nks

Nordisk kernesikkerhedsforskning
Norrænar kjarnöryggisrannsóknir
Pohjoismainen ydinturvallisuustutkimus
Nordisk kjernesikkerhetsforskning
Nordisk kärnsäkerhetsforskning
Nordic nuclear safety research

NKS-6
ISBN 87-7893-054-5

Proceedings of the NKS/SOS-2
Seminar on Risk Informed Principles
Bergendal 13.4.-14.4. 1999

Edited by
Urho Pulkkinen and Kaisa Simola

VTT Automation
Finland

1999-09-02

NKS-6
ISBN 87-7893-054-5

Afd. for Informationsservice, Risø, 1999

The report can be obtained from
NKS Secretariat
P.O. Box 30
DK – 4000 Roskilde
Denmark

Phone +45 4677 4045
Fax +45 4677 4046
http://www.nks.org
e-mail: annette.lemmens@catscience.dk

CONTENTS

*) Are not accessible in electronic form.
**) Only partly accessible in electronic form.

Foreword

Recently probabilistic safety assessments (PSA) have been increasingly applied in safety related decision making. The decisions are related for example to establishing maintenance programmes, optimising inspection policies and justifying plant modifications, and revising technical specifications. Furthermore, there are applications in daily situations, such as accepting or rejecting exemptions from technical specifications. The above mentioned decisions belong to the domain of so called risk informed decision making, which is based on the results of plant specific PSA.

Authorities and power companies all around the world have initiated programmes in order to promote the use of risk informed principles. The form and application areas of such activities vary, and there is a need to compare and evaluate the approaches. The aim of this NKS/SOS-2 seminar was to present the status and plans of applications of Risk Informed Principles both by nuclear authorities and industry in Finland and Sweden. Furthermore, views from the off-shore industry were presented.

The seminar consisted of invited presentations and informal discussions. The presentations were given by Finish and Swedish nuclear power companies and nuclear safety authorities (SKI, STUK). Representatives from the Norwegian Petroleum Directorate (NPD) and SINTEF complemented the seminar by describing applications of quantitative risk analyses (QRA) within the oil and gas industry. The presentations are shortly summarised in the following.

Risto Himanen from TVO gave an overview on the scope of living PSA for Olkiluoto and presented examples of the use of PSA in plant modernisation programme. At TVO, the living PSA has proved to be a valuable tool in safety management. Himanen notified that PSA has become an important support for discussions between TVO and the nuclear safety authority STUK, as both the authority and the utility have the same model and code.

The presentation of Michael Landelius from OKG concentrated on the risk follow-up work at Oskarshamn. Landelius pointed out that risk follow-up is a practical way to use living PSA. The risk significance of occurred events are evaluated and suitable and effective improvements can be identified. Furthermore, the risk follow-up studies support the verification and updating of PSA models and data.

Göran Hultqvist from FKAB compared different safety analysis approaches as bases for decision making. He annotated that generic design criteria are a good starting point for safety development, and PSA is only used to support modifications in the cases they are expensive or they affect operating instructions.

Ingemar Ingemarson from BKAB presented the applications of risk informed principles at Barsebäck. The current PSA has been used as a tool for plant upgrading and modification since 1998. Next activity is the consolidation of the process for keeping the PSA living. In the plans for future PSA applications, Ingemarson mentioned risk-informed in-service inspections, evaluation of criteria in technical specifications, risk follow-up and classification of component importance as input to development of maintenance strategies.

Jussi Vaurio (Fortum) described the applications of risk informed principles at Loviisa plant. PSA has been used continuously to identify dominant accident sequences and to develop plant modifications for safety improvement. According to Vaurio, the most fruitful areas have included providing risk perspective and economic criteria for back-fitting and modification decisions, assessing the ageing-significance, and reducing testing requirements. Furthermore, the justification of temporary and permanent plant configurations and planning and prioritisation of training programs have been supported by PSA results.

P.O. Waessman (SwedPower) discussed roles of PSA and deterministic analyses in the present environment governed by deregulated electricity market context. SwedPower has established an interdisciplinary expert group for setting requirements for safety related questions. He mentioned that PSA is good in verification of safety levels and in optimising resources. The advantage of PSA is its ability to account for uncertainties. This is not the case with deterministic analyses which can treat uncertainties only in limited way, leading often to over-conservative results.

Björn Brickstad (SAQ) gave a presentation on a project on risk informed in-service inspection (RI-ISI) in Sweden. In the pilot study, the risk based inspection methods are used to determine the locations for ISI and inspection intervals. PSA is applied to evaluate the consequences of pipe ruptures, while the piping failure probabilities are obtained by probabilistic fracture mechanics models. The approach is compared to the more qualitative EPRI approach.

In his presentation Reino Virolainen from STUK told that the revised regulatory guide on PSA requires the use of PSA results in support of decisions on operational safety issues, such as plant modifications, training of plant personnel, working out of emergency operation procedures, application of technical specifications, etc. The PSAs are used in a living way, and both regulatory body and the utilities use the same model. Virolainen also shortly described the ongoing pilot studies on ISI, in which the methodology leans on the EPRI approach. Virolainen emphasised that PSA is always complemented by deterministic reviews.

Lars Gunsell from SKI described the role of risk analysis in safety work. In addition to requirements to perform plant specific PSAs, SKI has supported the PSA method and data base development. However, requirements and procedures for daily use of PSA have not been set up. Established methods combining quantitative safety criteria with fundamental safety principles, such as the defence in depth or fault-tolerance and robustness, are needed for enabling the development towards risk informed safety management.

Liv Nielsen from NPD described the regulatory regime and the use of risk informed principles in Norwegian oil and gas industry. Quantitative risk analysis (QRA) has been mainly used for assessing impacts of modifications and for planning emergency preparedness, but there is a growing need to move towards the use of QRA for operational purposes. Nielsen identifies needs for co-operation with the industry in the areas of developing common risk models and methods. The experience gained from other industries is seen important in the development of regulatory principles and practices.

Knut Øien from SINTEF highlighted the main differences between PSA for nuclear power plants and QRA for petroleum installations. The basic difference is that the QRA models and data bases are not as detailed as those of typical PSAs. Øien described also an application of QRA in developing risk indicators for offshore platforms. The indicators are used as a tool for risk control during operation, and they are seen as supplement to other techniques to keep the risk at acceptable level.

In the general discussion, the differences between Finland and Sweden in the use of current PSAs were recognised. In Finland, the utilities have wanted to use PSA results as an argument in discussing the requirements from the safety authority. At the same time, STUK has seen the advantage of common PSA models and tools. Another difference is that in Sweden PSAs are carried out mainly by consultants – in Finland STUK has required that the plant personnel has to be actively involved.

Issues of common interest to be considered in the NKS/SOS-2 project were also discussed. Some prerequisites for adopting risk informed principles were underlined, such as convincing the public, the authorities and own plant personnel, the correspondence of the models with reality and compatibility with deterministic analyses. It was noticed that these set requirements for developing and interpreting the risk models. In NKS/SOS-2 project, the above mentioned topics are already partially covered. In addition to these, the follow-up of the developments on risk informed in-service inspection and the applications of decisions analysis were identified as potential topics for the project.

September 2 1999
Urho Pulkkinen and Kaisa Simola

APPLICABILITY OF LIVING PSA IN NPP MODERNIZATION

Risto Himanen
Teollisuuden Voima Oy,
FIN-27160 Olkiluoto, Finland

SUMMARY

Recently the utility Teollisuuden Voima Oy (TVO) has modernized the Olkiluoto 1 and 2 nuclear units and increased the net electric power by 18 per cent. Level 2 PSA was performed during the modernization project and the living level 1 PSA was used to support the design of the plant modifications. The plant specific living PSA model was a powerful tool when evaluating modernization alternatives. Successive support of safety management with the PSA model requires, that both the utility and the Regulatory Body understand capability and limitations of the model in details.

TVO has prepared an internal procedure that presents in detail the practices and responsibilities concerning living PSA. The procedure is based on general guidelines and requirements on probabilistic safety analysis of nuclear power plants in Finland, released by the Regulatory Body. Living PSA requires that also the procedure for the use of living PSA is living. The recently published USNRC Regulatory Guides on PSA will be taken into account in the next version of the TVO PSA procedure. The PSA Peer Review Certification Process is one way to evaluate the quality of PSA in general, but also to detect the weaknesses of the PSA. However, the Certification Process covers only limited scope of PSA omitting e.g. all other external events except internal floods.

This paper gives an overview on the scope of living PSA for Olkiluoto 1 and 2, and. presents some examples on the real use of PSA concerning the modernization of the plant. Definition of quantitative dependability requirements for renovated systems is possible, but on the other hand, proving of these targets is in some cases extremely difficult, because of lacking dependability data. The problems are mainly concerned in systems with of programmable logic control..

1. INTRODUCTION

The Finnish Regulatory Body STUK has released in the YVL Guide 2.8 general guidelines and requirements regarding probabilistic safety analysis of nuclear power plants in Finland. [1] The utility TVO and the Regulatory Body have mutually agreed, how to apply the guidelines in the use and updating of the PSA for the BWR units Olkiluoto 1 and Olkiluoto 2, recently raised from 710 to 840 MWe,net. The utility has collected the practices in an internal procedure, which has support and acceptance from the management of the utility. The key issue is keeping the PSA living and up-to-date enough, for the purposes it is used. The updating procedure is described in several papers [2],[3],[4]. The procedure is updated biannually, and the next version will apply appropriate parts of the USNRC Regulatory Guides concerning risk informed decision making and PSA.[5, 6, 7, 8, 9]

The living PSA of the identical units Olkiluoto 1 and Olkiluoto 2 is a result from the plant specific PSA research program [10] shown in Figure 1. TVO started the program in the year 1984 and the development of living PSA began in the year 1990. The first completely updated version of the level 1 PSA for power operation modes including internal and external initiators was published four years later, in 1994. The modernization of Olkiluoto NPP required another revision of the PSA study. It was prepared simultaneously with the design of plant modifications thus supporting the design work of TVO and of the contractors. PSA was an important tool, when discussing with the Regulatory Body, on safety issues related to the modernization.

2. USE OF PSA

In the office for nuclear safety the utility TVO has at the moment a PSA group of four reliability engineers, who use and update the living PSA – keep the PSA living. However, specialists from the whole organization and external consultants continuously are in cooperation. Topical issues are applications and updating of the model instead of the earlier development and extension of the study. Reliability engineers continuously monitor the development of the safety level and support several kinds of safety improving modifications. From the results of PSA they can identify new safety related issues, evaluate the benefit of modifications and draw comparisons between competing modification alternatives. With rapid calculations they also can support decision making in incident situations.

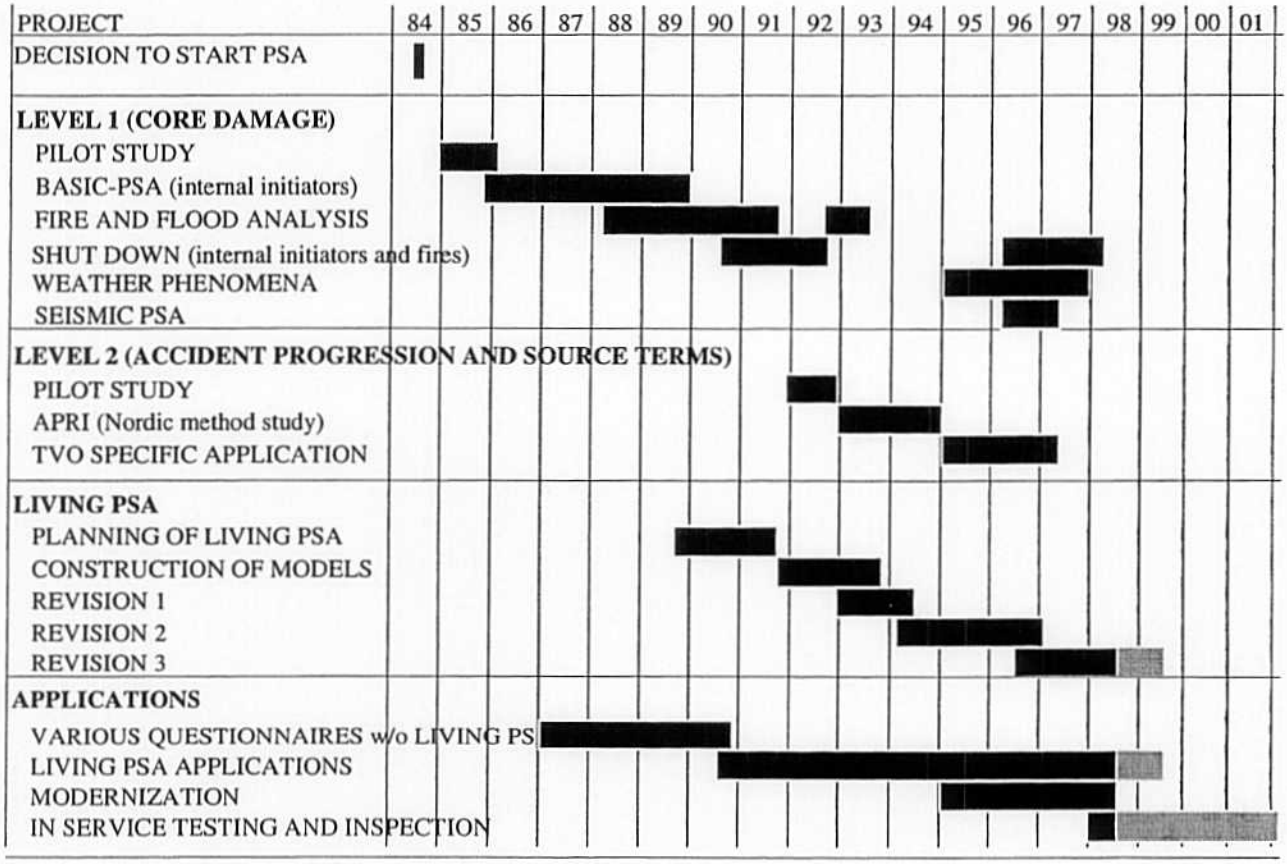


Figure 1: Olkiluoto 1 and 2 PSA research program is in the updating and application phase.

3. PSA PEER REVIEW CERTIFICATION

The Boiling Water Reactor Owners Group (BWROG) has applied PSA Peer Review Certification Process for almost all BWR units in USA[11]. The certification team consists of five to seven persons, with PRA expertise from the manufacturer, other utilities, and industry. Individual attributes of the plants analysis will be categorized in one of four categories:

- Grade 1 - Supports Assessment of Plant Vulnerabilities
- Grade 2 - Supports Risk Ranking Applications
- Grade 3 - Supports Risk Significance Evaluations w/Deterministic Input
- Grade 4 - Provides Primary Basis For Application

The idea is to permit various applications based on the PRA ranking. Similar programs are being established for Pressurized Water Reactors (PWRs). Basically this is an industry effort to assess the quality of PRAs and to establish uniform quality levels for PRAs. The evaluation is done by answering into 10-20 questions for each of the eleven elements of the PSA. Thus inadequacies can be identified in rather small details of the PSA. The elements considered are:

- Initiating Events
- Accident Sequences Evaluation
- Thermal Hydraulic Analysis
- Systems Analysis
- Data Analysis
- Human Reliability Analysis
- Dependency Analysis
- Structural Response
- Quantification and Results Interpretation
- Containment Performance Analysis
- Maintenance and Update Process

In USA the review is performed by an independent specialist team. Such procedure has not been applied into the PSA of Olkiluoto, but the Certification Process can be used also as internal quality assurance guide.

4. USE OF PSA IN THE MODERNIZATION PROGRAM

The modernization program of Olkiluoto 1 and 2 units was conducted during the years 1993-1999. The program was divided into about 40 projects, and the total costs were almost 800 MFIM ($160.000.000). At the beginning of the modernization program, a plan was made to support utility and contractors with PSA based examinations in 13 safety related projects. During the program, the number of supported projects increased to 17.

The core damage frequency before modernization was about $5.9 \cdot 10^{-5}$/reactor year. Without earthquakes, which were analyzed and integrated in the living PSA during the modernization project, the cdf was $3.5 \cdot 10^{-5}$/reactor year. At the moment the total cdf is about $1.3 \cdot 10^{-5}$/ry and the expected value after all improvements due to earthquakes is below $1 \cdot 10^{-5}$/ry. However, the risk

profile is changing whole the time, because new risks arise during operation, and some small modifications may have a great decreasing impact on risk.

Figure 2 shows the development of the estimate of the core melt frequency due to various causes of initiating events. Steps upwards represent extensions of the analysis. Decreasing of the estimate originates either from improvement of the model or from modifications on the plant.

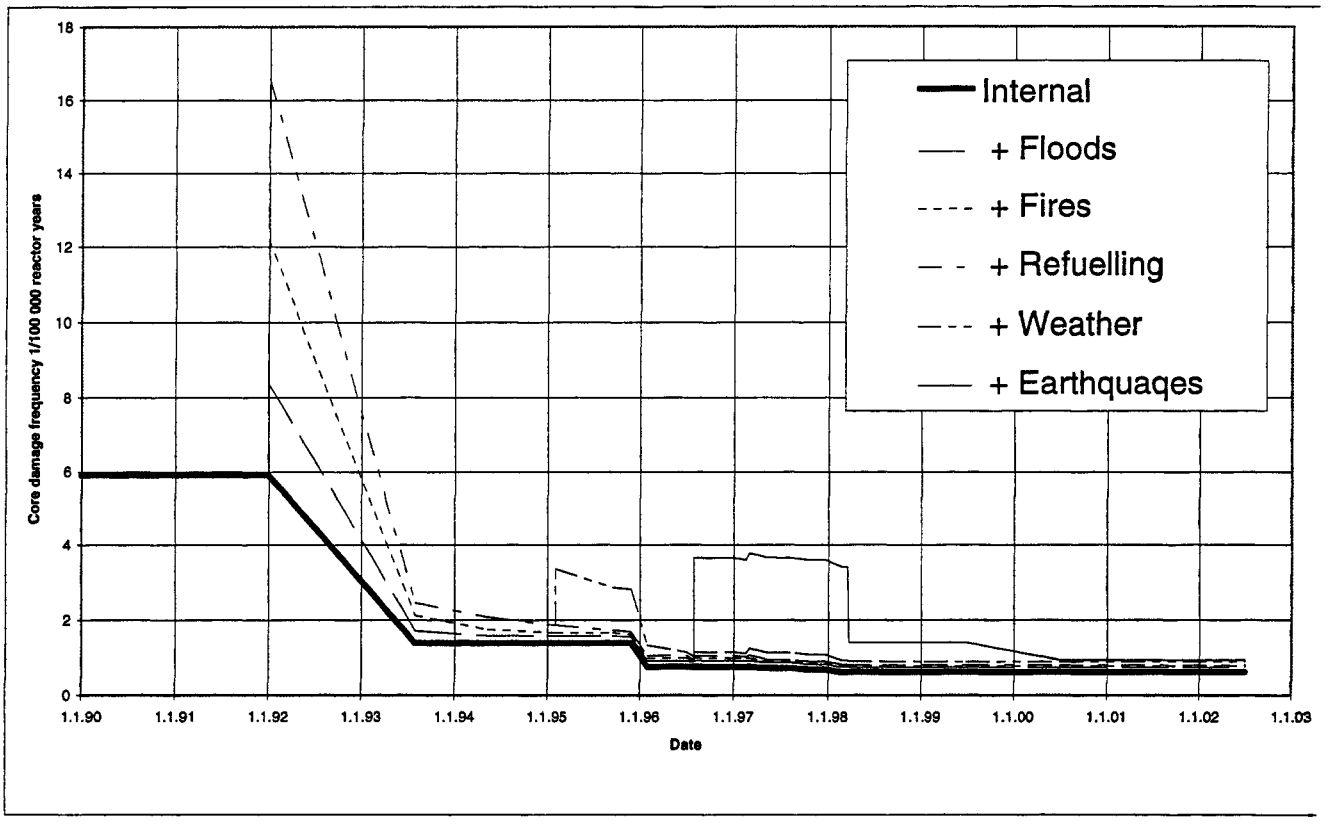


Figure 2: Development of the estimate of the core damage frequency of Olkiluoto 1 and 2.

4.1. Plant test program

Most of the plant tests in connection with power upgrading are necessary. However, some tests may cause remarkable risk compared with the value of test results. Also the test arrangements and procedures may benefit from risk studies. The planned risk increase from one reactor scram test is 5-20% of the annual core damage frequency, depending on the test type, isolations tripped in the test, and the end state (hot or cold shut down). Originally, the scram test was changed to a milder one, but the risk increase might be acceptable in Olkiluoto, especially, if comparing with the USNRC Regulatory Guide 1.174[5].

The Olkiluoto PSA is applicable in evaluation of different scram tests, because the hot shut down state after planned shut down, and different isolations have separate event tree models.

4.2. Seismic PSA

Seismic analysis was originally a part of the checking and updating of the design basis of the plant and systems. The seismic PSA revealed about ten weak points at the plant concerning seismic risk. Most important ones were free standing batteries and almost free standing cubicles containing relays and other instrumentation as well as AC bus-bars. Because the core damage

frequency of Olkiluoto units is rather low, and earthquakes have not been a design criterion, the relative risk impact from earthquakes became a risk leader. PSA allowed risk based ranking of weak points. TVO decided to modify the most important of them, resulting in the decrease of seismic core damage frequency from $2.5 \cdot 10^{-5}$ to $5 \cdot 10^{-6}$ 1/a.

Seismic analysis is wise to integrate into PSA, because the different risks can be evaluated on the same basis. It is another question, how large uncertainties are involved in the risk models for initiators from different sources.

4.3. Severe accidents and Level 2 PSA

The analysis of severe accidents was performed in connection with the level 2 PSA. The treatment of the phenomena in the severe accident analysis is conservative, but it is realistic in the level 2 PSA. In addition level 2 PSA can treat all phenomena with distributions and add the probabilistic dimension. Because the level 2 PSA and the conventional severe accident analyses were performed in parallel and in cooperation, it was possible to concentrate the further research and plant modifications in the most effective way.

Level 2 PSA is important in realistic risk studies. Most important is to perform a plant specific mapping of risk contributors. This includes:

- detailed structural model of the containment, not only global strength calculations,
- detailed analysis of separate phenomena with accurate codes, not only calculations with an integrated code like MAAP,
- an integrated PSA model (accident sequence analysis and radionuclide transport and release analysis) that allows rapid calculations when some parameters, like operator action times, are changed.

4.4. Freezing of sea water intake strainers

Under-cooled sea water having temperature below zero centigrade can freeze in the intake strainers in the sea water tunnel. This phenomenon has occurred at TVO twice, in the years 1988 and 1995. In January 1995 it caused loss of condenser, and simultaneously it degraded residual heat removal function. Originally the problem was considered as availability problem only, but PSA showed that core melt frequency decreased by more than 60%, when the heating system was built at the inlet of the sea water.

The PSA model of Olkiluoto is applicable in such analyses.

4.5. Increased capacity in safety systems

The upgrading of reactor thermal power from 2160 MW to 2500 MW required capacity increase also in some safety systems. The capacity of the residual heat removal systems was increased by increasing the number of plates in heat exchangers. This modification did not effect on PSA results.

The capacity of the S/R valves would have been too small to fulfill the conservative requirements. Adding two valves of the same type as the old ones would have increased the core damage risk slightly. The requirements for the new valves were specified with the support of PSA. The new valves had to be as diverse as possible compared with the old ones. The installation of two new diverse safety/relief valves did not significantly decrease the total core damage frequency, but it changed the plant damage state profile drastically by decreasing the frequency of

high pressure sequences by 60% (frequency of reactor overpressurization was decreased by a factor 50), which resulted in a significant decrease in the source term.

Level 1 PSA with level 2 interface was required for this analysis.

4.6. Instrumentation systems

The old **turbine plant control systems** were replaced with new programmable logic systems. The old "one out of two" (1/2) component protection circuits in the turbine plant were replaced with 2/3 or 2/4 ones. Only a minor part of these systems were important to safety. PSA showed, however, that the importance to core damage risk was some per cents, because the instrumentation failures are expected to cause less inadvertent scrams.

The **neutron flux measuring system** was also replaced with programmable logic. The core damage contribution was calculated to decrease, compared with the old relay logic. A lot of qualitative and quantitative reliability analyses were made to validate the design. However, the requirements of STUK were impossible to fulfill in the safety related parts of the neutron flux measuring system, and hard wired parts were installed in parallel with the programmable systems.

The **speed control system of the main circulation pumps** was replaced with programmable logic. The pumps stop too fast causing probably fuel cladding failures, if they have only their own inertia. Therefore an energy storage is required in case of loss of external grid. The new energy storage is based on flywheels. The requirements based on PSA calculations were easily fulfilled with the new system and even with the old hard wired logic. However, it was impossible to fulfill the deterministic requirements by STUK, and the control system for the soft stop of the pumps was hard wired.

The **instrumentation system of the reloading machine** was replaced with a programmable logic. A comprehensive FMEA was performed for the system, and it revealed a couple of design errors or weaknesses. Difficulties arose in licensing the automatic operation of the reloading machine.

Systems based on programmable logic are at the moment almost the only control systems available. They have a lot of operating experience from the industry use, but only a little from nuclear industry. The basic system solutions are in most cases more than ten years old, and the design of the systems does not fulfill the recent requirements.

PSA is a good tool when analyzing the importance of these systems as a part of the plant, but it is not sufficient tool to analyze the systems themselves. Most of the systems had only minor impact on core damage frequency. At the moment there seems to be no method that would be accepted by the Finnish Regulatory Body, to show the sufficient reliability of these systems qualitatively or quantitatively.

4.7. Safe shut down improvements

This project was initiated late in the modernization program. It includes several diverse safety functions, e.g., automatic depressurization of the primary circuit in case of ATWS or very low level in the reactor tank, and automatic start of boron injection in case of ATWS. PSA showed that this modification decreased the core damage frequency significantly. All modifications were fulfilled with conventional relay logic. The selection of the functions was based partially on PSA results and the design was supported by comparing design alternatives with PSA calculations.

The Olkiluoto PSA was applicable in the analysis of safe shut down instrumentation and logic.

4.8. Electric power systems

A lot of modifications in the electric power systems were performed, but most of them had only minor impact on core damage frequency. The most important one was the building of more rigid support for batteries to tolerate seismic events, discussed in chapter 4.2.

Rather detailed PSA model of electric power system was applicable in the analysis of modifications in the system, and definition of dependability requirements.

5. CONCLUSIONS

Regardless of the tens of man years used for the development of the living PSA, it has proved to be a valuable tool in the management of safety in Olkiluoto nuclear power plant. The utility and the Regulatory Body have the same model and same code. PSA has become a discussion forum between them [12]. One of the most important advantages from PSA is that it allows the arguing on safety issues using quantitative measures. However, the PSA calculations tend not to become as the only criterion when making decisions on safety issues. Some problems arose in connection with the modernization, especially in probabilistic treatment of new technology. In general, the dependability requirements for the modified systems are rather simple to calculate, but the tools are still missing to show quantitatively that the requirements are fulfilled in case of programmable logic systems.

6. REFERENCES

(1) YVL - Guide 2.8. Probabilistic safety analyses (PSA) in the licensing and regulation of nuclear power plants. Finnish Centre for Radiation and Nuclear Safety, 18 Nov. 1987.

(2) Himanen, R., Use of PSA as a tool to monitor and enhance safety of TVO NPP. TOPSAFE'95. Budapest, 24-27 September 1995.

(3) Himanen, R., Use and Updating of PSA at TVO NPP. IAEA TCM The role of PSA and PSC in NPP Safety Vienna, Austria December 4-8, 1995.

(4) Himanen, R., Development and use of living PSA at TVO NPP. WANO-PC Regional Workshop PSA APPLICATIONS. Leibstadt, Switzerland, 21st-23rd February 1996.

(5) USNRC Regulatory Guide 1.174. An Approach for using Probabilistic Risk Assessment in Risk-Informed Decisions On Plant-Specific Changes to the Licensing Basis (Draft DG-1061 issued 6/97) (Issued with SRP Chapter 19) -- 07/1998

(6) USNRC Regulatory Guide 1.175 An Approach for Plant-Specific, Risk-Informed Decisionmaking: Inservice Testing (Draft DG-1062 issued 6/97) (Issued with SRP Chapter 3.9.7) -- 08/1998

(7) USNRC Regulatory Guide 1.176 An Approach for Plant-Specific, Risk-Informed Decisionmaking: Graded Quality Assurance (Draft DG-1064 issued 6/97) -- 08/1998

(8) USNRC Regulatory Guide 1.177 An Approach for Plant-Specific, Risk-Informed Decisionmaking: Technical Specifications (Draft DG-1065 issued 6/97) (Issued with SRP Chapter 16.1) -- 08/1998

(9) USNRC Regulatory Guide 1.178 An Approach For Plant-Specific Risk-informed Decisionmaking Inservice Inspection of Piping (Draft DG-1063 issued 10/97) (Issued with SRP Chapter 3.9.8) -- 09/1998

(10) Himanen, R., Toivola, A., PRA Program on NPP TVO. PSAM, Los Angeles, February 1991.

(11) PSA Peer Review Certification Implementation Guidelines, BWROG, Revision 3, January 1997.

(12) Himanen, R., Vaurio, J., Virolainen, R., Introduction of Living PSA in Finland - cooperation between Utilities and Authorities. 3rd TüV-Workshop on Living PSA Application, Hamburg, May 1992.

