in regulatory work. The need of this task changed during the project, since there is little interest at the moment in the Nordic countries concerning implementation of quantitative safety goals. The work instead constitutes a review of the status. Furthermore, it is emphasized that any PRA is beneficial when used on a relative basis without depending upon absolute quantitative risk predictions. This means that the influence of absolute uncertainties in the quantitative predictions are deminished - uncertainties related to assumptions, simplifications, or truncations, as the relative results to the most part are insensitive with respect to many uncertainties.

The general conclusion of the project is that the available PRA techniques are useful tools which can help the licensing authorities evaluate the safety of nuclear power plants. The numerical results from such evaluations provide a means for referencing existing functions to a common scale allowing comparisons which otherwise would be non-tractable and subjective. It should be noted, that the design and regulating of plants in fact has been based on judgemental comparisons without the aid of systematic methods and without thorough documentation. When used with due regard to the current limitations, these results can also serve to identify weak points and help the licensing authorities evaluate proposed changes and select between alternatives.

3. DIFFERENCES AND SIMILARITIES BETWEEN NUCLEAR AND NON-NUCLEAR PLANTS

There exist differences between nuclear and non-nuclear industrial plants, some of which are based on historical reasons. Nuclear power plants were designed during the sixties and seventies of this century. This means that the technology is new and the developments in design took place at the same time as politicians and the public were focusing on safety aspects. The chemical industry started growing earlier this century at a time when the public and the authorities were not too much concerned about safety and risk. This difference in age has had an important influence on the design of the systems. The conventional chemical industry and the authorities has "learned by experience", which is not a desired path of development for nuclear energy or other modern technology with potential dangerous consequences.

The systems present at the nuclear power plants are in themselves straightforward but built into a complex network. A power plant contains a large number of safety systems which are operated automatically or manually under specific conditions. The safety systems require a large number of measurements in order to diagnose the status of the plant for possible system activation. Further, in order to increase the reliability of the systems the most essential subsystems or components are duplicated. In modern plants safety systems consist of up to four redundant parts. This increases the reliability of the system, but at the same time the complexity of the plant is increased.

Another important difference is that the operation of a nuclear power plant is supervised and controlled from one central control room with few people working directly on the operating plant. On the contrary the chemical plants in general have no central supervision of the entire plant. It is common that more than one control room is present controlling different process parts of the plant. Further, parts of the plant cannot be controlled from a control room and many people are directly involved in the operation of the plant.

Finally, the losses in connection with a serious accident are enormous for the owner of a nuclear power plant. Both the direct loss in investment and the expences necessary to substitute the lost production.

Therefore, there exist many historical reasons that non-nuclear plants are different from nuclear plants, both in design, in operation and with respect to authorities requirements.

These differences diminish, since at present the complexity, cost and size of non-nuclear plants is being increased. One reason is that the public is increasingly concerned with safety aspects - both safety for people working at the plant and people living in the surroundings as well as the environment. Furthermore, the losses of an accident are increased to an unacceptable level due to expensive investment in equipment and expences connected to lost production.

Still, differences exist between nuclear power plant and non-nuclear plant, but the developments of designs with increased complexity - redundancies, safety systems, computer supervision and control - will emphasize the similarities with respect to loss prevention and reliability assurance.

4. EXPERIENCES USING RISK ANALYSIS WITHIN THE NORDIC COUNTRIES

The applicability of risk and reliablilty analyses in decision making has been thoroughly studied in a previous Nordic project, the SCRATCH project (Scandinavian Risk Analysis Technology Co-operation). The results from the project are documented in (6). In this chapter some additional comments are added, emphasizing the use of risk analysis techniques in regulatory work.

The experiences collected here originate from discussions with industry, consultants and authorities in the Nordic countries performing or reviewing risk analyses. During the discussions the main question has been to what extent the PRA-techniques studied in NKA/SÄK-1 have been used and with which results. This means that the usefulness of the NKA/SÄK-1 were identified.