RISK FOLLOW-UP
Oskarshamn 1 1996
(1996-01-01 -- 1996-11-01)

A practical way to use Living PSA

OKG Aktiebolag

Stefan Eriksson / Michael Landelius

September 1998 / April 1999

The purpose of conducting a risk follow-up study

- Evaluate the risk significance of occured events
- Search for suitable and effective improvements
- Support the verification as well as the updating of the PSA model and data

Data sources

- LER (Licensee Event Reports)
  - During 1996 there were 66 LERs, 8 of which effected the C.D sequences in the LPSA model for O1
- Disturbance Records
  - 9 planned shut-downs were performed and 5 scrams occurred
- Test Records
  - 631 test records were reviewed (Basic events)
    - » TI 95 parameters
    - » TF 97 parameters
- Plant Operations Procedures
  - Information about test procedures

Problems

- Collect useful information
  - Where to find all the necessary information: LER, test records, disturbance records etc
- To conclude whether a certain failure may have been a CCF or not
- Risk-Spectrum
  - Quantification - One run for each IE and end state (HS2, HS3)⇒
    - » Many runs !
    - » The handling and evaluation of results from the runs (One data point for each day in every run)
    - »
- The PSA-O1 model in Risk-Spectrum
  - All LERs are not possible to implement - About 1/5 is possible to model (8 of 66 LERs)

ASSUMPTIONS

- The components' actual test-interval have not been possible to model
- Outcomes of the tests (if the component had failed) were not modeled
- Manual testing of components and activation of components during disturbances has not been taken credit for
- Activation of components during cold shut down and hot stand by has not been taken into account

Model modifications

- STEP 1: System configuration modelling
  - Specify the house events that are to be set TRUE to "switch in" the model variation that covers the particular plant configuration
- STEP 2: Test modelling
  - Periodize the model from the "0-timepoint"
    - » Set a 0-time point
    - » Adjust the parameter TF (Time to first test) for each component
- STEP 3: Failure and maintenance modelling
  - Model modifications due to components that are out of service, due to failures or maintenance

Analysis proceeding - Risk Follow-up

Analysis in two steps:

1. MCS analysis

2. Time dependent analysis

Many quantifications

- Due to pump changes (4 different model variations)
- 8 LERs to run

LERs possible to evaluate in the PSA model

- Rotating converter failures:
  - 677 MG132 (960126)
  - 677 MG132 (960611)
  - 675 MG121 (961027)
- Bus bar failure (Double earth fault):
  - 677 A0,2 S1 (960928)
- Pump failure:
  - 721 P1 (961007)
- Valve failure:
  - 314V13 (960722)
- Pressure transmitter failure:
  - 211K125 (960808)
  - 211K125 (960815)

Results from the Risk follow-up

- Two "0-profiles" for consequence HS2 (Core cooling function) and HS3 (Residual heat removal)
- Two actual Risk profiles for O1 during 1996
  - CDF-variations End state - HS2 (Core cooling function)
  - CDF -variations End state - HS3 (Residual heat removal)
- A methodology-model

"0-profiles" (Without any failures)

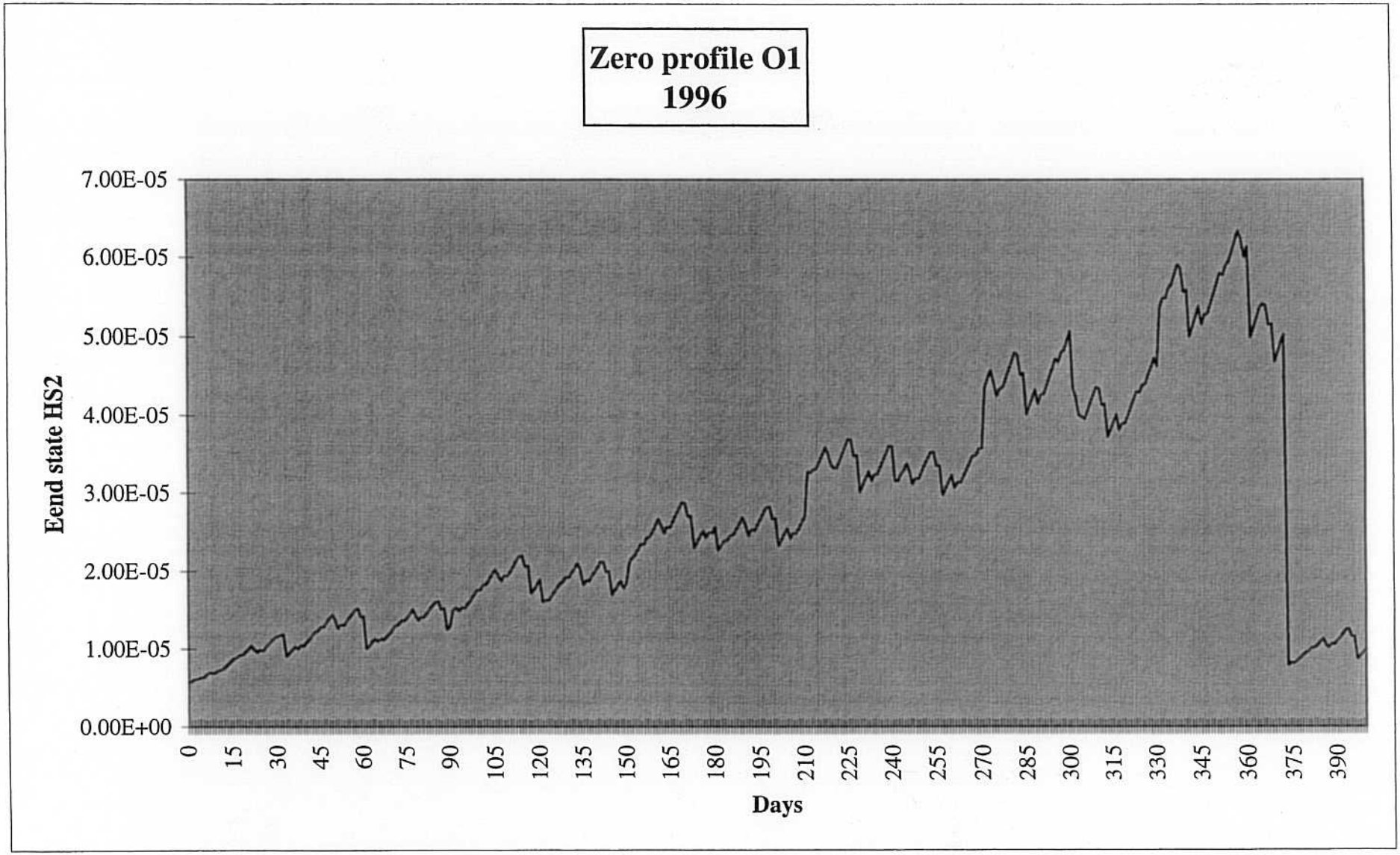
- Consequence HS2 (Core cooling function)
- Consequence HS3 (Residual heat removal)

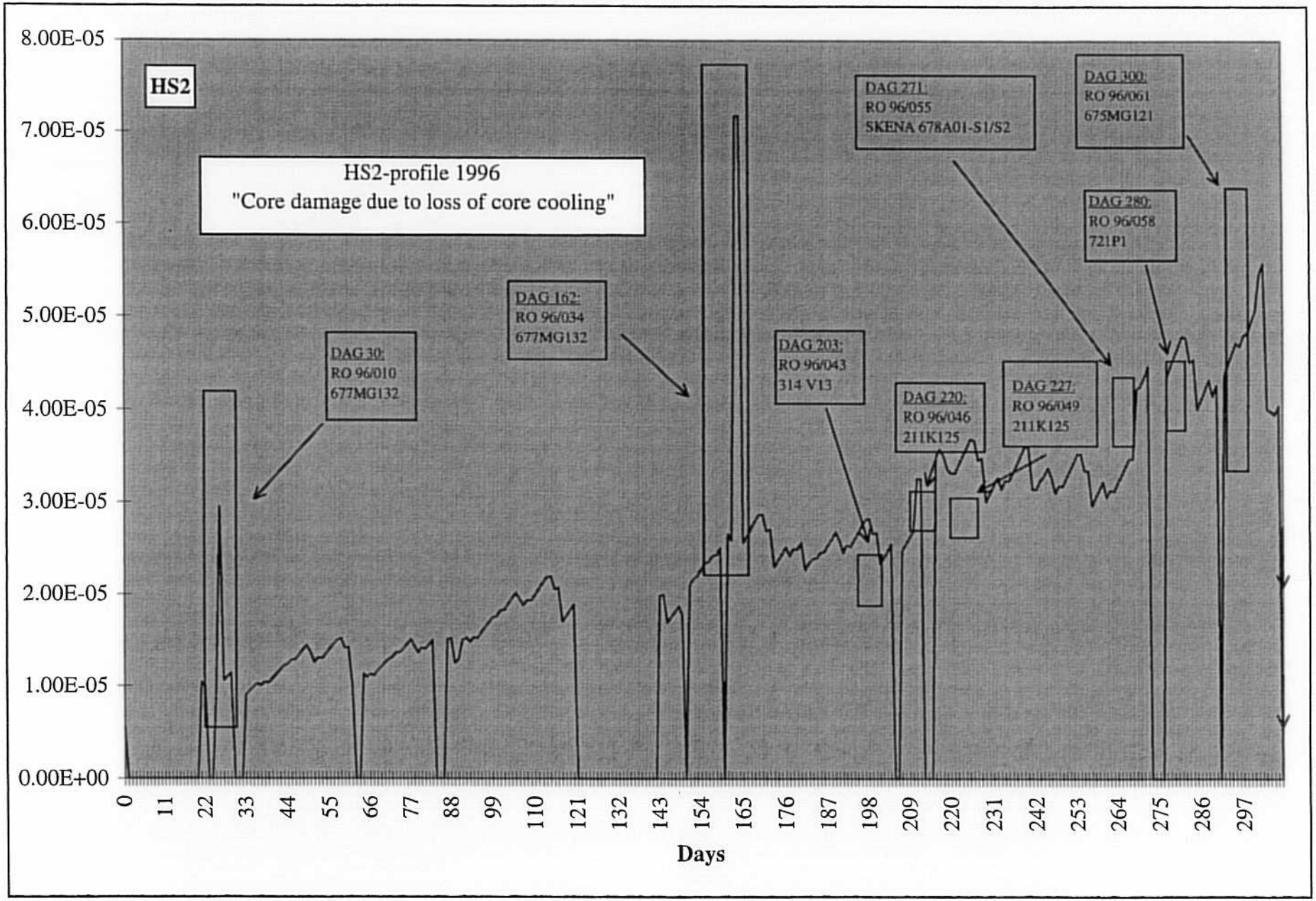
"Risk-profiles" (With failures)

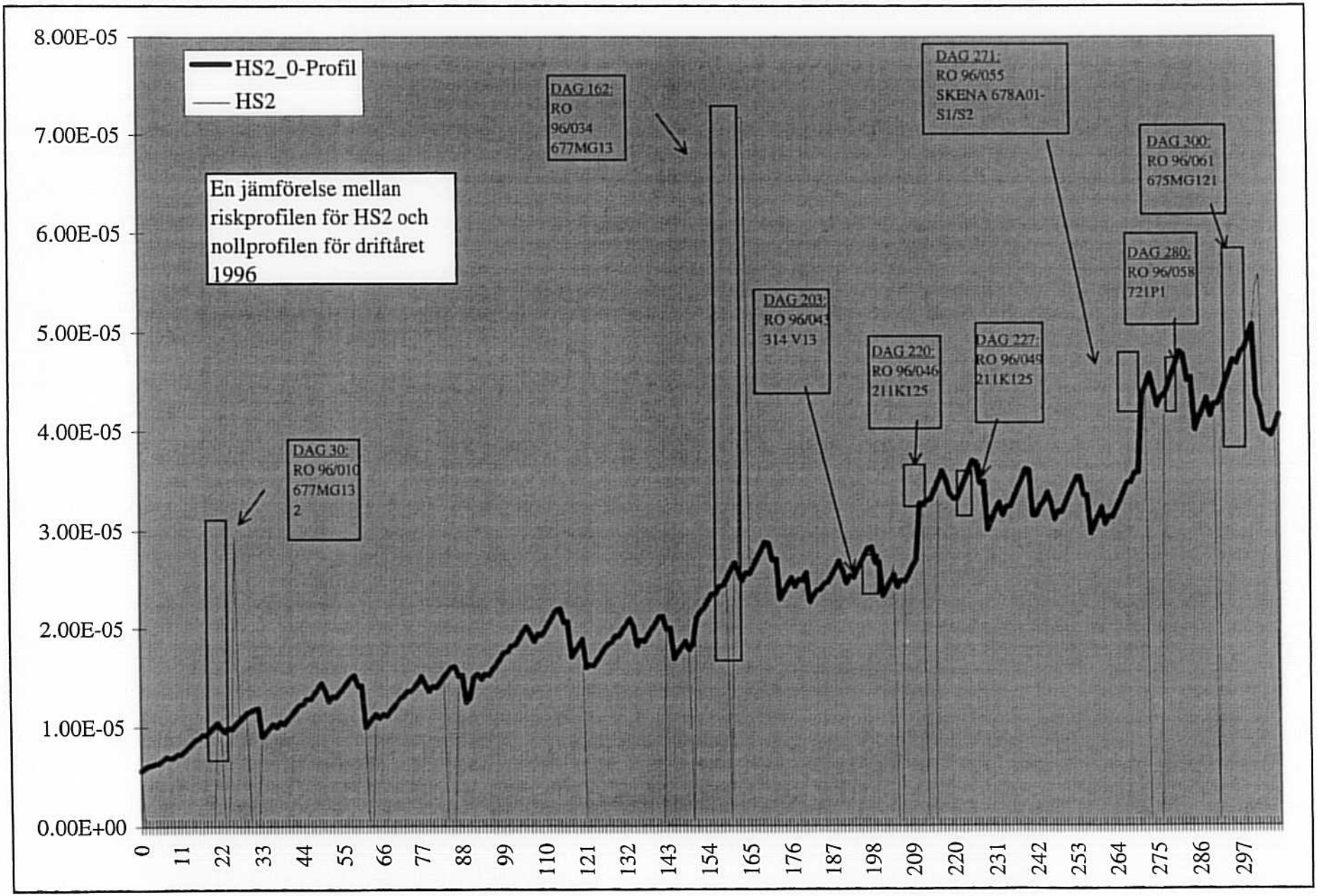
- *Consequence HS2 (Make-up water supply)*
- *Consequence HS3 (Residual heat removal)*

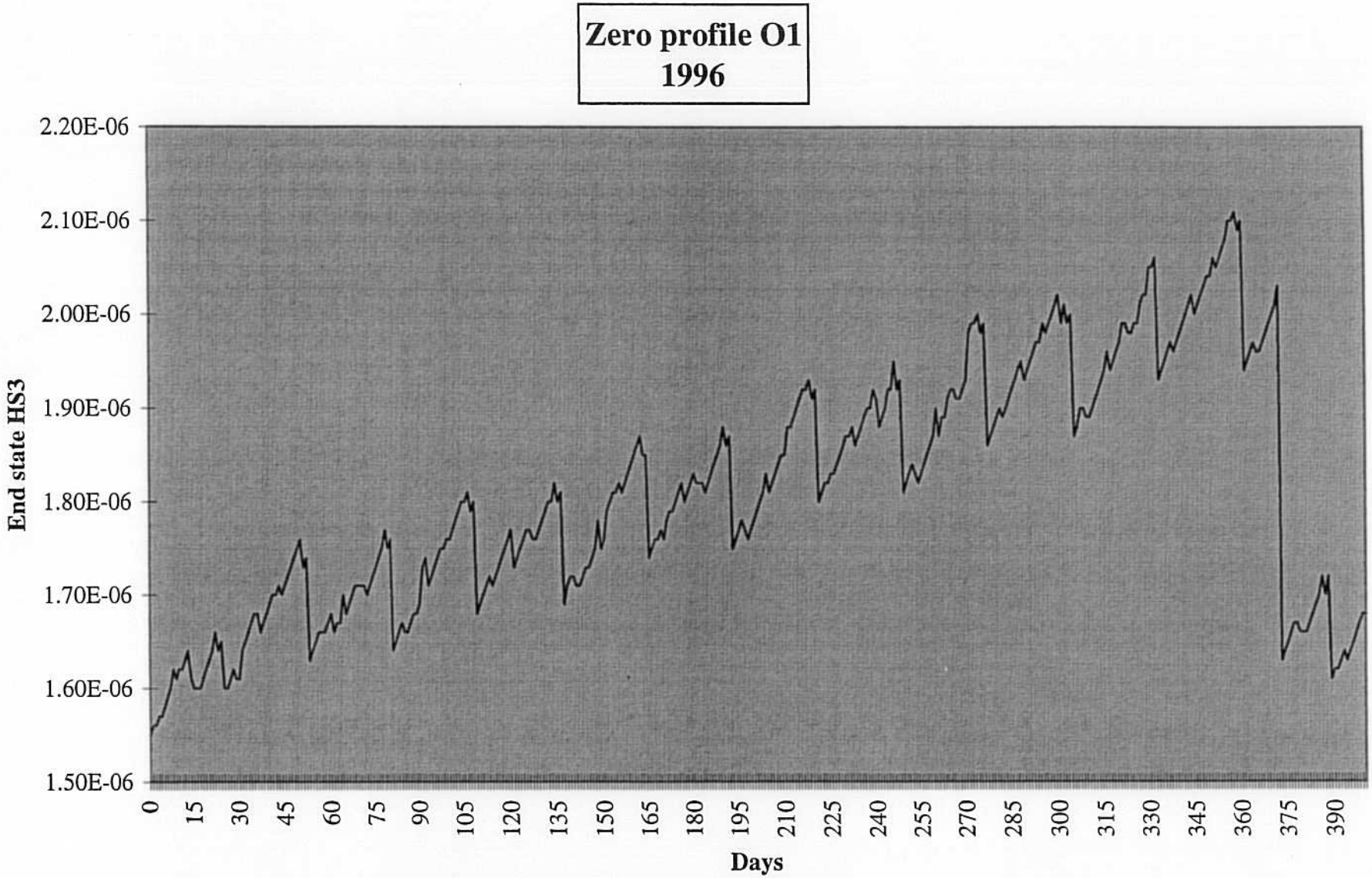
Future LPSA-work at OKG

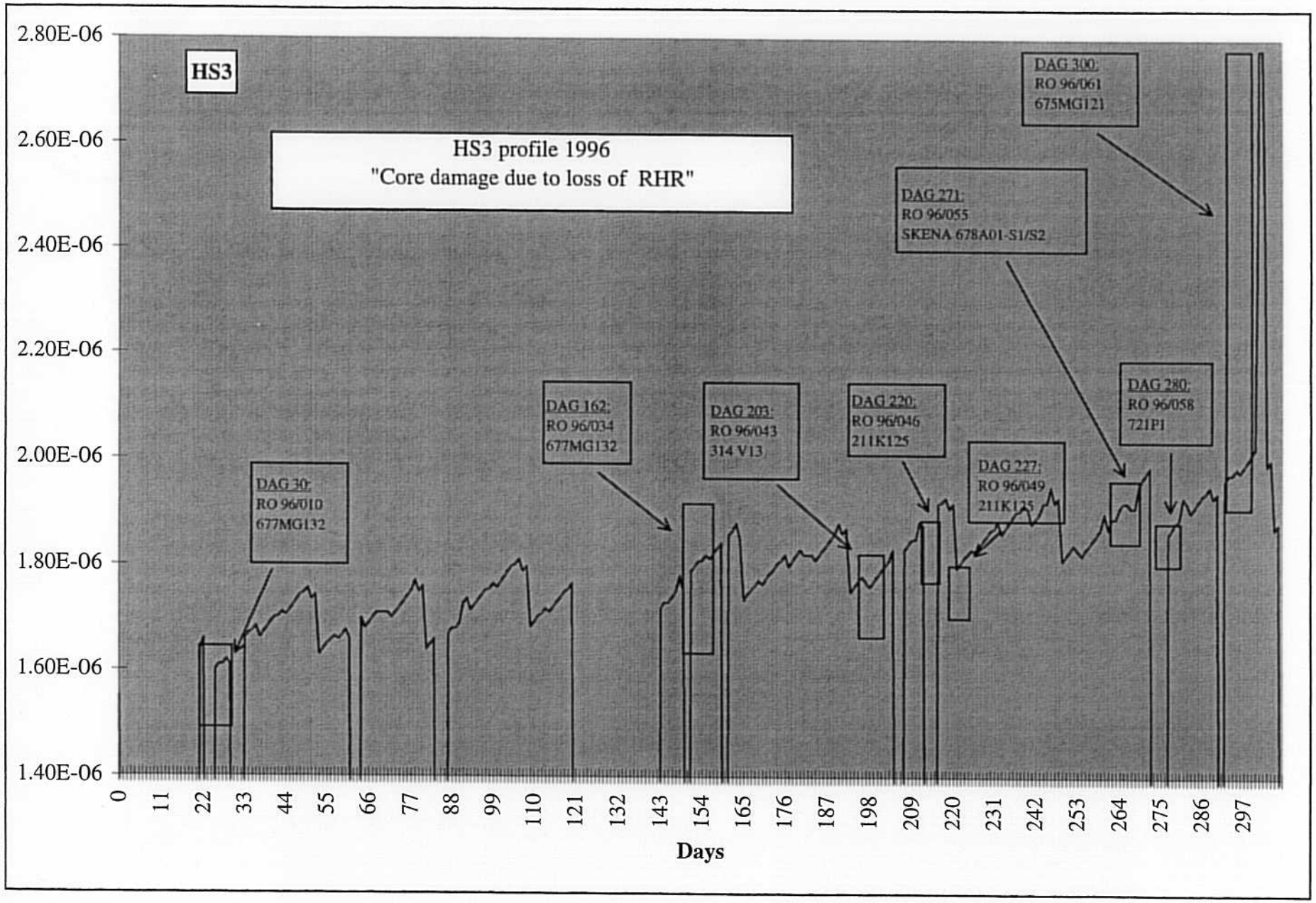
- A risk follow-up study for Oskarshamn 1 1997/1998, ongoing
- A risk follow-up for Oskarshamn 2 is planned for the season 1998/1999
- A risk follow-up for Oskarshamn 3 1998/1999 is not yet planned for the moment
- More accurate and better evaluation of risk follow-up results is expected due to the new PSA program PSA Professional

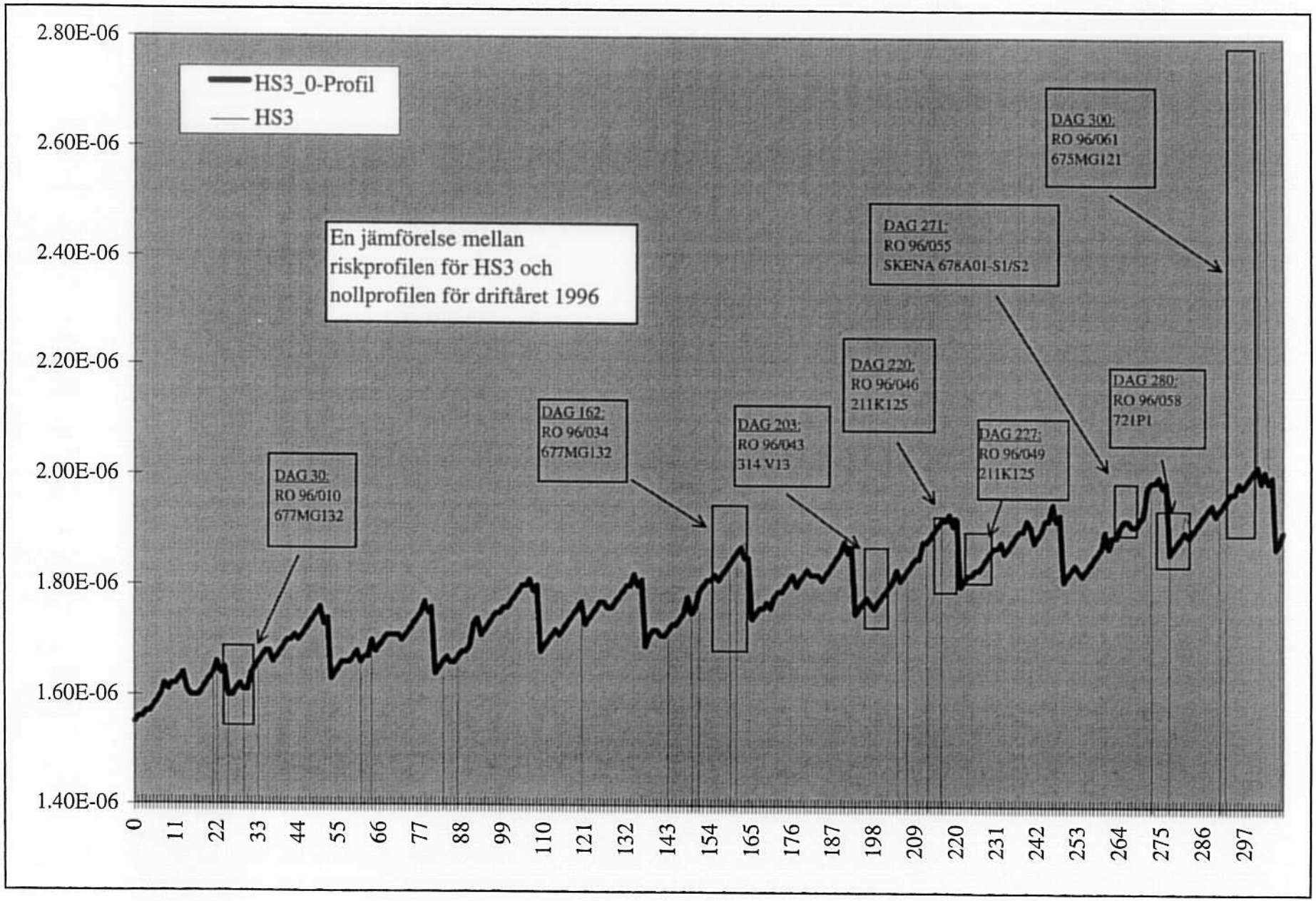

Zero profile O1
1996
Eend state HS2
7.00E-05
6.00E-05
5.00E-05
4.00E-05
3.00E-05
2.00E-05
1.00E-05
0.00E+00
0
15
30
45
60
75
90
105
120
135
150
165
180
195
210
225
240
255
270
285
300
315
330
345
360
375
390
Days


HS2
HS2-profile 1996
"Core damage due to loss of core cooling"
DAG 30:
RO 96/010
677MG132
DAG 162:
RO 96/034
677MG132
DAG 203:
RO 96/043
314 V13
DAG 220:
RO 96/046
211K125
DAG 227:
RO 96/049
211K125
DAG 271:
RO 96/055
SKENA 678A01-S1/S2
DAG 280:
RO 96/058
721P1
DAG 300:
RO 96/061
675MG121
8.00E-05
7.00E-05
6.00E-05
5.00E-05
4.00E-05
3.00E-05
2.00E-05
1.00E-05
0.00E+00
0
11
22
33
44
55
66
77
88
99
110
121
132
143
154
165
176
187
198
209
220
231
242
253
264
275
286
297
Days


HS2_0-Profil
HS2
En jämförelse mellan riskprofilen för HS2 och nollprofilen för driftåret 1996
DAG 30:
RO 96/010
677MG13
2
DAG 162:
RO
96/034
677MG13
DAG 203:
RO 96/043
314 V13
DAG 220:
RO 96/046
211K125
DAG 227:
RO 96/049
211K125
DAG 271:
RO 96/055
SKENA 678A01-
S1/S2
DAG 280:
RO 96/058
721P1
DAG 300:
RO 96/061
675MG121
8.00E-05
7.00E-05
6.00E-05
5.00E-05
4.00E-05
3.00E-05
2.00E-05
1.00E-05
0.00E+00
0
11
22
33
44
55
66
77
88
99
110
121
132
143
154
165
176
187
198
209
220
231
242
253
264
275
286
297


Zero profile O1
1996
2.20E-06
2.10E-06
2.00E-06
1.90E-06
1.80E-06
1.70E-06
1.60E-06
1.50E-06
End state HS3
0
15
30
45
60
75
90
105
120
135
150
165
180
195
210
225
240
255
270
285
300
315
330
345
360
375
390
Days


HS3
HS3 profile 1996
"Core damage due to loss of RHR"
DAG 30:
RO 96/010
677MG132
DAG 162:
RO 96/034
677MG132
DAG 203:
RO 96/043
314 V13
DAG 220:
RO 96/046
211K125
DAG 227:
RO 96/049
211K125
DAG 271:
RO 96/055
SKENA 678A01-S1/S2
DAG 280:
RO 96/058
721P1
DAG 300:
RO 96/061
675MG121
2.80E-06
2.60E-06
2.40E-06
2.20E-06
2.00E-06
1.80E-06
1.60E-06
1.40E-06
0
11
22
33
44
55
66
77
88
99
110
121
132
143
154
165
176
187
198
209
220
231
242
253
264
275
286
297
Days


HS3_0-Profil
HS3
En jämförelse mellan riskprofilen för HS3 och nollprofilen för driftåret 1996
DAG 30:
RO 96/010
677MG132
DAG 162:
RO 96/034
677MG132
DAG 203:
RO 96/043
314 V13
DAG 220:
RO 96/046
211K125
DAG 227:
RO 96/049
211K125
DAG 271:
RO 96/055
SKENA 678A01-S1/S2
DAG 280:
RO 96/058
721P1
DAG 300:
RO 96/061
675MG121
2.80E-06
2.60E-06
2.40E-06
2.20E-06
2.00E-06
1.80E-06
1.60E-06
1.40E-06
0
11
22
33
44
55
66
77
88
99
110
121
132
143
154
165
176
187
198
209
220
231
242
253
264
275
286
297

USE OF DIFFERENT SAFETY METHODOLOGIES

FOR THE DEVELOPMENT OF REACTOR SAFETY

AT LICENSED PLANTS

Risk-based evaluations

a complement

to other techniques

By Göran Hultqvist-FKA

NKS-seminar 99-04-13/14 and

DEVELOP THE DESIGN OF EXISTING PLANTS

it is important to withstand the demands from the authority and the public

Weaknesses in the plant design and higher demands on the plant are the bases for this development

METHODOLOGIES TO DEVELOP THE REACTOR SAFETY

at the plant can be based on

-operating experiences (LER-, RO-reports)

-implementing modified or new guides/ norms

- **evaluation of PSA-studies**

- **design of new reactor plants**

WHICH REACTOR SAFETY TECHNIQUE IS MAINLY USED

WHEN MODIFICATIONS ARE INTRODUCED ?

Each plant is licensed based on deterministic rules and a safety analyses and evaluation of research work documented in the FSAR.

The basic demands are developed from the General design criteria (GDC).

THE GDC ARE VERY GOOD RULES TO DEVELOP REACTOR SAFETY FROM.

1. OPERATING EXPERIENCES from the own plant
(2-4 years to implement a modification)

The modification is initiated from component or system failure in the plant

-Existing performances do not follow the demands from the deterministic design rules described in the FSAR.

Modifications are developed based on deterministic rules and techniques.

No PSA –evaluations are performed and is not necessary to perform.

2. EVENTS FROM OTHER PLANTS
(5-8 years to implement a modification)

The new knowledge are evaluated against
-the existing FSAR
- norms/guides
-performed safety analysis (calculations)

The modifications are developed based on a deterministic design technique and in some cases research work

The FSAR-norms are followed and specific new norms are used.

PSA-evaluations are performed to support the decisions if the modifications are very expensive

3. AUTHORITY DEMANDS
(2-5 years to implement a modification)

The demands are followed.

Modifications are developed based on

-deterministic rules and technique supported by research work to develop new knowledge

PSA evaluation are not performed.

4. PSA-EVALUATIONS
(5- 10 years to implement a modification)

The results from PSA –studies are evaluated and the frequencies for the main cut-set for core damages and high release rate shall be reduced

The modifications are developed based on a
-deterministic design technique

The FSAR-norms are followed and specific new norms are used.

Different solutions are evaluated by PSA-technique

5. NEW NORMS/guides

(5-12 years to implement a modification)

The benefits of the new norms are evaluated against
-existing FSAR
-modern plants
-new demands or coming demands from the authority
-experiences at the plant

The modifications are developed based on a deterministic design technique

The FSAR-norms are followed and specific new norms are used.

PSA-evaluations are performed if the modification is very expensive

6. DESIGN OF NEW PLANTS

(5-12 years to implement a modification)

The benefits of the new norms are evaluated against
-existing FSAR
-modern plants
-new demands or coming demands from the authority
-experiences at the plant

The modifications are developed based on a deterministic design technique

The FSAR-norms are followed and specific new norms are used.

PSA-evaluations are performed if the modification are very expensive

EXAMPLES FROM FORSMARK.

EVENT/ MODIFICATION	FIRST INITIATED FROM	SECONDLY INITIATED FROM	COMMENTS
CLOGGED STRAINERS/ CHANGE OF INSULATION TO METALLIC INSULATION	Barsebäck event	Authority letter	Norms inaccurate Knowledge inaccurate Research work needed No PSA evaluations
Diversified 314-blowdown system	Operating experiences from Holland and implementation in German reactors (PSA –evaluated in Germany)	Implemented in new reactors (Oskarshamn 3) Main cut-set in Forsmark 3-PSA-study	The scope was broadened during design and other weaknesses in the FSAR for plant where eliminated No PSA evaluation for F1/F2
No stop for 323 on H2-level in reactor vessel	Initiated based on safety philosophy that system shall not be stopped during an accident and to introduce diversification of system 321 for cooling the reactor during shutdown		Supported by PSA-calculations
Modification of level measurement in reactor vessel	Lack of qualifications and research work		Research work and safety analysis performed No PSA -evaluation
Modifications of system 649-converters for main circulation pumps	Ageing of components	Demands from deterministic analysis and design rules	No PSA -evaluation
Modification of tubes and valves in system 321	Cracks, and cost for in-service inspections		No PSA-evaluation
Modifications of controller	Ageing of components	Higher availability and changes of events to other event classes. Lower demands on safety systems	No PSA-evaluation
Severe accident upgrades	Authority demands	Operating experiences from TMI and Chernobyl	No PSA –evaluation

CONCLUSIONS

PSA is mainly used to evaluate the necessity to introduce modifications when they are very expensive and to support modifications when they have effect on operating instructions.

The main cut-sets for core damages in level 1 and 2 studies are evaluated to be eliminated or their frequencies reduced.

The main source for modifications are

OPERATING EXPERIENCES

TIME TO IMPLEMENT

It takes a lot of time to implement a modification in a plant.
1.The necessity has to be defined
2.The cost has to be accepted.

-The analysis of different options for modification has to be evaluated.

-Complementary research work has to be performed in some cases.

-Calculations have to be performed to develop technical specifications

-Analysis has to be performed to evaluated consequences on other systems and sequences.

-Purchasing and construction has to be performed.

-Verifications/validations has to be performed.

This process takes at least
2 years
and can in specific cases take more than 10 years.

WHY IS NOT PSA THE MAIN SOURCE FOR DEVELOPING THE DEMANDS ON MODIFICATIONS?

1. **PSA is based on the deterministic evaluations**
2. **PSA is based on the research work performed for the deterministic analyses**
3. **PSA has no specific failure rates for components acting in severe situations**
4. **The failure rates in PSA come from operating experiences.**
5. **The PSA has set the demands on system and components for much longer time than they are needed (often 24 hours) This makes the studies less realistic.**

PSA should be used to

- **develop the basis for the deterministic safety analysis by classify the different events into different event categories.**
- **modify the event into different event categories as new failure rates are published**
- **evaluate the necessity to modify the plant by introducing more redundancy or more diversification**

These are very costly modifications and have to have support from all kinds of evaluations to verify that they are cost-effective.

The main sources for modifications of plant has to be
The *deterministic analysis* of the plant based on

1. **Operating experiences from the own plant**
2. **Operating experiences from other plants or research work**
3. **Demands from authorities and the public**

The PSA is a complementary tool that shall be used to support decisions

NKS/SOS-2 Seminar on Risk Informed Principles. 13 - 14 April 1999

Applications of Risk Informed Principles at BKAB

Ingemar Ingemarson, Barsebäck Kraft AB

Summary

BKAB has developed a detailed and useful model for PSA Level 1 that was finished in the beginning of 1999. The PSA-model has already been used in several activities as a tool to form the basis for risk-informed decisions. First of all it is used to reduce the risks that have been identified in the PSA Level 1 but there are plans to use it in justification of criteria in the technical specification, in in-service inspection with focus on the reactor pressure boundary piping and in classifying critical components.

1 Introduction

Barsebäck Kraft AB (BKAB) performed its first PSA (Probabilistic Safety Assessment) Level 1 in 1984 in connection with the first ASAR (As Operated Safety Analysis Report) for BKAB. This study was updated in 1987 and 1991. It was later revised in 1995 and incorporated in the second ASAR, ASAR-90, that was delivered to SKI in 1995. In ASAR-90 a PSA Level 2 was also conducted. The PSA Level 1 in ASAR-90 was underdeveloped and had to be updated according to current requirements on degree of detail. It also had to be extended with a "close-to-reality" fire and flooding analysis and contain a start-up and shutdown analysis. The work with this PSA Level 1 started in 1996 and was completed in the beginning of 1999. This PSA is not actually an update of earlier BKAB PSA but more an adaptation of the PSA Level 1 for OKG´s NPP O2 that was under work at the time being and that will be concluded in the late 1999.

BKAB has also started the work with updating the PSA Level 2.

2 Some Characteristics of BKAB:s PSA Level 1

The PSA Level 1 model has a great level of detail in order to cover all dependencies that exists between different systems and components. Especially two areas have been surveyed in detail: the power supplies distribution with corresponding fuses and cable routings and the RCPB (Reactor Coolant Pressure Boundary)-piping.

Table 1 *Comparison between the new and older PSA Level 1 for BKAB for some characteristics in the PSA models*

Number of	PSA Level 1 for B1 (okt-98)	PSA Level 1 in ASAR-90
Systems	54	17
Components	1 500	150
Process-sensors	500	50
Fuses (MCB)	1 600	0
Fault-tree-pages	5 000	308

Two types of initiating events that was not covered in the earlier analysis have been incorporated in the current PSA: CCI (Common Cause Initiators) and internal fire and flooding. It was a tedious work to expand the analysis with these events since they require a systematic and complete mapping of supply- and service-systems with the corresponding control logic, power supply and cabling. Both these types of initiating events are associated with extensive uncertainties in their contributions to the resulting CDF (Core Damage Frequency). To some extent this uncertainty is caused by the large degree of development in the analysis. When large portions of the PSA-model are expanded in a way that completely new areas are incorporated, it takes both time and effort to consolidate the PSA-model and to stabilise the outcome.

Plant specific and individual PSA-models for both B1 (Barsebäck 1) and B2 (Barsebäck 2) have been produced. Three separate models have been developed: Internal events, fire and flooding and start-up/shut-down. The PSA-models for internal events and fire and flooding are going to be merged during 1999. The PSA-models are all built with the tool Risk Spectrum PSA Professional.

BKAB's PSA Level 1 is based on IAEA's guide for PSA Level 1 (Safety Series No. 50-P-4) and on PSA Level 1 for O2 (Oskarshamn 2). Further it is also based on a set of task descriptions covering the most important steps in performing the work focusing on the survey of the plant, fire- and flooding and the documentation.

The LOCA (Loss of Coolant Accident)-analysis is based on a detailed survey. The RCPB-piping has been broken down into about 3000 potential pipe rupture locations like bends, welds, suspensions, T-pieces etc. For each such location the frequency for rupture and guillotine break has been assessed.

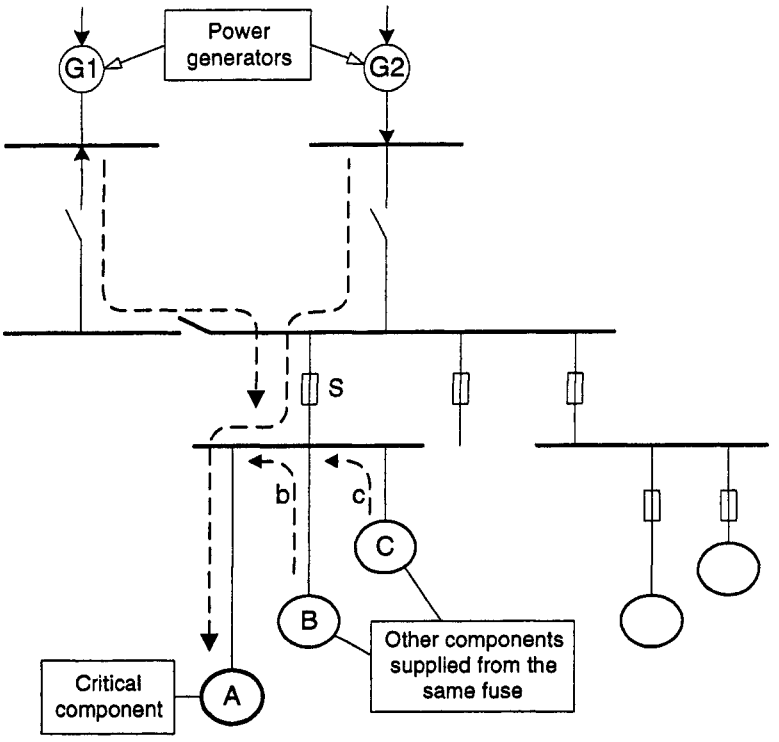


Figure 1 *Example on how the power supply routings must be surveyed for a single critical component*

Through FMEA (Failure Mode and Effects Analysis) all critical components with support systems have been identified. A critical component has a failure mode that is depicted in the PSA-model. For these critical components all necessary power supplies and control logic have been analysed in detail covering also the power supplies that can affect transducers, breakers etc. Further all fuses that feed current to critical components have been identified and also all cables that connects fuses, control logic and critical components.

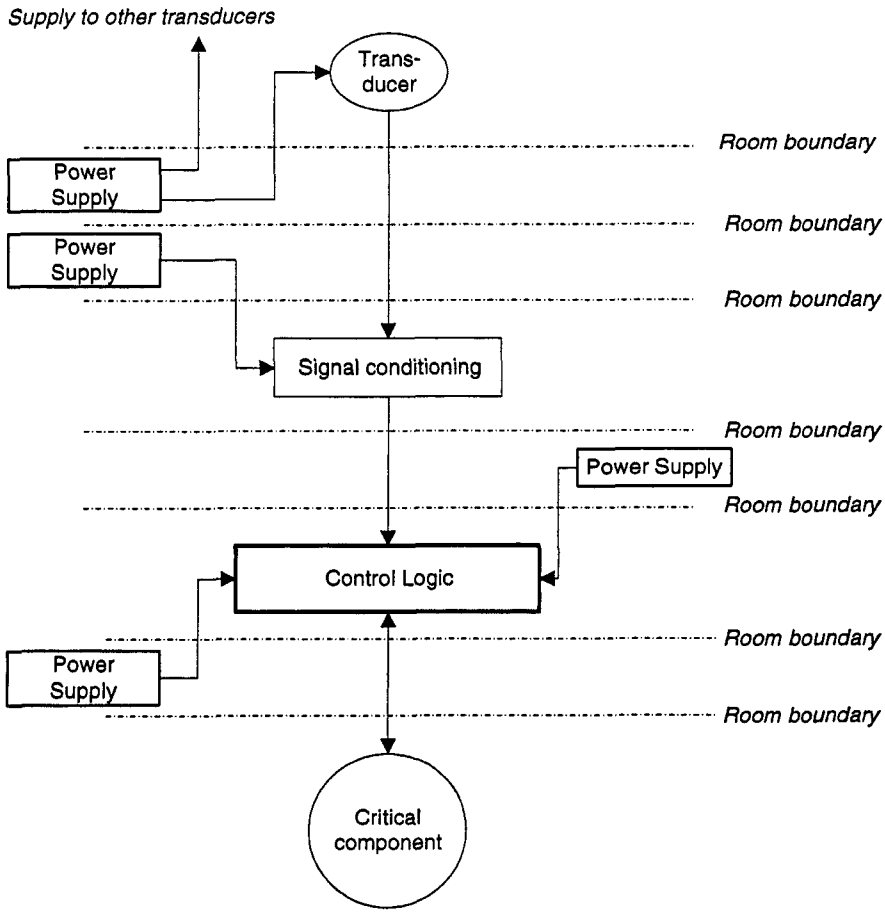


Figure 2 *A component can be dependant on the power supplies from several different sources*

Figures 1 and 2 above give an indication on how important it is to map all the relevant power supply sources with the corresponding cable routings.

The fire analysis is based on a model that is shown in figure 3 below.

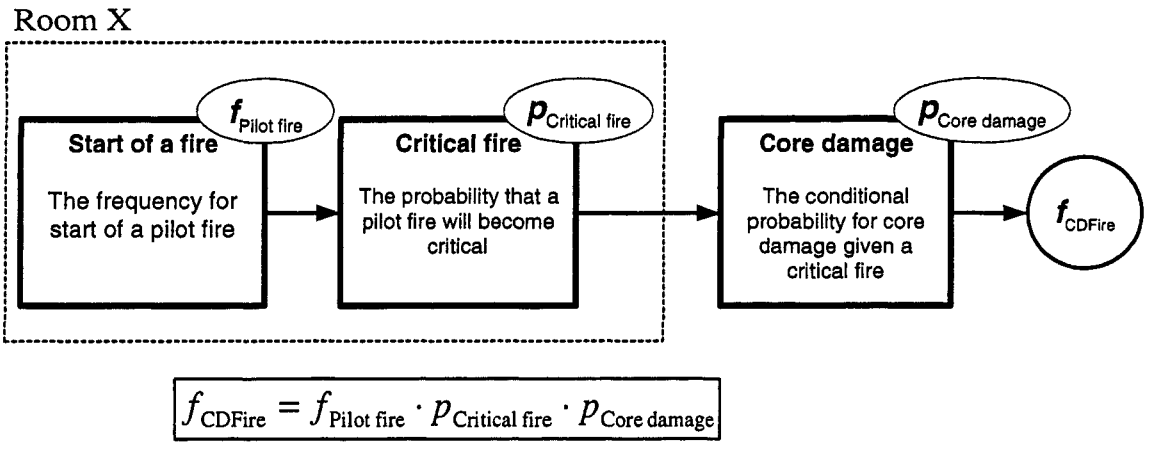


Figure 3 *The basic model for fire analysis in BKAB:s PSA Level 1*

The flooding analysis is based on a similar model.

3 Areas of use

The ambition is that the PSA shall continuously reflect the state of the plant and so be updated according to the changes that are made in hardware, maintenance and operation. All the necessary means for this work is not yet in place but there are several activities going on to improve routines and tools. A living PSA requires appropriate documentation of the plant, maintenance routines and operational experiences that can be accessed without unnecessary obstacles.

3.1 Support for plant modification

The current PSA Level 1 has been used as a tool for plant upgrading and modification since the beginning of 1998. Ideas and proposals regarding modification of both hardware and software that has some impact on safety are tried out with the PSA-model. This work is done in some sort of iterative process in an attempt to frame the most optimal solutions. A detailed PSA-model is sensitive to changes in that a change in one system can effect properties in several other systems.

The following activities have been performed or are ongoing.

- Dependability analysis of the cooling water intake and adjoining systems
- Supplying room ventilation and equipment in that room from the same auxiliary power-source (Safety Injection System and Auxiliary Feedwater System)
- Improved reliability performance for some DC-power supply systems at external power black-out
- Enhancement of the barriers against fires in rooms containing electrical equipment
- The impact from high- or low seawater level on the cooling water intake

There are also few other minor analyses performed.

3.2 Evaluation of ideas and proposals for modernisation

One clear objective with the current PSA Level 1 was that a PSA-model should be available at the beginning of 1998 for use in the TRIM-project. TRIM stands for the modernisation of the three sibling plants O2, B1 and B2 of ASEA Atom design. The objective with TRIM is to update and maintain the safety level of the plants for another 25 years of operation. Modification proposals from different manufacturers have been incorporated in the PSA-model and the impact on the result has been evaluated. This work was performed in close co-operation with OKG and with the assistance of the consulting firm RELCON.

The results were later presented to the manufacturers for feedback. The work is finished and the experience from the outcome is positive.

There is an advantage in not letting the individual manufacturers perform their own PSA but instead using the same team that apply the same modelling principles to all proposals. In this way it is easier to evaluate the different solutions.

4 Future plans

4.1 Consolidating the process of updating PSA

The main effort for the nearest future, e.g. the coming year, is to consolidate the whole process of keeping the PSA living. PSA involves a large amount of data processing and this has to be performed in an efficient way. Several activities at the plant will be more or less involved and the requirements from the work with PSA compete with other urgent needs. The best foundation is when the technical documentation is correctly updated and adapted to the needs of PSA. PSA also requires an updated, complete and available SAR (Safety Analysis Report). The interface between SAR and PSA has to be clear.

One planned project is to compile all FMEA in one database and supplement it with other relevant information like test-procedures and intervals, failure data etc.

4.2 Risk-based in-service inspection

Risk-based in-service inspection is focused on the RCPB-piping.

BKAB has in co-operation with SKI supported a research project where empirical data on piping failures from NPPs all over the world is combined with plant specific data in an effort to estimate unique pipe rupture frequencies for all the potential pipe rupture locations in the RCPB. The project is called B-LAP (Barsebäck 1 – LOCA Affected Piping) and the outcome of the project will be published in the coming SKI Report 98:30. The survey of the RCPB piping has in this project been extended even more in detail and counts about 4000 different locations. These new pipe rupture frequencies will further on replace the old ones that are based on data from WASH-1400.

The LOCA analysis in a PSA is based on the same information that is used in classifying the piping for in-service inspection. The pipe rupture frequencies correspond to the *damage category* and the CDF corresponds to the *consequence category*. At BKAB there are on going discussions to merge the information from PSA and in-service inspection. This will take both time and effort and must be achieved without any risks for unstable results.

4.3 Evaluation of criteria in the technical specifications

The technical specification for B1 and B2 shall be updated in accordance with the new SAR. As an option to this task the PSA- model shall be used to verify some parts of this work. BKAB has an advantage in that the start-up and shut-down sequences already are modelled in the PSA.

4.4 Risk follow up

The objective is to use the PSA-model to assess the safety impact from events that have occurred. In this way the risk from day to day can be monitored. There are several aspects on this type of activities. The work is tedious and the outcome in most cases just confirms what you already know. But it is good way to be familiar with the PSA-model and it can be a complement to the risk measures that are used today.

4.5 Classification of critical components

A detailed FMEA completed with additional information and used in combination with the PSA-model can be used to identify the safety importance for different components and the corresponding failure modes. This is useful for classifying components and for input to maintenance strategies and plans.

5 Needs for development

The tools and routines for information processing must be improved for cost efficiency. As much as possible shall be incorporated in the daily work with the technical documentation. A handful of key persons at the plant must be allocated for the different tasks: LOCA analysis, function- and system analysis, close co-ordination with maintenance and operation, easy access to data from process, operation and maintenance, efficient system for information and document handling. It should be as easy as possible to keep the PSA updated then there will be more time available for using it as a tool for safety improvements.

6 Conclusion

It requires quite a bit of effort to build and maintain a detailed PSA of sufficient quality and stability. But once you are there, the possibilities of application are many covering a wide range from cost-benefit analysis to risk-optimisation.

7 Literature

- *BVT PSA nivå 1. Sammanfattning*, Sydkraft Konsult, 1995-03-10, Diarienummer ES-9503m033, (in Swedish)
- *PSA Nivå 1 för B1 (okt-98). Sammanfattningsrapport*, BKAB 1998-12-09, D Nr T-9812-119, (in Swedish)
- *PSA Nivå 1 för B2 (okt-98). Sammanfattningsrapport*, BKAB 1999-02-08, D Nr T-9902-049, (in Swedish)
- "Rörbrott kan 'förutsägas' genom databasstudier", Nucleus 1/99, SKI, (in Swedish)
- *PSA Applications to Improve NPP Safety*, IAEA, 18 February 1998, Draft
- "An approach for using risk assessment in risk-informed decisions on plant-specific changes to the licensing basis", Reliability Engineering and System Safety, Vol. 63 No. 3 March 1999, p 231 - 242

RISK - INFORMED DECISION MAKING AT LOVIISA NPP

J. K. Vaurio
Fortum Power and Heat Oy
P.O. Box 23, 07901 Loviisa, Finland

1. INTRODUCTION

Loviisa nuclear power station is a two-unit plant with VVER-440 type reactors (model 213 PWR) in operation since 1977 and 1980, respectively. The plant is a hybrid of Western and Eastern technologies. The first Level 1 probabilistic safety assessment (PSA) was completed in 1989 for internal initiators at full power. Since then the scope has been extended to external events, and the work continues with focus on shutdown modes and level 2 studies.

PSA has been used continuously to identify dominating accident sequences and to develop plant modifications for safety improvement. Consequently, it has been necessary to update PSA annually and also merge new results from the expanded scope. PSA has also been used in many other ways for risk-informed decision making, as will be described.

The main focus over the period 1989-1999 was to identify risk-based plant modifications to reduce the core damage frequency (CDF) down to the level of an unofficial goal 10^{-4} /yr. These efforts are described in Section 2.

When the total risk is sufficiently reduced, one enters the region of diminishing return. It becomes more and more important to compare the costs and benefits of alternative decisions. The economic criteria developed at Loviisa plant are described in Section 3.

The same criteria apply to back-fitting decisions as well as to other applications concerning test intervals, temporary configurations, allowed outage times etc. Such applications are described in Section 4.

Ageing of nuclear power plants is an issue gaining more and more attention. Risk measures and reliability engineering techniques can be used in making ageing-related decisions, as described in Section 5.

2. PLANT BETTERMENT

Since 1989 the main objective of the PSA effort at Loviisa plant has been to identify dominating accident sequences and plant modifications to reduce the core damage frequency (CDF) down to the level of an unofficial goal 10^{-4} /yr. Fig. 1 indicates that this has been nearly accomplished by 1998.

Fig. 1 gives CDF-values at full power operation for internal initiators, floods, fires and severe weather phenomena, and the annual risk due to a refuelling outage (shutdown) for internal initiating events. Some of the values were estimated backwards in time from the years when partial PSA-studies were completed. The current risk values and the major plant modifications are listed below in Sections 2.1 through 2.5.

The following conclusions can be drawn from these back-fitting efforts:

- Dominating accident sequences and phenomena were quite plant-specific, with little possibility to learn from other plants (even with the same reactor type)
- Possible plant modifications were rather unique and often self-evident (few or no reasonable alternatives)
- New generic phenomena (ageing mineral wool insulation & boron dilution risk) caused major updating
- The driving force was the goal (CDF $\leq 10^{-4}$/yr) rather than balancing the risk-impact and the cost of a modification; nevertheless, cost-effective modifications such as changes in procedures or valve positions were often feasible.

2.1 PSA for Internal Initiating Events (IIE)

Fifteen plant modifications and several new or modified emergency operating procedures have been completed during 1989-1998 to reduce IIE-CDF from over 10^{-3}/yr to $1.5 \cdot 10^{-5}$/yr. The most important modifications were

- Improved air cooling system for instrumentation rooms, to reduce probability of spurious signals causing LOCA (1990)
- New sump strainers and a back-flushing system to prevent blockage of the ECCS sump by aged mineral wool insulation potentially released by LOCA (1993)
- Improved detection of primary coolant leakage outside of the containment via the coolant purification system (CVCS), and automated isolation of such leakage (1994)
- Reduction of risk due to steam generator (SG) leakage: automated isolation of a leaking SG, improved N^{16} detection, an additional pressurizer spray system and an additional emergency core coolant (ECC) tank (1994-1996)
- Modifications of the ECC system minimum flow lines to prevent alternating suction of the ECC between ECC tank and the sump (1996-7).

2.2 Flood PSA

Several modifications have been made to reduce CDF due to internal floods from $3 \cdot 10^{-4}$/yr (1994) below 10^{-5}/yr (1998). The main modifications were

- New wall (dam) to prevent turbine building floods from expanding to the reactor building basement through cable tunnels (threatening PCP seal cooling pumps and ECCS)
- Protecting feedwater system pipelines above the control building to reduce flood risk in the control and instrumentation rooms
- Improving drainage above the control and instrumentation rooms
- Re-routing service water and hydrant pipes to avoid floods in control and instrumentation rooms
- Moving up seawater system valve actuators and service water system pressure transmitters (in turbine building).

2.3 Severe Weather PSA

Several modifications have been made to reduce CDF due to severe weather such as high sea level, snow, storms, sea vegetation, frazil ice, extreme air & water temperatures, lightning (and combinations) from $4 \cdot 10^{-4}$/yr (1993) to $4 \cdot 10^{-5}$/yr (1998). The main modifications included

- Increased height of a temporary dam during refueling outages (high sea level risk)
- Improved detection and automated flow reduction in case of accumulating sea vegetation (blockage of sea- & service water flow)
- Redundant air-intake in the emergency diesel generator building (against blockage by snow or freezing rain)
- New procedures to remove the main condenser purification balls and ensure alternate intake of warmer seawater from the outlet side, in case of threatening icy, sub-cooled sea conditions.

2.4 Fire PSA

More than twenty protecting measures have been completed over the years 1989-1998 to reduce the fire risk from $7 \cdot 10^{-4}$/yr to $3 \cdot 10^{-5}$/yr.[3] Some changes were based on deterministic regulations, some on the estimated risk significance. Major changes included

- A new auxiliary emergency feed water system outside of the turbine building (the main FW and normal AFW system were vulnerable to turbine building fires in the original design)
- Separating the control building (and FW areas) from the turbine building by fire-walls
- Protecting high pressure hydraulic oil pipelines (to prevent oil jet fires)
- Protecting and re-routing critical cables
- Extension of the sprinkler system to cable areas and transformers

At present the control building contributes about 45% of the fire risk while the turbine building contributes 28%. In terms of room types, 32% is due to fires in cable areas or tunnels, and 17% is due to fires in process rooms. The risk is rather evenly spread around the plant.

In terms of accident sequences, about 44% of the fire risk is due to the primary coolant pump seal LOCA caused by loss of flow or cooling of the component cooling or service water. About 20 % is due to total loss of feedwater sequences.

2.5 Other PSA-related activities

A seismic PSA was completed in 1992 with conservative assumptions. Due to low seismicity the mean CDF was $3 \cdot 10^{-6}$/yr . No back-fitting was necessary.

A shutdown-state PSA for internal initiators during a normal refueling outage resulted[4] in CDF equal to $2{,}8 \cdot 10^{-5}$/yr. Half of this estimate is due to hoisting and transfer of heavy loads (pressure vessel lid and internals) inside of the containment building. Only limited possibilities have been identified so far for reducing the outage risk.

So far, level 2 PSA has been carried out for internal initiators and floods during full power operation. However, these are only predictions beyond year 2001 when a number of severe accident management backfittings will be completed. These include an ex-vessel system for cooling the core debris inside of the pressure vessel, installation of hydrogen recombiners and burners, and assuring timely operation of the ice-condenser doors. Means for primary pressure reduction and outside containment cooling have been installed. Some efforts are still needed to reduce the probabilities of containment bypass sequences.

Plans to reduce CDF even further include a separate residual heat removal system, and modifications to provide a redundant supply of the primary pump seal coolant. These are expected to reduce especially the fire and severe weather risks significantly, even beyond 24 hr mission times (cold shutdown).

3. COST/RISK CRITERIA

Economic criteria have been developed for tentative use at Loviisa NPP to decide which plant modifications can be justified on the basis of risk reduction vs. the cost of backfitting, and how to select an optimal combination from a set of possible modifications. Two risk-measures are used for a backfit or modification:

ÄCDF = change (reduction) of the core damage frequency (per year)
ÄLERF = change (reduction) of the large early release frequency (I, Cs ; per year)

The "expected benefit" of plant modification i can be presented as

$$R_i = \alpha\ \text{Ä}CDF_i + \beta\ \text{Ä}LERF_i, \qquad (1)$$

where α and β depend on the expected cost of an accident (including lost production), the remaining lifetime (n, years) and the interest rate (p). A proposed plant modification is justifiable if the cost C_i (investment and present value of future costs) is smaller that the expected benefit, i.e. $C_i < R_i$. In case of multiple choices for back-fitting measures, one should select the one with largest $R_i - C_i$:

$$R_i - C_i = \max! \qquad (2)$$

(Please observe that with k individual back-fitting options there are actually 2^k possible combinations of plant modifications to be compared, i.e. i = 1,2,... 2^k).[2]

In terms of c = annual cost of replacement power, taking into account that an accident can happen any year, one can calculate at least an approximate value $\alpha = b \cdot c$, where

$$b = \frac{1}{1+p} + \frac{2}{(1+p)^2} + \ldots + \frac{n}{(1+p)^n} = \frac{1-[(n+1)p+1](1+p)^{-n}}{p^2} . \qquad (3)$$

In case of Loviisa, assuming the remaining lifetime n = 20, interest rate p = 0.05 and the cost of replacement power 2.5 c/kWh yields $\alpha = 10^{10}$ \$. The same value can be obtained if one assumes the mean accident cost C_A equal to one billion dollars and $\alpha = aC_A$, where a is the discount factor $a = [1-(1+p)^{-n}]/p$. Typical values for the ratio β/α are 10...100.

Even if some of the parameters and assumptions in this formalism are uncertain, it provides a consistent way to rank alternatives. Usually the result is so clear that changing uncertain parameters somewhat would not change the conclusions. This was the case with virtually all backfitting measures mentioned in Section 2.

4. RISK-INFORMED APPLICATIONS

4.1 Limiting Backfitting of Motor Operated Valves

Opening and closing of a motor operated valve (MOV) is normally stopped by a limit signal and/or a torque limit switch. If the limit system fails, there is a danger that the valve jams or is damaged, causing internal or external leakage, especially if the valve is equipped with an oversized actuator. Loviisa plant has about 500 valve/motor combinations such that the maximum torque exceeds the

nominal strength of the valve structure in case the limits fail. Replacing all such valves or motors would cost several millions of dollars.

Detailed assessment of the reliabilities of the limit/switch systems, the ratios maximum torque/nominal strength, and the risk-significance of each valve, led to a significant reduction of the number of valve/motor combinations that needed to be changed. About 10 % of the valves contributed to more than 90 % of the risk, limiting the scope of modifications considerably.

4.2 Limiting Testing of Containment Isolation Valves

The containment isolation valves were originally tested for leak tightness once per year, and after any maintenance works. A task was given to the PSA project to identify groups of valves that could be leak-tested every other year instead of annually.

First, 52 valves (at each unit) were identified such that the maximum leakage in six latest tightness tests was no more than 20 % of the alarm limit. These were candidates for the extended test interval (ETI), and a reliability study was carried out to assess the additional risk due to ETI. The work was based on plant-specific failure histories. Based on the study of the failure causes, it was considered a good assumption that the tightness unavailability would double when doubling the test interval.

The acceptability of the test interval extension was studied line by line. The potential leak routes and leak sizes were evaluated (e.g. via closed or open systems). Based on the study, the extended test interval was approved for most of the 52 valves. Even if level 2 PSA has not yet been completed for this change, one can conclude that the relative risk-impact of the ETI is small.

4.3 Accepting Temporary Configurations

PSA has been used in several cases as a basis for accepting temporary configurations and other exceptions from Technical Specifications (TS), such as exceeding allowed outage times (AOT). Some examples:

- A check valve in the Chemical and Volume Control System was leaking slightly in excess of the leak rate limit specified in TS. Even under the conservative assumption that the valve would break in case of a certain medium LOCA initiator, the CD-risk increase until the next refueling outage would be less than $2 \cdot 10^{-7}$. Thus, plant operation was allowed without repair until the next refueling outage.

- A motor operated valve of the line used for warming up the ECC water was found to be failed. The valve could only be repaired during a long outage when the ECC tank is empty. A temporary rule of operation was issued, instructing the control valve in the same line to be kept normally closed. Conservatively estimated risk increase was $6 \cdot 10^{-7}$ /a. This additional risk was accepted until the next refueling outage.

- Certain pipe sections of the service water (SW) system were to be re-routed and replaced by a more durable material in order to reduce flood risks. The work was to be performed during power operation. It required certain parts of SW redundancies to be switched off consecutively for 5 days, preventing the air cooling of the emergency feed water pump rooms. Furthermore, one cooling unit of the instrumentation room ventilation could not be cooled for 5 hours. The additional risk was estimated to be as small as $8 \cdot 10^{-9}$ and the highest increase of CDF was about $7 \cdot 10^{-6}$ /a during those 5 hours, justifying the work.

- A containment internal spray system check valve under the ECC tank was found to be leaking. However, the CDF risk was estimated to be low, and repair was postponed until the next extended refueling outage.

- A crack was found in 1994 in a pressurizer spray system valve that is used for pressure reduction when the plant is shut down. This spray line has to be used when there is a need for rapid pressure reduction. Based on the assumption of a valve break in these situations the additional CDF was estimated to be almost $2 \cdot 10^{-4}$ /a, if the plant operation would be continued. The plant was shut down to replace this valve.

- Technical Specifications originally required in hot standby status that failure of any pump in emergency cooling (LPSI), containment spray, component cooling or service water systems has to lead immediately (in 8 hours) to cold shutdown of the plant.
  Assuming an AOT of 72 hours in hot standby (rather than cold shutdown) is equivalent to core damage probability of about 10^{-6}. Since this kind of situation is not expected to occur more frequently than once a year, the extended AOT is quite acceptable.

- The emergency power supply system of the plant includes four dedicated diesel generators (per unit). In addition, there is a power line to a nearby hydropower station, and two gas turbine power units on site.[5] The risk (CDF) due to a loss of offsite power event would be $3.6 \cdot 10^{-6}$/yr higher if the gas turbines were not available at all. Based on this and the cost criterion (Section 3) the gas turbines were sold to the national grid operator. Nevertheless, the gas turbines are still on site and available most of the time, if needed.

- A question was raised by safety authorities about the need to back-up the electric power supply to the auxiliary oil pumps lubricating the bearings of the motors of the primary coolant pumps. A detailed analysis pointed out that the risk reduction (CDF) would be only $2 \cdot 10^{-8}$/yr if the power supply were assured by DC batteries. This result satisfied the authorities and the question was dismissed. The economic criterion of Section 3 indicates that this kind of improvement is not justified if it costs more than $1000.

  About half a dozen other similar risk-informed decisions have been made in recent years.

Considering the goal 10^{-4}/yr for CDF, it is reasonable to approve temporary configurations and AOT until the next regular maintenance outage whenever the risk increase due to the temporary situation is less than $5 \cdot 10^{-6}$ /yr. Approval of delays up to one month are reasonable if the risk increment is between $5 \cdot 10^{-6}$ /yr and $5 \cdot 10^{-5}$ /yr, unless there is a serious threat to containment integrity (LERF) at the same time.

4.4 Risk-Informed Operator Training

Most of the plant modifications (mentioned in Section 2) required some changes in emergency operating procedures, and those had to be trained to the operators by simulator exercises. Besides this, PSA has been used to restructure and prioritise the whole simulator training program.

The risk-importance of human errors in post-initiator actions of the operators has been used for planning and prioritisation of transient types for simulator exercises in operator training. The higher the risk reduction worth of the operator error (diagnosis, decision and response), and the more complex the situation and actions, the more frequently the transient type is repeated in simulator exercises. The most important transients are repeated every one to two years, the second category every three to four years, and so on. Of course, the priorities change whenever plant modifications are made.

There has been significant feedback also from the simulator trainers to improve procedures and find new ways to deal with exceptional situations such as sub-cooled seawater or vegetation.

4.5 Risk Follow-up

In several cases after an operational event (an initiating event or some degree of loss of a safety function or barrier) the safety authorities have asked the utility to a estimate afterwards what the risk – significance of the event was. Supposedly, such an estimate could be used to assess the INES severity class of an event. However, if no core damage occurred, the true risk is known for sure to be (and have been) zero. This poses some philosophical problems as to what part of the now available a posteriori - information should or should not be taken into account in such follow-up assessments, and what conclusions or requirements should be made. Because the states of components are random variables (risk assessment indicating the time-average level), most of the time hidden states for standby safety components, it is difficult to justify strong conclusions based on few selected moments or cases on which information is gathered afterwards. At least one should not be biased by taking into account known failures with probability one while ignoring successful components (now known to have failed with probability zero).

5. RISK-INFORMED DECISIONS ON AGING

Particular attention has been paid on the following areas of plant ageing.

1. **Pressure vessel embrittlement.**
   Gradual embrittlement of the pressure vessel under neutron flux causes a increasing risk that a thermal shock (injection of cold water) under high pressure could fail the pressure vessel. Based on sample measurements of the pressure vessel properties, the critical transient temperature as a function of time(age) has been determined and the risk due to pressurised thermal shock (PTS) has been estimated. These led to annealing of the Loviisa 1 pressure vessel in 1996. This was done well before the risk would increase to a significant level.

2. **Ageing of active components.**
   Ageing of active components (pumps, valves, relays, breakers) may lead to an increasing failure intensity if repairs are imperfect or if preventive maintenance is ineffective. This can be detected by monitoring the numbers of failures in the failure history (a computerised system developed as a side-product of PSA), and performing statistical testing to confirm the significance. Both increasing and decreasing trends have been observed, even among nominally identical or rather similar components.[1] Because failure statistics are regularly reviewed by maintenance engineers, significant upward trends (if any) are nowadays normally detected without formal statistical tests.

3. **Ageing of electrical equipment, cables & instrumentation.**
   Recent measurements in the containment building indicate that in several locations the temperature exceeds 50 °C, the design temperature of the electrical equipment, instrumentation and cables. Because of this, increased failure rates were assessed for a number of valve actuators, seals, limit switches, protection instrumentation and associated cables. As a consequence the risk increased due to increased initiating event frequencies (due to increased probability of false signals or failing protection/limits) as well as increased

unavailabilities of safety system components expected to response to the events. A special complicating aspect was that some valves have oversize actuators so that the valves likely fail if the limit control or torque limit switches fail, and these limit systems also have higher failure rates due to the elevated temperatures. It turned out that the risk increase was dominated by the condition of two valves in the chemical and volume control system. Failure to close one of the valves in case of a certain medium size LOCA would eliminate HPSI and lead to core damage. Keeping one of the valves continuously closed turned out to be possible, virtually eliminating the risk increase without any cost or loss of production. With risk assessment a long shutdown outage and expensive renewals of cables and/or equipment were avoided.

4. Ageing of secondary circuit pipes and components.

Virtually no steam generator tube leakages have been experienced at Loviisa plant. However, significant erosion-corrosion ageing has taken place in other secondary pipes. This even caused two main feedwater pipe breaks, in 1990 and 1992. Extensive secondary pipe replacements have taken place since then, including the feedwater distribution lines in steam generators. The main condensers have been replaced with new ones made of stainless steel and titanium. The structural work on the secondary circuit is motivated by economy and production rather than risk or safety concerns, except for the feedwater pipelines.

5. In-Service Inspections.

A pilot project has been started in co-operation with safety authorities to prioritise in-service inspections (ultrasonic etc.) of primary and safety system pipes, based on the risk-significance of leakages. It is anticipated that this leads to a reduction in the total rate of inspections, while enhanced inspections could be needed in a limited set of pipe segments and welds.

6. SUMMARY

PSA has been used in many ways for risk-informed decision making at Loviisa power station. The most fruitful areas so far include:

* Identification of dominating risk contributors and possible means for reducing risk by plant modifications and improved procedures
* Providing risk perspective and economic criteria for assessing backfitting proposals
* Assessing the significance of ageing and needs for renewals
* Limiting, prioritising and optimising plant modifications
* Reducing testing requirements
* Justification of temporary as well as permanent configurations and extended outage times
* Planning and prioritisation of training programs.

REFERENCES

1. Jänkälä, K. E. & J. K. Vaurio: Component ageing and reliability trends in Loviisa nuclear power plant. Proc. PSA'89, ANS/ENS Topical Mtg., April 2 – 7, 1989, Pittsburgh, USA.
2. Vaurio, J.K.: Safety-related decision making at a nuclear power plant. Nuclear Engineering and Design 185(1998)335-346.

3. Lehto, M. et al.: Fire risk analysis for Loviisa 1 during power operation. Proc. PSA'96, Sept. 29 – Oct. 3, 1996, Park City, Utah, USA. American Nuclear Society.
4. Jänkälä, K.E., Mohsen, B. & J.K. Vaurio: PSA for shutdown modes of Loviisa NPP. Proc. PSAM 4 Conf., Sept. 13 – 18, 1998, New York, USA.
5. Vaurio, J.K. & P. Tammi: Modeling the Loss and Recovery of Electric Power. Nuclear Engineering and Design 157(1995)281-293.