The findings presented are in good agreement with the results of a similar study performed by International Study Group on Risk Analysis, Loss Prevention Working Party of the European Federation of Chemical Engineering (7).

4.1. Industry

Risk and reliability analyses are extensively used and the experience shows that methods and techniques for hazard identification are well established with methods as HAZOP (8) and FMEA (9). These methods have been used to identify design deficiencies with surprisingly good results. Further developments by computerization of these methods are suggested by the industry. This will improve both the speed and the thoroughness of the analyses and above all reduce the dependency of the study quality on the analysts.

It is found that quantification presents problems due to the lack of adequate reliability data, particularly for human errors, dependent failures, and rare events, such as vessel and pipe ruptures. The importance of data collection is strongly emphasized by the industry and more work on collection, treatment, and representation of reliability and incident data is suggested.

It is found that the models to be used in consequence analysis need to be improved. Specific areas are identified in which more research is needed, namely modelling of effects of fires and explosions, dispersion of heavy gasses, and two-phase flow releases. The models can benefit from verification and comparison by, for example, doing a Benchmark study.

Finally, it is emphasized that risk analysis cannot replace all other efforts in assuring the safety of a plant neither in licensing or in design, but it is a very beneficial tool which can supplement other investigations. The benefit of performing a quantitative analysis is dependent on the complexity of the system. For most simple systems a qualitative analysis will be sufficient, since their function can be checked in detail and the weak points can easily be identified. For complex systems it is often impossible to identify all the weak points and to assign priorities to these without performing a quantification. In these cases a quantitative analysis adds new information to the qualitative analysis - an information which otherwise would be impossible to obtain.

4.2. Authorities

Risk analyses have not been applied systematically in regulation of industrial plants, but there is an increasing interest in application of these techniques. For some specific purposes risk analysis techniques are being used by the authorities, namely for off-shore installations in Norway and Denmark and for regulation of plants producing hazardous substances in Denmark.

Risk analysis can be used by the authorities in the following cases:

- licensing of new plants
- evaluation of design modifications
- evaluation of conditions for operation
- evaluation of safety precautions.

In all cases the authorities can benefit from identification of design deficiences and selection between alternatives.

In the following sections the above mentioned specific applications of risk analysis are discussed.

4.2.1. Off-shore

The Norwegian Petroleum Directorate's (NPD) guidelines for safety of platform conceptual design was implemented in Norway in 1981. In order to achieve approval of a new facility the operator shall provide a safety analysis based on a set of rules, called the NPD-guidelines (10). These guidelines specify the a list of events to be analysed including:

- blow out
- fire
- explosion
- falling objects
- ship and helicrash.

It is emphazised that special attention should be paid to new design features.

Each of these events should be analyzed separately. If the probability of occurrence is greater than 10^{-4} per year then a design change is required to reduce the probability of occurrence or specific arrangements must be provided to ensure evacuation of the personnel in case of occurrence of the event.

The acceptance criterias are based on the principle that the above studied design accidental events do not impose danger to personel outside the immediate vicinity of the accident. This is satisfied if the following three criterias are fulfilled:

- at least one escape way from central positions available for at least one hour during an accident
- shelter areas shall be intact until evacuation is possible
- the structural integrity shall be maintained for a specified period of time.

The NPD-guidelines are to be used in safety analysis concerning a new facility in the Norwegian part of the North Sea. This means that a probabilistic safety analysis as an integrated part of the documentation is established since the analysis is based on quantitative measures using a cut-off value of 10^{-4} per year.

The number of analyses where the guidelines have been applied is large and it seems that the safety analysis based on the guidelines gives a suitable documentation to be used by the licensing authorities for checking of the standard of the design compared to other similar facilities.