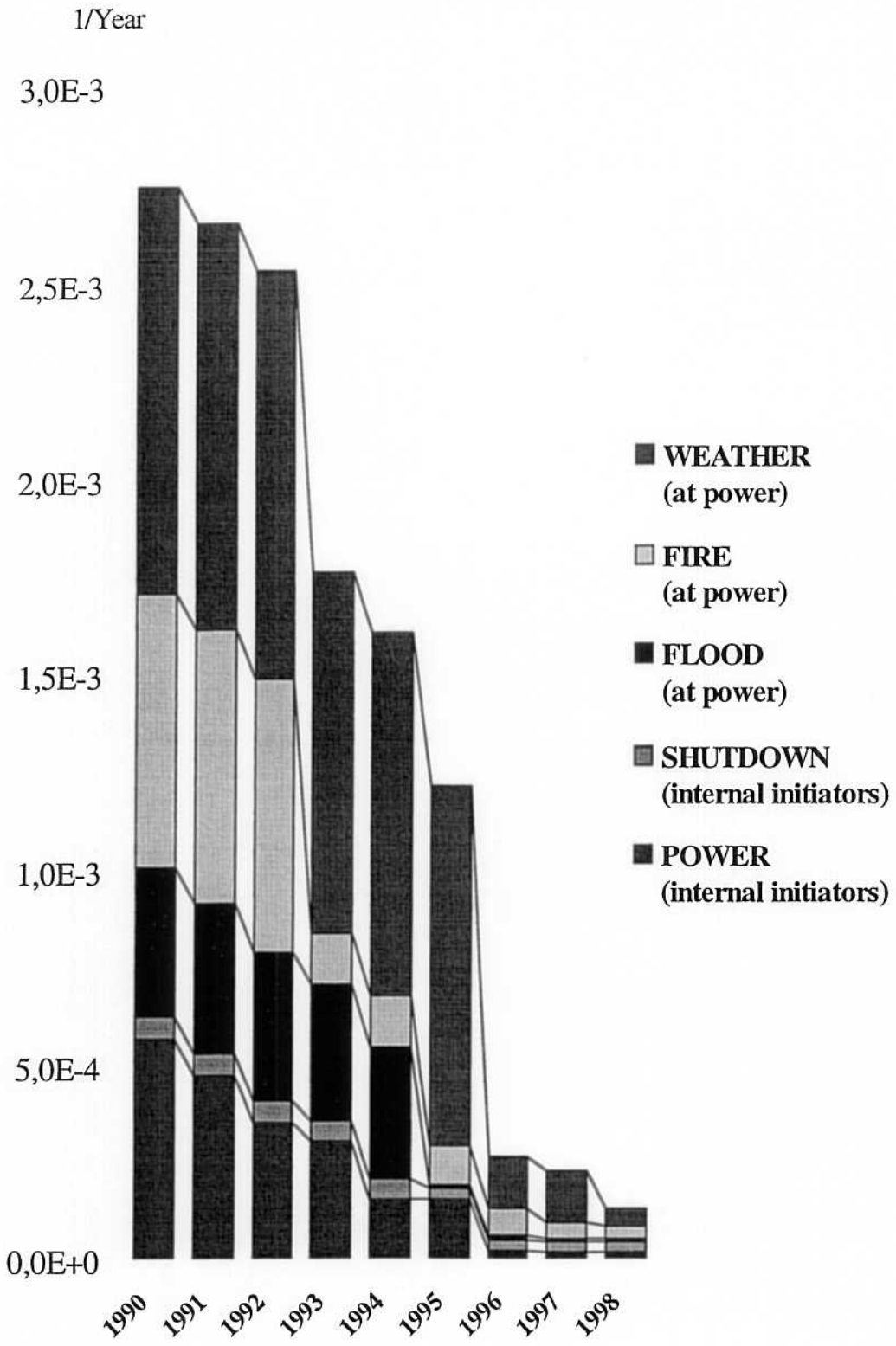


Fig. 1 The effect of plant modifications on the core damage frequency

Nya krav på säkerhetsanalysen-Samspel mellan PSA och deterministiska analyser

PO Waessman

Swedpower

Energiteknik

Kärnkraftteknik

"CV"

Energikommissionen	*1978*
R1 Risktopografi	*-1980*
R1 PSA Yttre Händelser	*-1984*
F1/F2 RAK	*-1998*
F1/F2 PSA2000	*-1998*
R12k	*-1999*
Branchgemensamma Kärnkraftkrav	*-1999*

SwedPower

Innehåll

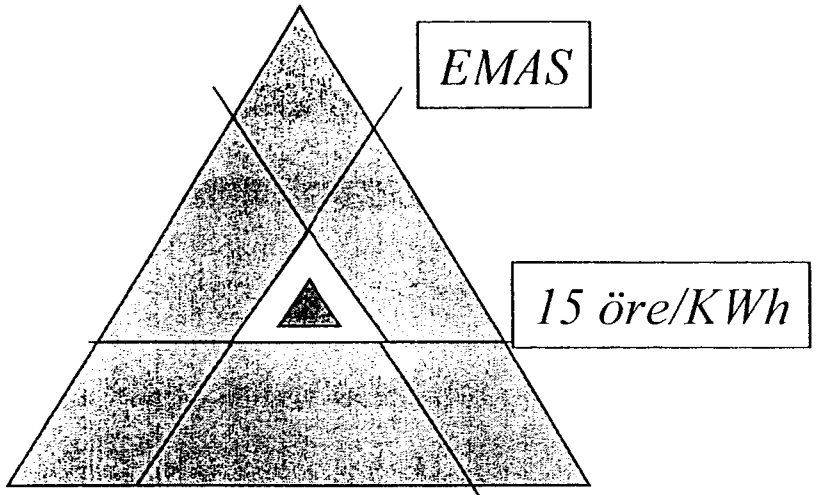
- Säkerheten i styrsystemet
- Säkerhetskrav och Mål
  - Probabilistiska kontra deterministiska krav
- Säkerhetsanalys
  - metodik,analysredskap och indata
- Samspel mellan PSA och deterministiska analyser

SwedPower

Säkerheten en del i styrsystemet

Konkurrens kraftigt elpris ---------- Lönsamhet

- Uthålligt
- Säkert
  - Produktionssäkerhet--Resultaträkning
  - Anläggningssäkerhet--Balansräkning
  - Omgivningssäkerhet=Reaktorsäkerhet
    - Resultaträkning--"körförbud"
    - Balansräkning--image+investering
  - Personsäkerhet--Restriktion
- Miljöriktigt
  - Utsläpp
  - Gruva--Grav



Reaktor säkerhet

Miljö riktigt

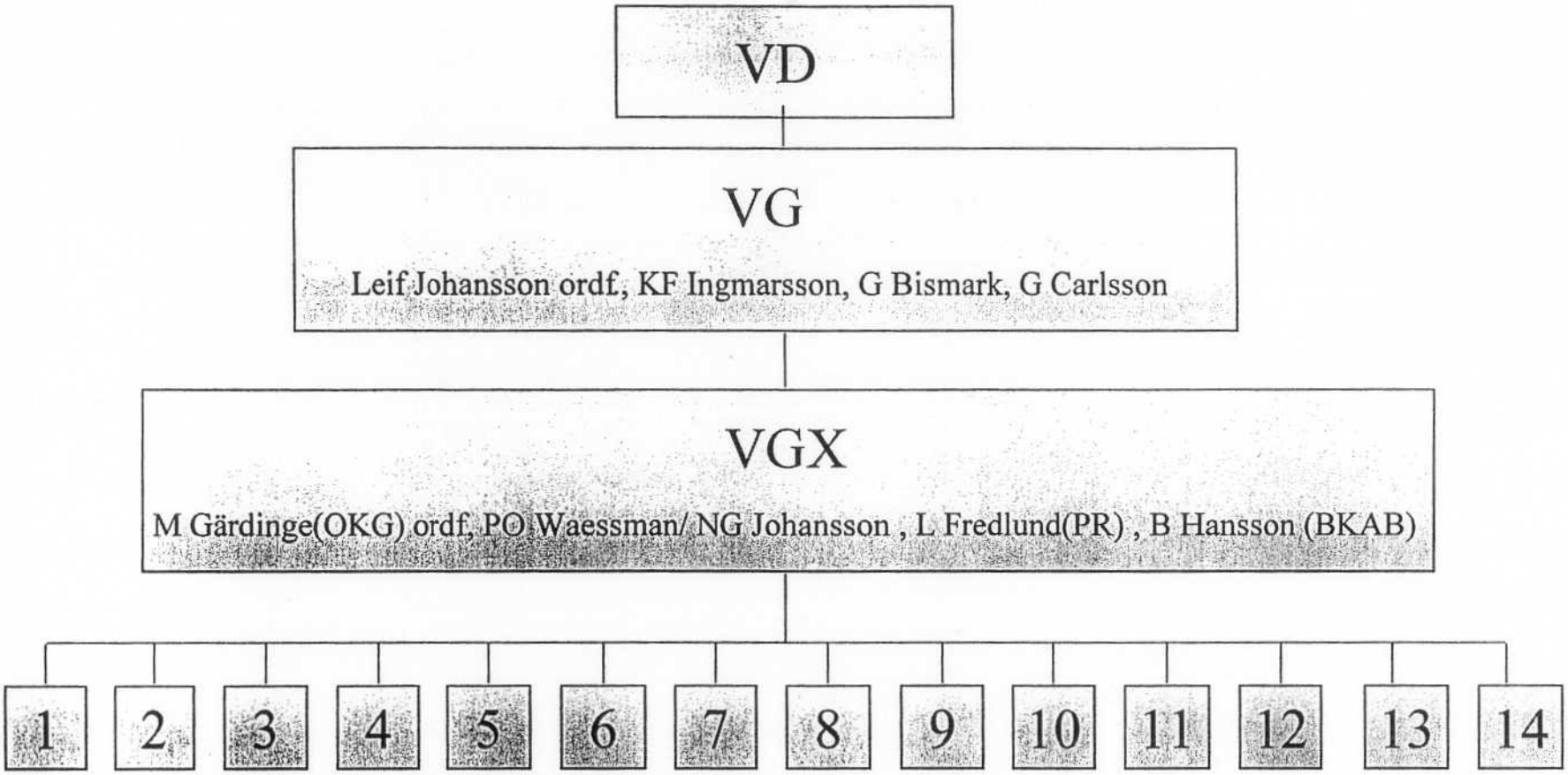
SwedPower

Branchgemensamma kärnkraftkrav för 2000 talet
Mål och syfte

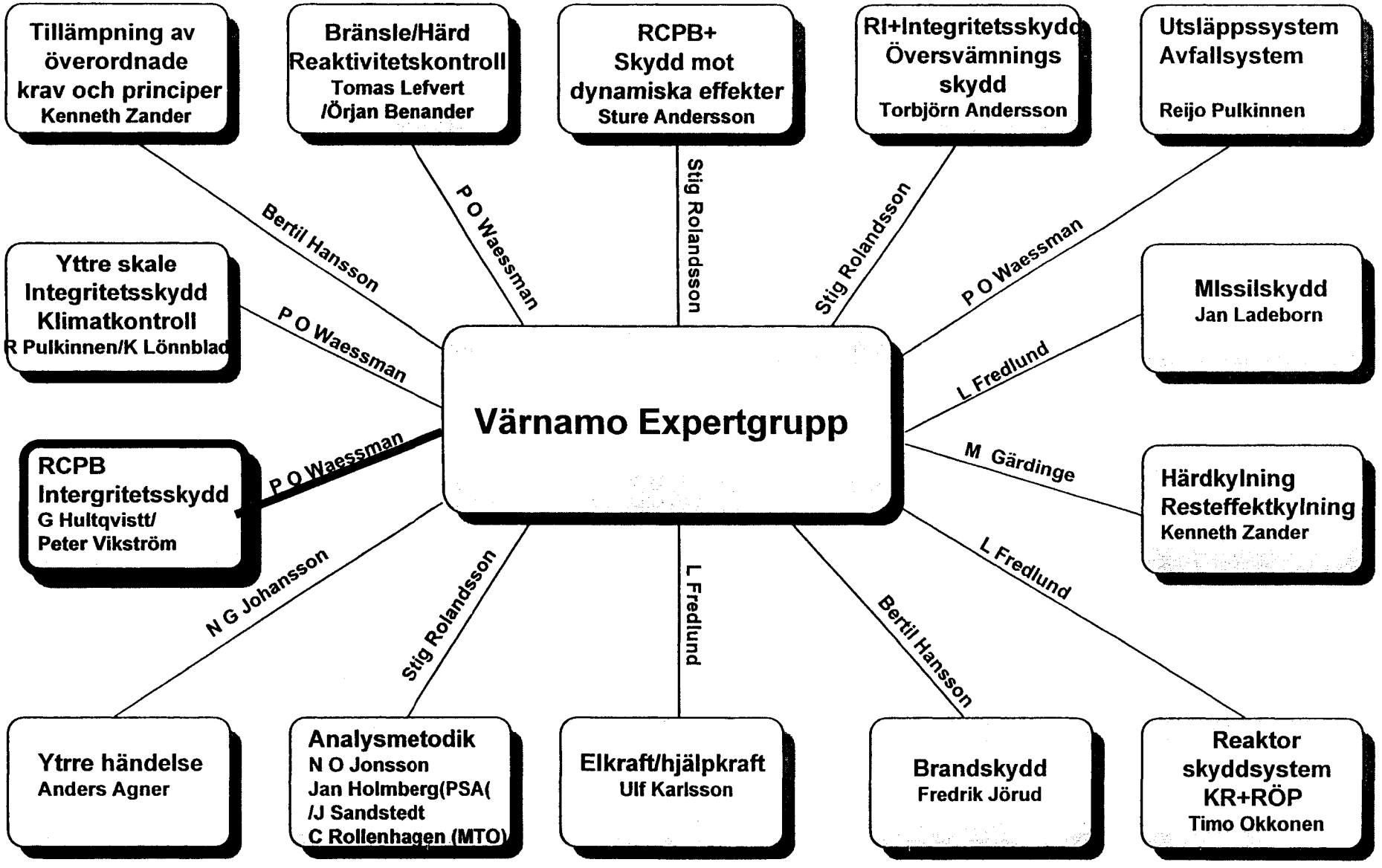
- Definiera
  - Konstruktionsstyrande Reaktorsäkerhets principer och krav
  - Tillämpningsregler
- Utgångspunkt
  - Möjliggöra ett maximalt utnyttjande av respektive anläggnings goda egenskaper och personalens kunskap om den egna stationen
  - Företags säkerhetspolicy+Befintliga SKI föreskrifter
  - Baseras på RAK/REDA/BOKA/DART erfarenheter
  - IAEA/USA/EUR krav
- Inriktning
  - Främja en mänsklig, verifierbar och robust utveckling av säkerheten
  - Stimulera en kostnadseffektiv och kontinuerlig reaktorsäkerhetsutveckling
    - Flexibel tillämpning av krav via regler

SwedPower

Organisation



SwedPower


Tillämpning av överordnade krav och principer
Kenneth Zander
Bränsle/Härd Reaktivitetskontroll
Tomas Lefvert
/Örjan Benander
RCPB+ Skydd mot dynamiska effekter
Sture Andersson
RI+Integritetsskydd Översvämnings skydd
Torbjörn Andersson
Utsläppssystem Avfallsystem
Reijo Pulkinnen
Yttre skale Integritetsskydd Klimatkontroll
R Pulkinnen/K Lönnblad
MIssilskydd
Jan Ladeborn
RCPB Intergritetsskydd
G Hultqvistt/
Peter Vikström
Värnamo Expertgrupp
Härdkylning Resteffektkylning
Kenneth Zander
Ytrre händelse
Anders Agner
Analysmetodik
N O Jonsson
Jan Holmberg(PSA(
/J Sandstedt
C Rollenhagen (MTO)
Elkraft/hjälpkraft
Ulf Karlsson
Brandskydd
Fredrik Jörud
Reaktor skyddsystem KR+RÖP
Timo Okkonen
Bertil Hansson
P O Waessman
Stig Rolandsson
Stig Rolandsson
P O Waessman
L Fredlund
M Gärdinge
L Fredlund
Bertil Hansson
L Fredlund
Stig Rolandsson
N G Johansson
P O Waessman
P O Waessman

SwedPower

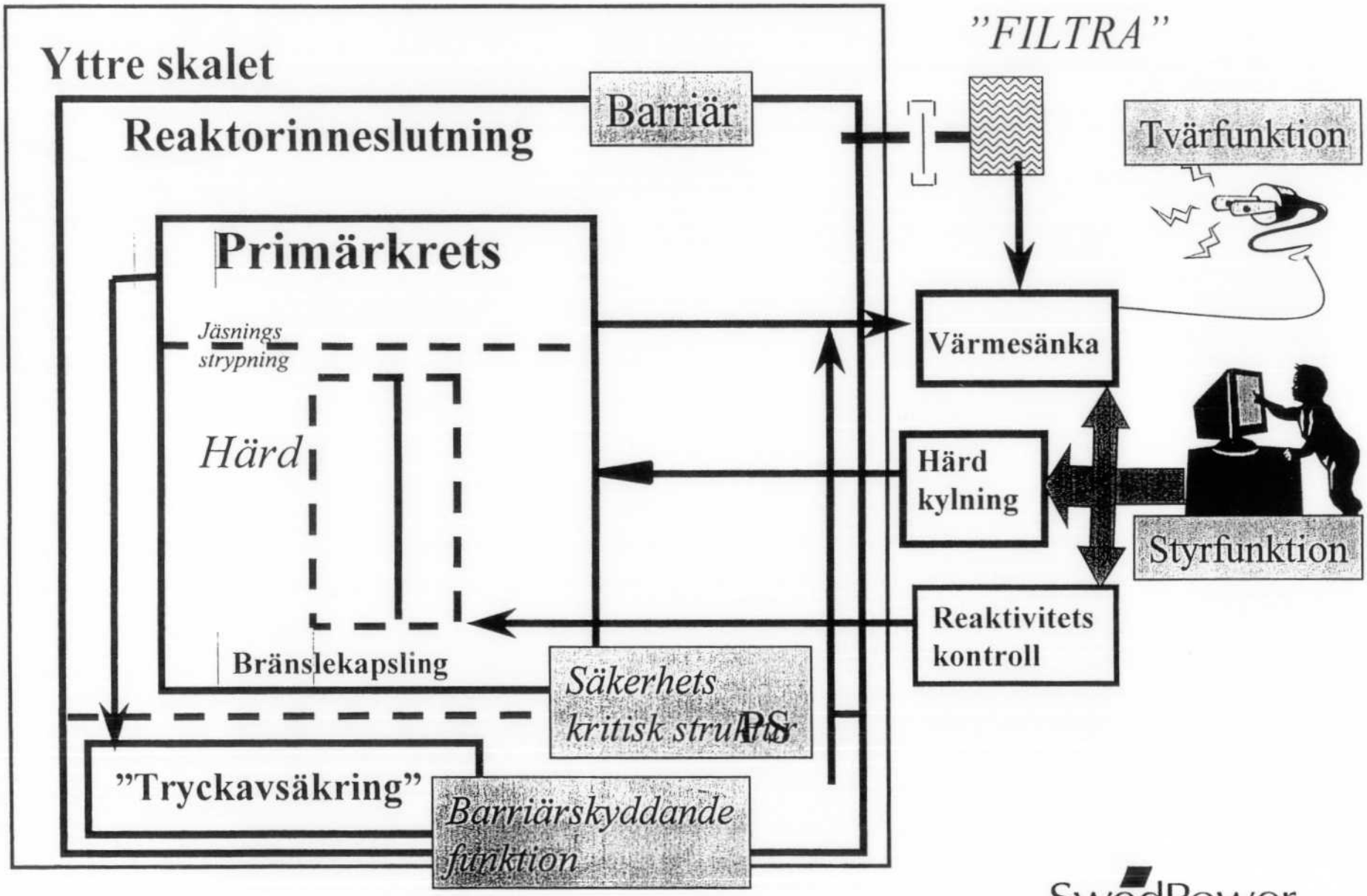
Säkerhetskrav och mål

- Att skydda människor, samhälle och miljö mot skador genom upprätthållande av ett effektivt försvar mot radiologiska olyckor.

- Att under normal drift begränsa, så långt som möjligt (ALARA), den joniserade strålningens skadeverkningar, inom anläggningen och till följd av utsläpp av radioaktivitet från anläggningen samt från bildat avfall.

- Att vidta alla rimliga praktiska åtgärder för att förhindra radiologiska olyckor samt mildra konsekvenserna av strålskador om olyckor ändå sker.

Barriärtänkande



POW 990412

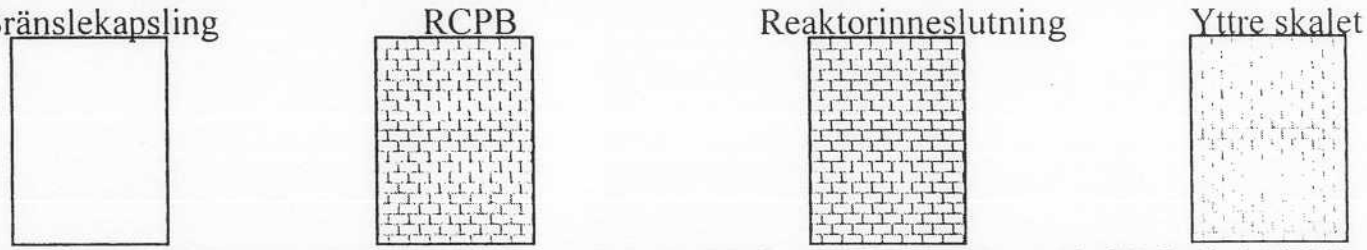
SwedPower

Kravstruktur

Grundkrav

Deterministiska: Djupförsvar =INSAG 3,10 (EUR & 2.2.1)
Generella krav=GDC 1-5 (EUR & 2.1.3-2.1.5)
Kvantitativa: Härdskada < 1E-5/år 0.1% < 1E-7/år (EUR & 2.1.2)
MTO: INSAG4+GDC 19 (EUR &2.0.2.2.9-10, 2.10)

Barriärer



GDC 11-13(EUR 2.8.2.2) GDC 14-15,30-32(EUR 2.8.2.3.2) GDC 16,50-55(EUR 2.9) GDC 60-64(EUR 2.8.2.9)

Kritiska strukturer

Härd
Jäsningsstrypning
PS funktion
Översvämningsskydd
Brandskydd

Reaktivitetskontroll :GDC 25-28 (EUR 2.8.1.1.5/2.4.7)

Barriärskyddande funktioner

Isolering :GDC 56-57 (EUR &2.9.4)
RCPB integritetsskydd :ASME III 89 (EUR 2.8.2.3.2...)
Härdkylning :GDC 33,35-37 (EUR 2.8.2.4.3-4)
Värmesänka :GDC 34, 38-39,44,46 (EUR 2.8.2.4.1-2)

Skydds/styrfunktioner

Reaktorskyddsystem:GDC 20-24,29 (EUR 2.8.12-13)

Tvärfunktioner

Elkraft:GDC 17,18 (EUR 28.2.7)

SwedPower

Kravstruktur

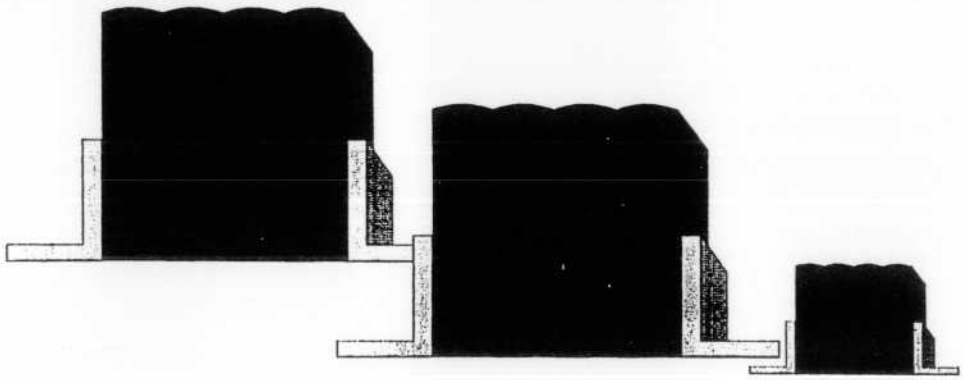
”Miljö”krav
Anläggning+Omgivning

Acceptanskrav för barriärer och funktioner=Säkerhetsgränsvärden

Dimensioneringskriterier
=Krav på utformning-allmänna/specifika

Allmänna kvalitetskrav

Krav på verifierande analys
DSA=Dimensionerande händelser
+säkerhetskritiska egenskaper+metodik
PSA=metodik



Anläggning

Barriär

Säkerhetskritisk struktur

Barriärskyddande Funktioner

Skydds Funktioner

Tvär Funktioner

500

600

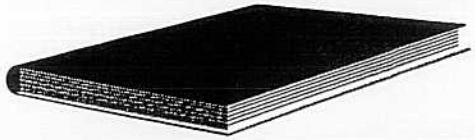
Komponent

El kvalite

Signal kvalite

SwedPower

Kravstruktur



”Miljö”krav
Anläggning+Omgivning

Acceptanskrav =Säkerhetsgränsvärden

Dimensioneringskriterier
=Krav på utformning-allmänna/specifika

Allmänna kvalitetskrav

Krav på verifierande analys
DSA=Dimensionerande händelser
+säkerhetskritiska egenskaper-metodik
PSA=metodik

Säkerhetsanalys

Anläggning

Barriär

Säkerhetskritisk struktur

Barriärskyddande Funktioner

Skydds Funktioner

Tvär Funktioner

System

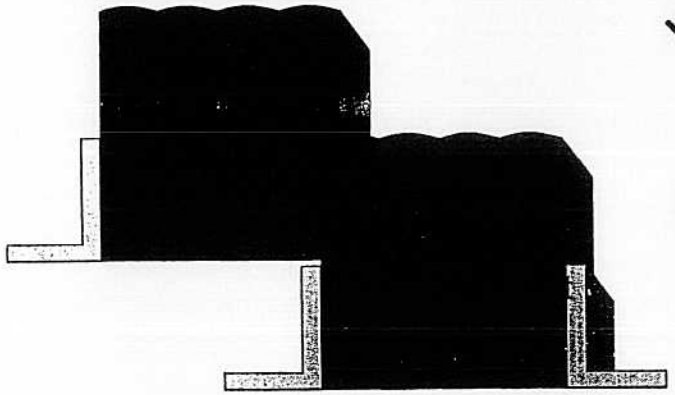
500

600

Komponent

El kvalite

Signal kvalite

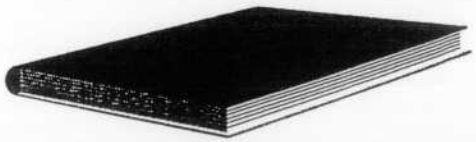


Konstruktionsstyrande egenskaper

Krav på prestanda

SwedPower

Säkerhetsanalys



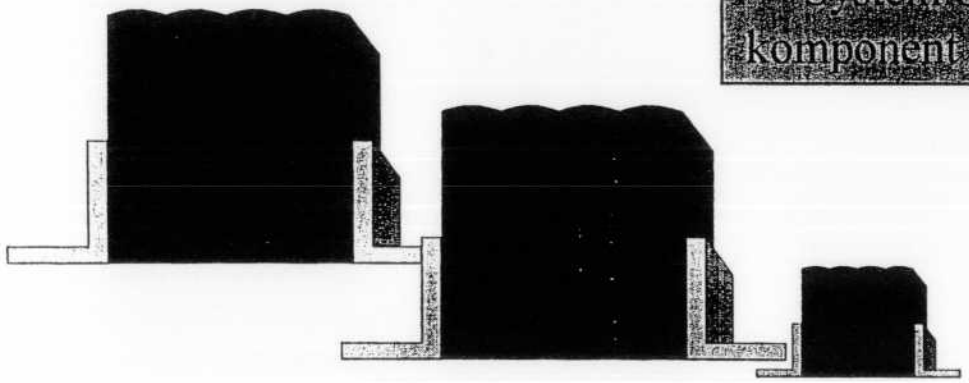
”Miljö”krav
Anläggning+Omgivning

Acceptanskrav för barriärer och funktioner=Säkerhetsgränsvärden

Dimensioneringskriterier
=Krav på utformning-allmänna/specifika

Allmänna kvalitetskrav

Krav på verifierande analys
DSA=Dimensionerande händelser
+säkerhetskritiska egenskaper+metodik
PSA=metodik



Anläggning

Anläggnings analys

Barriär

Säkerhetskritisk struktur

Barriärskyddande Funktioner

Skydds Funktioner

Tvär Funktioner

Mekanisk integritetsanalys

Mekanisk integritetsanalys

500

600

System och komponent analys

Komponent

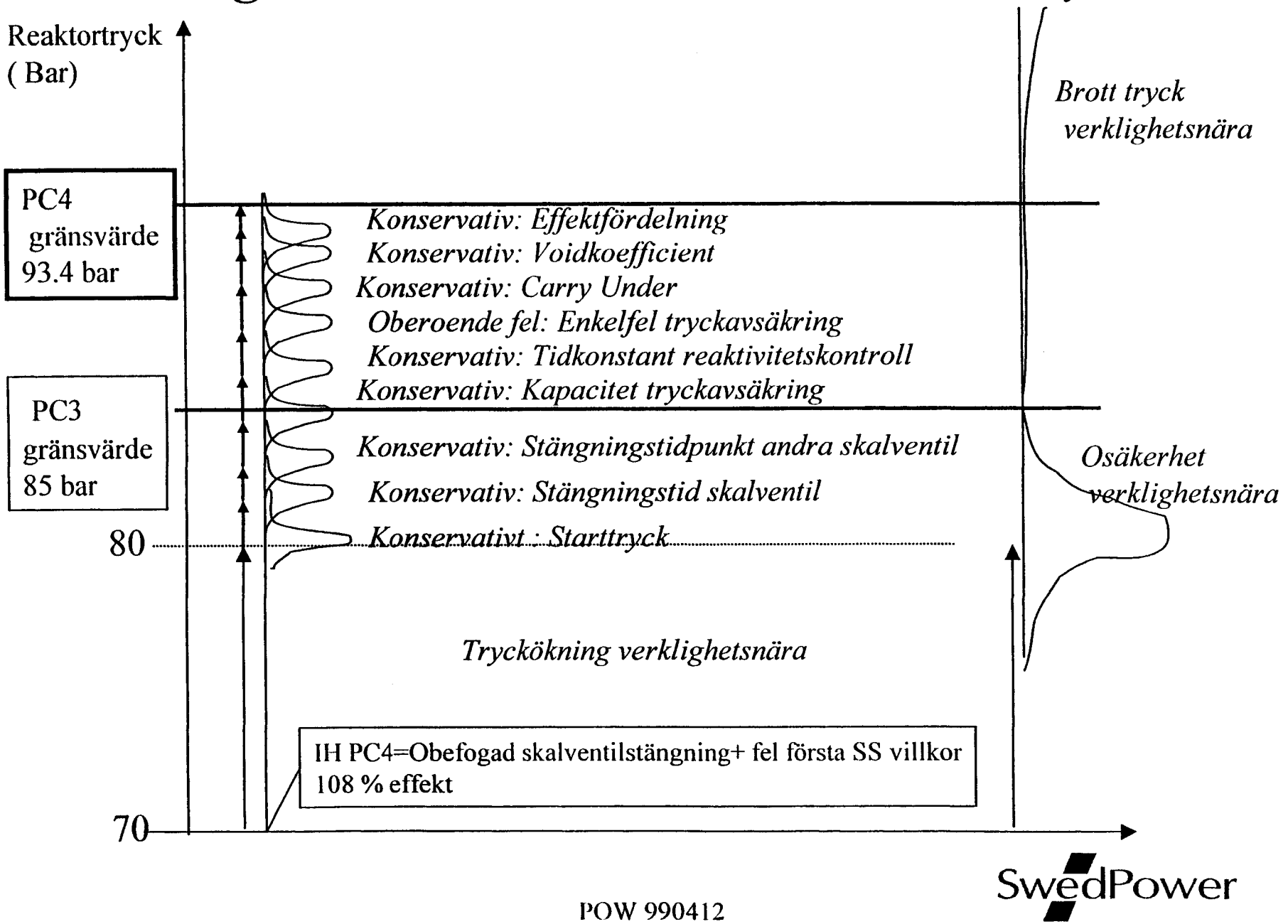
El kvalite

Signal kvalite

POW 990412

SwedPower

Verklighetsnära kontra konservativ analys



SwedPower

Säkerhetsanalys

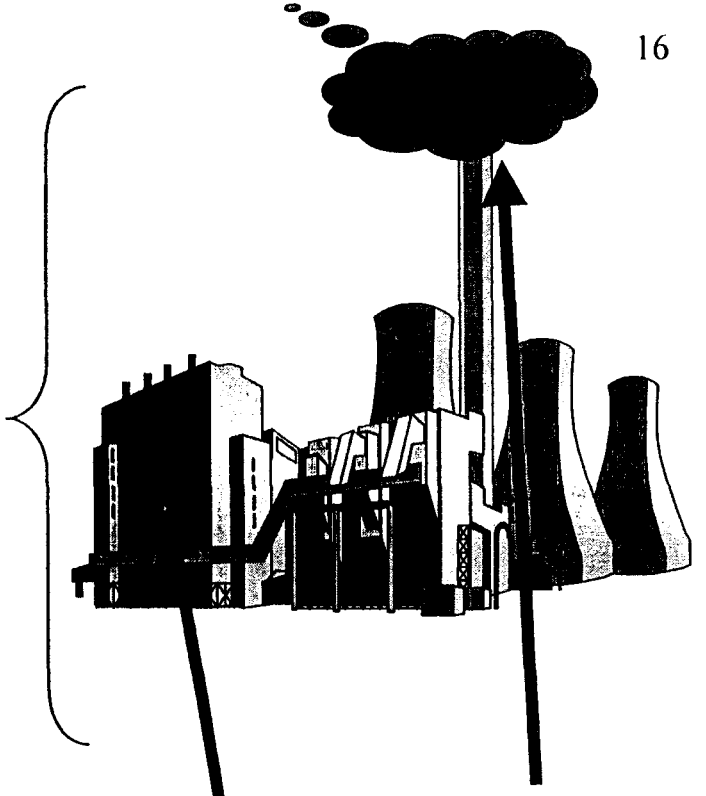
- Syfte
  - påvisa förmåga att motstå transienter och störningar utan att äventyra säkerheten
    - för personal, omgivning och allmänhet
- Acceptanskrav
  - visa att de Konstruktionsstyrande kraven innehålls
    - deterministiska
    - probabilistiska
- Kvalitetskrav
  - Omfattning och metodik för analys skall defineras
    - tillstånd
    - oberoende och beroende fel
    - val av prestanda