The NPD-guidelines do not constitute a full scale risk analysis in its normal sense, since the systematic search for identification of failures and accident sequences is replaced by a predescribed list of events to be analyzed. But the analyses required are well suited for comparison of a platform at the conceptual design stage with other similar ones.

4.2.2. Process Plants

EEC has passed the directive, the so-called Seveso-directive, which has to be modified according to existing legislation and implemented in each member country. As a member of the EEC Denmark is implementing a directive on major hazard accidents in connection with certain industrial activities (11). The directive is implemented in Denmark by an instruction (12) and an accompanying guide, which will be put into force by the end of 1985.

According to the directive an assessment is required if a plant has a production or a storage of certain hazardous substances. These substances are explicitly listed with the corresponding maximal permitted limits. The assessment must document

- the hazards related to the activity
- the systems where hazardous substances are present
- the precautions taken to avoid or limit the consequences of an accident (both equipment and procedures).

The documentation should always be available at the operator in a updated version. Updating can be caused by

- changes in design
- replacement of process or safety equipment
- new findings from experience concerning safety aspects
- new research results.

Furthermore, if none of these conditions are fulfilled the authorities propose an updating every five year.

The authorities have described the requirements concerning the contents of the analysis and some recommandations concerning risk and reliability techniques to be used when performing the required risk assessment.

It is known that between 50-100 plants in Denmark have to submit an analysis according to the directive. Existing plants were expected to supply the authorities with a preliminary registration by January 1985 and a full documentation before 1989.

New plants have to provide the analysis as a part of the documentation for approval. The same is also the case if an existing plant applies for modifications, which will significantly change the safety of the plant.

The risk analysis which is performed can also be used in preparation of an emergency plan, if needed.

The authorities in Norway, Sweden and Finland have shown a great interest in the implementation of the directive in Denmark. They have explained that they will follow the development and gain from the experience in order to adjust the national legislation.

5. APPLICABILITY OF SÄK-1 RESULTS

The usefulness of the PRA techniques studied within the SÄK-1 project are discussed with industry, consultants and authorities.

It was described in chapter 4 that risk analysis techniques are formally used in two industrial areas. Concerning the safety of off-shore systems the analysis required by the authorities can be supplemented by systematic investigations which can be helpfull in operation planning, decreasing the number of production shut downs, etc, which at the same time will improve the safety - even when the required analysis will assure a certain level of safety. The SÄK-1 results provide good insight into such systematic investigations.

The implementation of the Seveso-directive in Denmark forces the industry as well as the authorities to use some kind of risk analysis technique. To which extend the various techniques are used depends upon the complexity of the plant and the goal of the analysis, but the report describing the SÄK-1 results constitute a very good handbook, even though some elements of a risk analysis are not described. This means, that for system functional modelling and reliability calculation available methods and techniques are described and documented which will save time for the industry or the authorities who need these types of tools in documentation of the safety of a plant.

The outcome from the discussions of the SÄK-1 results is divided into different parts related to the objectives of project given in section 2.1.

For further description and details of the methods, see the corresponding section of the report of the SÄK-1 project (1).

5.1. Methods

The methods which are studied for failure identification, system function modelling, and quantification can be used for any system - nuclear or non-nuclear. It must be emphasized that some methods which are common in risk analyses of non-nuclear plants, have not been studied in the SÄK-1 results. Firstly, HAZOP (Hazards and Operability Studies, (8)) useful for hazards identification has not been subject to investigations. Secondly, methods and modelling techniques for level 2 PRA and level 3 PRA were outside the scope of the SÄK-1 project. This means that modelling of the physical processes and analysis of the consequences of an accident, which is very important and emphasized in evaluation of the safety of non-nuclear industrial plants, was not considered in the project.

In discussions, it was generally expressed that more research on modelling of consequences is needed. The areas which were explicitly mentioned are:

- modelling of the physical processes
- systematic methods to identify undesired chemical reactions
- releases of toxics, especially releases of heavy gases
- dispersion of toxics and calculation of the doses as a function of distance from the source, weather conditions, terrain, and countermeasures taken to limit the consequences

- characteristics of a fire, for instance ignition rate for flamables, distribution of the temperature, flamelength
- charasteristics of an explosion, calculation of the shockwave
- calculation of the effects on a structure (a vessel, a building, a wall) originating from an accident.

The usefulness of the methods studied in the SÄK-1 project is commented below.

5.1.1. Modelling techniques

Risk analyses are performed in order to ensure that accidents and losses are prevented. To which extent the use of methods and modelling techniques is beneficial depends on the complexity of the system and the objective of each specific analysis. Similarly, the usefulness of a quantification of frequencies and consequences of a failure or an accident is dependent on the complexity of the system. For simple systems it can be easy to identify and understand system malfunctions and assign priorities to different design modifications. For more complex systems systematic techniques are needed to assign these priorities - an assignment which otherwise would have been impossible.

Furthermore, it must be underlined that a risk analysis is not a sufficient documentation in evaluation of the safety of a plant. The risk analysis supplements but does not replace the use of well established codes and standards, deterministic calculations of the equipments ability to withstand the loads, the procedures for operating, the education of the operators, the management of the risks, etc. This means that a risk analysis does not replace other investigations, but it is a valuable additional tool.

The general experience is that the HAZOP method is extensively used and sometimes in combination with the FMEA method (Failure Mode and Effects Analysis (9)), which has been used for specific parts of a system, for instance an arrangement of valves and pumps in a water supply system.

The cause-consequence method and other similar models of event sequences can be used to identify and illustrate the causal interconnections between accidental events and states of a plant. It is recommended to use fault trees in combination with the cause-consequence method to investigate malfunction of a specific system. In order to be quantified, a cause-consequence diagram has to been simplified and transferred to an event tree.

Since no method guarentees completeness it is highly recommended to use methods in combination and to perform the analysis iteratively using several reviews by the designers, the operation staff, and others with expert knowledge on the function of the plant. In order to improve the completeness and the tractability of analyses it is suggested to increase efforts in the development of automated methods which can support risks identification and evaluation.

5.1.2. Operation Planning

One subtask of method improvement within SÄK-1 was to apply PRA methodology in operation planning. Within SÄK-1 testing strategies for stand-by equipment and the question of allowed component unavailability during continued plant operation have been investigated with regard to basic methodology. This subject is important in re-evaluation of the safety technical specification and limiting conditions of operation.

Some promising results are already available on use of PRA methods in evaluation of the additional risk during the presence of component failures in safety-related systems and in comparison of the safety benefits with the additional transient risks associated to a plant shut down, (13). Such investigations are not unique for nuclear power plant applications, but can be of great importance in any complex industrial plant.

The development work on this subject will be continued in a practically oriented way in the new NKA/RAS 450 project, "Optimization of Technical Specifications by Use of Probabilistic Methods".

5.1.3. Computer Codes

A varity of computer codes available within the Nordic countries for reliability calculation are verified and compared within SÄK-1 (see section 3.5. of (1)). These codes can be used in reliability calculations of any system with the aim to identify design deficiences and to constitute a framework for evaluation of alternative design improvements. It was found that different codes give similar results when used to solve the same problem. Further, familiarity with a code is essential when assigning preferences to different codes.

The computer codes today are developed to a standard where they are directly useful in reliability calculations.

5.1.4. Common Cause Failures

The use of redundant systems to provide safety functions will reduce the probability of independent failures leading to accidents. However, a potential for dependency between the redundant systems is created. This means, that in order to improve the safety by installation of a redundant system it is important to ensure that one failure cannot lead to failures in both systems simultaneously. This type of failures is common cause failures - failures which occur simultaneously or in a short time interval due to a common cause.