SwedPower

Probabilistisk Säkerhets Analys

- Säkerhetsanalys baserad på
  - deterministisk anläggningsmodell
- Analyserad med sannolikhetsbaserad metodik
  - inledande händelser
  - beroende fel
  - oberoende fel
- Värderad mot sannolikhetsbaserade godhetstal

Anläggningsmodell



Nivå 1

Nivå 2

Styrsystem

Stödsystem

Start signal

Kraft

Kylning

Komponent RX1 M

Objekt P1 V1

System

Funktion Härdkylning

415 329 416 314TB 323 322/711/715

RI

isolerad 362

Inledande Händelse

=Matarvattenbortfall

(Minskat kylmedieinventarium)

ja

nej

ok

HS

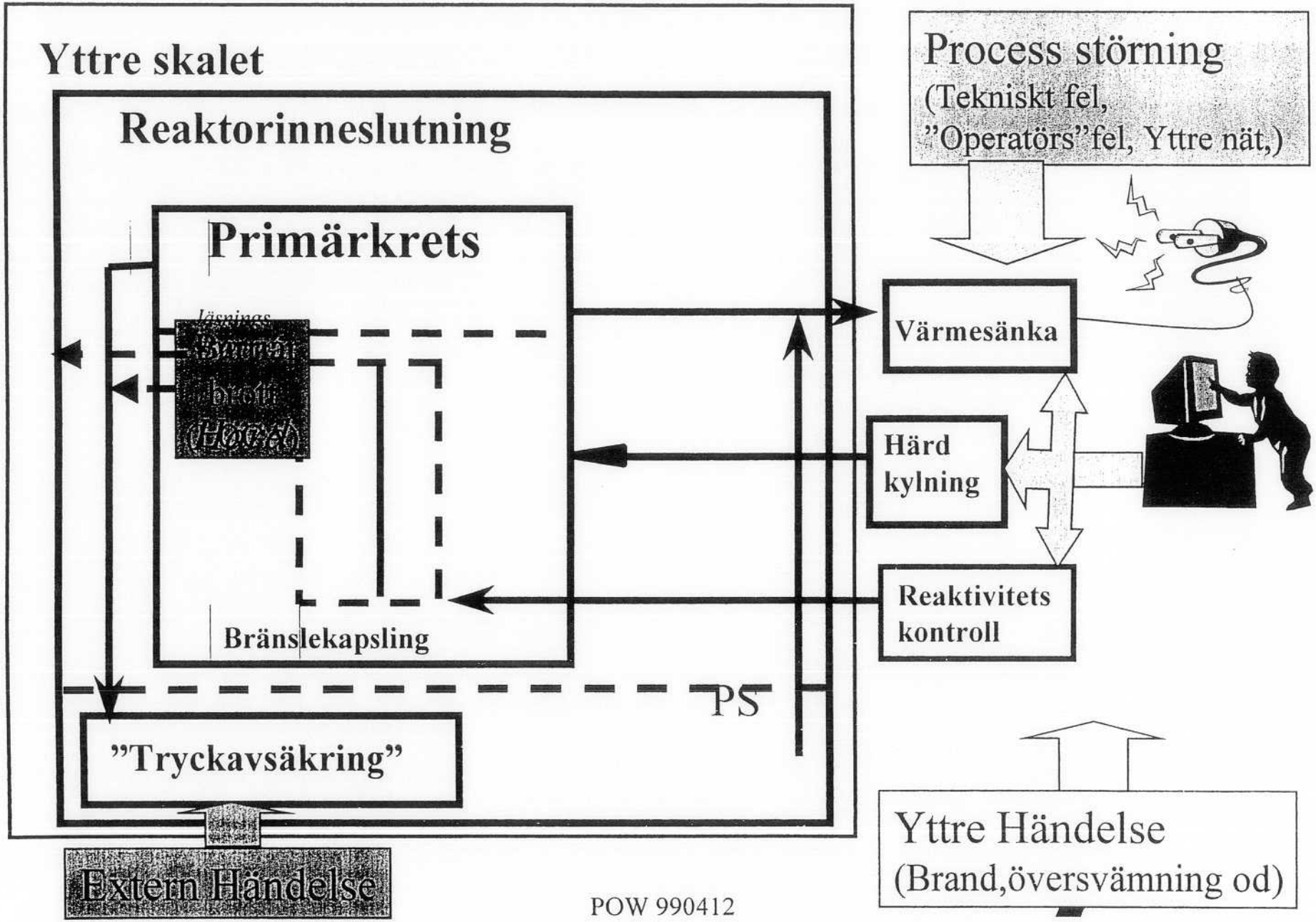
Utsläpp < 0.1%

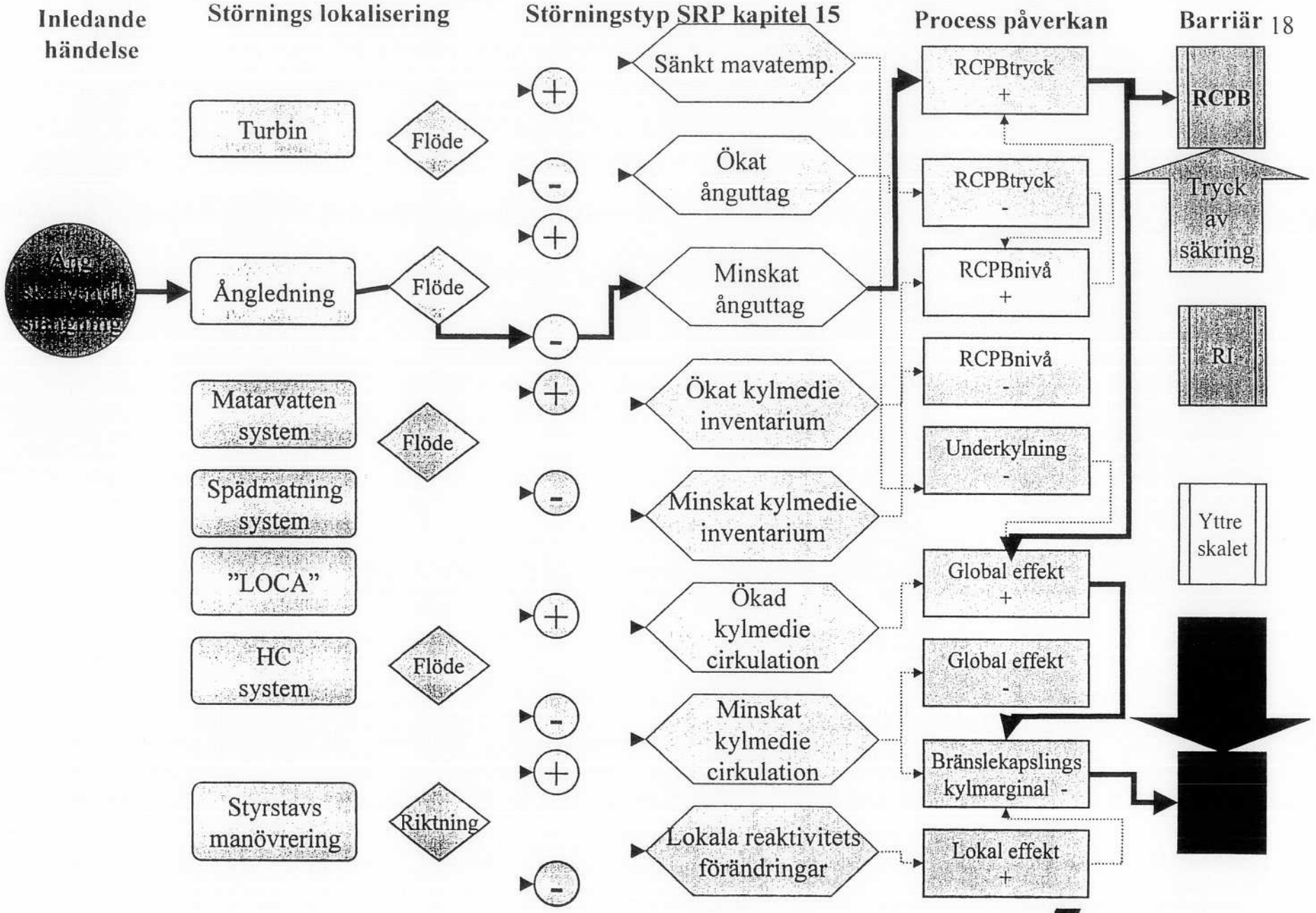
Utsläpp

POW 990412

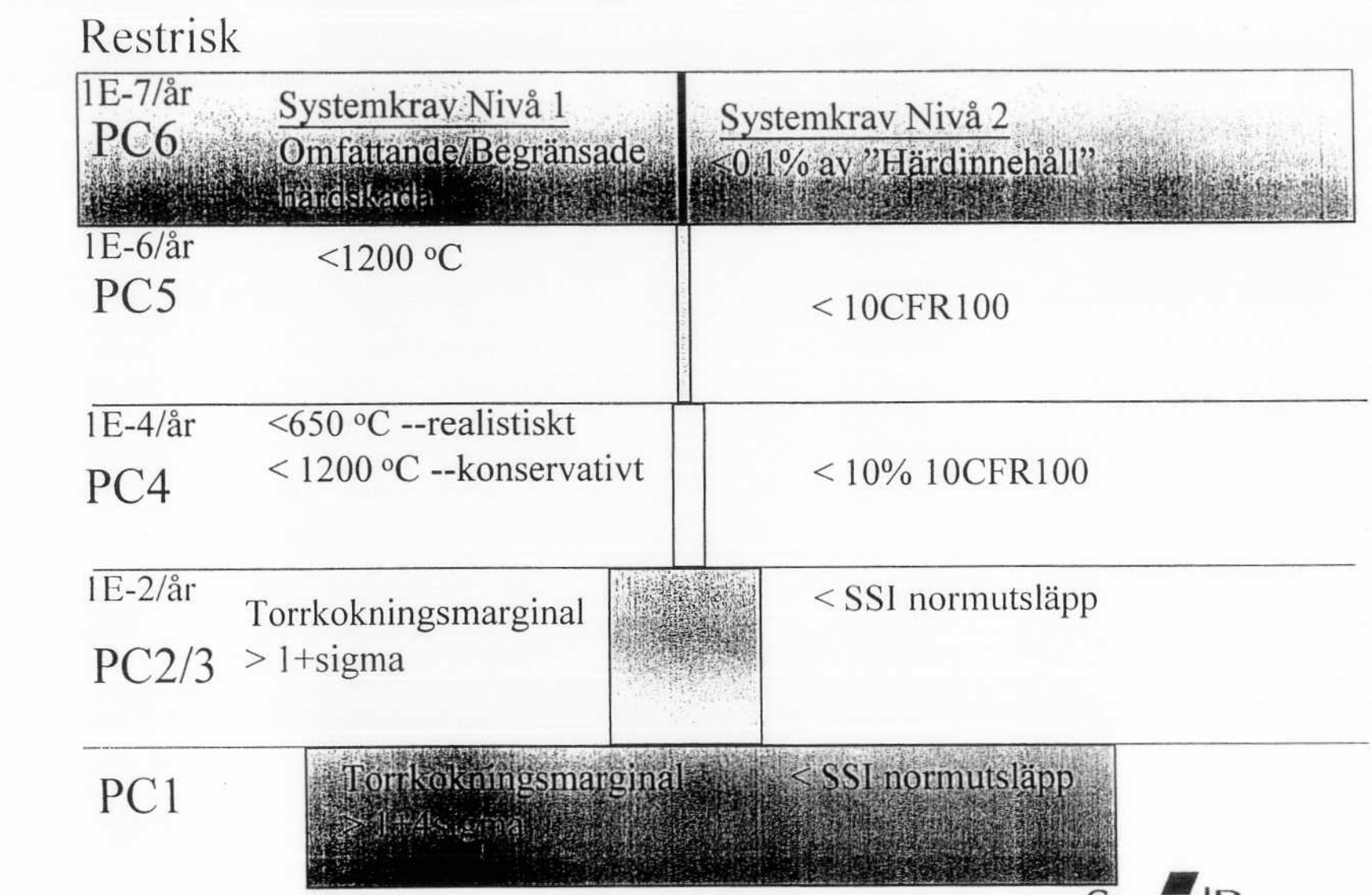
SwedPower

Inledande Händelse vad är det?




Inledande händelse
Störnings lokalisering
Störningstyp SRP kapitel 15
Process påverkan
Barriär
Ång- ledningsbrott
Ångledning
Turbin
Matarvatten system
Spädmatning system
"LOCA"
HC system
Styrstavs manövrering
Flöde
Flöde
Flöde
Flöde
Riktning
+
-
+
-
+
-
+
-
+
-
Sänkt mavatemp.
Ökat ånguttag
Minskat ånguttag
Ökat kylmedie inventarium
Minskat kylmedie inventarium
Ökad kylmedie cirkulation
Minskat kylmedie cirkulation
Lokala reaktivitets förändringar
RCPBtryck +
RCPBtryck -
RCPBnivå +
RCPBnivå -
Underkylning -
Global effekt +
Global effekt -
Bränslekapslings kylmarginal -
Lokal effekt +
RCPB
Tryck av säkring
RI
Yttre skalet
SwedPower

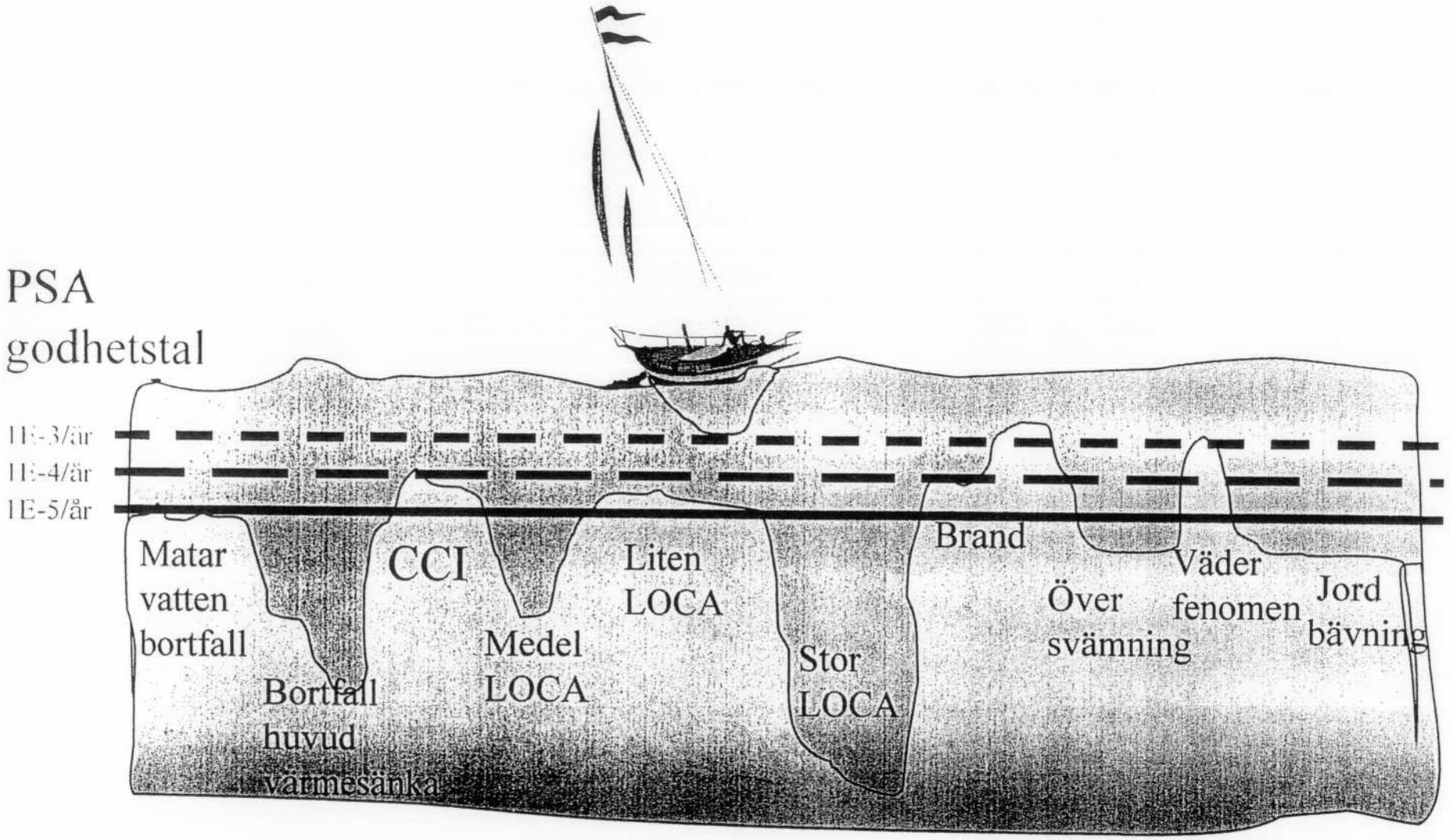
Acceptanskrav för barriärer



SwedPower

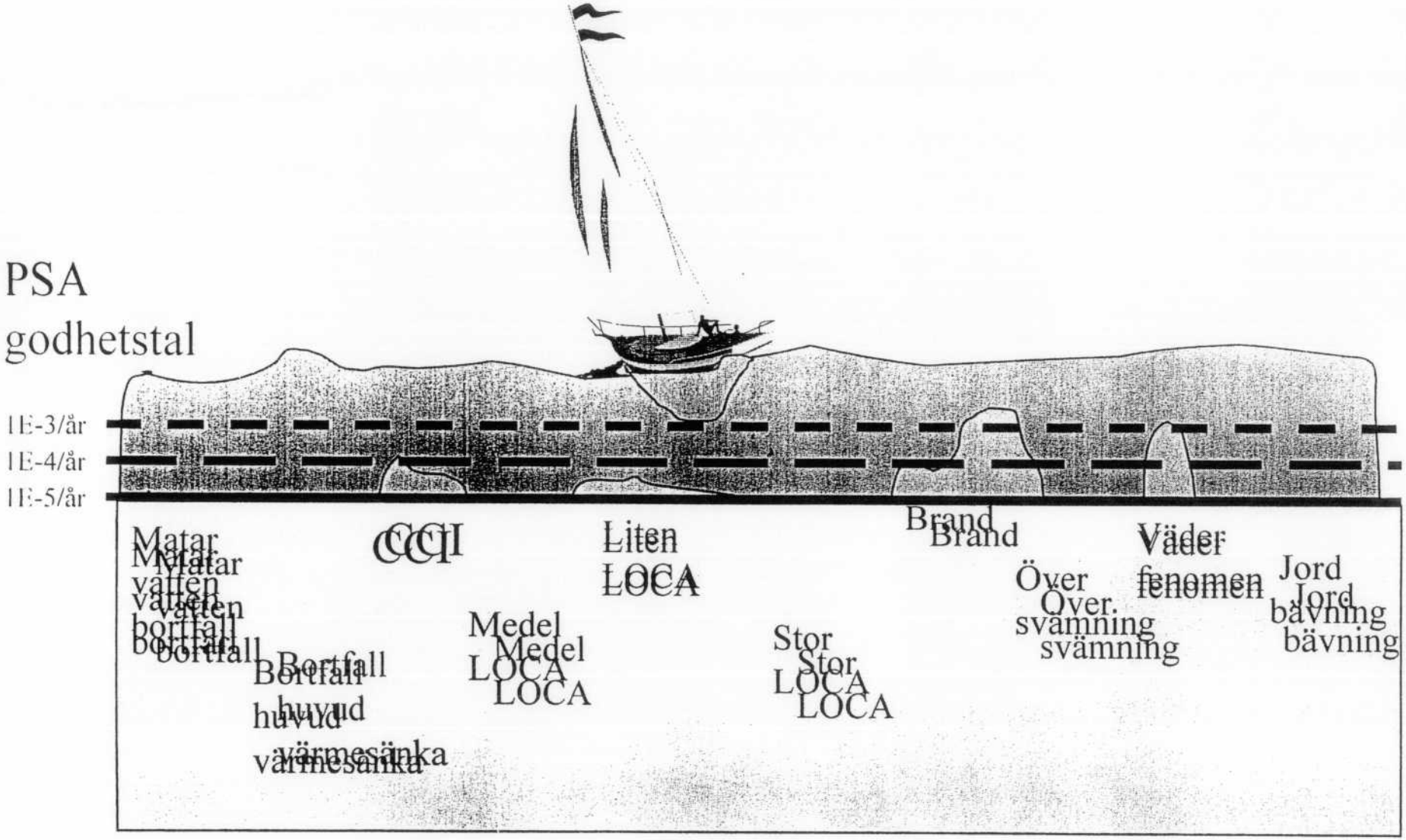
Risktopografi

PSA
godhetstal



SwedPower

PSA kontra godhetstal



SwedPower

Moderna krav på säkerhetsanalys

- Krav på omfattning
  - Inledande Händelser
- Acceptanskrav
- Metodikkrav/Tillämpning:
  - Identifiering av dimensionerande störningar --gallringsmetodik
  - Anläggningsmodell--Indata
  - Bestämning av säkerhetskritiska egenskaper
    - Startillstånd/Driftfunktion/Härd/Säkerhetsfunktion
  - Bestämning av oberoende fel (Enkelfelsanalys+CCF)+ följdfel
  - Konfidens
    - Verklighetsnära analys med sannolikhetsbaserad acceptansvärde
    - Konservativ analys med ”lagom” konservatism i säkerhetskritiska egenskaperRedovisning
- Metodkrav

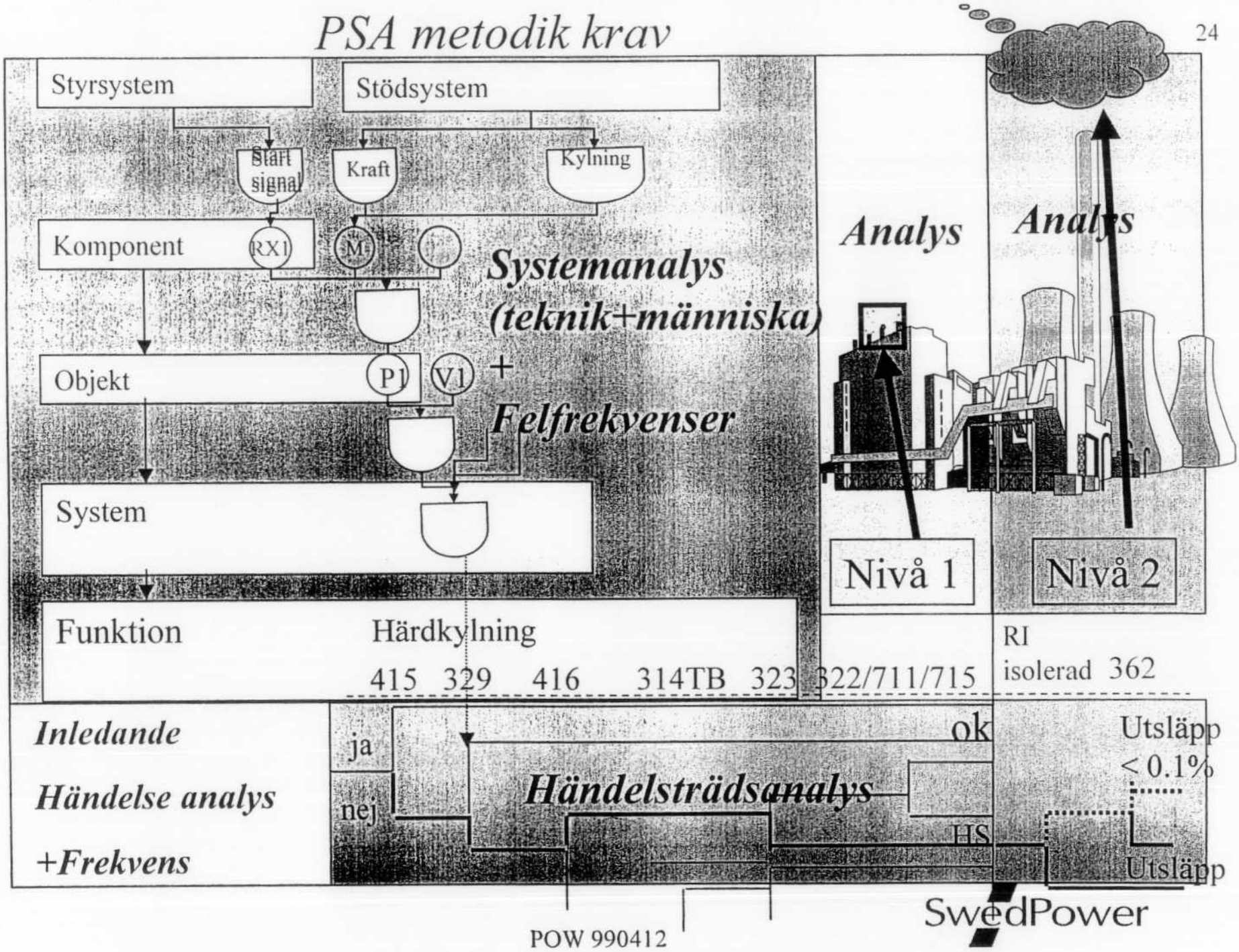
SwedPower

Struktur--Krav på analysmetodik

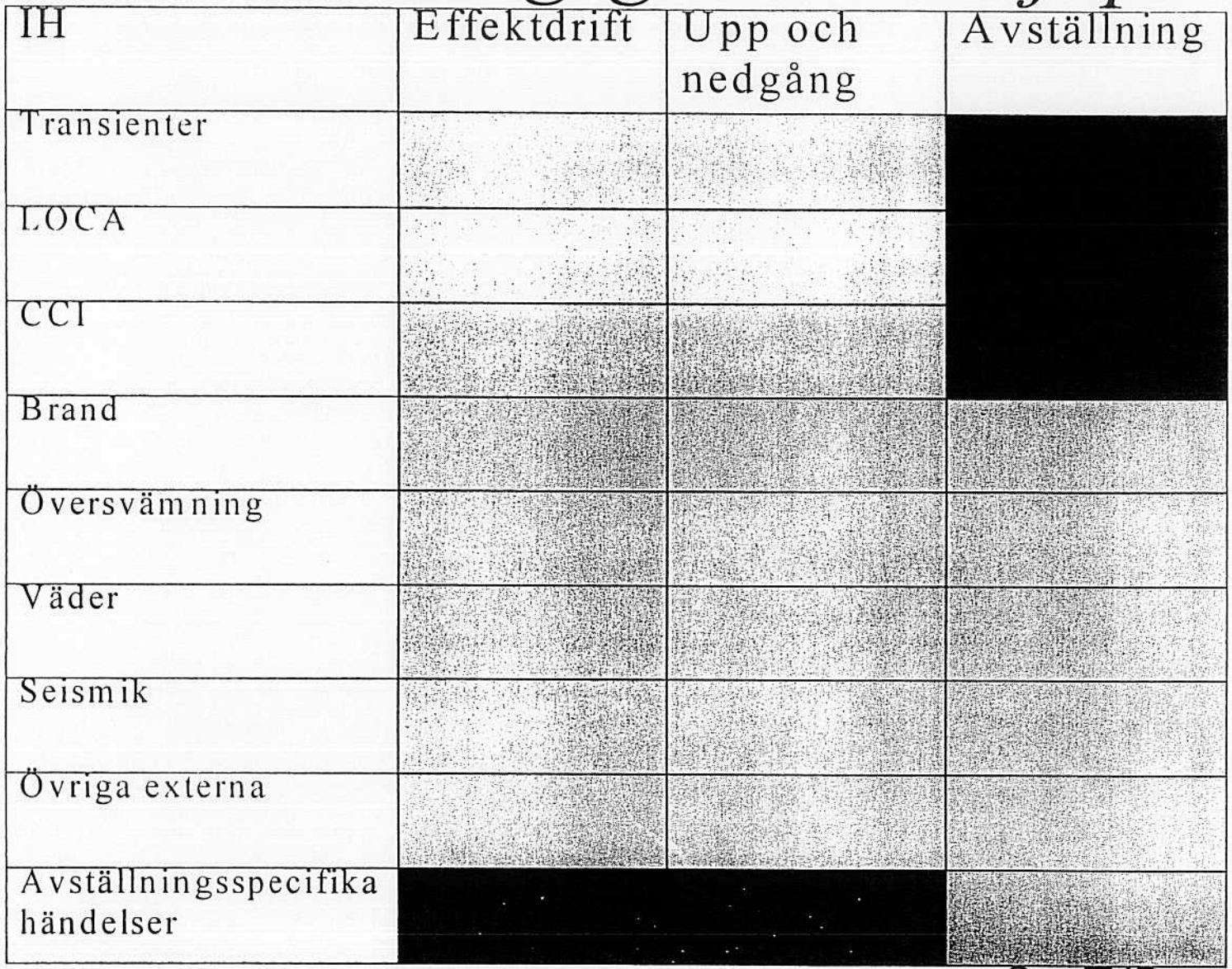
- Allmänt
  - Analysens syfte och mål
  - Analysens genomförande, resultat och redovisning
- Anläggningsanalysens genomförande, resultat och redovisning
  - Normaldriftsanalys
  - Konsekvensanalyser
- System-och komponentanalysens genomförande, resultat och redovisning
- Den mekaniska integritetsanalysens genomförande, resultat och redovisning
  - Krav på bestämning av laster och lastkombinationer
  - Krav på bestämning av materialegenskaper
  - Krav på hållfasthetsanalyser
- ”MTO”analysens genomförande, resultat och redovisning
- PSA genomförande, resultat och redovisning

SwedPower

PSA metodik krav



PSA täckningsgrad och djup



SwedPower

Vad är likheter och skillnaden mellan Deterministisk (DSA) och Probabilistisk säkerhetsanalys (PSA)?

	DSA	PSA
Inledande Händelser	Sannolikhet - händelseklasser (H1-H5)	Sannolikhet - känslighetanalys
Indata - prestanda - konfiguration	-uppmätt med konservatism - STF	-uppmätt -STF med och utan AU/PLI
Beroende fel	- fysikaliskt med postulat - sannolikhetsbaserad kombination av laster (konservativt) - sannolikhetbaserad (konservativ) anläggningsmodell	- dito - dito utan konservatism (känlighetanalys) - dito utan konservatism (känslighetsanalys)
Oberoende fel	Postulat - enkelfel - bortfall yttre nät	Sannolikhet - känslighetsanalys
Acceptanskrav	Sannolihetsrelaterade (H1-H5)	Risk relaterade (H5)

SwedPower

Vad är likheter och skillnaden mellan Deterministisk (DSA) och Probabilistisk säkerhetsanalys (PSA)?

- All säkerhetsanalys är probabilistisk!