Methods for identification and quantification of common cause failures are discussed within SÄK-1. In nuclear applications evaluation of common cause failures is very important, since improvements have in many cases reduced the contribution from independent failures, negligible compared with common cause failures. Furthermore, systems consisting of up to four redundant subsystems will almost eliminate independent failures. In such systems one cause which can fail several or all subsystems simultaneously must be avoided.

Even if the non-nuclear plants in general have only two redundant subsystems the problem of common cause failures is present, calling for methods to evaluate the impact of such failures. The state-of-the-art of treatment of common cause failures is given in the SÄK-1 report and the subject will be further investigated in the new NKA project "Risk Analysis Methods".

5.1.5. Human Errors

Treatment of human errors was the subject of another Nordic project during 1981-84, LIT, (14). In the SÄK-1 project it was studied as a part of the second Benchmark exercise with the emphasis on the identification of operator errors and the modelling of such errors in the context of system function modelling. Some maintenance errors were identified and they were treated directly in the fault trees. Some operational errors were identified and treated in the event trees or in the cause-consequence diagrams. To support the insight into the latter problem, the project team worked two days at an operator training simulator, in connection to Benchmark 2 in order to get better information on how operators behave in a control room. Experience from this exercise shows that simulation of accident sequences on a training simulator can provide useful information and familiarity with the way operators act in case of plant disturbances.

It is very difficult to quantify human errors, in particular operating errors. The reason is that the systems are very complex and the number of signals and alarms present in the controlroom during an accident sequence is so large, that it is very difficult to predict how operators will act and what are the possibilities of improper actions.

In (15) treatment of human errors in PRA is discussed more thoroughly, pointing out that an increased effort is needed to imledge about operators and their behaviour during accident sequences. In a new design, the logic of the systems and the information available in the control room must be easy to interpreat so that the operators quickly can get a diagnosis of the state of the plant.

5.2. Data

The compilation of Swedish reliability data from experience with Swedish nuclear power plants given in the T-book (4) has proved very useful in PRA studies underway at the Nordic nuclear power plants. Reservations must, however, be stated for its use in other applications, specially concerning mechanical process equipment. For the electrical components, however, the majority of data are valid also in non-nuclear application. Furthermore, some information concerning the distribution of failures among different failure modes is relevant, f.ex. failures of valves are divided into three failure modes: valve does not close on demand, valve does not open on demand, and external leakage from valve.

It is important to collect operating experience systematically, as in the ATV data bank (5) which is the main source of information for the T-book. Similarly, an evaluation of the operating experience, as the T-book, is recommended, since data collection in itself is not enough.

Another important data source is the OREDA hand-book (16), describing the operating experience from off-shore platforms in the North Sea.

The principles of data collection and the classification systems are of interest in general. Similarly the methods and computer codes for statistical treatment of failure records can be used directly for any set of data.

5.3. Benchmark Studies

Comparison and verification of methods within SÄK-1 has been based mainly on two Benchmark studies. This type of approach is very advantageous when several teams are available.

It was found that comparison and verification of methods and techniques performed by Benchmark exercises is very efficient. It is possible to identify incompletenesses doing a Benchmark exercise - incompletenesses, which otherwise would have been detected only by chance. This means that the advantages and the limitations of a method are thorougly adressed. The same result is formulated as a result of another Benchmark study performed in the reactor safety research programme within the EEC (17). This type of benchmarking is therefore highly recommended for comparison and verification of the methods and techniques unique for non-nuclear applications. The SÄK-1 project can be used for guidance in undertaking such efforts.

5.4. Risk Analysis as a Tool in Regulatory Work

As described in section 4.2. risk analysis techniques are already to some extent applied for certain purposes in regulation of complex industrial plants. It is likely that it will become more and more common to require risk analyses for evaluation of the safety of plants. As seen from the SÄK-1 project many methods and techniques are available in a form suitable for application for any complex system. The methods and techniques are concerning identification of failures, modelling of system function, and reliability quantification. A lot of research is going on in the areas of consequence modelling, such as modelling of fires, explosions, and releases and dispersions of toxics.

The use of probabilistic techniques with its systematic approach will be needed as systems get more complex through installation of automatic control and safety systems and through installation of redundant systems to improve safety functions.

Finally, risk analyses provide a well-suited framework for discussion between designers and operating staff, and between operators and the authorities. Further, it is very important to use the operating experience to adjust the design of the systems and the operating procedures. The influence of any design modification and significance of abnormal occurrences can be efficiently addresses in the framework of a systematic risk analysis.

6. ACKNOWLEDGEMENT

The main part of this work would not have been possible without help from many people within industrial companies, consulting companies, research institutes, and regulatory bodies, to whom I will express my gratitude.

Finally, I will express my thanks to Tuomas Mankamo for fruitful and inspiring discussion during the writing of the report.

7. REFERENCES

1. "PRA Uses and Techniques - A Nordic Perspective", Summary report of the NKA project SÄK-1. Edited by S. Dinsmore, Studsvik Energiteknik. NORD, June 1985.

2. "Experiences from the Nordic Benchmark Analyses". T. Mankamo, et al. International ANS/ENS Topical Meeting on Probabilistic Safety Methods and Applications, San Francisco, USA. February 1985.

3. "Probabilistic Risk Assessment and Licensing", Proceedings of project seminar 2, Helsingør, Risø National Laboratory-M-2363, 29-31 March 1982.

4. "T-boken. Tillförlitlighetsdata för komponenter i svenska kraftreaktorer". J.-P. Bento et al. RKS 85-05.

5. "Vad är ATV?" Booklet issured by the ATV staff, Vattenfall Kärnkraft, 1983.

6. "Sikkerhetsanalyse som beslutningsgrundlag", Vol.I: Teori og metoder, Vol.II: Praktiske eksempler. Slutrapport från SCRATCH-programmet. Nordforsk, 1982

7. "Risk Analysis in the Process Industries". International Study Group on Risk Analysis, IChemE, A5, Paperback, 1985.

8. "A Guide to Hazards and Operability Studies". Publications Department Chemical Industries, Ass.LTD. London 1977.

9. "Analysis Techniques for System Reliability - Procedures for Failure Mode and Effects Analysis (FMEA)". IEC TC 56, Publishers no.812 (1985).

10. "Guidelines for Safety Evaluation of Platform Conceptual Design". The Norwegian Petroleum Directorate, 1981.

11. "Rådets Direktiv af 24. juni 1982 om risikoen for større uheld i forbindelse med en række industrielle aktiviteter". 82/501/EØF.

12. "Bekendtgørelse om risikoen for større uheld i forbindelse med en række industrielle aktiviteter". Bekendtgørelse nr. 204 af 1. maj 1984.

13. "Applications of the Use of PRA-Methods in the Re-Evaluation of Technical Specifications at the TVO Power Plant". TVO-report 1985.

14. LIT - Final Reports.

    1. The human component in the safety of complex systems.

    2. Human errors in test and maintenance of nuclear power plants - Nordic project work.

    3. Organization for safety.

    4. The design process and the use of computerized tools in control room design.

    5. Computer aided operation of complex systems.

    6. Training in diagnostic skills for nuclear power plants.

15. "Trends in Human Reliability Analysis". Jens Rasmussen, Risø. Ergonomics, 1985, vol.28, no.8.

16. "OREDA - Offshore Reliability Data Handbook". OREDA Participants 1984

17. "Systems Reliability Benchmark Exercise". Final Report, Part I: Description and Results. Edited by A. Amendola, Joint Research Centre, Ispra, Italy. Technical Note No. I.05.C1.85.131, P.E.R. 1050-A, October 1985.

Copies of this report can be ordered from

Risø National Laboratory
Systems Analysis Department
Risk Analysis Group
DK-4000 Roskilde
Denmark

gotab Stockholm 1986