- PSA inkluderar osäkerheter
  - känslighets
  - osäkerhetsanalys

- DSA beaktar osäkerheter
  - mångdubbel konservatism
  - paraplyanalys
  - expertbeslut

SwedPower

Metodik för Deterministisk Säkerhetsanalys

-1- Inledande Händelseanalys

-2- Definition av Acceptanskrav

-3- Identifiering av dimensionerande störningar, gallring

-4- Kvalitetssäkrade Indata och metod (program)

-5- Bestämning av säkerhetskritiska egenskaper

- -4a-Allmän metodik
- -4b-Tillämpning per störningstyp och barriär

-6- Bestämning av oberoende fel och följdfel per händelseklass och störningstyp

-7- Bestämning av konfidenskrav- probabilistisk eller rimlig konservatism

- -7a-Allmänna krav
- -7b-Verklighetsnära analys med sannolikhetsbaserade acceptansvärden (95/95%)
- -7c- Konservativ analys med rimlig konservatism i säkerhetskritiska egenskaper

-8- Analys av störningar enligt -3- med förutsättningar enligt -4----7-

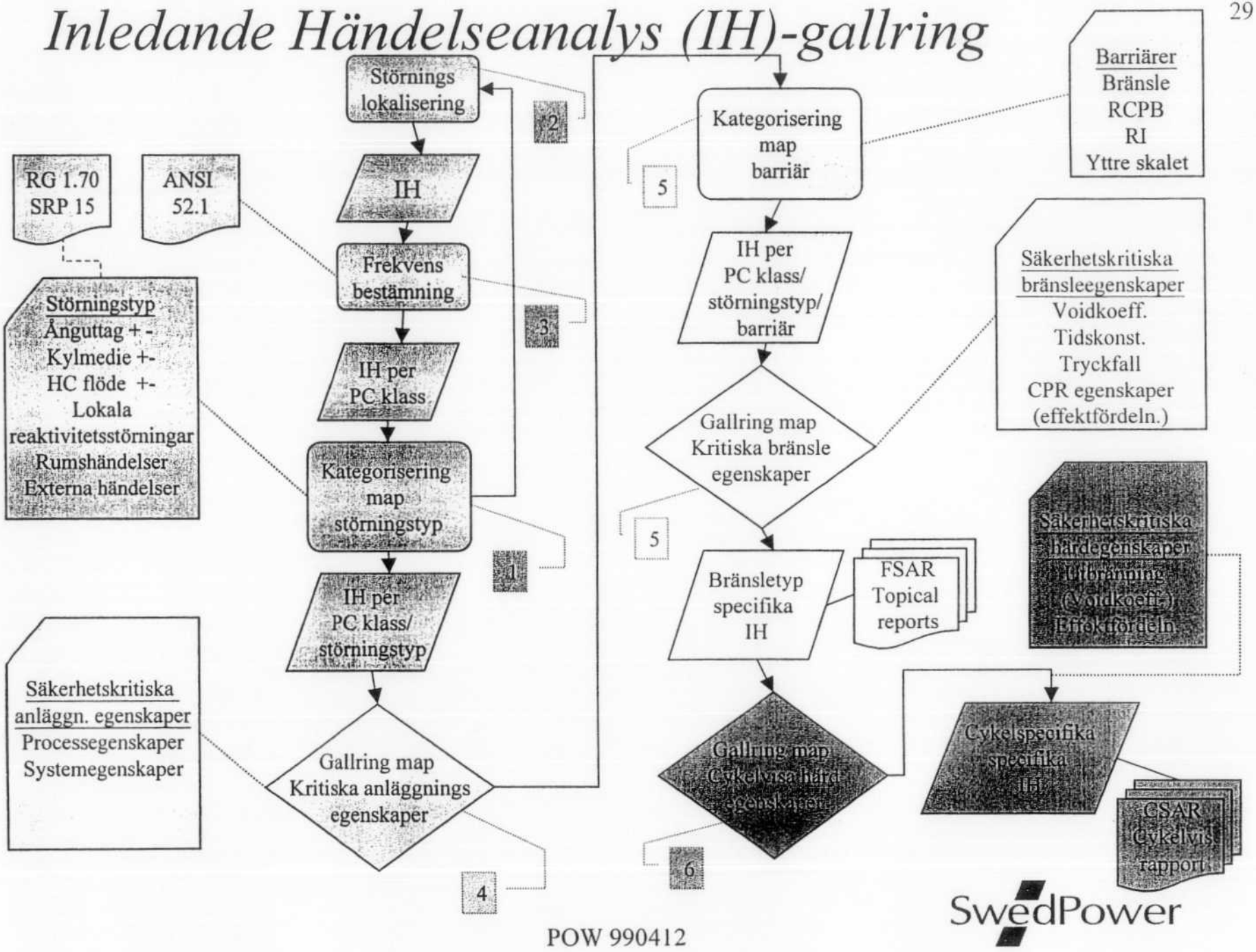
- -8a- Verklighetsnära analys för att definiera ev. konservatism i säkerhetskritiska egenskaper
- -8b- Rimligt konservativ analys eller känslighetsanalys av verklighetsnära analys

-9- Redovisning av resultat mot acceptanskrav enligt -2-

- -9a-Diskussion av säkerhetskritiska egenskaper
- -9b- Diskussion av resultat

SwedPower

Inledande Händelseanalys (IH)-gallring



SwedPower

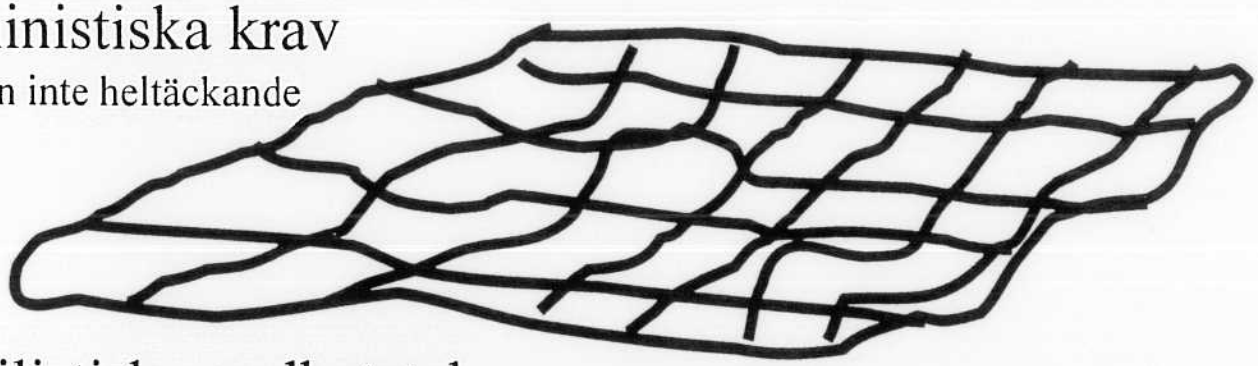
PSA vad är det bra för?

- Verifierar att säkerhetskrav är uppfyllda
- Optimerar resurser
  - teknik
  - drift
  - underhåll

Deterministiska kontra probabilistiska krav

Deterministiska krav

Robust men inte heltäckande

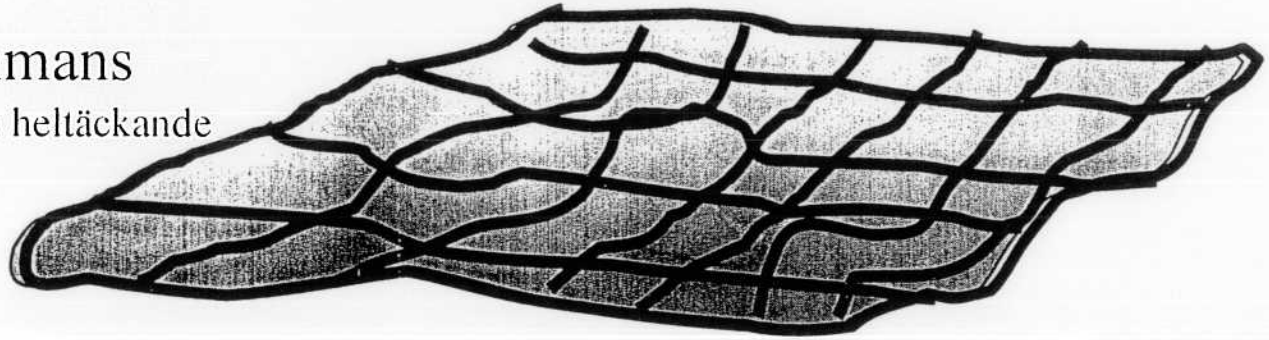


Probabilistiska godhetstal

Heltäckande men ej robust

Tillsammans

Robust och heltäckande



SwedPower

Krav på probabilistisk säkerhetsanalys

1 Mål med PSA

2 Omfattning av PSA

3 Nivå 1, grundanalys av risk för en härdskada

3.1 Övergripande struktur av modellen

3.2 Analys av inledande händelser

3.2.1 Omfattning

3.2.2 Kylmedelsförluster

3.2.3 Transienter

3.2.4 Common Cause Initiators

3.2.5 Rumshändelser

3.2.6 Yttre påverkan

3.3 Händelseträdsanalys

3.3.1 Definition av sluttillstånd

3.3.2 Fastställande av systemfunktionskrav

3.3.3 Sekvensanalys

3.3.4 Modellering av händelseträd

3.4 Systemanalys

3.4.1 Systemanalys

3.4.2 Analys av mänskligt påverkan

3.4.3 Analys av beroenden

Procedures for Risk Based Inspection of Pipe Systems in Nuclear Power Plants

Björn Brickstad, SAQ/Teknik

NKS/SOS-2 seminar, April 13, 1999

What is the purpose of ISI?

The purpose of ISI is to identify degradation before leakage occurs which later may lead to rupture.

- Defence in depth argument.
- An understanding that a large leak may have relatively large consequences for some pipe components.

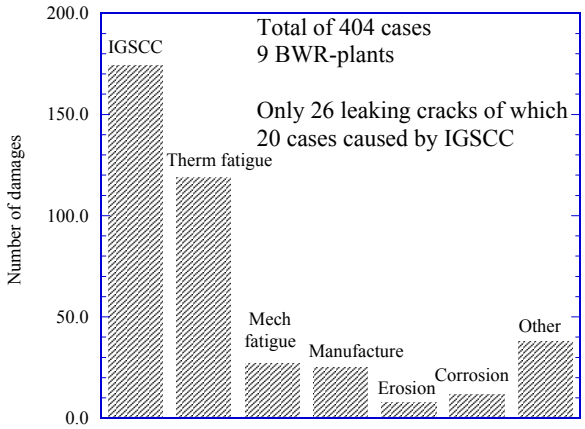
What mechanisms cause leaks and ruptures in pipe systems?

Damages are usually caused by mechanisms not anticipated during design.

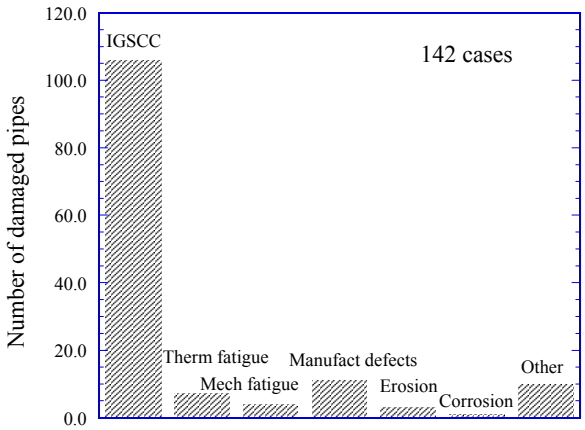
- IGSCC
- Thermal fatigue
- Erosion-corrosion
- Vibration-fatigue

SKIs database STRYK
(entry date 1998-02-09)

Damage mechanisms, all BWR-components



Damage mechanisms, pipes



How shall the components be selected for ISI?

Inspect components for which the contribution to the Core Damage Frequency (CDF) or Large Early Release Frequency (LERF) are the largest.

How is the core damage frequency estimated?

$$CDF = P(\text{small leak}) \cdot C(\text{small leak}) + P(\text{large leak}) \cdot C(\text{large leak}) + P(\text{rupture}) \cdot C(\text{rupture})$$

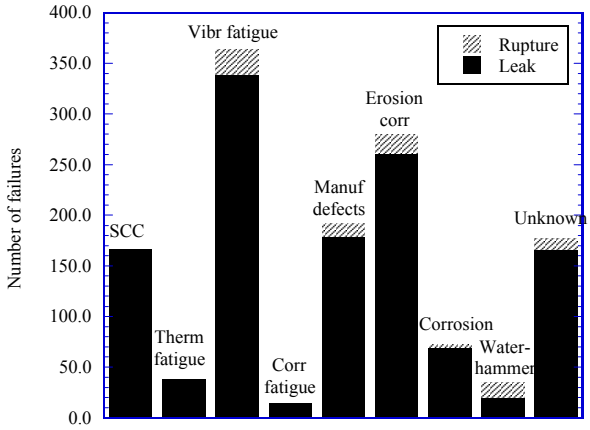
where P = probability of leak or rupture

C = consequence of leak or rupture

Estimation of probability of failure:

- by failure statistics
- by models based on probabilistic fracture mechanics
- by expert panels

Total number of failures in US Nuclear piping, BWR + PWR, 1961-1995. Total of 1338 cases.



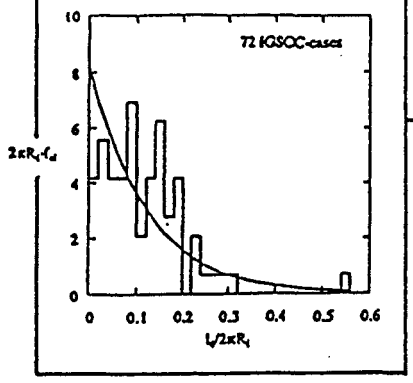
Models based on probabilistic fracture mechanics

In a physical model for growing cracks and how fracture occurs, some key variables are treated as probabilistic and the probability of leak or rupture is obtained by integration of the frequency functions.

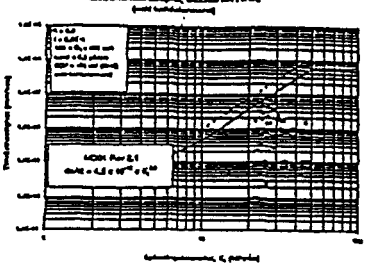
- WinPRAISE (Eng. Mech. Technology, 1998)
- LEAKPROF (WOG, 1997)
- PIFRAP (SAQ, 1999)

PIFRAP

Initial crack length distribution

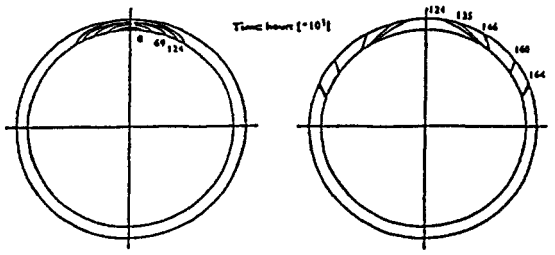


$\frac{da}{dt} = C \cdot K_I^n$ IGSCC rate

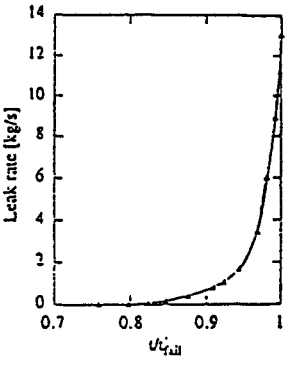


STRESS STATE
- operating stress
- residual stress
- vibration stress
- level A/B-loads
- water hammer
- seismic loads

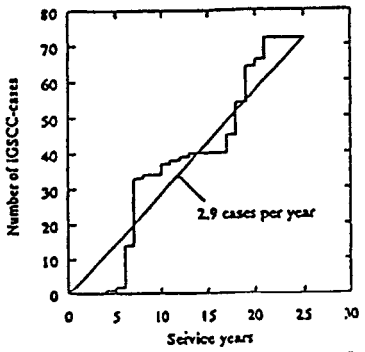
Crack size and COD as function of time



Leak rate evaluation



Initiation probability

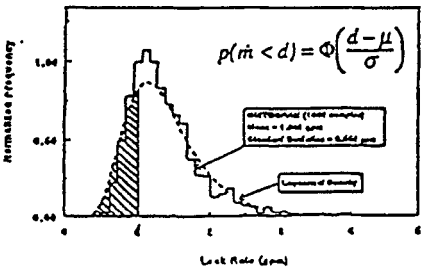


Failure criterion

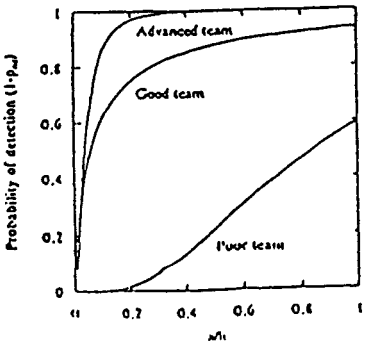
$J = J_{Ic}$ or

$P = P_L$

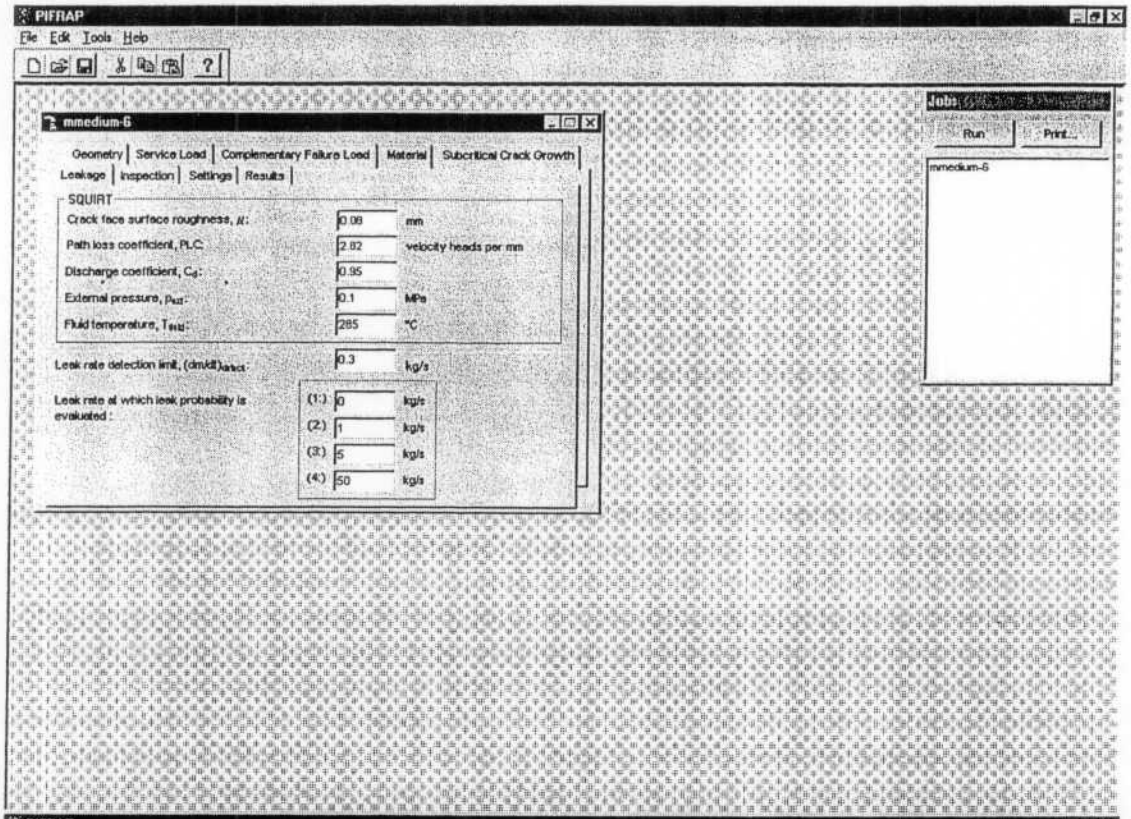
Probability of not detecting a leak rate

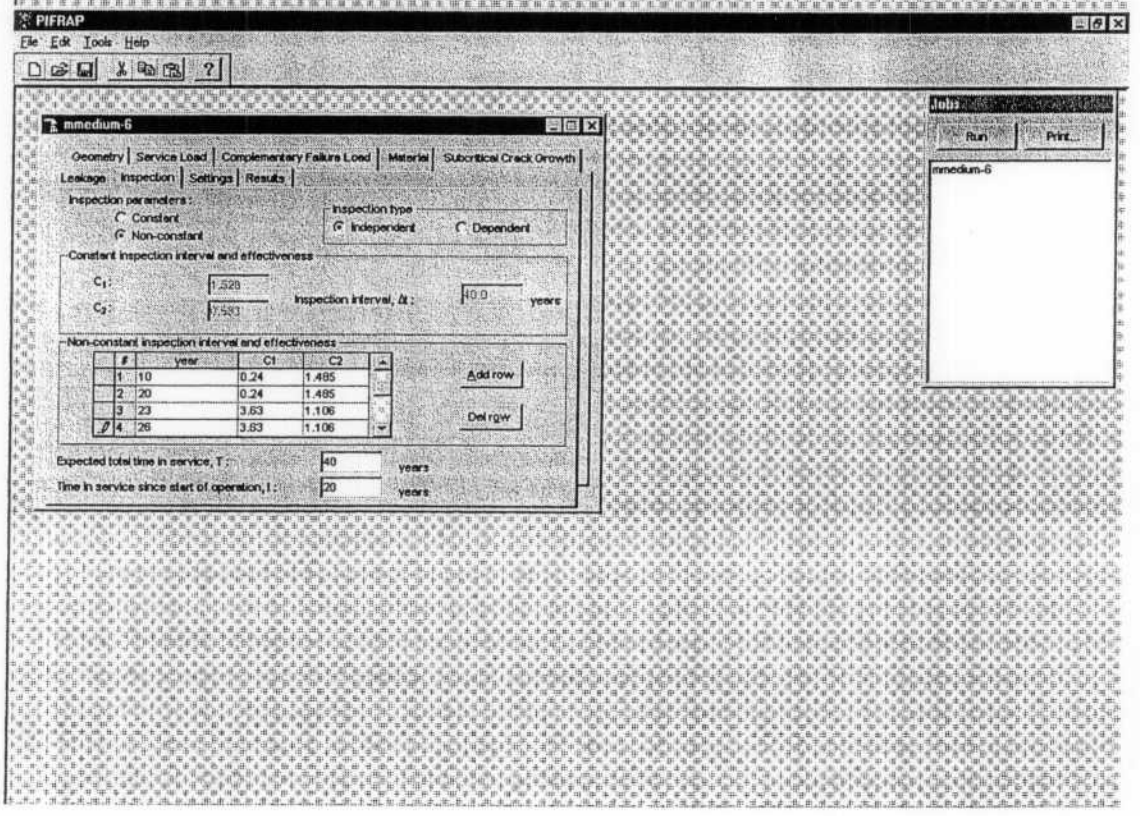


Probability of non-detection during ISI

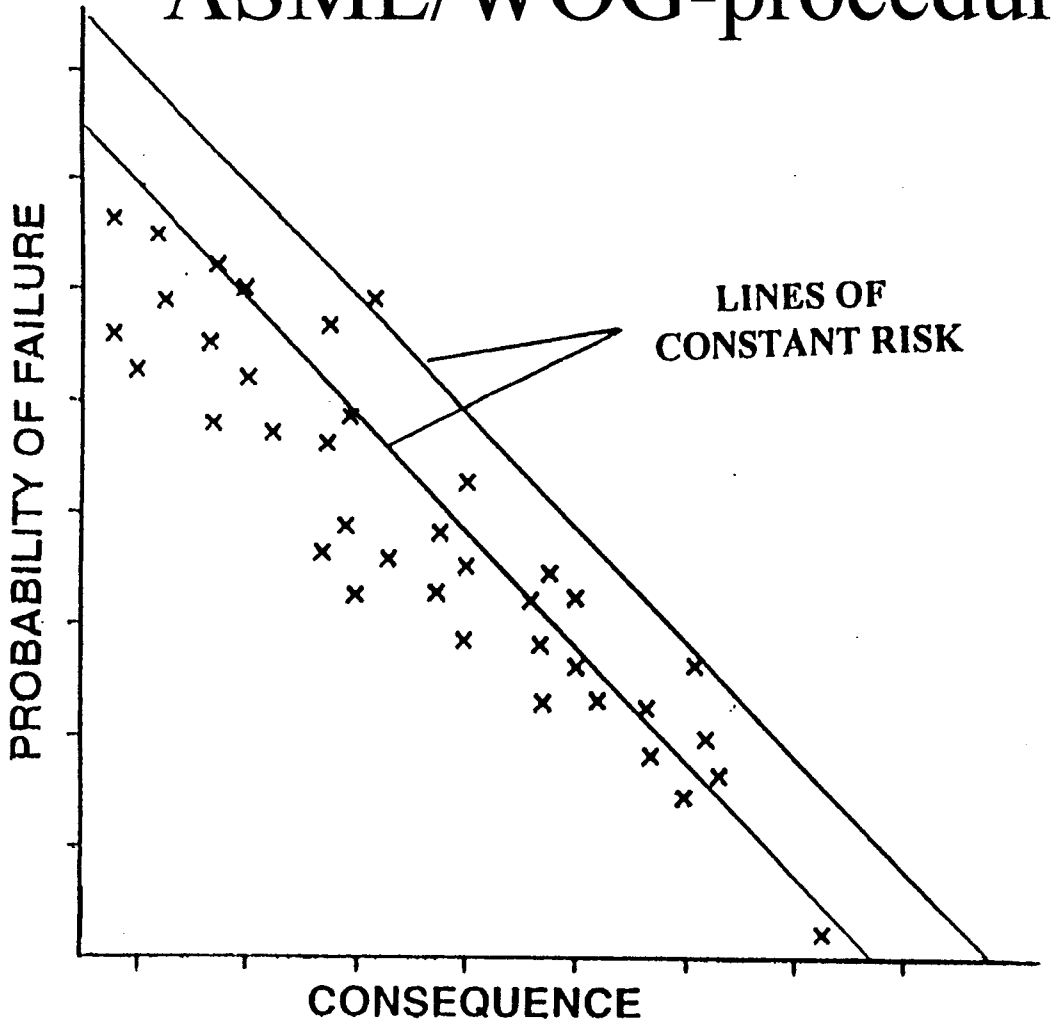


Pipe break probability p_f per year per weld


PIFRAP
File Edit Tools Help
mmedium-6
Geometry | Service Load | Complementary Failure Load | Material | Subcritical Crack Growth
Leakage | Inspection | Settings | Results
SQUIRT
Crack face surface roughness, R:
0.08
mm
Path loss coefficient, PLC:
2.82
velocity heads per mm
Discharge coefficient, Cd:
0.95
External pressure, pext:
0.1
MPa
Fluid temperature, Tfld:
285
°C
Leak rate detection limit, (dm/dt)detect:
0.3
kg/s
Leak rate at which leak probability is evaluated :
(1:)
0
kg/s
(2:)
1
kg/s
(3:)
5
kg/s
(4:)
50
kg/s
Jobs
Run
Print...
mmedium-6


PIFRAP
File Edit Tools Help
mmedium-6
Geometry | Service Load | Complementary Failure Load | Material | Subcritical Crack Growth
Leakage | Inspection | Settings | Results
Inspection parameters :
Constant
Non-constant
Inspection type
Independent
Dependent
Constant inspection interval and effectiveness
C1 :
1.528
C2 :
7.583
Inspection interval, Δt :
40.0
years
Non-constant inspection interval and effectiveness
| year | C1 | C2
1 | 10 | 0.24 | 1.485
2 | 20 | 0.24 | 1.485
3 | 23 | 3.63 | 1.106
4 | 26 | 3.63 | 1.106
Add row
Del row
Expected total time in service, T :
40
years
Time in service since start of operation, t :
20
years
Jobs
Run
Print...
mmedium-6

ASME/WOG-procedure



Requirements of the probabilistic software

- All relevant damage mechanisms should be adressed.
- The codes should be able to distinguish between leak and rupture
- The codes should be able to account for ISI and leak detection.

No probabilistic software can be considered to be perfect. Validation of new codes can be done by comparison with failure statistics and with other validated codes (WinPRAISE).

Estimations of failure consequences:

PSA

- Level 1, CDF
- Level 2, LERF
- Level 3, Environmental damage caused by radioactive release

Leak and ruptures in pipe systems are usually modelled in 3 categories in PSA:

- Small leak, can be replaced by auxiliary feedwater.
- Big leak, decrease of pressure is needed to inject water through the ECCS.
- Guillotine break

Project: Pilot study of Oskarshamn 1

Objective: Determination of locations for ISI and inspection intervals by using RBI-methods. A comparison shall be performed with the current Swedish procedure in SKIFS 1994:1 using the procedures by ASME/WOG and EPRI.

Project team

SAQ (project manager)
OKG Aktiebolag
SKI
NUSAB Aktiebolag
Vattenfall AB, Ringhals
SAFETECH Engineering

Scheduled to be completed by September 30, 1999.

Example 1:

IGSCC in a weld in the feedwater system, Oskarshamn unit 1.

$$CDF = P_1 \cdot C_1 + P_2 \cdot C_2 + P_3 \cdot C_3 + P_4 \cdot C_4$$

P = probability of a pipe leak or rupture
C = consequence of a pipe leak or rupture

PIFRAP, version 2.0

$P(\text{small leak}) = 2 \cdot 10^{-4}$ per reactor year

$P(\text{large leak}) = 7 \cdot 10^{-8}$

$P(\text{guillotine break}) = 7 \cdot 10^{-8}$

Credit is taken for leak detection but not for inspections.

PSA - O1 $\Rightarrow$

$C(\text{small leak}) = 5 \cdot 10^{-7}$

$C(\text{leak} > 15\ \text{kg/s}) = 2 \cdot 10^{-5}$

$C(\text{leak} > 30\ \text{kg/s}) = 3 \cdot 10^{-3}$

$C(\text{guillotine break}) = 3 \cdot 10^{-3}$

Core damage due to unsufficient core cooling is dominating in C

$$CDF = P_1 \cdot C_1 + P_2 \cdot C_2 + P_3 \cdot C_3 + P_4 \cdot C_4$$

$$CDF = 2 \cdot 10^{-4} \cdot 5 \cdot 10^{-7} + 7 \cdot 10^{-8} \cdot 2 \cdot 10^{-5} + 7 \cdot 10^{-8} \cdot 3 \cdot 10^{-3} + 7 \cdot 10^{-8} \cdot 3 \cdot 10^{-3}$$

$$= \quad 1 \cdot 10^{-10} \quad + \quad 1 \cdot 10^{-12} \quad + \quad 2 \cdot 10^{-10} \quad + \quad 2 \cdot 10^{-10}$$

$$= 5 \cdot 10^{-10}$$

The risk is dominated by large disabled leak and guillotine break in this example.

Definition of an inspection program

1. Selection of pipe systems and components to inspect in these systems
2. Technique to detect and size potential damages.
3. Determination of a suitable inspection interval.

Tabell B2.1

Konsekvens-index / Skade-index	1	2	3
I	A	A	B
II	A	B	C
III	B	C	C

USNRC Reg. Guide 1.174 contains acceptance guidelines in terms of changes in CDF or LERF in order to accept a new RBI-program in a plant

$\Delta CDF = CDF(\text{new ISI-program}) - CDF(\text{old ISI-program})$

- If $\Delta CDF < 0$, then OK
- If $\Delta CDF > 0$, then it should be less than 10^{-6} per reactor year

EPRI's RBI-procedure for ISI
ASME Code Case N560 and N578

		Consequence Category			
		None	Low	Medium	High
Degradation Category	High	Low	Medium	High	High
	Medium	Low	Low	Medium	High
	Low	Low	Low	Low	Medium

EPRI's definition of pipe break potential depending on degradation mechanism

Large Pipe Break Potential	Leak Conditions	Degradation Mechanism
High	Large	Erosion Corrosion Waterhammer
Medium	Small	Thermal Fatigue Corrosion Fatigue/Cracking Stress Corrosion Cracking Local Corrosion Attack (O_2, MIC, Pitting) Erosion/Cavitation
Low	None	No Degradation Mechanisms

EPRI's definition of consequence categories

Consequence Category	Corresponding CCDF Range	Corresponding CLERF Range
High	CCDF > 1E-4	CLERF > 1E-5
Medium	1E-6 < CCDF ≤ 1E-4	1E-7 < CLERF ≤ 1E-5
Low	CCDF ≤ 1E-6	CLERF ≤ 1E-7

ASME/WOG-procedure	EPRI-procedure
Includes models for both failure probability and failure consequence.	**Failure potential assessed by failure statistics.**
ISI-selection driven by high risk (R = P*C).	**ISI-selection driven more by consequences.**
Can provide ΔCDF.	**Simple to apply but can not in general provide estimates of ΔCDF.**
Requires more detailed information of each component.	

Example 2

Determination of an inspection interval in system 321, Forsmark 1.

- D = 168 och 273 mm, t = 7.1-19 mm
- Damage mechanism IGSCC
- Detection limit, crack depth a_0 = 2 mm

Pipe section (D x t)	Inspection interval (deterministic)	Rupture probability PIFRAP (per year)
168 x 7.1 mm High loads	1 year	$0.36\ 10^{-5}$
273 x 11.6 mm High loads	4 years	$0.14\ 10^{-6}$
168 x 12.9 mm Low loads	10 years	$0.27\ 10^{-7}$
273 x 19 mm Low loads	> 10 years	$0.91\ 10^{-10}$

APPLICATIONS OF RISK BASED METHODS

- Guide the selection of ISI-locations.
- Provide information of the effectiveness of a certain ISI-method.
- Determine the change of CDF due to a new selected ISI-program.
- Provide an alternative way of determining inspection intervals.
- Guide economic decisions of if and when maintenance efforts should be done.

Use of Living PSA in Regulatory Decision Making in Finland

Reino Virolainen
Radiation and Nuclear Safety Authority (STUK)
Nuclear Reactor Regulation, P.O. Box 14 FIN-00881,
Helsinki, Finland

1 Introduction

Consideration of severe accidents beyond the traditional design basis, including full core melt accidents, has become an important ingredient of regulatory process in Finland. Increasingly, decisions are being based, at least in part, on results of plant-specific Probabilistic Safety Assessments (PSA) studies. Plant-specific level-1 and level 2 PSA studies, including internal initiators, fires, flooding and harsh weather conditions are required by STUK. These studies are used in a living fashion both at the utilities and at STUK. PSA has got an important role in the safety management at Loviisa and Olkiluoto (OL) plants and in the regulatory process of STUK.

2 Living PSA in Regulatory Use

The guidelines for applying the Living PSA are set forth in the Regulatory Guide YVL 2.8 "Probabilistic Safety Analyses (PSA) in the Licensing and Regulation of Nuclear Power Plants" issued by STUK [1]. The Living PSA is formally integrated in the licensing procedure already in the early design phase and it is to run through the construction and operation phases all through the plant service time.
In compliance with the requirements posed in the revised Regulatory Guide YVL 2.8 (published 1996) the licensee has to use the results of PSA in support of decisions on operational safety issues e.g. as follows:

- plant changes and backfits
- training of plant personnel
- working out of emergency operation procedures
- applications of Tech Specs
- case by case assessment of risks resulted from component failures
- risk follow-up of Licensee Events
- directing and weighting the In- Service Inspections and Testing
- maintenance and surveillance programme planning

Many specific applications of the Living PSA have are already been introduced [2,3,4] but some are still waiting for further development such as ISI, IST and Risk Based Tech Specs.

2.1 Plant modifications and backfits

PSA has identified at Finnish NPPs numerous safety issues which were not recognised with deterministic reviews. It is a regulatory requirement that the utility must provide STUK with the assessment of safety significance of the proposed modification in conjunction with the pre-inspection documentation. In the course of the regulatory process the candidate hardware or software changes have to be modelled in the PSA, and the risk reduction potential is to be assessed in support of resolution of the

safety issue. A kind of assessment has to be submitted to STUK independent of the safety class which the modified systems belong to.

STUK uses constantly deterministic reviews to ensure the conclusions made by PSA, and to complement the PSA review. The deterministic reviews and analyses are necessary for demonstrating that the systems and components fulfil the design objectives set for them. The assumptions on the loading of components, operating parameters of systems, and faults impairing the performance of systems, which are made in the analyses, are defined in the design requirements. In the course of past several years the core damage probability of Loviisa plant has been lowered with no less than one order of magnitude [5].

2.2 Emergency Operation Procedures and Training of Personnel

New EOP's have been written to provide guidance for operators in certain accident sequences which the Olkiluoto I and II (BWR) PSA indicated to be of high importance to risk as follows

- refilling of the emergency feed water tank and condenser
- crossconnection of the diesel generators of neighbouring plant units
- manual depressurization of the reactor tank from the relay room

Insights from PSA have also been taken into account in the contents of operator training programmes. Both utilities have used the most important accident sequences of the PSA in the simulator training as well as in improving the emergency operating procedures.

2.3 Technical Specifications

Some temporary exemptions from Technical Specifications (Tech Specs) requirements have been approved on the basis of risk evaluations. If the utilities apply for a temporary exemption from Tech Specs, they have to assess the safety significance of the respective exemption with PSA. In such a case however it is provided that the extension of the Allowed Outage Times (AOT's) contributes only a tiny increment to the core damage probability compared with normal operation. The procedure is based on the use of deterministic and probabilistic reviews as complementary methods to each other.

Furthermore, the meaningfulness of some AOT's given in Technical Specifications has been evaluated by PSA techniques. Certain inconsistency with the deterministic AOT's and actual risk impact has been identified. The following example illuminates the issue. The core damage probability within 30 days implies a risk contribution of e.g. a latent failure during typical surveillance test period. The PSA results show (Table 1) that the impact of the different type of safety systems on risk can be fairly remarkable. Accordingly a twofold CCF in the service water system (721) implies the same risk as a fourfold CCF of diesel generators (653) and auxiliary feedwater systems (327). An explanation to that is an inter-unit crossconnection back-up to the failed dieselsystem and a manual depressurization back-up to the failed auxiliary feedwater system (327). In addition a certain asymmetry of the risk contributions appeared inside the safety systems. The two-fold failure of the trains A and C of the auxiliary feed water system resulted in much higher contribution to the core damage probability than the trains A and B. An explanation to the asymmetry is that the trains A and C are more sensitive to CCF initiators like fire and flooding than trains A and B because of less mutual isolation.

Table 1. Risk based rating of hypothetical safety systems failures at a BWR plant (CDF=$2{,}5 \cdot 10^{-5}$/a)

Multiplicity of sybsystem failures		Core damage probability within 30 days
Auxiliary feed water	327 AC	$3{,}4 \cdot 10^{-5}$
	327 AB	$1{,}5 \cdot 10^{-6}$
	327 ABC	$3{,}9 \cdot 10^{-5}$
	327 ABCD	$2{,}1 \cdot 10^{-4}$
Diesel generator system	653 AC	$4{,}5 \cdot 10^{-7}$
	653 ABCD	$3{,}1 \cdot 10^{-4}$
Service water system	721 AC	$1{,}2 \cdot 10^{-4}$

An analysis of the comparison of shutdown risk versus risk of continued operation has been made by TVO power company to support the reconsideration of the Technical Specifications (TS). The comparison enlightens how reasonable the considered TS rule is. TVO pursues changes to the Allowed Outage Times when at least three or four redundant subsystems in the service water system is failed. The present rule requires immediate shutdown. TVO proposed that a continued operation is allowed at most for three days for triple and quadruple failures. The proposal is based on the view that a shutdown of the plant is not safer than a continued operation until the failures are repaired.

Additional items have been included in the Technical Specifications for Shutdown States based on the results from shutdown mode PSA. STUK decided that the lower air lock of the containment of OL units will be kept closed when the maintenance of the main coolant pumps is underway, in order to reduce the risk the risk of a large LOCA in the lower head of the pressure vessel [6]. If large lower head LOCA takes place and the lower air lock remains unlocked, the coolant escapes out of the containment and prevents adequate core cooling function which leads to core uncovery and core damage within few hours.

2.4 Analysis of Operational Events

In the area of operational events PSA is becoming a standard tool to assess the safety significance of component failures and incidents. Accordingly systematic risk follow-up studies are being made at STUK. A risk follow-up study of Olkiluoto nuclear power plant's unit 1 and 2 was completed in September 1994 at STUK. In this study the identification of safety related component failures and possible precursors were investigated and their contribution to the core melt frequency was assessed. The study was made according to the operating experiences of these units during years 1986-1991 (OL 1) and 1985-1994 (OL 2) [7,8]. All incidents were gathered from Licensee Event Reports provided monthly and daily by the TVO and were analysed with the STUK's living PSA-code and the updated version of TVO's PSA model.

The contribution of component failures and operational disturbances to the expected annual core damage probability during the studied time period was only few per cents in both units. It appeared that the infrequent, significant precursors (LOCAs, transients, fires etc.) would provide the main contribution to the total cumulative risk. The risk contribution from safety related component failures and other operational events seems to remain insignificant.

Based on the insights received from the risk follow up studies, STUK has set forth a internal risk based objective for operational events at Finnish NPPs. The objective is that the annual share of operational events (component failures, preventive maintenance, exemptions from Tech Specs, incident) is equal to or less than 5 % in the predicted annual core damage probability. This objective constitutes the strategy by STUK to lessen the number and contribution of operational events at NPPs.

Table 2 Contribution Of operational events to the annual core damage probability

Classification	Description	Tua	Ax	%
Incidents	OL: Reactor sram caused by frazil ice in the sea water channels	0.6	113.94	0.732
	LO: Unavailability of emergency feed water system because of crossfailure	9	12.70	1.344
Exemption from Tecs. Spec.	OL: One subsystem's dieselgenerator was disconnected during normal operation to carry out modifications in diesel's air inlet	52.8	1.04	0.022
	LO: Pipe modifications in service water system during normal operation causing unavailability in heat exchangers of residual heat removal system	10	1.11	0.014
Failure	OL: The pump of shutdown cooling system tripped because of overcurrent during startup. Pump was mechanically jammed	28.6	1.01	0.002
	LO: The cooling compressor of air conditioning plant system fails to work	48.07	1.17	0.114
Preventive maintenance	OL: Preventive maintenance: diesel package in subsystem C.	156.9	1.75	1.392
	LO: Periodic inspection of the protection system of residual heat removal system pump	27.48	1.04	0.014

Tua = Unavailability time [hrs], Ax = Risk Achievement Worth, % = Percentage from the annual core damage probability

2.5 Risk based ISI and IST

Use of PSA has up to now been rather limited for regulating and controlling in-service testing and inspections (ISI/IST). Some test intervals, such as diesel generator testing have been modified at OL 1 and 2 in order to reduce negative impact of tests to the equipment ageing. Preventive maintenance of diesel generator systems, high and low pressure core cooling systems during operation has been re-scheduled at OL 1 and 2 based on insights from PSA.

A new project dealing with PSA support to regulatory audits has been initiated at STUK in 1997. The aim of the project is to explore on how the plant specific PSAs can best be used effecting specific regulatory tasks such as ISI, IST, preventive and corrective maintenance activities. The pilot studies on ISI of piping both of PWR and BWR plants are in progress. The systems subject to the pilot study are the high pressure injection system and emergency feed water system at PWR and the shut down cooling system and the feed water system at BWR plant.

The STUK's risk-informed procedure combines both the plant specific PSA information and the deterministic insights in support of the system specific, detailed ISI program selection. Piping of all systems important to safety are exposed to the selection procedure irrespective of the ASME class (1,2,3 or even non-code piping). The selection procedure includes several steps such as selection of systems and identification of the evaluation boundaries and functions, consequence evaluation and qualitative degradation mechanism evaluation of piping and division of the segments into different inspection categories. Division of pipe segments into various degradation categories is to be based mainly on qualitative identification of the mechanism which the pipe segment is exposed (such as erosion corrosion, vibration fatigue, water hammer thermal fatique, stress corrosion cracking and others). Division of pipe segments into various consequence categories is based on conditional core damage probability estimated by PSA applications. Finally the expert panel containing all affecting engineering disciplines combines the deterministic and probabilistic information as emphasize by the EPRI's approach and the NRC's regulatory guides [9,10]. The pipe segments are divided into different inspection categories containing high, medium and low risk segments, respectively.

3 Concluding remarks

While PSA is recognised as an effective tool and review method for many different regulatory and safety management purposes, we have to acknowledge its limitations which are often related to the level of modelling or methods, not yet mature enough for some specific applications. Hence, in context of the aforementioned activities, STUK has to use both deterministic and probabilistic reviews in parallel while controlling and regulating the issues.

References

1. Regulatory Guide YVL. 2.8, Probabilistic Safety Analysis (PSA) in the Licensing and Regulation of Nuclear Power Plants, Finnish Centre for Radiation and Nuclear Safety (STUK), Helsinki 1987.
2. Virolainen R, Niemelä I, Implementation and Introduction of Living PSA in Co-operation with Finnish Utilities and Authorities, PSA`93- International Topical Meeting on PSA, Clearwater Beach; Florida, January 26-29, 1993.
3. Okkonen T, Niemelä I, Sandberg J, Virolainen R, Development of a parametric containment event tree model for a severe BWR accident. A pilot Study, Proceedings of Probabilistic Safety Assessment and Management`96- ESREL`96 - PSAM-III, June 24-28, 1996, Crete, Greece.
4. Reiman L, Expert Judgment in Analysis of Human and Organizational Behaviour at Nuclear Power Plants, (Doctor Thesis), STUK-A118, Finnish Centre for Radiation and Nuclear Safety, December 1994
5. Vaurio J, Jänkälä K, Safety Management of a VVER Plant by Risk Assessment, PSA`96- International Topical Meeting on PSA, Moving toward Risk-Based Regulation, Park City, Utah, September 29-October 3, 1996
6. Sandberg J, Virolainen R, Niemelä I, On the Regulatory Review of the TVOI/II Low Power and Shutdown Risk Assessment, Proceedings of Probabilistic Safety Assessment and Management`96- ESREL`96 - PSAM-III, June 24-28, 1996, Crete, Greece
7. Julin A. and Virolainen R, PSA Based Event Analysis of Incidents and Failures at TVO BWR, PSA`96- International Topical Meeting on PSA, Moving toward Risk-Based Regulation, Park City, Utah, September 29-October 3, 1996
8. Tiippana P, Development of Safety Assessment of Nuclear Power Plants Using Indicators, Diploma thesis (in Finnish), STUK.YTO-TR, Helsinki 1997, 76pp +appendices
9. US NUCLEAR REGULATORY COMMISSION, "An Approach for Plant -Specific, Risk-Informed Decisionmaking: In-Service Inspection of Piping", Draft Regulatory Guide DG-1063, January 9, 1998
10. S.R.Gosselin, " EPRI's new in-service inspection program", Nuclear News, November 1997

The use of PSA in regulatory activities, in the past and in the future

Lars Gunsell, Swedish Nuclear Power Inspectorate, SKI.

Introduction

This report gives a short description of the role and the historical development of risk analyses to support design and operation. The role of SKI is mentioned. The aim of the report is to give a platform for a further development of risk analyses towards a more risk informed safety work.

The role of risk analyses in developing safety

Risk based principles has recently been referred to as a new element of safety works. To understand what is new we have to look back at the historical development of safety. The deterministic safety principles that existing plants are designed to do indeed consist of a large portion of risk based thinking. As examples we have the categorisation of initiating events to be considered in design, which are guided by their occurrence frequency, the use of single failure criterion and allowed time to repair components during operation. This indicates that there should not be any fundamental contrasting difference between the original deterministic base and a more risk based approach. The main difference is the fact that we today have access to much more powerful methods and tools to perform risk analyses. We have also more operating experience and failure data to support the risk analyses.

The use of risk analyses and its development can be described as three phases. The first phase is to identify the risks, evaluate them and define safety demands to bring the risk to an acceptable level. In the second phase risk analyses could give guidance to safety principles, specifications and measures on technical and administrative systems to meet the demands. A third phase could be to demonstrate that a specific plant meet the safety demands. Such a demonstration must be repeated during the lifetime of a plant if conditions are changed.

On the following pages three figures are used to show the relation between risk analyses, deterministic demands and the plant design and operation. The figures also illustrate how risk analyses has developed. The figures represent the situation when the early deterministic demands were developed, the situation when PSA was introduced and finally the situation when Living PSA is fully used.

Introducing more detailed risk analyses may reveal some areas where the demands have to be more stringent and some where it may be eased. The deficiencies in safety that PSA has pointed out have been of different kind. Some are shortcomings in fulfilling the demands, some are deliberately made deviations from safety principles that are found to have an unacceptable consequence, and some are resulting from insufficient demands. In the latter case it is not sufficient to make changes in the plant only, but there also has to be changes made in the demands (SAR) using the insight that PSA has given. PSA has mainly been used

to identify deficiencies and not to find areas of large conservatism where demands can be eased, thus we do not have many examples of such studies.

The development of Living PSA should lead towards a tool with sufficient degree of completeness, quality and user friendliness to be used daily in safety work. Common applications to start with are evaluation of changes in design and Technical Specifications, support for exemptions and risk follow-up of operating experience.

As the risk analyses get more detailed, it increases the possibility to use it to define more differentiated demands on system and components. The general assumptions and demands in general roles and regulation may to some extent be replaced with individually determined demand that are more suitable for the actual plant design and situation. Conservative and expensive demands that do not contribute to safety can be avoided. This is especially important for existing units that can find plant specific design solutions to safety issues and to increase flexibility in operation and maintenance. This way of treating safety issues may play an important role in the near future in Sweden and in other countries where the challenge is to implement more modern safety demands on older plants with the object to upgrade safety. How fare risk informed principles can be used is a matter of credibility of the analyses and what is practically achievable. There is also a need to established roles how to combine quantitative safety goals with basic safety principles e.g. defence in depth, single failure criterion and robustness.

The role of SKI in safety work

The operator has the undivided responsibility for safety of the nuclear power plant. The responsibility of SKI as a regulator is to define the roles and review that the operator takes his responsibility. SKI shall also promote the development of safety. SKI has the same task regarding risk analyses.

After the TMI Accident in 1989 individual PSA studies became mandatory for all plants in Sweden. During the eighties PSA was focusing on level 1 studies and during the nineties most plants has also performed level 2 studies and external event analyses. Some plants have included risk during shut down. The schedule to perform the studies is defined by SKI.

Initiating and supporting different research projects is the most pronounced promotion of risk analyses done by SKI. One example is the large benchmark exercise that took place in the late eighties that included all PSA studies finalised in Sweden at that point. Other SKI supported activities are development of Living PSA methods, external event PSA methods, integrated safety analyses, and development of data bases such as component failure rate, initiating events frequencies, pipe failure rates and CCF probabilities.

The Regulatory work at SKI is going towards more general roles and demands and the original individual permits will be of less importance in the future. Examples are the SKI regulations "SKIFS 1994:1" regarding demands on mechanical equipment and "SKIFS 1998:1" which is a general top level document regarding nuclear safety. Work is also going on at SKI to define common demands on existing plants to be used in the modernisation process

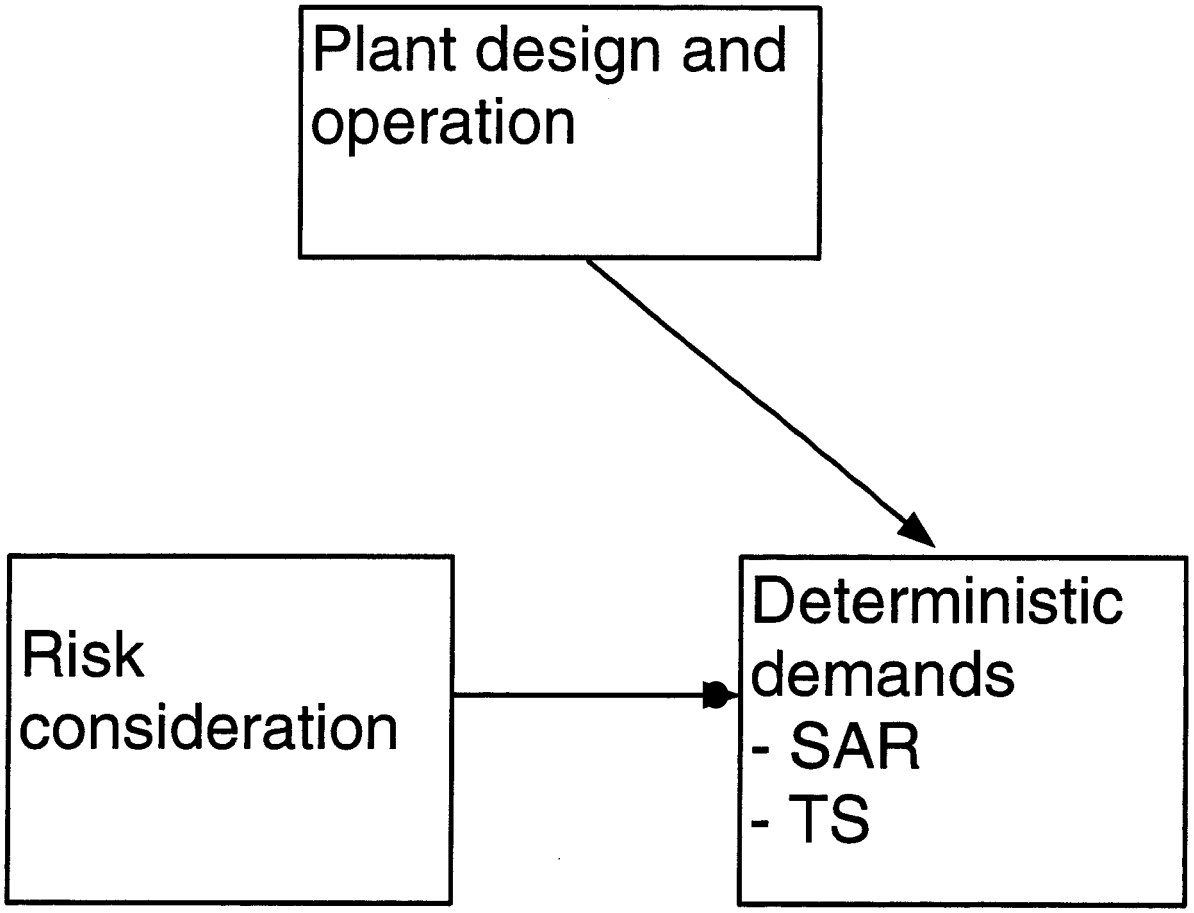
that has started. The challenge in this situation is to apply common safety demands to plants original built to different safety standards and with different design. Risk informed principles might be the tool to evaluate that the increased safety demands are met although the technical solutions may differ between the plants (as mentioned in previous chapter).

Developments to follow

To reach the goal of Living PSA and a considerable lager use of risk informed principles there are several tasks to carry out. (Refers to Swedish situation)

- The PSA has to be complete regarding initiating events, operating states and conditions.
- Improve methods and routines for evaluating plant changes, changes in Technical Specifications and exemptions.
- Improve methods for risk follow-up of plant operation and evaluation of results.
- Update the Safety Analyses Report (SAR) where PSA has identified that the demands are insufficient.
- Establish methods to combine quantitative risk goals with fundamental safety principles.

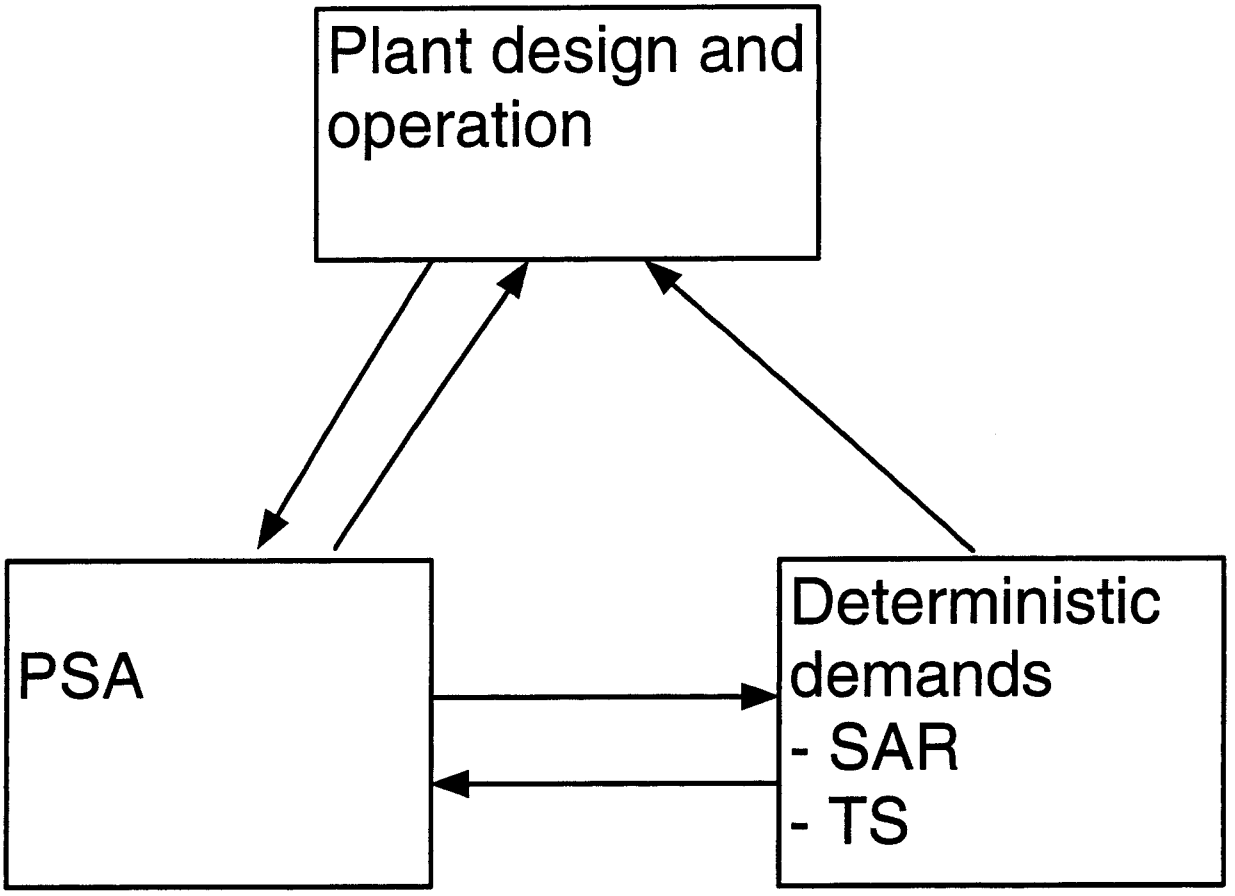
Development of the deterministic demands



Examples where the risk considerations are visible:

- Categorization of initiating events
- Single failure criterion
- AOT for repair during operation
- "Service limit" for mechanical equipment

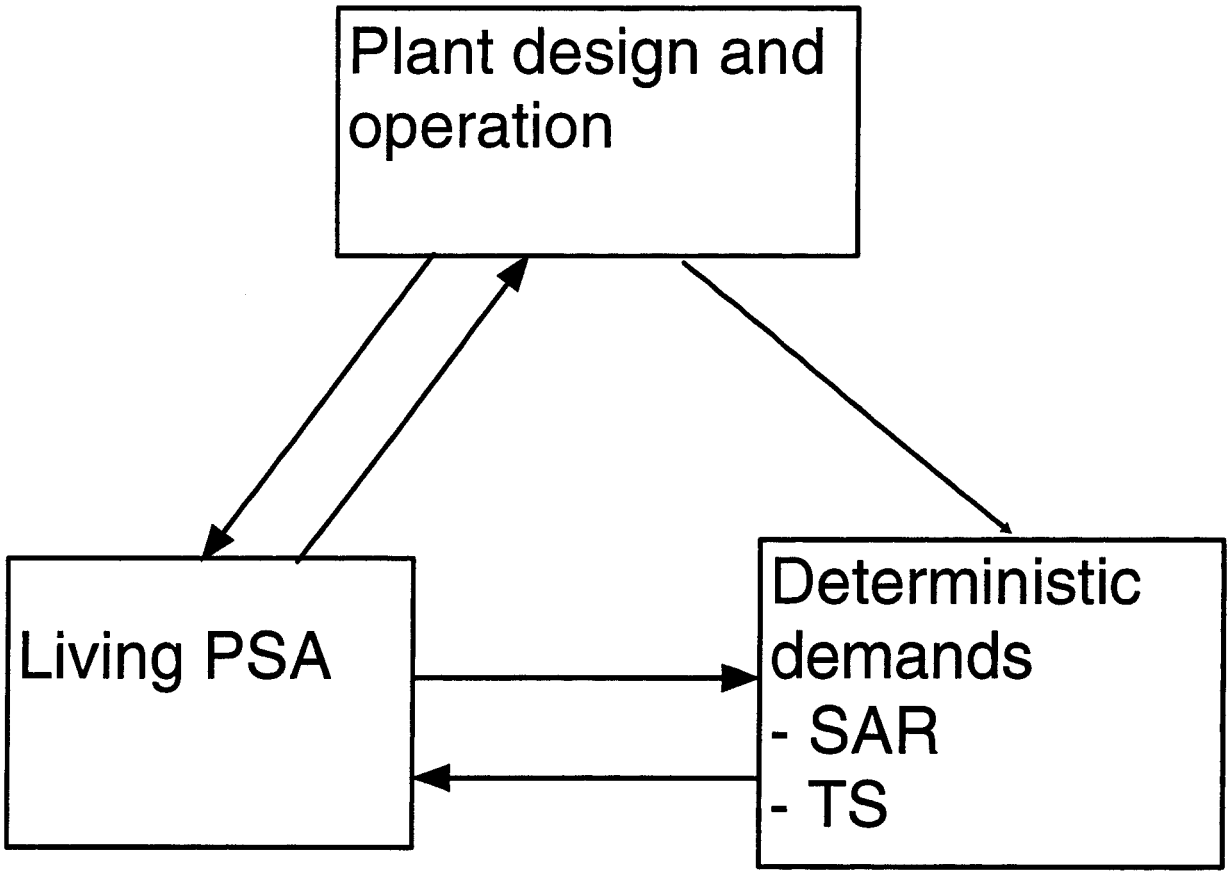
Introduction of PSA



Applications:

- Safety evaluation of design and operation
- Identification of shortcomings
- Definition of individual safety improvements
- Development of safety demands to support desired safety level

Introduction of Living PSA



Applications:

- Safety evaluation of plant changes, changes in TS and exemptions
- Safety evaluation of plant risk during operation
- Development of individual and situation adjusted demands without unnecessary conservatism

SOS-2-SEMINAR ON RISK INFORMED PRINCIPLES

DEVELOPMENT OF NEW RISK BASED REGULATIONS

Liv Nielsen
Norwegian Petroleum Directorate (NPD) Post Office Box 600 N-4003 Stavanger Norway

1. INTRODUCTION

In this presentation I will start by a short presentation of the oil and gas industry in Norway. A brief overview of the regulatory regime in the petroleum sector in Norway will be given. Risk analysis has been performed in Norway since 1981 and the various applications will be described. These risk analyses are quite different from a nuclear PSA and some of these differences will be commented.

Risk based optimisation techniques such as RCM and RBI is used in our industry, with very limited support from the risk analysis. Some of the limitations that exist when such techniques are imported from other industries will be commented on.

NPD is revising our regulations and some of our future plans when it comes to risk informed regulatory requirements will be presented.

2. NORWEGIAN OIL AND GAS INDUSTRY

All of our petroleum production comes from offshore fields, we have both subsea installations, and various types of platforms, varying from large integrated platforms with both drilling, production and accommodation to minor rather simple platforms performing one major function, e.g. drilling or gas compression.

We produce approximately 3 millions barrels of oil pr day, in addition to daily average gas quantity of 120 mill Sm3. Oil and gas is produced from more than 70 platforms in addition to several subsea production wells. The water depth range from 70 meters in the south up to 380 m in the Norne field in the north. The lasted discoveries of gas are located in a field with water depth of around 1200 m. The investment costs of an "average field" is around 20-30 billions in Norwegian currency.

Among the main internal contributors to risk are blowouts from the wells, which can cause both major environmental damage and if ignited, to the loss of a platform with substantial loss of lives. Another major risk contributor is process leaks leading to fire and explosion and thus impairing vital safety functions such as escape evacuation and control.

Among the dominant external risk factors are ship collisions, helicopter crashes and dropped objects.

3 BACKGROUND - REGULATORY REGIME IN NORWAY

The Norwegian Petroleum Directorate (NPD) is supervising the safety and working environment of the petroleum industry in Norway based upon the following main principles:

- focus on each individual operating oil company's own responsibility for prudent operations through regulations focusing on management and different types of administrative and organisational requirements
- objective or goal oriented regulations, moving away from prescriptive regulations
- regulations based on the various deterministic safety principles
- use of risk informed regulations

The first risk based NPD guideline was issued in 1981. Ten years later the current risk analysis regulation came into force.

4. RISK ANALYSES AND THEIR APPLICATIONS

4.1 Quantitative risk analysis

4.1.1 Acceptance criteria

The risk analysis regulation requires the Oil Company, often referred as the operator, to establish acceptance criteria covering risk for personnel, environment and material assets. These acceptance criteria should function as a decision tool for the management. In the NPDs experience, the acceptance criteria have not quite functioned as intended.

The way these criteria are formulated can lead to an inconsistency between the acceptance criteria and the complexity of the risk picture on a large integrated platform (with drilling, production and accommodation). To give an example, an acceptance criteria for personnel risk expressed as an average FAR value, can be insufficient as a decision tool because there is not enough focus on the risk level for risk exposed areas or risk exposed personnel groups.

The results of and QRA are presented as a given number, for instance as a FAR-value. The uncertainties attached to this given number are not discussed in most QRAs. Furthermore it is a challenge to find methods in order to achieve a better follow-up of analysis in the operational phase.

4.1.2 Application of QRA in the design phases

The QRA was originally developed as a design tool, to optimise the various platform concepts from a safety point of view.

The risk modelling has been consequence oriented and of the "short event tree, few fault tree" type. Much emphasis is put on gas dispersion models, simulations of gas explosions and fires and consequent impairment of vital safety functions like escape, evacuation and control. Given the design accidental loads, the layout of the platforms could be changed, even if some concepts rejected, until an acceptable safety level was achieved.

The QRAs have been used to assess the risk impact of major modifications on existing platforms.

The QRA has always supported emergency preparedness planning both in design and operational phases.

4.1.3 Application of QRA in operations

After the Piper Alpha catastrophe in UK sector, the NPD ordered the operators to perform risk analysis on existing platforms; also those being built before the requirement to perform risk analysis in the engineering phase. In this cases the risk analysis served as a way of identifying the platforms with the highest risk level. The risk model, level of detail etc used in the design phases is applied also for platforms in operations.

Even today, the QRAs are "purpose built" for the design phases, not for operations. In the design stages, the consequence picture can be altered by changes in layout, by adding and modifying safety systems etc. In operations focus should be on preventing accidents and their causes. In this perspective, it is striking that human and organisational factors with a few exceptions not are taken into consideration.

Another challenge is to find ways of a consistent follow up of assumptions from one analysis to the next, and also to find a way of keeping track of operational assumptions made in the engineering phase when moving into operations.

For platforms already being put into operation, the choice of efficient technical risk reducing measures are somewhat limited. In some cases the NPD has experienced that it is not possible to improve the risk level significantly by doing modifications. In these cases the essential issue is to find methods and techniques to control the risk level and to focus on the factors that may change the risk level in an adverse direction.

The NPD also have some observations when concerning updating of QRAs. Large accidents, major modifications etc lead to updating of existing QRAs. Minor changes both in technical solutions, manning levels, maintenance strategies, doesn't automatically lead to an update of the QRA, even if many small changes can add up to a significant change in the risk level.

4.1.4 Modelling

Compared to the situation in Sweden and Finland, there are some striking differences. The PSA are more standardised than the case in Norway. Risk Spectrum is used widely, in Norway we have several computer-based tools. None of them is close to the functionality of Risk Spektrum.

Likewise the T-book and I-book give input data and the industry has established guidelines for how to use installation specific and generic data. Providing reliable and valid input data is a more complex effort in our industry. Evaluation of different QRAs indicates a lack of standardisation both related to the databases used and basic assumptions. There is use a mixture of use of world wide databanks, OREDA data, North Sea data, platform specific data.

With the "short event tree, few fault tree" approach the effect of the safety systems is not studied in detail, in stead point values are given. Dependencies and common cause failures are to a large degree not considered. Uncertainties are not quantified and often not even discussed. Sensitivities are rarely used.

After the Piper Alpha catastrophe, several industry initiatives have been taken to improve the North Sea QRAs. HSE has played a major role, due both to generous R&D budgets and obligations to follow up offshore safety after Piper Alpha. HSE has also undertaken an extensive internal training program to ensure that the inspectors have sufficient training and competence in the risk analysis area.

Recently the industry has participated in a joint project related to ignition probability and explosion calculation. These projects are examples that demonstrate that common improvements can be made through co-operation.

4.1.5 Risk communication

In order to meet the intentions of the risk analysis regulation, both authorities, the management of the operating companies, the experts and the safety delegates, need to be able to understand the nature of risk analysis, their advantages and their disadvantages.

In the NPD's view, the successful implementation of risk analysis in petroleum industry requires a mutual learning- and communication process across the industry and involving both the experts performing the analysis and the different users such as the management, the authorities and the safety delegates.

In the NPD's view, there is room for substantial improvement when it comes to presenting the analysis to the different users. More emphasis needs to be put on communicating the results to different users.

4.2 Risk-based optimisation techniques

Risk based techniques such as RCM (Reliability Centred Maintenance) and RBI (Risk based Inspection) was developed in the defence and aviation industries, and are also used in the nuclear industry. In these industries with very high safety and reliability objectives, they have proven effective when it comes to cost reduction, and they have also maintained a high safety level.

Since maintenance cost can be significantly reduced by these techniques, the use of these techniques seems attractive.

There is however some safety concerns which must be taken in consideration. The aviation and nuclear industries have much better risk models and risk analysis than what is the case at least on the Norwegian Continental Shelf. There are several problems associated with importing methods and techniques from other more advanced environments.

Implementing such techniques is not easy in an industry that isn't fully prepared with respect to competence and training, development of analysis tools, new computer programs, investments in refined data collection etc. Top management tends to endorse techniques that can lead to significant cost reductions, but managers tend to be reluctant to support additional investments that are needed to ensure an effective implementation.

We have seen two different approaches to introduce and implement RCM/RBI in the industry. One approach started with developing an offshore version of criticality classification in order to reduce the workload. For safety reasons the criticality classification had to be very conservative,

and ended up with many subsystems and equipment classified as most critical. Some moderate cost reductions was achieved by this approach.

The other approach has been to carefully select and follow international standards, use competent consultants, run extensive training and competence building in parallel with the RCM process (learning by doing). The process was reviewed both internally and by the use of external experts. This process required extensive resources and therefore top management support, but the outcome in terms of cost reductions was impressive. So far, three years after the assessment of the first platform, there is no indication of safety related maintenance problems.

The assessment of the first platform, a small/average wellhead platform in the design stage, was a resource and time-consuming effort that took 20 man-years. The assessment of the next platform, a large platform for the processing and exporting oil and gas, was done with less manning requirements (14 man-years).

5 NEW OFFSHORE REGULATIONS

5.1 Description of the project

NPD has established a project revising existing regulations. Today we have 15 regulations that will be merged into four new regulations covering the following areas:

- technology
- operations
- documentation
- management

The present risk analysis regulation and risk-based requirements will be included in the management regulation.

The new regulations will be written and owned by three different and independent regulators, NPD, the State Pollution Agency and the Health Directorate. The new regulations are also written in close co-operation with the industry. Experts from the oil companies are members of regulation groups that work closely together with the regulators.

Hopefully, the new regulation will enter into force in January 2001.

5.2 QRA requirements

Based on what is said earlier about the quality f the QRA, there are needs for improvements. The need for a QRA better suited for operational purposes is widely recognised, but there are many different opinions on how this can be done.

With more than 80 platforms and pipeline systems in operation, the focus should change from the need for risk informed decision support in the design phases to the need for support during operations.

With the recent oil price fluctuations and the effect of the deregulation of the European energy markets might have on the gas price, risk based optimisation techniques will be used extensively to

reduce operating costs. The maintenance people now want QRAs that can be used for various maintenance purposes.

NPD also sees a need for the industry to co-operate in order to develop common risk models, methods and also to standardise the use of software. In the recent years some progress have been made, but there is still room for improvements. The new regulations will encourage the industry to move in this direction.

NPD will also encourage further development by initiating pilot project. Our first priority is to support in developing a QRA that have potential for wider applications than the existing one.

We are also trying to gain some experience from other industries. In this process experience from using risk analysis in the operational phase will be of great interest to us.

Methodology for development of risk indicators for offshore platforms

Knut Øien & Snorre Sklet
SINTEF Industrial Management
Safety and Reliability

Abstract

This paper presents a generic methodology for development of risk indicators for petroleum installations and a specific set of risk indicators established for one offshore platform. The risk indicators should be used to control the risk during operation of platforms. The methodology is purely risk-based and the basis for development of risk indicators is the platform specific quantitative risk analysis (QRA). In order to identify high risk contributing factors, platform personnel are asked to assess whether and how much the risk influencing factors will change. A brief comparison of probabilistic safety assessment (PSA) for nuclear power plants and quantitative risk analysis (QRA) for petroleum platforms is also given.

1. Introduction

Over the last few years, the use of risk-based decision-making has increased in the nuclear industry. Probabilistic Safety Assessment (PSA) is used both in design and operation of nuclear power plants (NPP) and in the area of incident and accident mitigation and management. In the petroleum industry Quantitative Risk Assessment (QRA) has been performed as part of the design process since the beginning of the 1980s when the Norwegian Petroleum Directorate (NPD) issued their "Guidelines for safety evaluation of platform conceptual design" (/1/). The QRA has primarily been used as a tool in the design phase. The use of QRA in the operational phase has mainly been limited to assessment of the effect of major modifications.

In 1994, the NPD initiated a pilot project (/2/, /3/ and /4/) with the purpose to develop a tool, a set of indicators, that could be used to measure changes in risk level during operation of petroleum platforms. These indicators should be used in the surveillance of changes in the risk level on the platform. The QRA was chosen as the basis for the development of risk indicators for two reasons. First, the QRA models were presumed to include those factors giving the most significant contribution to the total risk. Second, the QRA expresses the risk for personnel quantitatively and we wanted to develop a quantitative tool. The pilot project was followed up by another project where a set of risk indicators was developed for a specific installation (/5/).

The purpose of this paper is to present the generic risk-based methodology for development of risk indicators developed in these two projects and to present a set of risk indicators established for a specific platform. In addition we will give an overview of some of the differences between PSA for NPP and QRA for petroleum installations. Such a comparison is believed to provide the "PSA-community" with a better understanding of the basis of this "QRA-application".

The methodology for development of risk indicators is generic and can be applied to any petroleum platform and may also be applied in other similar industries. However, the platform (or plant/system) specific QRA must provide the basis for establishment of risk indicators. The

risk indicators should be used to control the risk during operation of platforms. The set of risk indicators presented in this paper is thus platform specific.

2. Risk-based decision-making

The usefulness of risk-based decision-making as a complement to the traditional deterministic approach, depends on the quality of the risk analysis, i.e. the coverage or scope of analysis, level of details of the models, input data, etc. There are differences in applications of PSA in the nuclear industry and QRA in the petroleum industry. In this chapter we will compare the applications of PSA and QRA and give a brief description of the differences between PSA and QRA.

2.1 Types of PSA-applications

Areas of applications of PSA in the nuclear industry are shown in Figure 1 (based on /6/). We have also indicated in Figure 1 the type of application presented in this paper, i.e. "safety indicators". Results from QRA are used in risk-based decision-making in a lesser extend than the PSA is used in the nuclear industry. Compared to the applications shown in Figure 1, QRA are mainly used in the design phase in order to:

- Evaluate and compare different platform concepts with regard to total risk
- Verify fulfilment of the risk acceptance criteria (i.e. total risk less than acceptable risk)
- Identify safety critical areas, systems and (to some extent) components
- Evaluate the effect on risk of major modifications.

As indicated in Figure 1, the methodology for development of risk indicators presented later in this paper is comparable to safety indicators in the nuclear industry.

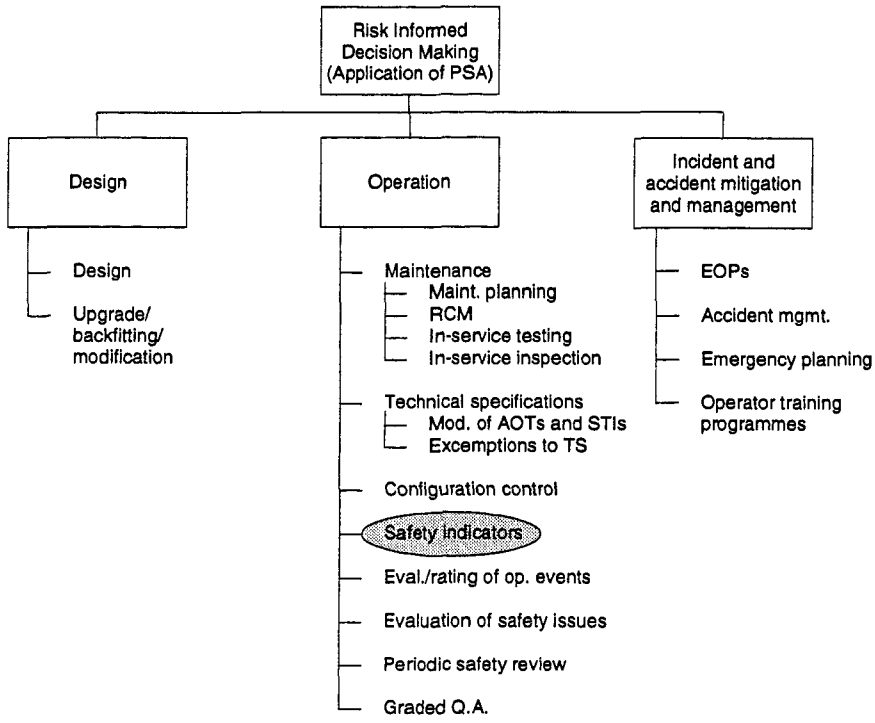


Figure 1. Areas of application for PSA (based on /6/).

2.2 Comparison QRA/PSA

This comparison between the quantitative risk assessments for nuclear power plants and offshore petroleum installations will only cover some aspects, and the main focus is on methodological aspects of interest in order to develop risk indicators[1].

Of course, there are some fundamental differences between risk associated with a nuclear power plant (NPP) and an offshore petroleum platform (OPP). The energies and processes are totally different, and the risk potential and type of consequences are different. The main focus of a PSA is public risk. There is both short-term (early fatalities) and long-term (latent cancer fatalities) consequences. Occupational risk, environmental risk and damage of material assets are normally not included in a PSA. Due to isolation, risk for platform personnel, including occupational risk, is focused in a QRA. Environmental risk (increasing focus) and potential damage of material assets are also covered in a QRA. Except for environmental accidents there is only short-term consequences.

Although the Reactor Safety Study (WASH-1400) (/11/) and some other plant-specific PSA have calculated the public risk (i.e. a level 3 PSA), most of the PSA are of level 1, i.e. calculating the core damage frequencies (CDF). This is somewhat similar as to stop the calculations in a QRA after assessing the risk of loss of the main safety functions (e.g. the integrity of the structure) and not assess the effect on the safety of platform personnel. The QRA can therefore be judged to have broader coverage than the PSA, both with respect to how far out the consequences are followed, and the type of consequences assessed. The depth of the analysis is, however, much larger in a PSA than in a QRA.

The main results from the comparison are shown in Table 1.

Initiating events

In the nuclear power industry there exists both tables of initiating events to be considered (e.g. IAEA lists) and data handbooks (e.g. the Swedish I-book). The latter also gives plant-specific frequencies of the initiating events. A second approach to this predefined list of initiating events is to deduce the initiating events based on what could threaten each safety function (for each core barrier). The root causes are also investigated and presented in a fault tree.

In the QRA, initiating events for process accidents[2] are the leakage of oil and gas themselves. The frequencies are established based on either the amount of leakage points (e.g. valves) times their generic leakage frequencies or plant-specific experienced leakages. The root causes of the leakages are normally not assessed.

Event tree and fault tree analysis

Compared to PSA, the QRA can be said to model the accident sequences by 'small event trees/small fault trees', i.e. the amount of accident sequences and the complexity of system models are much lower than in the PSA. In addition to have a broader spectrum of initiating events in a PSA, all systems including support systems (e.g. power supply) are explicitly modelled (in either the event tree or the fault tree).

---

1 This comparison is based on a review of PSA literature that describes how to perform a PSA (/7/, /8/, /9/ and /10/). However, no actual plant-specific PSA has been reviewed. The review of QRA covers both an actual plant-specific QRA and a general description on how to perform QRAs (/12/).

2 OPP accidents other than process accidents (i.e. oil and gas release) will be discussed under the topic of external events.

Table 1. Typical features of PSA and QRA.

Topic	PSA	QRA
Initiating events	Root cause analysis of initiating events presented in fault trees. Identification of common cause initiators (CCIs). Predefined lists and handbooks.	No root cause analysis No CCI assessment Predefined categories of leakage Frequencies based on counting leakage point, or platform data.
Fault tree and event tree analysis (system modelling)	Detailed modelling Support systems explicitly modelled. Link between event trees and fault trees. (Time-dependent models for living PSA).	Rough model Support systems not included Only partly use of fault trees No linking of event and fault trees.
Data and parameter estimation	Best estimates and confidence intervals. Classical and Bayesian framework. 'Weighted' plant-specific data	Best estimates Generic data and separate plant-specific data
Human reliability	Thorough analysis of important human actions (e.g. by THERP, SHARP, etc.).	Almost non-existing
Dependencies	Partly inherent in models Separate dependency analysis Regarded as crucial	Partly inherent in models No separate analysis
Uncertainty	Always included, at least qualitatively. Regarded as important	Absent (Some sensitivity analysis)
External events	Covers some external events Linked to the 'internal' event	Covers many external events Separate analysis (Limited modelling effort)
Results	Best estimate and uncertainty in short and long term fatalities. Cumulative distribution functions.	Single best estimate FAR-, and PLL-values

A lot of systems at OPP are only considered implicitly via failure rates or initiating event frequencies. (E.g. power supply to fire water pumps may implicitly be included in the failure rate of the pumps. Trip of a compressor in the process could result in a transient leading to an increased probability of leakage in nearby leakage points. This may be implicitly included in the initiating event frequencies).

Not all the branches in the QRA event tree are modelled and calculated using fault trees. In some cases simple equations are established to describe and calculate the top event of one branch. This means that minimal cut sets will in general not be possible to obtain on a component level, but maybe on a system level. Even if fault trees are used in some of the event tree branches, these are not linked and minimal cut sets on the basic event level cannot be obtained, (i.e. a tool that can combine both event trees and fault trees is not used).

Data and estimation of model parameters
With respect to data estimation two different statistical frameworks could be chosen: Classical or Bayesian framework. In PSA both frameworks are considered since uncertainty analysis normally is included.

In QRA only best estimates are calculated, without any assessment of uncertainties, and the normally used framework for data estimation is the classical approach. If uncertainty in data (and the total analysis) is of no interest, then sparse amount of platform-specific data could be chosen for the estimation of e.g. failure rates, instead of using generic data, even if this implies a large increase in error bands (uncertainty). This is a potential pitfall in QRA.

Human reliability analysis
Human reliability analysis is emphasised in PSA (e.g. due to the large uncertainties associated with human interactions) and methods like THERP and SHARP are used. In QRAs the topic of HRA is almost non-existing. Human errors are often considered to be implicitly covered by the component failure rates and initiating event frequencies.

Dependencies
Analysis of dependent failures is one of the most important and stressed aspects in a PSA. Separate analyses of possible dependencies are carried out. The functional dependencies and shared-equipment (component) dependencies are inherently accounted for in the modelling process (FTA, ETA) both in the PSA and the QRA. Inter-component dependencies, however, requires a specific analysis of the failure causes to search for potential common causes. This seems to be more emphasised in PSA than in QRA. (E.g. in the nuclear power industry they have developed lists of generic and special causes of CCFs).

Uncertainty analysis
The largest methodological difference between a PSA and a QRA is that uncertainty is viewed as a very important topic in the treatment of NPP risk, whereas it is totally absent in a QRA. One very serious consequence of not treating uncertainties at all is that there is less feedback or incentives to include adequate amount of knowledge, information and resources into the analyses. The approximately same best estimates could be obtained whether a rough or a quite thorough analysis is performed. There is little credit gained in carrying out a comprehensive analysis. If uncertainty analysis is carried out, then the efforts (knowledge, information, resources) put into the quantitative risk assessment are reflected in the error bands. The confidence intervals decrease when knowledge about the phenomena analysed increases. The absence of uncertainty analysis can lead to stagnation of further development of the QRAs.

Sensitivity analysis is performed in QRAs as well as in PSAs. Normally, however, this is for QRAs only carried out for risk contributors specified by the operating company (it is not a default task to carry out sensitivity analysis). The development of new modelling tools (e.g. OHRAT) has made it easier to perform sensitivity analysis. To some extent sensitivity analysis covers for the lack of knowledge represented by a risk result without uncertainty bands.

External events
For NPP the external events can be earthquakes, floods, fires, aircraft impact, etc. A part of the external event analysis is to evaluate the fragility and vulnerability of components (e.g. in safety systems). At some point these consequences are included in the 'internal' event analysis. I.e. external events can give rise to initiating event frequencies and/or component failure rates, in addition to the possible direct damage to the plant. Only some of the external events are normally considered thoroughly.

For an offshore petroleum platform other hazards than process accidents could be viewed as 'external events' (i.e. 'external' to the process). These hazards are e.g. helicopter crashes, ship collisions, and dropped objects. Blowout, however, could be viewed as a 'transient' leading to the loss of control of the production process. (This is comparable to the loss of reactivity control in a NPP). It leads to the same consequences as process accidents, i.e. the release of oil and gas, and ultimately fires and explosions (if ignited). Other external events (e.g. earthquakes, winds, etc.) are covered under the heading of environmental impact. In addition to these internal and external events with large accident potential, a QRA also assesses occupational hazards. This is, however, normally just a generic statistical analysis.

The analyses of the different 'external events' are carried out separately and are rarely included in the analysis of process accidents. (However, the impact on, and consequence of damaging process equipment are included in the separate studies).

Presentation of results
The result of a QRA can be compared to a level 3 PSA best estimate result. Normally a single quantitative number is used (e.g. a FAR-value) instead of a cumulative distribution function (e.g. F-N curves). Also the contribution from the different types of hazardous events, and the distribution of risk in the various areas (modules) of the platform are presented.

3. Methodology for development of risk indicators

The methodology for development of risk indicators presented is developed through two pilot projects performed in co-operation with the Norwegian Petroleum Directorate and two oil companies.

3.1 Concepts for development of risk based indicators

Two important concepts used in order to develop risk indicators are:

- *Risk Influencing Factor*, i.e. a factor (condition, attribute) that influences the risk level of a system or activity (here operation and maintenance of a particular offshore installation). Example: Hot work.
- *Risk Indicator*, i.e. a measurable (countable, observable) value used for surveillance of change in a given risk influencing factor. Example: Burning time per period.

The link between these two concepts and the risk level is shown in Figure 2. The effects on risk from changes in the risk indicators can be established through sensitivity analyses. Thereby the relationship between the relative change in the risk indicators and the relative change in risk level can be calculated. By measuring the changes of risk indicators, we are able to follow-up changes in the total risk level on a platform.

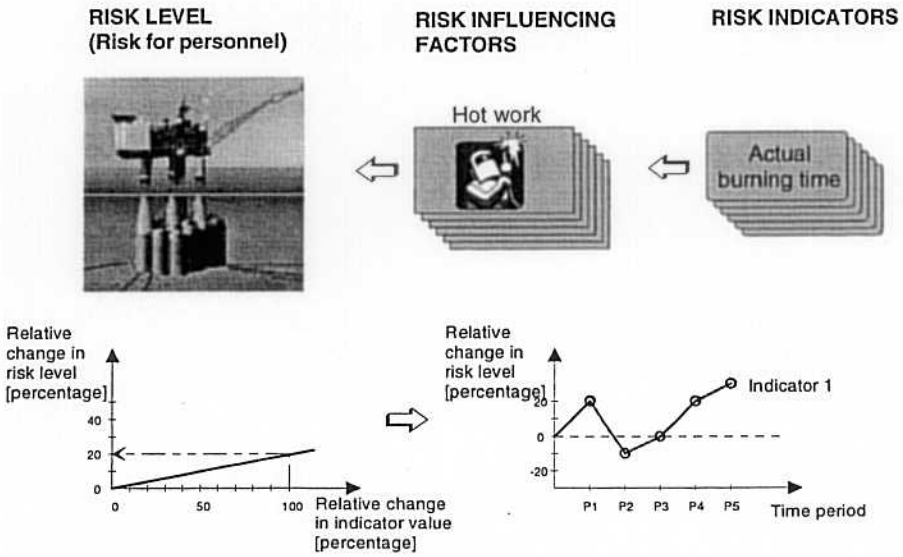


Figure 2. Concepts for development of risk level indicators.

3.2 Methodology for development of technical risk indicators

A brief overview of the methodology for development of risk indicators is shown in Figure 3.

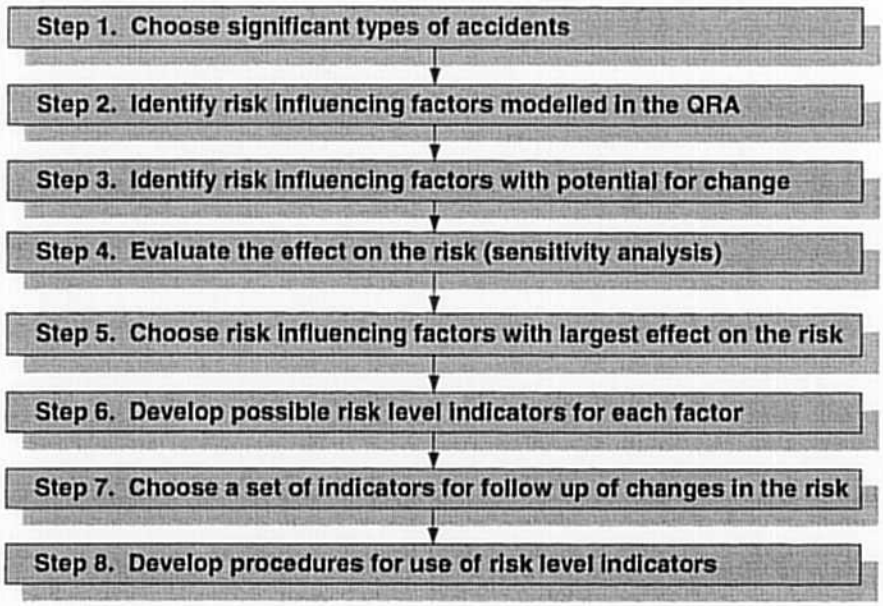


Figure 3. Overview of the generic methodology for development of risk indicators.

In the following description of the methodology we have focused in particular on step 6 and 7.

Step 1 typically include e.g. process accidents (i.e. fires and explosions), riser and pipeline accidents, blowouts and helicopter accidents. In step 2 all factors modelled in the QRA for each accidental event (e.g. process accidents) are identified, listed in tables and illustrated (using e.g. event trees and fault trees). In step 3 the potential change of each single factor or parameter is evaluated by the operating personnel.

In step 4 the effect on risk of change in each factor is assessed using sensitivity analysis. Those factors potentially contributing most to a change in total risk are selected in step 5 using a Pareto diagram and some subjectively chosen cut off criteria.

The pre-establishment and final choice of a set of risk indicators is covered in step 6 and 7. There are several criteria attached to the evaluation of the appropriateness of an indicator. Attaining a relatively high level of control requires frequent registrations (e.g. quarterly). This will affect the amount of data possibly gained by a given indicator, which has to be sufficiently large in order to avoid problems with statistical significance. The indicators should also preferably be based on existing registrations or databases, and not place extra registration burden on the operating company. However, this has to be balanced against the selection of indicators that are sufficiently accurate (i.e. the indicators have to be representative for the risk influencing factors they measure). Need for increased accuracy may result in less simple data collection.

The pre-establishment of (possible) indicators is based on discussions with the operating personnel. However, the final choice also has to be based on testing of the proposed indicators. Such testing also involves personnel responsible for relevant databases (e.g. accident databases, maintenance databases, and different daily reports). The simplicity of registration might turn out to be quite different from what was initially perceived. The willingness to implement new

registrations or to modify existing registrations depends on the perceived benefit gained from the use of a specific indicator (and also on the perceived adequacy of the indicator).

The final step, step 8, is the establishment of routines for use of risk level indicators. The relative change in risk should be illustrated showing the total contribution, along a time axis. This illustration will provide a signal or a warning for the need of assessing risk-reducing measures. The results can be documented and discussed in a quarterly report to the management. The report should include proposals for risk reducing measures.

4. Results

In addition to the review of the differences between QRA and PSA presented in chapter 2, there are two major results from our work. First, the generic methodology for development of risk indicators presented in chapter 3. Secondly, the establishment of a set of risk indicators for a specific petroleum installation. This set of risk indicators will be presented in the following.

4.1 Established set of indicators for a specific installation

The generic methodology was utilised to establish a set of risk indicators for a specific petroleum installation. The risk influencing factors assessed likely to change and contributing most to the total risk were identified, and a set of risk indicators was established for the risk influencing factors. The proposed risk indicators for the different risk influencing factors are shown in Table 2.

Table 2. Proposed set of indicators for a specific platform.

No	Risk influencing factor	Risk indicator	Effect on risk *%
1	Process leak frequency	Number of all leaks	46.4
2	Ignition due to failure on electrical equipment	Number of all failures on electrical equipment	18.0
3	Hot work	Number of hot work permits class A and B	5.3
4	Ignition due to pumps and compressors	Number of hours of critical maintenance backlog	2.3
5	Ignition due to driving units (e.g. turbines)	Number of all failures on electrical driving units	7.2
6	Ignition in neighbour module	Number of alarms indicating loss of overpressure	28.0 **
7	Drilling and completion	Number of days with drilling and completion activity	11.0
8	Workover (on wells)	Number of days with workover	10.4
9	Blowout frequency	Number of trips (i.e. withdrawals of the drillpipe)	4.3

* The effect on risk is based on 100% change in the risk indicator values

** This refers to change in ignition probability and not to the proposed risk indicator

The effect on risk stated in the table is based on a potential change in risk indicator values of 100 %, for the reason of comparison. Be aware that this is not the maximum potential change in risk that was the result of the sensitivity analysis.

4.2 Testing of indicators

As we mentioned in section 3.2 (step 6 and 7), it is important to test the proposed risk indicators prior to a final decision on the appropriate set of risk indicators. Only through such testing can it

be verified to what extent the different appropriateness criteria are fulfilled for each of the risk indicators. Data for the first and second quarter of 1998 were chosen for the purpose of this test.

It was possible to obtain values for six of the nine proposed risk indicators (indicator no. 1, 3, 4, 5, 7 and 8). However, for one of these (the process leak frequency) the number of leaks reported were much less than anticipated (based on the QRA). The amount of data for this risk indicator is too small for registration (and control) based on periods of three months.

For risk indicator no. 2 and no. 9 we did not obtain data due to the need for manual data retrieval. However, for future use of these risk indicators only minor adjustments in the reporting procedures are foreseen.

The appropriateness of risk indicator no. 6 has not yet been confirmed. However, due to modelling inadequacy in the QRA, this risk indicator has no direct link to the total risk. The effect on risk due to a change in the risk indicator value thus cannot be estimated. It has to be treated separately, looking at the change in risk indicator value from one quarter to the next, without calculating the corresponding change in total risk.

To summarise, we assume that seven of the nine proposed risk indicators will be appropriate for use as a tool for risk control. One has to be further analysed (e.g. looking for root causes and possibly organisational risk influencing factors) and one has to be treated in a "non-risk" manner, or replaced by an alternative risk indicator.

5. Discussions

5.1 Risk-based decision-making in the petroleum industry

Ideally, all decisions should be made on sufficient decision basis. This criterion should also be fulfilled for risk-based decisions in the petroleum industry. Due to limitations in the existing QRA-methodology, the application areas of the QRA for risk-based decision-making today are limited. The limitations arise from e.g. uncertainty associated with input data, modelling assumptions and the completeness of the existing analyses.

Increased use of risk-based decision-making, in order to maintain and improve the existing safety level in the Norwegian petroleum industry, should not exceed the extent supported by the state-of-the-art of QRA-methodology and data. The present situation is such that there is a need for further development of the QRA-methodology in order to expand the possible and suitable applications of QRA (ref. section 2.2).

5.2 General methodology for development of risk indicators

The general methodology for development of risk indicators has been gradually developed through two pilot projects. It is a purely risk-based approach where low risk contributors are screened out. Risk contribution is defined in relative terms, i.e. it is not the absolute risk contribution that is of interest but rather the potential change in risk. This means that e.g. a specific safety system may well be important to the risk level in absolute terms, but if this system most likely remains equally efficient over time (i.e. no change is foreseen), then the relative change in risk due to this system will be negligible. Thus, there will be no justification for the use of resources to control risk through the use of risk indicators. It is important that the operating personnel assess the "realistic" (most likely) foreseen change.

These two distinct features of this methodology, i.e. the purely risk-based approach and the assessment of potential change by the operating personnel, are important when we compare this methodology with other relevant methodologies.

Within the nuclear industry it has been developed a lot of different types of "safety indicators", some of which are described in (/13/). These indicators are ranging from fairly general performance indicators (e.g. the ten WANO[3] indicators) which are only presumed to influence safety, to probabilistic safety indicators which are "known" to have influence on safety. However, even these latter indicators are not developed using the risk analysis (PSA) as a starting point. Instead they are identified from incident databases, and in second hand the effect on risk is determined based on the plant specific PSA. The coverage of these indicators thus remains unknown.

Holmberg et.al. (/14/) describe the development and testing of what they term risk-based PSA indicators. These indicators are used for risk follow-up of events and unavailability of safety related systems. The results are presented as average values for one year of operation. The main aim is to classify the safety significance of events, and not to use the indicators as a tool for "continuous" risk control. In addition, they cover only some selected safety systems. The aim and use of these indicators is therefore quite different from the risk indicators presented in this paper.

5.3 Established set of risk indicators for a specific platform

Of the nine risk indicators proposed, seven are assumed (with minor adjustments in the reporting routines) to be appropriate for use as a tool for risk control, whereas further analyses are required for the last two factors/indicators.

Risk indicator no. 3, 7 and 8 were established as more or less "direct" measures of the corresponding risk influencing factors (i.e. the risk indicator is identical or almost identical to the parameter used in the QRA). For all the other risk influencing factors a direct measure was inappropriate due to low probability (or frequency) of occurrence. These risk indicators are therefore representing a more "indirect" measure of a larger population in which the set of interest is included (e.g. the set of critical failures as part of the number of all failures). Of course, by doing so we make assumptions and introduce uncertainties, but this is the only way to measure changes as frequently as each quarter. These "indirect" measures are still far more direct than organisational risk indicators, which also may be regarded as "indirect" risk indicators.

For the risk influencing factor no. 1 it was not even sufficient to count all leaks (including those being regarded as too small to be reflected in the QRA). For this risk factor we foresee an analysis of possible root causes including organisational factors. It will provide a potential link to organisational aspects, see (/4/).

Provided that an appropriate risk indicator (or set of risk indicators) can be established for the process leak frequency, we believe that the total set of risk indicators provide a reasonable good coverage in relation to the total risk picture (as modelled in the QRA). However, risk indicator no. 9 only covers a part of the corresponding factor. The blowout frequency depends upon failure

---

[3] WANO – World Association of Nuclear Operators

in both barriers (hydrostatic pressure and safety valves), whereas the risk indicator (number of trips) only addresses one of the barriers (hydrostatic pressure).

5.4 Limitations of the presented methodology

The set of risk indicators presented is platform specific, but the methodology described is generic and can be applied to any platform. The risk indicators can be used as a tool for risk control during operation of petroleum installations.

The risk indicators express changes in risk in relative terms, it cannot be used to measure the risk level in absolute terms. For this a complete update of the QRA is necessary.

So far, the scope of the work has been limited to focus on risk for loss of personnel and events having major accident potential, but the same methodology can be used to develop risk indicators for environmental and material damage. Some safety systems may turn out to be more important with respect to material damage risk compared to personnel risk (/15/).

The QRA for the chosen installation has been used as a basis for the work, and all assumptions and limitations in the QRA have been adopted. Due to lack of detailed cause analyses in the QRA, the established set of indicators do not cover all risk influencing factors. Additional work has to be done to establish "non-technical" risk indicators, i.e. in order to develop risk indicators for human and organisational factors.

5.5 Application of risk indicators

The practical application of the established set of risk indicators (based on the methodology developed and presented in this paper) is to control risk during operation. Risk control can thus be based on quarterly registrations instead of just an update of the QRA with several years time interval.

5.6 Further development

In order to increase the use of risk-based decision-making in the petroleum industry, there is a general need for further development of the QRA-methodology applied in the petroleum industry.

With regard to further development of the methodology for development of risk indicators, the main research challenge is the modelling of organisational factor's effect on the risk. Focus will be on the most important risk influencing factors identified in the QRA. Our purpose for the further work is to identify organisational risk indicators that complement the QRA-based indicators presented in this paper.

6. Conclusions

Risk-based decision-making based on QRA in the petroleum industry is applied in a lesser extend than PSA is used in the nuclear industry. One explanation is the difference between the state-of-the-art of QRA versus PSA. Some of the differences have been addressed in this paper.

We have described a purely risk-based approach for development of risk indicators for petroleum installations. The basis for the work is the QRA for a specific installation and the determination

of risk importance of each risk influencing factor. The risk importance is based on a judgement performed by the operating personnel of "realistic" changes in each factor.

The risk indicators can be used as a tool for risk control during operation of petroleum installation, and should be seen as a supplement to other techniques to keep the risk at an acceptable level.

7. References

/1/ Norwegian Petroleum Directorate (NPD). Guidelines for safety evaluation of platform conceptual design. Issued 1. September 1981, Stavanger, Norway.

/2/ Nielsen, L., Sklet, S. & Øien, K. 1996. Use of risk analysis in the regulation of the Norwegian petroleum industry. *Proceedings of the Probabilistic Safety Assessment International Topical Meeting*. American Nuclear Society, IL, USA, 1996: 756-762.

/3/ Øien, K., Sklet, S. & Nielsen, L. 1997. Risk Level Indicators for Surveillance of Changes in Risk Level. *Proceedings of ESREL'97*, Lisbon, Portugal, 17-20 June: 1809-16: Pergamon.

/4/ Øien, K., Sklet, S. & Nielsen, L. 1998. Development of risk level indicators for a petroleum production platform. *Proceedings of the 9th International Symposium of Loss Prevention and Safety Promotion in the Process Industries*, 4-7 May, 1998, Barcelona, Spain: 382-393.

/5/ Øien, K. & Sklet, S. Risk Control during Operation of Offshore Petroleum Installations. Paper submitted for publication on ESREL'99, München, Tyskland.

/6/ IAEA, Draft-document, *PSA Applications to Improve NPP Safety*, IAEA-J4-97-CT-06876, February 1998, Vienna, Austria.

/7/ *PRA Procedures Guide-A Guide to the Performance of PRAs for Nuclear Power Plants*, NUREG/CR-2300, January 1983.

/8/ US Nuclear Regulatory Commission: *Severe Accident Risks: An Assessment for Five US Nuclear Power Plants, report NUREG-1150*, draft, April 1989.

/9/ Knochenhauer, M., *Status and Use of PSA in Sweden*. SKI Report 96:40, May 1996, ISSN 1104-1374, ISRN SKI-R—96/40—SE.

/10 IAEA Safety Series No. 50-P-4. *Procedures for Conducting Probabilistic Safety Assessments of Nuclear Power Plants (Level 1)*. IAEA. Vienna, 1992.

/11/ US Nuclear Regulatory Commission: *Reactor Safety Study: An Assessment of Accident Risks* in *US Commercial Nuclear Power Plants*, report WASH-1400 (NUREG-75/014), October 1975.

/12/ Vinnem, J.E. *Quantified Risk Assessment for Offshore Petroleum Installations*. NTNU Faculty of Marine Technology, Department of Marine Structures, January 1996.

/13/ Johansson, G. and Holmberg, J. (editors), *Safety Evaluation by Living PSA-Procedures and Applications for Planning of Operational Activities and Analysis of Operating Experience*. SKI Technical Report 94:2, NKS/SIK-1(93)16, January 1994, ISSN 1104-1374.

/14/ Holmberg, J.E., Söderlund, A., Forss, A. & Gunsell, L. 1998. Operating experience feedback by risk-based PSA-indicators. *Proceedings of ESREL'98*, Trondheim, Norway, 16-19 June: 509-14: Balkema.

/15/ Vinnem, J.E. 1997. On the sensitivity of offshore QRA studies. *Proceedings of ESREL'97*, Lisbon, Portugal, 17-20 June: 745-53: Pergamon.